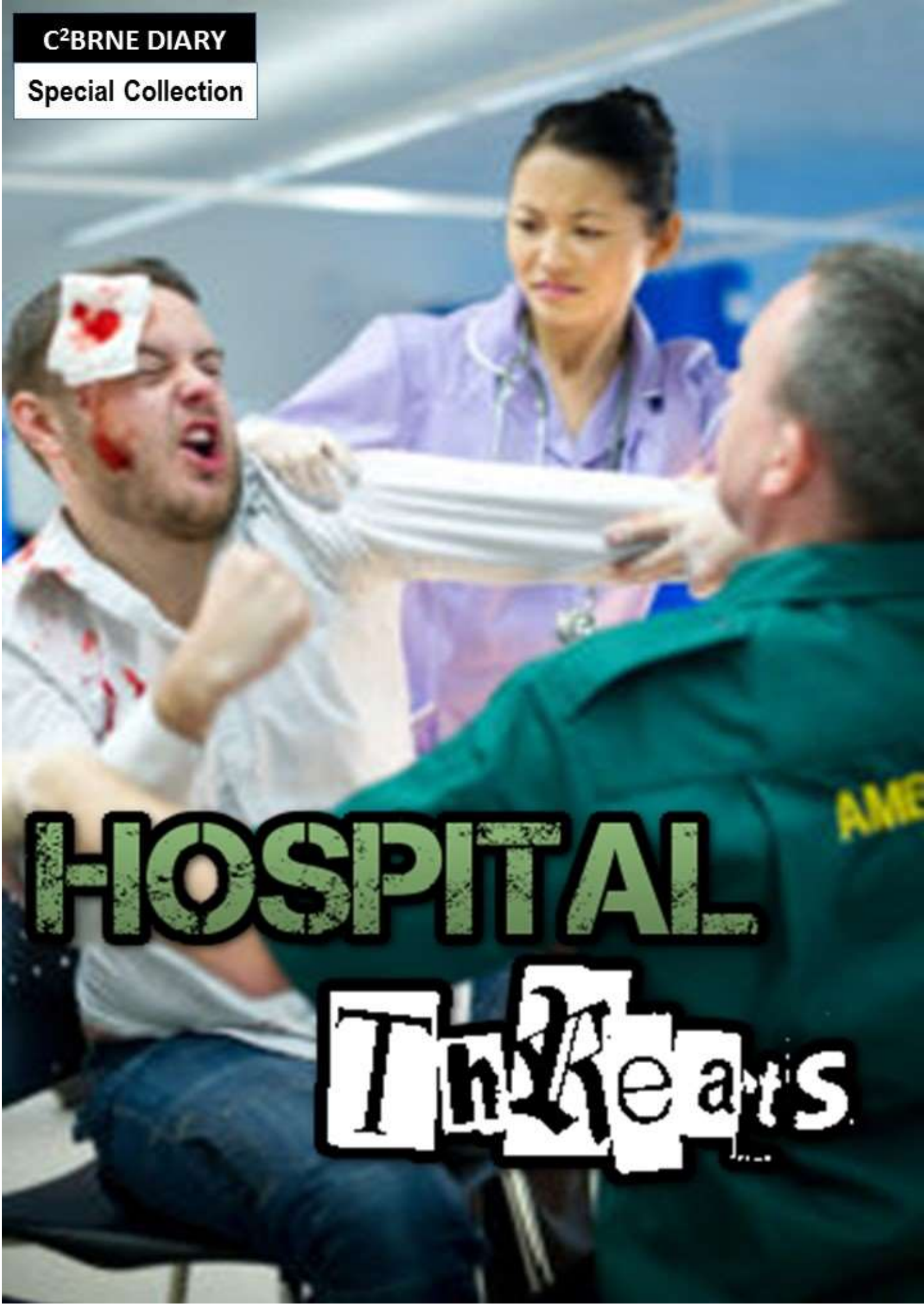


C²BRNE DIARY

Special Collection



HOSPITAL

Threats

HOSPITAL THREATS

Introduction

Hospitals supposed to be oasis of peace and tranquility since pain and sickness are independent of violence, politics, or extreme behavior. Unfortunately, the situation is not ideal not only during war time but also during everyday activities.

We all know that all casualties end up at hospitals regardless of the cause – illness, terrorist action, conventional or asymmetric causes. If you “kill” a hospital during an emergency, you kill the victims twice! A hospital can be confronted with both external and internal threats. The latter might be caused by a dissatisfied employee that can damage, set fire, sabotage equipment, assist intruders all the way to theft or application of physical force against hospital personnel.

Hospitals should be prepared to deal with the case of a contaminated chemical or radiological plume directed towards the hospital and be prepared to shelter-in-place since the evacuation process is time consuming and such incidents happen out of nowhere.

Hospital should also be prepared to receive chemical, biological, radiological/nuclear (CBRN) casualties following an urban terrorist attack. But hospitals might also be targeted with the same agents – especially radiologicals with long half lives that will take years to eliminate transforming this critical infrastructure to a “ghost hospital”.

Daily attacks of doctors and nurses is a very common global threat that might affect the function of emergency departments and outpatient clinics and affect the moral of the medical personnel and subsequently its performance.

Hospital defense should be taken seriously and certain measures should be taken to ensure that peace will always rule in the corridors of a facility full of pain, anxiety, agony, and hope.

This Special Collection presents some cases of different threats against hospitals and provides additional references for further study.

The C²BRNE Editor



HOSPITAL THREATS

Violence against nurses is on the rise, but protections remain weak

By Jacqui Pich

Source: <http://theconversation.com/violence-against-nurses-is-on-the-rise-but-protections-remain-weak-76019>



May 2017 – Two recent violent episodes against nurses in emergency departments have again highlighted the issue of inadequate protections for nursing staff.

In both cases the nurses, from [Wyong Hospital](#) on the central coast of NSW and [The Royal Melbourne Hospital](#) in Victoria, were held hostage by knife-wielding patients. These cases seem extreme, but they are not isolated.

Nurses are exposed to high levels of [physical and verbal violence](#), to the point where this has become an expected and even accepted part of their job.

In 1999, the [Australian Institute of Criminology](#) ranked the health industry as the most violent workplace in the country. According to US statistics, health-care workers are [five to 12 times more likely](#) than other workers to experience violence in the workplace.

Worldwide, nurses are [more likely to be attacked at work](#) than prison guards and police officers. And yet such incidents remain under-reported and existing protections are not enough to ensure the safety of nurses and their patients.

Extent of violence

Nurses are at the [front line of violence](#) in hospitals, particularly those working in emergency, aged care and mental health. The frequency and severity of violent [incidents are increasing](#), yet such episodes remain vastly under-reported.

Government figures show the number of “code blacks” – incidents where the safety of hospital staff is threatened – is rising. By February this year, [6,245 code blacks](#) had been reported so far for 2016-17, compared to 4,765 at the same point in 2015-16, in South Australian public hospitals.

Emergency departments have the highest incidence of violence in health care. Up to 90% of emergency department staff [have experienced some type of violence](#) in their careers. Violence covers a range of behaviours, from verbal abuse and threats through to physical violence.

HOSPITAL THREATS

Verbal abuse, especially swearing, is the most common type of violence. Nurses in emergency departments [experience daily verbal abuse](#). Physical violence [often occurs at the same time](#) as verbal abuse and can include the use of weapons on hand – such as syringes, scalpels, scissors and furniture. Patients are responsible for most of the violence committed against nurses. This includes [children](#) and their [parents or carers](#). Patients under the influence of alcohol or drugs, including ice, and those with mental health issues are the [most likely to become violent](#).

Impact of violence

The impact of patient-related violence on nurses is far-reaching. Verbal abuse can cause [significant psychological trauma](#) and stress to nurses, even if no physical injury has occurred. This can include symptoms of depression, post-traumatic stress disorder, drug and alcohol abuse and even chronic pain – all of these can last up to 12 months after an incident.

The types of physical injuries nurses sustain range from minor scratches and bruises, [through to serious injuries](#) such as fractures, stab wounds, attempted strangulations and even death.

In 2011 a nurse was [punched in the face](#) and stabbed with a butter knife in the arm, back and breast area. In 2011 a patient [stabbed a mental health nurse to death](#) in regional NSW. And in 2016, a [remote area nurse was abducted](#), raped and murdered in northern South Australia.

Exposure to patient-related violence can also affect the way nurses interact with patients. They can [feel less empathy](#) and their [quality of care can suffer](#). There's a [link between violence](#) experienced by nurses and subsequent adverse events in patients. These included late administration of medications and an increase in the number of patient falls and medication errors.

Preventing violence

Some strategies can prevent and manage violence. These include using security guards, duress alarms, workplace design and training in aggression minimisation for front-line staff.

[The Australasian College for Emergency Medicine](#) recommends a lack of hiding spaces outside emergency departments, the use of CCTV cameras, a visible security presence, physical barriers such as glass screens at triage (the area where the nurse assesses the severity of your condition in relation to other emergency department patients), a restricted access area and good lighting.

The use of such strategies is inconsistent in Australia. Training in aggression minimisation is designed to improve the knowledge and skills of staff in recognising and responding to potentially violent people. It is compulsory for those working in high-risk clinical areas like the emergency department. Yet [large numbers of nurses](#) have not completed any training or have not completed the regular refresher programs required. Security guards are not present in all Australian emergency departments, and are often ill equipped to deal with the levels of violence they encounter. They are unarmed and do not carry handcuffs. As they are meant to observe and report on episodes, they lack powers to restrain or detain people who threaten or assault hospital staff.

In 2016 a patient under the influence of ice [shot a security guard and police officer](#) at Sydney's Nepean Hospital. In some smaller hospitals no [security is provided after hours](#). This is despite the fact regional nurses experience the same levels and types of violence as their metropolitan colleagues.

Little has changed

In response to increasing violence in NSW public hospitals, in February 2016 the then NSW health minister, Jillian Skinner, issued a [12-point action plan](#) for increasing security. A detailed security audit was conducted in 20 emergency departments.

Wyong Hospital was one of those audited. But the recent violent attack on two nurses seems to indicate not much has changed.

Given the strategies in place are inadequate and staff continue to be attacked on the job, changes must be introduced as a priority. The management of violence needs to catch up with the daily reality facing health-care staff, to ensure workplace and personal safety are valued alongside patient safety.

Jacqui Pich is Lecturer in Nursing, University of Technology, Sydney (AUS)

HOSPITAL THREATS

Report: Hospitals vulnerable to cyber attacks that can harm patients

Source: <https://www.wmar2news.com/news/in-focus/report-hospitals-vulnerable-to-cyber-attacks-that-can-harm-patients>

Report: https://www.securityevaluators.com/wp-content/uploads/2017/07/securing_hospitals.pdf

A new report from a Baltimore-based tech security company poses an alarming question. Could hackers take control of hospital computer systems to kill patients? The short answer: yes.

As CEO of [Independent Security Evaluators](#), Stephen Bono is in the business of problem solving. A few years ago, he and his staff brainstormed the worst possible outcome of a cyber attack.

"A person actually being harmed through a cyber attack or dying in a cyber attack would be the worst case scenario," he said. "So then we asked ourselves, 'Well, is that really a feasible situation?' And what we found out was, 'Yes.'"

"[Securing Hospitals](#)" is the end product of a two-year study of 12 hospitals across the country, including ones in Baltimore, Towson and Washington, D.C. With the cooperation of the hospitals, ISE's team breached each medical center physically and virtually to identify key weaknesses in their operations.

"Year by year, terrorism gets more technologically savvy and at some point, they're going to start attacking our infrastructure and healthcare is a major part of our infrastructure," Bono said.

While most hospitals' IT security focus is on protecting patient records and privacy, ISE identified potentially deadly vulnerability elsewhere. The team found it was possible to hack into medical devices attached to patients, as well as the systems that monitor patient conditions and care.

		Patient Health		Patient Records	
Adversary		Targeted (Specific Victims)	Untargeted (Indiscriminate)	Targeted (Specific Victims)	Untargeted (Indiscriminate)
	Individual / Small Group				YES
	Political Groups / Hacktivists /			YES	
	Organized Crime	YES		YES	YES
	Terrorism / Terrorist Org.	YES	YES		
	Nation States	YES	YES	YES	YES

"Modifying a medical record to say, change somebody's allergies, change the medicines they are allergic to, change their medical histories to say, maybe there are diabetic or they are not diabetic," he said.

"Pretty much across the board, we found similar issues that would always allow us access to these types of systems."

The report also offers solutions, a blueprint that ISE hopes hospitals nationwide will use to tighten up their cyber security. The biggest challenge? Massive underfunding and understaffing for security departments.

"Hopefully, the idea is that people will start to wake up to this issue and start to fix it, before anybody actually does get hurt," Bono said.

He said this can't be fixed overnight. Rather, hospitals have to make cyber security a priority because it's a constant battle against new technology. Just last month, hackers attacked the computer systems of a hospital in Los Angeles. Malware blocked access to patient records until the hospital paid a ransom to the cyber criminals.

HOSPITAL THREATS

Defending Hospitals against Life-Threatening Cyber Attacks

Source: <https://www.scientificamerican.com/article/defending-hospitals-against-life-threatening-cyber-attacks/>

Apr 25 – Like any large company, a modern hospital has hundreds—even thousands—of workers using countless computers, smartphones and other electronic devices that [are vulnerable](#) to security breaches, data thefts, and ransomware attacks. But hospitals are unlike other companies in two important ways. They keep medical records, which are among the most [sensitive data about people](#). And many hospital electronics help keep patients alive, monitoring vital signs, administering medications, and even breathing and pumping blood for those in the most dire conditions.

A 2013 data breach at the [University of Washington Medicine](#) medical group [compromised about 90,000 patients' records](#) and resulted in a US\$750,000 fine from federal regulators. In 2015, the [UCLA Health system](#), which includes a number of hospitals, revealed that attackers accessed a part of its network that handled information for [4.5 million patients](#). Cyberattacks can interrupt [medical devices](#), close emergency rooms and cancel surgeries. The [WannaCry attack](#), for instance, disrupted a [third of the UK's National Health Service organizations](#), resulting in canceled appointments and operations. These sorts of problems are a [growing threat](#) in the health care industry.

Protecting hospitals' computer networks is crucial to preserving patient privacy—and even life itself. Yet recent [research](#) shows that the health care industry lags behind other industries in securing its data.

I'm a systems scientist at MIT Sloan School of Management, interested in understanding complex socio-technical systems such as cybersecurity in health care. A former student, [Jessica Kaiser](#), and I [interviewed hospital officials in charge of cybersecurity](#) and industry experts, to identify how hospitals manage cybersecurity issues. We found that despite widespread concern about lack of funding for cybersecurity, two surprising factors more directly determine whether a hospital is well protected against a cyberattack: the number and varied range of electronic devices in use and how employees' roles line up with cybersecurity efforts.

A wide range of devices

A major challenge in hospitals' cybersecurity is the [enormous number of devices with access to a facility's network](#). As with many businesses, these include mobile phones, tablets, desktop computers and servers. But they also have large numbers of patients and visitors who come with their own devices, too—including networked medical devices to monitor their health and communicate with medical staff. Each of these items is a potential on-ramp for injecting malware into the hospital network.

Hospital officials could use software to ensure [only authorized devices can connect](#). But even then, their systems would remain vulnerable to software updates and new devices. Another key weakness comes from [medical equipment](#) offered as free samples by device manufacturers who operate in a competitive market. They're [often not tested](#) for proper security before being connected to the hospital network. One of our interviewees mentioned:

"In hospitals ... there's a whole underground procurement process whereby medical device vendors approach clinicians and give them lots of stuff for free that eventually makes its way on to our floors, and then a year later we get a bill for it."

When new technologies bypass regular processes for purchase and risk assessment, they aren't checked for vulnerabilities, so they introduce even more opportunities for attack. Of course, hospital administrators should balance these concerns against the improvements in patient care that new systems can bring. Our research suggests that hospitals need stronger processes and procedures for managing all these devices.

Staff buy-in

Getting hospital administrators to understand the importance of cybersecurity is fairly straightforward: They told us they're worried about costs, institutional reputation and regulatory penalties. Getting medical staff on board can be much more difficult: They said they're focused on patient care and don't have time to worry about cybersecurity.

People typically treat cybersecurity protections as secondary to what they're trying to get done. One person we interviewed described why some staff committed the cardinal cybersecurity sin of sharing a password:

HOSPITAL THREATS

"To use an ultrasound machine [you need a password, which] has to change every 90 days. [Staff] just want to use the ultrasound machine. It's not holding a lot of patient data ... so they create a shared login so that they can provide patient care."

The needs can vary widely across a hospital, in ways that can be surprising—such as access to sites likely to carry malicious software. A chief information officer at a research hospital told us,

"I personally believe that hardcore pornography has no purpose on hospital supported devices. What did I do five years ago? I put up internet content filters that prevented people from navigating to pornography. Within five minutes, the director of psychiatry calls to tell me that we have a grant to study pornography in a medical context [so we had to modify our filters]."

These experiences are why we concluded that budget limitations are not as crucial to hospital cybersecurity as employee involvement. A hospital can buy as many pieces of hardware and software as it wants. If workers aren't following organizational procedures, the technology won't keep hospitals safe. Our research suggests that cybersecurity is as much about managing people as it is about technology.

Compliance is not security

The threat is nationwide, and keeps getting harder to defend against, as one chief information security officer told us:

"The nature of attacks is increasingly sophisticated. It used to be my biggest threat was ... students. Today, it's state-sponsored attacks, terrorism and organized crime. It's more threats than ever before of a more serious nature."

Unfortunately, many hospital administrators seem to believe that protecting data is as simple as meeting state and federal regulations. But those are minimum standards that don't adequately address the threat. As one of our interviewees said,

"Compliance is a low bar. I guarantee that little health care organizations and hospitals would do nothing (without regulation). They would have a piece of paper on a shelf called their security policy. It's needed as a backstop to get companies at least thinking about it. But being compliant does not solve the greater risk management problem."

Our research shows that hospitals need to think beyond compliance. Also, with so few hospitals well defended against cyberattacks, all hospitals appear more attractive as potential targets. In our view, it's not enough for hospitals to improve their own defenses—nor for regulators to raise standards. They should manage, and evaluate the security of, the devices on their networks and ensure medical staff understand how good cyber-hygiene can support good patient care. Further, policymakers, health care leaders and hospitals themselves should work together to make the industry as a whole less susceptible to attacks that threaten people's privacy and their very lives.

Syria war: Hospitals being targeted, aid workers say

Source: <https://www.bbc.com/news/world-middle-east-42591334>

Jan 06 – At least 10 hospitals in rebel-held areas of Syria have suffered direct air or artillery attacks over the past 10 days, aid workers say.

An adviser to a coalition of medical charities told the BBC that the attacks had been the most intense for a year.

A senior UN official also told the BBC that health facilities in Syria had been hit "yet again".

Meanwhile, 17 civilians died in air raids in Eastern Ghouta, near Damascus, on Saturday, a monitor said. The most deadly raid was in Hammuriyeh where 12 people, including two children, died, the UK-based Syrian Observatory for Human Rights said.

Last week, at least 25 civilians were reported killed in air strikes on two towns in rebel-held Eastern Ghouta. About 400,000 people there have been under siege by Russian-backed Syrian government forces since 2013.

The Syrian government and Russia military have consistently denied targeting civilian areas.

Aid agencies said medical centres hit by recent air strikes included a maternity hospital in Maarrat al-Numan, in Idlib province, which was reportedly hit three times in four days.

Five people died in the worst attack, on Wednesday, according to the Syrian American Medical Society (Sams), and the hospital was temporarily put out of service.

HOSPITAL THREATS

Hamish de Bretton-Gordon, who advises the Union of Medical Care and Relief Organizations (UOSSM), said other attacks in recent days had targeted hospitals predominantly in Eastern Ghouta, on the outskirts of the capital.

"This has been at a level, again, we haven't seen," he said.

Mr De Bretton-Gordon said many children in Eastern Ghouta needed medical evacuation.

"There are over 125 children needing live-saving surgery, including three very young children [whose injuries are] too graphic almost to describe," he said.

"A six-month old who has lost an eye who will die if he doesn't receive surgery and an eight-year old girl who weighs only 8kg [17lb] who is dying of malnutrition."

The UN's Humanitarian Co-ordinator for Syria, Jan Egeland, also told the BBC that several of the remaining health facilities in the Eastern Ghouta had been hit "yet again".

"This war is continuing as bad in 2018 as it ended in 2017," he said.

Other attacks on medical facilities documented by UOSSM include:

- An air strike on a health centre in Harasta, Eastern Ghouta, on 31 December that injured two nurses and damaged the building
- A paramedic was killed when an artillery shell struck a hospital in Harasta on 30 December
- A barrel bomb attack in Maarat al-Numan, Idlib, on 28 December killed a woman and injured three children at a primary health care centre

"This fresh wave of attacks on medical facilities is sickening and unacceptable," he said in a statement.

"These attacks force facilities to shut down, terrorise staff and result in undue hardship for patients already suffering."

He added: "Since the beginning of the crisis, there have been hundreds of well-documented attacks on medical facilities in Syria. It's shameful that there has never been a formal prosecution for these war crimes and it severely undermines the UN's credibility."

The Syrian government recently allowed Red Cross teams to evacuate 29 critically-ill patients from the Eastern Ghouta as part of a deal that saw rebels release the same number of prisoners.

However, hundreds more patients are in urgent need of evacuation from the enclave.

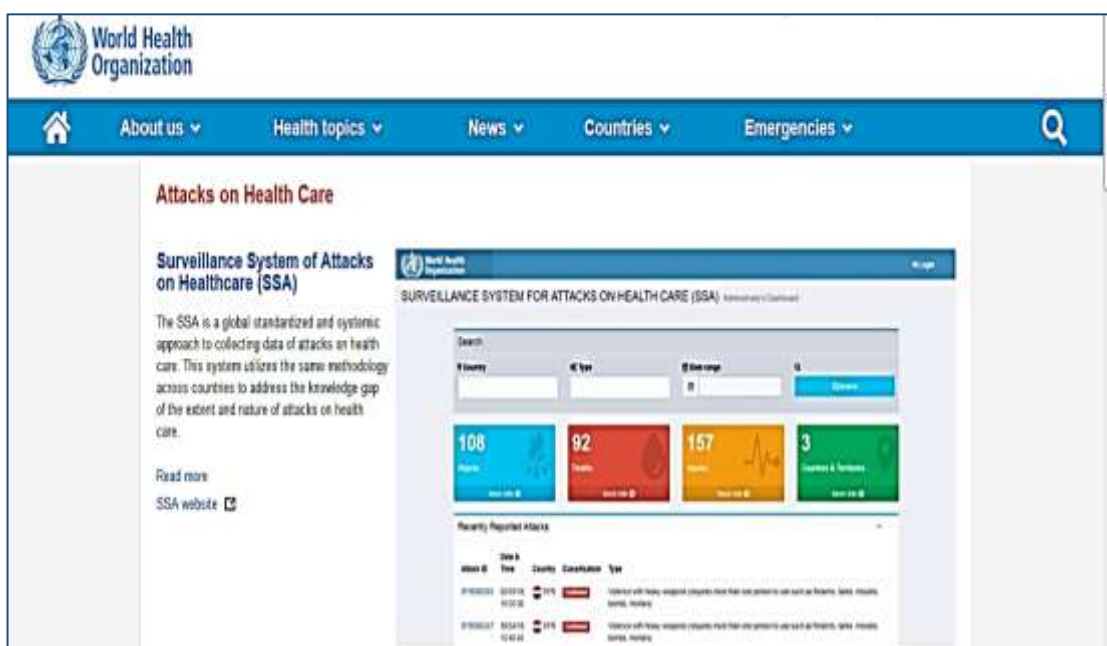
The Eastern Ghouta is designated a "de-escalation zone" by Russia and Iran, the government's other main ally, along with Turkey, which backs the rebels.

But hostilities intensified in mid-November when the Syrian military stepped up air and artillery attacks on the enclave in response to a rebel offensive.



Attacks on Healthcare

Source: <http://www.who.int/emergencies/attacks-on-health-care/en/>



HOSPITAL THREATS

World Humanitarian Day: WHO urges more health aid to address Ukraine's humanitarian crisis

Source: <http://www.euro.who.int/en/health-topics/emergencies/health-response-to-the-humanitarian-crisis-in-ukraine/news/news/2017/08/world-humanitarian-day-who-urges-more-health-aid-to-address-ukraines-humanitarian-crisis>

Aug 2017 – Thousands of children living in conflict-affected areas of Ukraine are at risk due to low vaccination coverage and problems in the surveillance system. WHO and health partners support vaccination campaigns in these areas.

After 3 years of conflict, health-care resources in conflict-affected areas of Ukraine are severely stretched and humanitarian funding is plummeting. At the same time, health facilities continue to be damaged by heavy shelling. The health of millions of Ukrainians is hampered by limited access to health facilities and services, and by insufficient funding for humanitarian health interventions.

"In the midst of Europe we are leaving millions of people with poor or no health care; hundreds of health facilities without infrastructures and medicines; and health-care workers with the fear of being shelled or having to leave their country. This is the situation in eastern Ukraine today," says Dr Nedret Emiroglu, Director of the Division of Health Emergencies and Communicable Diseases at WHO/Europe. "The international community urgently needs to target this humanitarian crisis and provide health aid. It is far from being over."

For World Humanitarian Day on 19 August 2017, WHO/Europe highlights urgent humanitarian health needs in eastern Ukraine, and recognizes the critical and often dangerous work of health professionals in delivering services to those most in need.

Disruption of health facilities and services

What makes the situation so severe?

- ◆ Since the start of the conflict, at least 160 health facilities have been shelled on both sides of the contact line, while some 130 facilities remain either partially or fully nonoperational. This seriously limits access to critical health care. WHO is concerned by such violations and maintains that health facilities and personnel, strictly protected under international humanitarian law, are not a target for violence (Twitter hashtag #NotATarget).
- ◆ Access to health care remains most difficult in areas closest to the contact line. There, the health-care system faces shortages in qualified medical staff and disruptions in the delivery of supplies. Over 400 health facilities in these conflict areas in Ukraine report insufficient stocks of medicines.
- ◆ The number of health partners present in the field is very low due to accreditation issues in non-government controlled areas (NGCA), security restrictions on both sides of the contact line and continuing funding shortfalls. Limited and unpredictable access to NGCA is a major challenge for delivering humanitarian assistance to those in need.

Almost 4 million people in need of health care

The crisis has affected 5 million Ukrainians on both sides of the contact line so far and has led to the internal displacement of about 1.6 million people. Most of those affected live in NGCA. An estimated 3.8 million of the affected people are in need of health care.

Health needs range from general services and essential trauma care, to access to diagnosis and therapy for tuberculosis, HIV, poliomyelitis and sexually transmitted infections. Communicable diseases can easily spread due to malfunctioning surveillance and lack of preparedness and prevention measures. Child health is compromised by low vaccination coverage, with increasing outbreaks of rubella and mumps. Although under-reported, cases of sexual and gender-based violence are also on the rise, especially along the contact line, and treatment services are very limited. Access to life-saving medicines and treatment for chronic diseases such as mental ill health and diabetes is also an issue of concern.

WHO's continued support

WHO has been working with health partners since the start of the conflict to provide primary health-care services, medicines, ambulances and other essential medical items, and to ensure that Ukraine's most

HOSPITAL THREATS

vulnerable communities receive support. It also undertakes health prevention, preparedness and recovery activities such as vaccinations, training and surveillance.

In 2016 alone, WHO and partners set up 35 mobile emergency primary health-care units (MEPUs) that operate along the contact line, where the provision of health services has been cut or severely disrupted. Last year MEPU personnel provided over 230 000 consultations, mostly to internally displaced persons. In addition, multidisciplinary MEPUs teams assisted in the provision of mental health and psychosocial support. Health partners also established 70 sentinel sites and started regular reporting on infectious diseases.

Throughout 2016, WHO delivered over 170 tons of medical supplies for more than 350 000 people, including medicines for chronic diseases, life-saving support for 50 000 diabetic patients, some 14 000 rapid blood tests and supplies for 1800 complex and lifesaving surgical operations.

Donor funding essential but insufficient

The funding WHO requested in the 2017 Ukraine Humanitarian Response Plan – about 21% of the funding for the whole health sector – addresses very critical health interventions only. To date, one third of this amount remains uncovered. In 2016, only 15% of the funding needs of the overall health sector were met. Public health activities and quality care for patients are under pressure, raising concern about possible disease outbreaks.

In 2017, generous contributions by Canada, Germany and Italy have allowed WHO to provide critical support for access to primary health care, to cover some gaps in care for noncommunicable chronic diseases, and to support laboratory services, trauma care and mental health-care needs. However, low vaccination coverage and poor surveillance of communicable diseases, inadequate access to medications for cancer patients, and lack of access to mental health and rehabilitation care remain critical gaps that require urgent action.

“WHO provides a lifeline to people in need of essential health care. However, the current funding gap is limiting our capacity to deliver vaccination and emergency and public health services to those in need,” says Dr Marthe Everard, WHO Representative in Ukraine. “We call on the donor community to return their attention to Ukraine’s crisis. This will enable us, together with United Nations agencies and health partners, to support the Ministry of Health, continue to protect civilians from hostilities and support health facilities in conflict-affected areas.”

Preventing patient-to-worker violence in hospitals: outcome of a randomized controlled intervention

By Judith E. Arnetz, Lydia Hamblin, MA, Jim Russell, BSN, et al.

J Occup Environ Med. 2017 Jan; 59(1): 18–27.

Source (full paper): <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5214512/>

Abstract

Objective

To evaluate the effects of a randomized controlled intervention on the incidence of patient-to-worker (Type II) violence and related injury in hospitals.

Methods

Forty-one units across 7 hospitals were randomized into intervention (n=21) and control (n=20) groups. Intervention units received unit-level violence data to facilitate development of an action plan for violence prevention; no data were presented to control units. Main outcomes were rates of violent events and injuries across study groups over time.

Results

Six months post-intervention, incident rate ratios of violent events were significantly lower on intervention units compared to controls (IRR 0.48, 95% CI 0.29-0.80). At 24 months, the risk for violence-related injury was lower on intervention units, compared to controls (IRR 0.37, 95% CI 0.17-0.83).

Conclusion

This data-driven, worksite-based intervention was effective in decreasing risks of patient-to-worker violence and related injury.

HOSPITAL THREATS

Hospital Violence Hits Home

By Thomas R. Collins

The Hospitalist. 2015 March;2015(3)

Source: <https://www.the-hospitalist.org/hospitalist/article/122542/hospital-violence-hits-home>

Hospitalists could hardly be faulted for wondering: Am I safe? After all, the inpatient setting can be a tense place, and it's where hospitalists work day in and day out.

David Pressel, MD, PhD, FHM, a pediatric hospitalist and medical director of inpatient services at Nemours Children's Health System, which has locations in Delaware, New Jersey, Pennsylvania, and Florida, says it's no wonder violence can erupt in the hospital setting.

"Violence is an issue in hospitals that is a reflection of our society, unfortunately," says Dr. Pressel, a member of Team Hospitalist. "And it happens because these are very stressful places where people's behavior can get outside the norm given the stress of the problems."

Dr. Pressel, in collaboration with many others, has developed a workplace violence prevention program at Nemours aimed at de-escalating situations to avoid physical violence. The program teaches providers how to respond when something violent does happen. It's a tiered training regimen that involves more training for those most involved in handling violent situations.

Dr. Pressel is no stranger to violence himself. Although he is a pediatric hospitalist and his patients are younger, some adolescent patients can have the physical presence of adults and pose just as serious a threat. He said that before the training program was put into place about a year ago, an episode of violence every month or two would require a patient to be placed in restraints.

"Staff has been hurt," he explains. "I've been bitten twice by a patient. I have a scar on my arm that will be with me for life from one episode."

A Slow, Disheartening, Upward Trend

Whether violence in hospitals and medical facilities is really a growing problem—or whether awareness of the issue is simply greater given these recent, high profile incidents—is not entirely known.

But according to the latest figures available from the Bureau of Labor Statistics (BLS), provided by the Occupational Safety and Health Administration (OSHA), violent incidents in hospitals did appear to be on the rise through 2013. The number of hospital assaults rose from 5,030 in 2011 to 5,500 in 2012 to 5,660 in 2013.

The number of assaults rose across all private sector industries over that span, but the percentage of those assaults that occurred in hospitals grew greater during that time—an indication that hospitals might be getting more violent at a faster pace than other workplaces. In 2011, according to BLS data, 21.4% of all assaults in private sector industries occurred in hospitals. That number rose to 21.8% in 2012 and to 22.1% in 2013.

According to the 2014 Healthcare Crime Survey, published by the International Association for Healthcare Security and Safety (IAHSS)—an organization of hospital security officials and administrators—violent crime at U.S. facilities rose from two incidents per 100 beds in 2012 to 2.5 incidents per 100 beds in 2013. That category includes murder, rape, aggravated assault, and robbery.

Assaults rose from 10.7 incidents per 100 beds in 2012 to 11.1 incidents per 100 beds in 2013.

BLS data also show that more injuries in hospitals are due to assaults compared with the private sector overall. In 2011, 2.6% of all private sector injuries were due to assault; in 2012, the number rose to 2.8%; and, in 2013, it was 2.8%. In hospitals in 2011, 8.6% of all injuries resulted from assaults. That percentage rose to 9.5% in 2012 and to 9.8% in 2013.

"BLS data show that nonfatal injuries due to violence are greater in the healthcare/social assistance setting than in other workplaces," an OSHA spokesperson says. "Assaults represent a serious safety and health hazard within healthcare, and data indicate that hospitals comprise a large percentage of workplace assaults."

Incident Prevention

Programs aimed at preventing violence can reduce these incidents.

"How well prepared hospital workers are in dealing with violent situations depends on the workplace violence prevention program implemented at a facility," the OSHA spokesperson says. "Some states have

HOSPITAL THREATS

passed legislation that specifically requires workplace violence prevention programs in the healthcare setting.”

These programs should address management commitment and employee participation, worksite analysis, hazard prevention and control, safety and health training, and recordkeeping and program evaluation. These elements should be assessed regularly, with changes made to respond to changing conditions, OSHA says.

A large number of OSHA inspections in the healthcare setting occur because of complaints regarding lack of protections against workplace violence. In 2014, the agency did 35 inspections in response to such complaints; 25 of those were in a healthcare setting, with 12 specifically at hospitals. As a result, five citations were issued, all of which were in healthcare, including two at hospitals.

The stories send chills through the healthcare world:

- A patient at Mercy-Fitzgerald Hospital outside Philadelphia shoots and kills a caseworker and injures a psychiatrist; the gunman is shot when the psychiatrist returns fire.
- A patient at St. John's Hospital in St. Paul, Minn., grabs an IV pole and rampages through a unit beating nurses with the pole, leaving one with a collapsed lung and another with a broken wrist.
- In January, a man asks to see a cardiologist at Brigham and Women's Hospital in Boston, then shoots and kills the cardiologist when he enters the exam room.

Last year, Brookdale University Hospital and Medical Center in Brooklyn, N.Y., was fined \$78,000 after an OSHA inspection found 40 incidents of workplace violence between Feb. 7 and April 12. They included employees who were threatened or verbally or physically assaulted by patients and visitors or while breaking up fights between patients. In the worst attack, a nurse sustained severe brain injuries.

The bulk of the hospital's fines came as a result of a willful violation—an intentional or voluntary disregard for laws meant to protect workers against hospital violence.

You have to do a vulnerability assessment, and you specifically have to look at your demographic. You specifically have to look at what is the history and the culture of the facility [to determine a hospital's specific risk factors]. —David LaRose, president, IAHS, director of safety, security, and emergency management, Lakeland Regional Medical Center, Florida.

While data from IAHS and the BLS show an increase in hospital violence, those national figures aren't as important as what is happening at your own facility, says David LaRose, MS, CHPA, CPP, the president of IAHS and director of safety, security, and emergency management at Lakeland Regional Medical Center in Florida.

“You have to do a vulnerability assessment, and you specifically have to look at your demographic,” he says. “You specifically have to look at what is the history and the culture of the facility” to determine a hospital's specific risk factors.

Although it's crucial that a hospital track its own statistics on violence, that's not to say that incidents elsewhere are irrelevant.

“You also want to look at what's happening in the real world,” he says. “Somebody else's unfortunate (occurrence) is a learning experience for my system, so we can try to be proactively preventing that.”

Educate, Recognize, React

At Nemours, Dr. Pressel didn't develop the training in response to a perceived rise in incidents there. It was apparent, he says, that deficiencies in readiness needed to be addressed.

In the Nemours program, every staff member with some level of patient care responsibility gets basic training in aggressive child emergencies: identifying these situations, responding appropriately, and keeping safe. This group includes doctors, nurses, and nurse's aids. The training involves actually playing out scenarios of violence, with staff members attempting to subdue a would-be attacker.

Depending on the job, each worker receives extra training that is specific to the role he or she would play in handling violent scenarios.

The training is designed to help individuals respond to such situations with “the same alacrity and acuity as they would respond to a Code Blue,” Dr. Pressel says. “Drop what you're doing and run. These events are dangerous. That's what they teach people. They're dangerous and they're scary and they're chaotic, just like a Code Blue. That's how people need to treat it.”

HOSPITAL THREATS

The goal is to de-escalate a situation, verbally or physically, without more aggressive means. But if that doesn't work, physical restraints, medication, or both are used.

Throughout the medical field, training in this area is scarce, Dr. Pressel says. In nursing school and medical school, "for the most part, it's zero," he says.

"If you're in a psychiatric facility, these events happen," he adds. "And then you get a lot of enhanced training." But, he notes, "I had no formal training until I became tasked with dealing with this."

Since the program was implemented at Nemours, it seems to have worked.

"We have had many of these episodes that have been resolved by verbal de-escalation, as opposed to physical restraints or medication," he says.

His hospital has also made other changes. The facility used to have multiple entrances and exits that were unsecured, and anybody could walk into any unit "with no challenge whatsoever." Now, everyone entering has to pass hospital personnel. And, to get into a patient unit, visitors have to check in and be issued a photo ID. Also, in response to an incident in 2013, the hospital now has "constables" who are trained and licensed to carry firearms, Dr. Pressel says.

Above all, he notes, is personal safety. If you yourself are hurt, you won't be able to help anyone else.

"That's absolutely the first thing that people hear, the last thing that people hear, and it's repeated over and over again," he says.

Both Dr. Pressel and LaRose say that even with the drumbeat of high profile incidents, they haven't heard from colleagues that health professionals are concerned about people losing interest in entering the field or are feeling burned out because of safety concerns. Being prepared is the key, and the level of preparedness varies by facility, LaRose says. The IAHS provides security and healthcare safety guidelines at iahss.org.

"We recognize that we are in an occupation that tends to be on the receiving end of more aggression and more violence than the average worker," LaRose says. "Therefore, how proactively does the organization or the institution take that knowledge and provide the tools and the training to the staff?"

"What can we do as a team to increase our sense of security and safety and make this a great place to continue your career?"

Tom Collins is a freelance writer in South Florida.

Workplace Violent Incidents at Hospitals – July 1, 2017 through September 30, 2017

DEPARTMENT OF INDUSTRIAL RELATIONS

DIVISION OF OCCUPATIONAL SAFETY AND HEALTH – California, USA

Annual Report Posted in January 2018

Source: <https://www.dir.ca.gov/dosh/Reports/Annual-Report-WPV-Incidents-2018.01.16.pdf>

Violence in the Hospital: Preventing Assaults Using a Clinical Approach

Source: <https://www.hhnmag.com/articles/8306-violence-in-the-hospital-preventing-assaults-using-a-clinical-approach>

June 09 – Jessica Rosing, R.N., has been punched, kicked and threatened, but she never reported those incidents to supervisors, figuring they were just part of the job.

Often, she reasoned, patients were not in control of their actions, or there was a justifiable reason for their aggression. But when a patient violently yanked Rosing's arm and threatened to stab her with a syringe about a year ago, her views began to change.

"I've been trying to advocate to my co-workers that, regardless of the circumstances, getting punched in the face is getting punched in the face, and that's something that we shouldn't be tolerating," she says.

HOSPITAL THREATS

So, too, has the attitude shifted at the 15-hospital, Milwaukee-based Aurora Health Care system where she works, and it's shifting at hospitals across the country. Violence appears to be on the rise in the health care setting, fueled by myriad issues, many unrelated to mental health. Those include emergency room wait times, domestic disputes, an opioid epidemic that's bringing desperate patients to hospitals for drugs or addiction treatment, and by a general shortage of beds for behavioral health.

Violent crimes taking place in such institutions have risen from two such events per 100 beds in 2012 to almost three in 2015, according to the Joint Commission. About 50 percent of all workplace assaults occur in the health care setting, according to the Bureau of Labor Statistics.

To address the problem, Aurora Health Care put together a systemwide steering committee about a year ago, on which Rosing participated. Leaders found violence to be grossly underreported at Aurora and elsewhere in the field, says Mary Beth Kingston, R.N., executive vice president and chief nursing officer of the Wisconsin system. With that in mind, Aurora piloted a call center and urged employees at its behavioral health hospital to report any incident, whether verbal or physical. Eventually, Aurora may have those reports skip the call center middleman and go directly to loss prevention or the employee health division. Without solid data, says Kingston, "we're not able then to identify where we need to put our resources. We just don't have an idea of the scope of the issue, and it makes developing strategies to address it much harder."

In just the first three weeks of the pilot, Aurora saw more reported incidents than in all of 2015, which Kingston believes is a sign of progress. She'd like to see a consistent, user-friendly system spread to other hospitals in the system, and is eyeing further remedies to document and respond to such violence. Already, they are training gatekeepers who answer phones to de-escalate touchy situations, along with placing red flags in the electronic health records of patients to warn employees of a patient's history of violence.

Kingston says hospitals must embrace a "systems approach" to addressing assaults in their organizations, not just doing so in a reactive fashion at local sites.

"Across the country, we really do need to work with all of our providers and folks in health care to change the mindset and say, 'Yes, we're caring for people at a very vulnerable time, but no, we want to put systems in place so that we all can see that this really isn't part of our job,' and ask ourselves how we can prevent such violence. That's where we're at," she says.

Executive Corner: A BERT response from start to finish

In a December American Hospital Association webinar, experts from Mission Health in Asheville, N.C., detailed how they have deployed a Behavioral Emergency Response Team to move upstream and prevent staff assaults before a situation escalates. The intervention was developed through a process of data analysis and continuous improvement. Sonya Grack, R.N., senior vice president of patient safety net services and behavior health, emphasized that there is likely no end point to these efforts. "You can never get complacent in this work. It's a constant quest," she says. Here are the nine steps in the initiation of the BERT team:

1. Patient behavior escalates.
2. Staff on the floor attempt to de-escalate the situation.
3. Patient behavior continues or escalates.
4. Code BERT is activated by calling hospital operator; team is paged overhead.
5. Team arrives to floor within 15 minutes, with security arriving sooner.
6. Verbal de-escalation is led by a behavioral health clinician.
7. Medications are obtained and administered by a primary nurse, as needed.
8. The team debriefs.
9. House supervisors continue to round on patient daily.



HOSPITAL THREATS

Adding up

Mission Health, in Asheville, N.C., has found that violence prevention is in the numbers. The seven-hospital system had been working to solve this “major national issue” for years, but a call from its board and leadership to begin benchmarking and tracking violence-related data helped to crystallize those efforts, says Chris DeRienzo, M.D., chief quality officer for the health system.

Fueled by support from its governing body, Mission Health formed a multidisciplinary assault-reduction team, incorporating all hospital staff affected by this issue — nursing, psychiatry, security, quality improvement, risk management, etc. The team began meeting monthly to review data on assaults and started looking for opportunities to prevent violence and improve staff safety, DeRienzo says. They came up with approaches specifically tailored to each part of the health system that was prone to attack, including the medical-surgical unit, the ED, psychiatric units and its regional hospitals.

For instance, Mission Health’s med-surg unit began utilizing what it calls a Behavioral Emergency Response Team. With it, a single phone call to the hospital operator sends a “Code BERT,” which activates a multidisciplinary team of professionals at any time of day, 24/7, to respond to any potential or actual violent situation. First deployed in the 760-bed flagship Mission Hospital in Asheville, the health system is now working to spread the BERT concept across its enterprise, DeRienzo says. In concert with those efforts, they’ve eyed other strategies to decrease assaults in the ED: training staff to recognize the early signs of escalating behavior, using crisis intervention and prevention techniques, providing medications in a more consistent manner so that patients don’t grow agitated waiting for them, and ensuring that security and behavioral health specialists are consistently available during crises.

DeRienzo cautions that having reliable data for a hospital’s board and leadership teams to act upon is crucial, but organizations must not get bogged down by the numbers. He encourages hospitals to try a strategy, evolve it, perform iteration and try again.

“You can only spend so much time getting your data right, and then you have to take action. I think it’s important for groups to be mindful that they’re taking action on data that are as good as they can get, but that they don’t land in analysis paralysis and never try an intervention,” he says.

As one early sign of success, DeRienzo notes that within the first year of the Code BERT program, about 75 percent of the nearly 300 nurses surveyed feel safer on the job. An equal percentage say they’re comfortable working with patients who are experiencing a behavioral health emergency. Since 2013, Mission Health also has seen a drop in the number of days employees are absent because of injury, as well as the total number of reportable cases of assault — the only two nationally benchmarked stats tied to workplace assaults.

Leaders at the North Carolina system believe violence perpetrated on hospital staff constitutes a “burning platform” that should fuel the field to aggressively track and decrease violent incidents. In an article written for *Hospitals & Health Networks* in March, Mission Health CEO Ronald Paulus, M.D., underscored the need for centralized assault-related databases or registries to help hospitals and policymakers understand the issue. Stats tracked by those repositories might include the number of staff calls for immediate intervention each month or the number of assaults on staff and incidents with injury per month.

DeRienzo believes such data will enable health care providers to address and eliminate workplace violence in the same way that data-driven solutions helped to reduce patient falls or central line-associated bloodstream infections. Fifteen years ago, CLABSIs were seen as one of the inevitabilities of health care, but today they’re entirely preventable. DeRienzo says the field must view assaults similarly, regardless of the myriad unpredictable factors that may cause them.

“Once you have something that can be preventable, then zero is a realistic option,” he says. “I’m not saying it’s realistic tomorrow. I’m not saying it’s realistic in three months or nine months or 12 months, but once you have the data and you can begin driving interventions based on that data, then, yes, I firmly believe that, as with any construct across the quality and safety universe, zero is the ultimate goal.”

Big picture prevention

From a national perspective, the American Hospital Association has pegged workplace violence as a key concern in 2017. In a letter to the Occupational Safety and Health Administration in April following a request for comments, the AHA echoed the need for data and sharing best practices to help mitigate workplace violence.

As part of its yearlong Hospitals Against Violence initiative, the association recently hosted a series of webinars tied to the issue, AHA General Counsel Melinda Reid Hatton wrote in the letter to Dorothy

HOSPITAL THREATS

Dougherty, OSHA's deputy assistant secretary of labor and health. The webinars cover a range of topics, including how to prepare for an active shooter and risk-mitigation strategies to avoid assaults in the hospital's corridors. Up next, the AHA's American Organization of Nurse Executives has collaborated in recent months with the International Association for Healthcare Security and Safety, with plans to host an upcoming webchat on June 13.

Two years ago, AONE, alongside the Emergency Nurses Association, released a list of eight guiding principles to help mitigate violence in the workplace. Extending from that original work, AONE is now planning an updated version, "Mitigating Workplace Violence 2.0," that looks outside of the nursing sphere by incorporating security to gain further perspective on the approach, says CEO Maureen Swick, R.N. Her hope is to give nurse executives real examples of health facility safety assessments that they could implement in their own organizations, as well as de-escalation training techniques from a security standpoint.

"It's really to broaden the scope and have a more inclusive, interprofessional look at workplace violence, especially with the experts," says Swick, who is also the chief nursing officer of the AHA. "Security [personnel] are folks who are intimately involved in the safety of our health care organizations, and have done some tremendous work on training, on de-escalation and on preventing violence in the workplace. So, we want to make sure that we capture that in [expanding] the work that was originally done."

The need for such broadening of the scope of anti-violence work within the hospital has been one of the major findings for the Washington State Hospital Association. The group recently released its own toolkit following an extensive literature review and gap analyses at member hospitals.

One key takeaway for Lucia Austin-Gil, senior director of patient safety at WSHA, is the need to integrate the work of security, patient safety and employee health experts who typically all report to different members of the C-suite. The toolkit notes that the current decentralization of safety functions "can make efforts to establish a single organizational focus on safety very difficult and is a main point of frustration with professionals addressing the risk of aggressive behavior in health care."

The WSHA released its draft toolkit in the spring with an aggressive goal of reducing violent incidents by 20 percent before winter.

Boards and executives alike, on a widespread geographical scale, are frustrated by this issue, Austin-Gil says, but momentum seems to be building toward a solution.

"This problem is not new, clearly, but because of the increase in rates and the impact on not only patient outcomes, but staff morale, we're hearing from the front line all the way up to the C-suite and board level, that there's an urgent need for support around this topic," she says. "Some CEOs sound, quite frankly, exasperated because it's so complex and multifaceted, but we have come together and committed to starting somewhere."

7 steps to prepare for a gunman

Active-shooter situations may occur in hospitals much less frequently than physical assaults, but the outcome is much more devastating, says Kevin Tuohey, board president-elect of the International Association for Healthcare Security and Safety. In a January webchat hosted by the American Society for Healthcare Engineering of the American Hospital Association, Tuohey spelled out seven steps hospitals can take to prepare for an active shooter. According to ASHE, about 95 percent of hospitals have a plan in place, and Tuohey believes awareness is building that hospitals are no longer immune from mass shootings. "While hospitals have always been looked at as places of refuge, as places that were really safe, I think in the last 10 years that's changed, and I think that they are no longer exempt," he says.

Visit [AHA.org/hav](https://www.aha.org/hav) to find webinars on both "4 Universal Precautions to Shift a Hospital's Culture" and the Behavioral Emergency Response Team approach to preventing staff assaults, plus additional resources.

- STEP 1 | Assess risks and vulnerabilities.
 - STEP 2 | Determine prevention and response actions.
 - STEP 3 | Reduce workplace violence.
 - STEP 4 | Plan mock drill exercises and training.
 - STEP 5 | Collaborate with outside law enforcement.
 - STEP 6 | Build communication and crisis awareness among staff.
 - STEP 7 | Debrief and recover from an incident.
-

HOSPITAL THREATS

Don't lose sight of lateral violence

While recent attention in the field has focused on violence inflicted on hospital staff by patients or their families, experts say that it is important not to lose sight of lateral violence in the workplace, which can come in the form of bullying, general incivility among colleagues or, in some cases, physical altercations between staff members. Some — like Lisa Wolf, R.N., and director of the Emergency Nurses Association's research institute — believe that lateral violence can contribute to, or exacerbate, other violent incidents perpetrated by patients.

Wolf speculates that new nurses are the most vulnerable to both bullying by colleagues and attacks by patients — and that the two behaviors are linked. Rookie nurses may be given complex patients beyond the nurses' experience level with no support from more seasoned staff and be forced to work long hours. New nurses also may feel too intimidated to report incidents.



If a nurse is not given information about a potentially violent patient or not supported in the care of such a patient, the likelihood of an incident occurring is much greater. "External violence, when we think of workplace violence, may actually be facilitated and encouraged by nurses' own workplace bullying behaviors," Wolf says. Wolf has preliminary data demonstrating the connection and plans to test the theory in future research. In recent literature, the American Nurses Association, the Occupational Safety and Health

Administration and others have mentioned the connection between bullying and violence, along with patient and nurse safety. Bullying, as defined by the ANA, is "repeated, unwanted harmful actions intended to humiliate, offend and cause distress in the recipient."

OSHA offered mitigation strategies to help prevent bullying and violence in its 2015 guide "Preventing Workplace Violence: A Road Map for Healthcare Facilities." St. John Medical Center, Tulsa, Okla., which is part of Ascension Health, has an incident-reporting system that allows a worker to bypass supervisors who might be perpetrating the abuse.

Bullying often can arise from "clinical hierarchies," i.e., the long-tenured surgeon who yells at an assistant to remind him to wash his hands. St. John has engaged its physicians in designing anti-bullying strategies led by Chief Medical Officer John Forrest, M.D., who has a zero-tolerance policy toward such behavior. Forrest believes it's crucial to take seriously all bullying complaints and to respond immediately before tensions fester. More recently, St. John began expediting responses to such complaints with a newly installed electronic reporting system. The medical center also hopes to break down clinical hierarchies and foster collaboration with physician-nurse rounding.

"You have to continually maintain the culture of an open, free line of communication," Forrest says. "I try very hard to show my face around every nook and cranny of the medical center about once a week so that people know you're there and approachable. With these sorts of issues, you've got to create an environment in which communication goes in both directions, and it's not just a one-way street."

Preventing violence in Healthcare – Gap analysis

Source: <https://www.mnhospitals.org/Portals/0/Documents/ptsafety/workplace%20violence%20prevention/Preventing%20Violence%20in%20Healthcare%20Gap%20Analysis.pdf>

Preventing Hospital Violence Requires Proactive Strategy

Source: <https://www.ahcmmedia.com/articles/140589-preventing-hospital-violence-requires-proactive-strategy>

May 2017 – Hospitals are focusing more on violence and how to prevent it in the healthcare setting, but they still need to adopt a more proactive approach that includes all forms of violence, not just the big notable incidents, experts say.

HOSPITAL THREATS

More hospitals have addressed violence in recent years, partly to comply with requirements or guidelines from The Joint Commission, OSHA, and other regulatory bodies. Most are not going far enough, says Monica Cooke, BSN, MA, RNC, CPHQ, CPHRM, FASHRM, a behavioral risk management and quality improvement consultant with Quality Plus Solutions in Annapolis, MD.

"Healthcare organizations are beginning to get more of an idea that they need to take a stand on workplace violence, but we're still pretty far behind," Cooke says. "They're developing workplace violence programs and policies, but they still tend to be reactive. They are all about how to respond when the event happens, as opposed to a more proactive approach to violence prevention and mitigation."

Organizations often make the mistake of focusing their efforts on Sentinel Event violence, the unusual incidents such as an active shooter or hostage-taker, Cooke says. Just as important, and perhaps even more so, are the far more common smaller incidents of violence, she says.

"These are the daily incidents of aggression and abuse that staff have to tolerate from patients, visitors, and even staff to staff. This occurs all the time and sometimes doesn't get the attention it deserves," Cooke says. "You need the plans in place for the big Sentinel Events, but you also need plans for mitigating the day-to-day aggression. I have not seen a whole lot of that."

Time to Act

Failing to address those more common incidents can lead to the bigger incidents when aggression is left unchecked and people see there are no consequences for bad behavior, she says. In addition, people are unlikely to be effective in addressing serious incidents of violence if they have not been provided the training and resources to respond to more common everyday incidents, she says.

Hospitals have taken a big step forward in awareness of the problem, Cooke says, and they have changed the healthcare culture so that violence is not seen as an unsolvable problem or a byproduct of clinical work that must be tolerated. The next step, she says, is to produce a meaningful effect on violence.

"It's time to implement practices, and programs, and systems that can work to minimize the level of aggression in your facility, to prevent it or minimize it," Cooke says. "We don't want to wait until the patient is screaming and banging the walls or throwing things before people get alarmed and take action. We need to develop training and promote competency in this among all staff, including receptionists, housekeeping, maintenance, and anyone else that comes into contact with the patients and the public."

That training should include issues such as what the hospital expects of them when they encounter an aggressive or violent person, methods for de-escalation, and the steps to take before calling for help from security or others, she says.

Response Teams for Violence

Knowing at what point to step back and call for help is a key component of staff training, Cooke says. Also, the organization must determine who is going to respond to that call for help and it's not always going to be security officers. It might be co-workers or a supervisor, and many hospitals employ rapid response teams (RRTs) similar to the clinical RRTs and code teams that nurses rely on when a patient's medical condition needs immediate attention.

The violence RRTs include various staff members who have advanced training in de-escalation and physical defense, as well as behavioral health professionals who can talk to the violent person and, if necessary, provide medications.

Without such a resource, the same nurses and other clinicians who depend on clinical RRTs are left with few options in a different kind of emergency, Cooke notes.

"Too many hospitals have a policy that essentially says, 'Call security.' In reality, security should be the last resort because their presence often escalates a situation and it can turn into something bigger than it had to be," Cooke says. "There should be an effort to de-escalate and prevent the violence that will need a security response, and that can only happen if staff are given the right training and resources."

Code Violet Brings Help

Nationwide Children's Hospital (NCH) in Columbus, OH, takes a proactive approach to violence, which is especially necessary because the facility treats a high number of young people for behavioral health issues. The hospital's response plan for violence uses the name "Code Violet," notes Dan Yaross, MSM, CPP, CHPA, director of security at NCH. A violent patient will prompt staff to call a Code Violet, and that brings representatives from several different departments to help.

HOSPITAL THREATS

The Code Violet response alerts a security officer, nurses, a member of the hospital's behavioral health crisis management team, the attending physician, and a pharmacist who can provide sedation if necessary.

"Everyone has a role, and we also have enough people to implement safe holds if necessary," Yaross explains. "De-escalation is the goal, but if we have to go hands-on, we need a number of people with the right training to do that. There's a specific procedure for controlling each limb and securing the head so they don't slam it on the floor, and the people on the response team have that training."

NCH uses a broad definition for violence or aggression that may require intervention, Yaross says. In addition to physical violence, aggression includes verbal threats or passive aggressive comments suggesting a threat, yelling, throwing objects, and body language. All NCH employees have been trained to recognize the signs of potential violence and are authorized to call for help.

"Every employee is authorized to activate Code Violet whenever they see the need," Yaross says. "We don't restrict that to just certain people like supervisors or someone else with authority."

Violent History Documented

For violent persons other than patients, the staff calls a "Code Violet — Security," which alerts a security officer and, in the evening, the nursing supervisor who is in charge of the hospital at night when administrators are away. These incidents may involve siblings and parents, other visitors, and people who have no business at the hospital but come in off the street and cause a disturbance, Yaross says. (See the story in this issue for information on how NCH screens visitors for security.)

The hospital also notifies the social work department after an incident with a non-patient so they can follow up with family members if they were victims, or with unrelated patients or visitors who may have witnessed the violence.

NCH made the program more proactive over the past couple of years after witnessing harm to employees that could have been mitigated if staff had known certain information beforehand, Yaross says. The hospital now documents any Code Violet in its electronic medical record (EMR) system, and that puts a purple warning banner on the patient's record. In the notes section, the hospital details the nature of the incident, what triggers to avoid, and anything else that might prevent or de-escalate violence.

"If that record indicates that the only way to control the individual and prevent him or her from verbally abusing staff is to have security present, we will have a security officer right there when the parent arrives with the child," Yaross explains. "The child sees the officer and behaves. We don't do that with every child with a history of violence, but we know that's what works for this family."

To be even more proactive, the EMR system produces a list every Monday of patients scheduled for appointments at the hospital in the coming week who have a history of violence, Yaross explains. That list is seen by several administrators, including security, which reaches out to the clinic where the patient will be seen. Security alerts the staff that the patient could be violent and offers to have a security officer present with the patient or available nearby, whichever the clinic staff prefer.

"That has been useful in reducing the number of employee injuries because we can anticipate the problem and prevent it, rather than responding after the fact," Yaross says.



Source: <https://www.osha.gov/Publications/OSHA3826.pdf>

HOSPITAL THREATS

A FRAMEWORK FOR MAKING HOSPITALS A SAFER WORKPLACE FREE FROM WORKPLACE VIOLENCE

Health care workers have the right to do their jobs in a safe environment free of violence. Hospitals that are safer workplaces benefit everyone because a safe environment enables health care workers to better meet the evolving needs of all patients.

Source: https://www.pshsa.ca/wp-content/uploads/2017/03/P1_VPRTLYEN0217-Accountability-Framework-2.pdf

Preventing HealthCare Workplace Violence Toolkit®

Source: http://www.wsha.org/wp-content/uploads/FINAL_2017_05_12_WS_Toolkit.pdf



NHS seeks to recover from global cyber-attack as security concerns resurface

Source: <https://www.theguardian.com/society/2017/may/12/hospitals-across-england-hit-by-large-scale-cyber-attack>

May 2017 – The [NHS](#) is working to bring its systems back online after it became the highest-profile victim of a global ransomware attack and faced renewed concern about the strength of its infrastructure.

The National Cyber Security Centre (NCSC) said teams were “working round the clock” in response to the attack, which resulted in operations being cancelled, ambulances being diverted and documents such as patient records made unavailable in England and Scotland.

Computers at hospitals and GPs surgeries in the UK were among tens of thousands hit in almost 100 countries by malware that appeared to be using technology stolen from the National Security Agency in the US. It blocks access to any files on a PC until a ransom is paid.

The British prime minister, Theresa May, and NHS Digital said they were not aware of any evidence patient records had been compromised in Friday’s attack, which is thought to have [affected computers in nearly 100 countries](#).

May said: “This is not targeted at the NHS, it’s an international attack and a number of countries and organisations have been affected.”

Amber Rudd, the home secretary, refused to confirm on Saturday morning whether patient data had been backed up, and said the NHS would upgrade its software in the wake of the attack. She said data “should” be backed up, but would not say whether it actually had been.

The shadow health secretary, Jonathan Ashworth, urged the government to be “clear about what’s happened”, describing the attack as “terrible news and a real worry for patients”.

HOSPITAL THREATS

The unprecedented attacks, using software called [WanaCrypt0r 2.0 or WannaCry](#), exploits a vulnerability in Windows. Microsoft released a patch – a software update that fixes the problem – for the flaw in March, but computers that had not installed the security update were vulnerable.

In December it was reported that nearly all NHS trusts were using an obsolete version of Windows for which Microsoft had stopped providing security updates in April 2014. Data acquired by software firm Citrix under freedom of information laws suggested 90% of trusts were using Windows XP, then a 15-year-old system.

It is not known how many computers across the NHS today are still using Windows XP or recent variants Windows 8 and Windows 10.

About 40 NHS organisations are thought to have been affected by Friday's bug, which was released the day after a doctor warned that NHS hospitals needed to be prepared for an incident precisely of the kind seen.

In an article published in the British Medical Journal, Dr Krishna Chinthapalli, a neurology registrar at the National Hospital for Neurology and Neurosurgery in London, said hospitals "will almost certainly be shut down by ransomware this year".

Ross Anderson, of Cambridge University, said the "critical" software patch released earlier this year may not have been installed across NHS computers. "If large numbers of NHS organisations failed to act on a critical notice from Microsoft two months ago, then whose fault is that?" Anderson said.

Alan Woodward, a visiting professor of computing at the University of Surrey, said the attack's success was "likely to be because some organisations have either not applied the patch released by Microsoft, or they are using outdated operating systems."

NHS Digital said on Friday night it was unable to comment on the suggestion.

Marco Cover, a systems security researcher, said critics should take into account the complexity of keeping systems up to date. "It's easy to blame people who don't upgrade," he said. "But in practice things are often more complicated: operations teams may not touch legacy systems for a number of reasons. In some cases they may even be unaware that such legacy systems are running in their infrastructure."

The same malicious software that hit NHS networks attacked some of the largest companies in Spain and Portugal, including phone company Telefónica, and has also been detected on computers in Russia, Ukraine and Taiwan among other countries. The international shipping company FedEx was also affected. Kaspersky Lab, a cybersecurity company based in Moscow, estimated that 45,000 attacks had been carried out in 99 countries, mostly in Russia. In a blogpost, [it added](#) that the totals could be "much, much higher".

In the UK, computers in hospitals and GP surgeries simultaneously received a pop-up message demanding a ransom in exchange for access to the PCs.

A warning was circulated on Friday within at least one NHS trust of "a serious ransomware threat currently in circulation throughout the NHS", but the attack proved impossible to stop. Patient records, appointment schedules, internal phone lines and emails were rendered inaccessible and connections between computers and medical equipment were brought down. Staff were forced to turn to pen and paper and to use their own mobile phones.

Last year the government established the NCSC to spearhead the country's defences. In the three months after the centre was launched, there were 188 "high-level" attacks as well as countless lower-level incidents. The chancellor, Philip Hammond, disclosed in February that the NCSC had blocked 34,550 potential attacks targeting UK government departments and members of the public in six months.

The Patients Association condemned the criminals behind Friday's attack, and said lessons from earlier incidents had not been learned. "It has long been known that the NHS struggles with IT in multiple respects and that this includes serious security problems," it said.

Infected computers show a message demanding a \$300 (£233) ransom per machine to be paid to a Bitcoin wallet address. It says: "Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

"You only have three days to submit the payment. After that the price will be doubled. Also if you don't pay in seven days, you won't be able to recover your files forever."

NHS Digital confirmed that a "number of NHS organisations" had been affected and refused to confirm or deny reports that put the total as high as 40. "The investigation is at an early stage but we believe the

HOSPITAL THREATS

malware variant is Wanna Decryptor," it said. "At this stage, we do not have any evidence that patient data has been accessed. We will continue to work with affected organisations to confirm this.

"NHS Digital is working closely with the National Cyber Security Centre, the Department of [Health](#) and NHS England to support affected organisations and to recommend appropriate mitigations."

British law enforcement agencies said they believed the attack was criminal in nature, as opposed to a cyber-attack by a foreign power, and was being treated as serious but without national security implications.

One NHS worker, who asked to remain anonymous, said the attack began at about 12.30pm and appeared to have been the result of phishing. "The computers were affected after someone opened an email attachment. We get a lot of spam and it looks like something was sent to all the trusts in the country. Other hospitals have now been warned not to open these emails – all trusts communicate with each other."

Another NHS worker, who works at an Essex hospital and also asked to remain anonymous, said her team's computers went down at about 2pm. "We were told to shut down, take out network cables and unplug the phones," she said. "A message came up for just one of our team about the fact that all the files would be wiped in two hours unless we gave \$300 in bitcoins."

Dr Chris Mimmagh, a GP in Liverpool, said his surgery had "severed links" to the wider NHS network as a precaution. He said: "Unable to access our clinical system – as a precaution our area has severed links to the wider NHS, which means no access to our national systems, no computers means no records, no prescriptions, no results. We are dealing with urgent problems only. Our patients are being very understanding so far."

Lorina Nash, 46, from Hertfordshire, was bringing her mother for an appointment at Lister hospital in Stevenage when systems went down. "We have been here since 12.30pm and the computers were affected at about 12pm – patients are still waiting around but most of the A&E patients have been sent to other hospitals. I have never seen accident and emergency so empty.

"They gave my mum a blood test but have had to send her blood to Cambridge by courier for testing. They said it could take two or three hours before it comes back with a result."

Dr Asif Munaf, a gastroenterologist at Chesterfield hospital, said there was a backlog of patients in its A&E, which he said had been badly affected because it was unable to book new patients on the system. "From my ward's point of view, we're not able to make referrals to, for example, psychiatry because they use a different system to us," he said. "Everything's getting delayed. Patients who were supposed to go home this afternoon won't go home until Monday because they now won't be seen and get a follow-up plan. It's quite unfortunate for the patients."

Dr Christopher Richardson, the head of the cybersecurity unit at Bournemouth University, said the process of recovering the NHS's IT systems would involve a painful and longwinded "deep strip" of affected computers.

"You go down to the basic machine, you take everything off it, you reconfigure it and then you build it back up again," he said. "If you're talking national health, you're talking a lot of machines on a single site and you've got to get them all because these nasty pieces of malware, they float around, so they only have to remain on one machine and when you reboot it will deliver the same thing again."

'Accidental hero' halts ransomware attack and warns: this is not over

Source: <https://www.theguardian.com/technology/2017/may/13/accidental-hero-finds-kill-switch-to-stop-spread-of-ransomware-cyber-attack>

May 2017 – The "accidental hero" who halted the global spread of an unprecedented ransomware attack by registering a garbled domain name hidden in the malware has warned the attack could be rebooted.

The ransomware used in Friday's attack wreaked havoc on organisations including FedEx and Telefónica, as well as the [UK's National Health Service](#) (NHS), where operations were cancelled, X-rays, test results and patient records became unavailable and phones did not work.

But the spread of the attack was brought to a sudden halt when one UK cybersecurity researcher tweeting as [@malwaretechblog](#), with the help of [Darien Huss](#) from security firm Proofpoint, found and inadvertently activated a "kill switch" in the malicious software.

HOSPITAL THREATS

The researcher, who identified himself only as MalwareTech, is a 22-year-old from south-west England who works for Kryptos logic, an LA-based threat intelligence company.

"I was out having lunch with a friend and got back about 3pm and saw an influx of news articles about the NHS and various UK organisations being hit," he told the Guardian. "I had a bit of a look into that and then I found a sample of the malware behind it, and saw that it was connecting out to a specific domain, which was not registered. So I picked it up not knowing what it did at the time."

The kill switch was hardcoded into the malware in case the creator wanted to stop it spreading. This involved a very long nonsensical domain name that the malware makes a request to – just as if it was looking up any website – and if the request comes back and shows that the domain is live, the kill switch takes effect and the malware stops spreading. The domain cost \$10.69 and was immediately registering thousands of connections every second.

MalwareTech explained that he bought the domain because his company tracks botnets, and by registering these domains they can get an insight into how the botnet is spreading. "The intent was to just monitor the spread and see if we could do anything about it later on. But we actually stopped the spread just by registering the domain," he said. But the following hours were an "emotional rollercoaster".

"Initially someone had reported the wrong way round that we had caused the infection by registering the domain, so I had a mini freakout until I realised it was actually the other way around and we had stopped it," he said.

MalwareTech said he preferred to stay anonymous "because it just doesn't make sense to give out my personal information, obviously we're working against bad guys and they're not going to be happy about this."

He also said he planned to hold onto the URL, and he and colleagues were collecting the IPs and sending them off to law enforcement agencies so they can notify the infected victims, not all of whom are aware that they have been affected.

He warned people to patch their systems, adding: "This is not over. The attackers will realise how we stopped it, they'll change the code and then they'll start again. Enable windows update, update and then reboot."

He said he got his first job out of school without any real qualifications, having skipped university to start up a tech blog and write software.

"It's always been a hobby to me, I'm self-taught. I ended up getting a job out of my first botnet tracker, which the company I now work for saw and contacted me about, asking if I wanted a job. I've been working there a year and two months now."

But the dark knight of the dark web still lives at home with his parents, which he joked was "so stereotypical". His mum, he said, was aware of what had happened and was excited, but his dad hadn't been home yet. "I'm sure my mother will inform him," he said.

"It's not going to be a lifestyle change, it's just a five-minutes of fame sort of thing. It is quite crazy, I've not been able to check into my Twitter feed all day because it's just been going too fast to read. Every time I refresh it it's another 99 notifications."

Proofpoint's Ryan Kalember said the British researcher gets "the accidental hero award of the day". "They didn't realise how much it probably slowed down the spread of this ransomware".

The time that @malwaretechblog registered the domain was too late to help Europe and Asia, where many organisations were affected. But it gave people in the US more time to develop immunity to the attack by patching their systems before they were infected, said Kalember.

The kill switch won't help anyone whose computer is already infected with the ransomware, and it's possible that there are other variants of the malware with different kill switches that will continue to spread.

The malware was made available online on 14 April through a dump by a group called Shadow Brokers, which [claimed last year](#) to have stolen a cache of "cyber weapons" from the National Security Agency (NSA).

Ransomware is a type of malware that encrypts a user's data, then demands payment in exchange for unlocking the data. This attack used a piece of malicious software called "[WanaCrypt0r 2.0](#)" or [WannaCry](#), that exploits a vulnerability in Windows. Microsoft released a patch (a software update that fixes the problem) for the flaw in March, but computers that have not installed the security update remain vulnerable.

HOSPITAL THREATS

The ransomware demands users pay \$300 worth of cryptocurrency Bitcoin to retrieve their files, though it warns that the "payment will be raised" after a certain amount of time. Translations of the ransom message in 28 languages are included. The malware spreads through email.

"This was eminently predictable in lots of ways," said Kalember. "As soon as the Shadow Brokers dump came out everyone [in the security industry] realised that a lot of people wouldn't be able to install a patch, especially if they used an operating system like Windows XP [which many NHS computers still use], for which there is no patch."

Security researchers with [Kaspersky Lab](#) have recorded more than 45,000 attacks in 74 countries, including the UK, Russia, Ukraine, India, China, Italy, and Egypt. In Spain, major companies including telecommunications firm Telefónica were infected.

By Friday evening, the ransomware had spread to the United States and South America, though Europe and Russia remained the hardest hit, according to security researchers [Malware](#) Hunter Team. The Russian interior ministry says about 1,000 computers have been affected.

Trump says London hospital is like 'a war zone' from knife attacks

Source: <https://edition.cnn.com/2018/05/05/politics/trump-london-hospital-nra/index.html>

May 2018 – President Donald Trump compared an unnamed London hospital to a "war zone" on Friday, saying despite tough gun laws in the UK, it has blood all over the floors from victims of knife attacks.

Trump [made the comments in apparent defense of gun ownership at the National Rifle Association](#) convention in Dallas.

"They don't have guns. They have knives and instead there's blood all over the floors of this hospital," Trump said. "They say it's as bad as a military war zone hospital ... knives, knives, knives. London hasn't been used to that. They're getting used to that. It's pretty tough."

It's unclear what hospital Trump was referring to. But the [BBC reported that a trauma surgeon](#) at the Royal London Hospital recently told the network that his fellow doctors have compared it to an Afghan war zone. "Some of my military colleagues have described their practice here as being similar to being at (Helmand province's former Camp) Bastion," Dr. Martin Griffiths told the BBC. "We routinely have children under our care -- 13, 14, 15 years old are daily occurrences, knife and gun wounds."

British media outlets cited his quotes [in stories published last month](#).

Amid the furor over Trump's comments, Griffiths tweeted Saturday: "Happy to invite Mr Trump to my (prestigious) hospital to meet with our mayor and police commissioner to discuss our successes in violence reduction in London."

London Mayor Sadiq Khan's office declined to comment to CNN following Trump's remarks.

Hospitals may be targets for attacks, police counter-terrorism experts warn

Source: <https://www.independent.co.uk/news/uk/home-news/hospitals-counter-terrorism-office-warning-target-attack-guidelines-a7784196.html>



June 2017 – New guidance issued by a police [counter-terrorism](#) unit has warned hospitals and GP surgeries that they may be targets for attacks.

The National Counter Terrorism Security Office released an updated '[Crowded Places Guidance](#)' document, which tells medical professionals: "It is possible that your surgery, for example, could be the target of a terrorist incident. This might include having to deal with a bomb threat or suspicious items left in or around the area."

HOSPITAL THREATS

"The worst-case scenario is your staff, patients and visitors could be killed or injured, and your premises destroyed or damaged in a 'no warning' multiple and co-ordinated terrorist attack."

Hospitals are warned that the nature of such an attack may be covert, "through interference with vital information" or "enabled by an insider or someone with specialist knowledge or access to your venue". Security services are on heightened alert following two terror attacks in the past month in Manchester and London.

The former [took the lives of 22 children and adults](#), making it the worst the country has seen since the 7/7 London bombings in 2005.

The latter saw eight people killed and 48 injured after a lorry and knife attack in [London Bridge](#).

'It was pandemonium' says officer who helped London Bridge attack victims

NHS staff in London were praised for [preventing the death toll from rising](#) in the wake of the attack, and for the work they did to keep the injured alive, many of whom had entered the hospital in critical condition. Deputy Assistant Commissioner Lucy D'Orsi said: "Terrorist attacks are rare in the UK, but recent events have shown that an attack could happen anywhere and without warning.

"Those locations, either public or private, where large groups of people gather for reasons such as entertainment, business, transportation, sporting or social occasions, have always been preferential targets for terrorists.

"The UK threat level from international terrorism is severe, which means that an attack is highly likely. Such an attack can come in many forms, not just a physical.

"It can include interference with vital information or communication systems, causing disruption and economic damage. Against this background there is a need to make our crowded places as accessible as possible and to minimise the threat," she added.

There has been no intelligence to suggest a terror attack targeting hospitals or surgeries is imminent, according to [The Sunday Times](#), however the guide emphasises crowded places are vulnerable to attack.

Body cameras deter attacks and abuse at Welsh hospitals

Source: <https://www.bbc.com/news/uk-wales-43725809>

Apr 2018 – Body cameras are being used to record attacks and abuse towards hospital staff at five of Wales' health boards in a bid to deter violent behaviour.

Aneurin Bevan is the latest to give security staff the cameras after 15,113 incidents in the last five years. One A&E nurse said he was threatened on a weekly basis and once had a patient grab him by the throat. He said the cameras meant "it's no longer just our word against theirs".

[First introduced at the University Hospital of Wales in Cardiff in 2013](#), body cameras are now being worn by all security staff at sites managed by Cardiff and Vale University Health Board.

Head of security, Damian Winstone, said the cameras were more effective than traditional CCTV and had led to successful convictions for a range of offences.

"The use of body cameras is improving how patients, staff and visitors conduct themselves," he said.

Aneurin Bevan, Cwm Taf, Betsi Cadwaladr, and Abertawe Bro Morgannwg (ABMU) health boards also use the equipment at some sites.

No staff at Hywel Dda or at Velindre Cancer Centre in Cardiff, wear body cameras, while there are no district hospitals in Powys.

The cameras, which are the size of a smart phone, are worn by security staff, and some car park and smoking enforcement officers.

People are warned they are being switched on before recording begins.

On Friday, legislation introduced by Rhondda MP Chris Bryant to impose harsher prison sentences on those who attack 999 workers, passed a major hurdle in the bid to become UK law.

An A&E nurse, who did not want to be identified, said he received threats and verbal abuse on an "almost weekly basis".

"Physically it is not that bad but it is always a threat," he said.

"The people using abusive language are often under the influence of a substance, or have behavioural issues.

"We try to talk to them and treat them as someone who is distressed. We try to calm the situation. It doesn't always work."

HOSPITAL THREATS

The nurse said he had once been grabbed around the throat by a patient who was cautioned by the police - he was later diagnosed with mental health issues.

"The security guys do wear body cams," he said.

"It helps because it means it's no longer just our word. They can allege we were rough, but this goes some way to backing up what we said."

From April security, car park and smoking enforcement officers at the Royal Gwent Hospital, Newport, and Nevill Hall Hospital in Abergavenny, will be wearing the cameras.

Aneurin Bevan health board said the measure had been brought in to reduce "the likelihood of violent assaults against staff".

New figures show in 2017-18 alone, almost 1,400 violent incidents were reported at Cwm Taf premises.

The board said cameras, worn by security staff at the Royal Glamorgan Hospital, in Llantrisant, and Prince Charles Hospital, in Merthyr Tydfil, had "been used to capture evidence for prosecutions and convictions".

They are worn by security staff at Glan Clwyd Hospital, in Denbighshire, with staff at all north Wales' district hospitals given violence and aggression training to "teach techniques designed to de-escalate situations".

In 2017, 1,136 staff working for ABMU were physically assaulted while at work.

While no staff wear body cameras, Hywel Dda said it encouraged staff to report incidents of violence and aggression and worked closely with the police.

Hindu extremists attack nuns, destroy hospital wall in India

Source: <http://www.catholicherald.co.uk/news/2018/03/14/hindu-extremists-attack-nuns-destroy-hospital-wall-in-india/>



March 2018 – Suspected Hindu extremists demolished the wall of a Catholic mission hospital and manhandled staff, including nuns, in the latest incident in Madhya Pradesh state, considered a hotbed of anti-Christian violence in central India.

Ucanews.com reported some 60 people, with the help of a bulldozer, razed the boundary wall of 44-year-old Pushpa Mission Hospital in the temple town of Ujjain March 12. They blocked its emergency entrance and destroyed equipment, including power generators.

The hospital has been facing trouble since January after Gagan Singh, the personal assistant of a local legislator, staked a claim over disputed land, said Fr Anthony Pulickamandapam, hospital director.

He told ucanews.com that the land in front of the hospital was given to the hospital by the local civic body for use as a parking area and to maintain its greenery.

HOSPITAL THREATS

The dispute has gone to court after members of the Bharatiya Janata Party, the pro-Hindu party that runs the state government, attempted to take over the land on January 27, accusing the church of illegally occupying the site.

On February 2, hospital authorities obtained a stay order from the Madhya Pradesh High Court to maintain the status quo until a further hearing. But the court transferred the case to a lower court for a police investigation and hearing.

On March 8, the lower court said that, as the case and investigation were proceeding peacefully, there was no need for a stay order, Bishop Sebastian Vadakel of Ujjain told ucanews.com.

The attack happened two days after church authorities sought another stay order.

Fr Pulickamandapam said the attackers came armed with a bulldozer and sharp-edged weapons. They demolished the boundary wall, erected a fence and put up some makeshift shops to claim the land.

“Our staff, including Catholic nuns, who attempted to resist the advance were manhandled and forced to flee for safety,” he told ucanews.com. “They also destroyed the backup power generator and disconnected the water supply, putting the lives of nearly 200 patients – including 12 in the intensive care unit – in serious danger.”

Bishop Vadakel said hospital staff were surprised by police inaction. The local police station and other senior officials refused to respond to calls for help.

“Even our staff nurses, who approached the women’s police station to lodge a complaint, were turned away,” he said.

A Catholic delegation led by Bishop Vadakel met Governor Anandiben Patel, who was visiting the town, and sought protection for Christians and their properties.

Bishop Vadakel said he believes the attack was an attempt to intimidate poor people to keep them away from Christians and their institutions, ucanews.com reported.

Archbishop Leo Cornelio of Bhopal said the attack was part of “a systematic plan to bring disturbance and violence among a peace-loving community.” He wanted the state government to arrest the culprits immediately.

The BJP, which has ruled the state for 15 years after winning three successive elections, will seek another term in the state election due at the end of this year.

Church officials say Hindu groups present themselves as protectors of Hindu rights to garner Hindu votes, and an easy way to that end is to attack Christians, who constitute less than 1 percent of the 73 million people in the state.

Madhya Pradesh had the greatest number of anti-Christian incidents in India last year, according to a report by Persecution Relief, an ecumenical forum that records Christian persecution in India. The state witnessed 52 attacks against Christians in 2017, up from 28 in 2016, the report said.

Attacks have increased since the BJP came to power in New Delhi in 2014. There were 736 reported attacks against Christians in 2017, up from 348 in 2016, said Persecution Relief.

In Ranchi, Cardinal Telesphore Toppo told Catholic News Service, “What happened in Ujjain shows how the BJP is treating the religious minorities.”

“Police and government officials are told to keep quiet and not to intervene when BJP cadres do what they want. Similar shocking incidents are happening in parts of the country,” said Cardinal Toppo, former president of Catholic Bishops’ Conference of India.

Fertility clinic hacked and held for ransom — why your hospital could be next

Source: <https://www.marketwatch.com/story/hackers-are-stealing-more-patient-medical-records-from-hospitals-2017-05-12>

December 2017 – Imagine speeding to the hospital in an ambulance, only to be redirected to a different location due to a hostage situation there — not involving people, but the hospital’s computer system. Or what if you get a letter saying you’ve had a major operation that you have absolutely no memory of?

Chances are you (or your hospital) have been the victim of a cyberattack.

One such attack occurred at a Minnesota fertility clinic, which reported data of patients is being held hostage by cyber attackers. The Colorado Center for Reproductive Medicine network (CCRM), which runs the clinic, reportedly notified patients of the hack in October. Nearly 3,300 patients of the clinic have been

HOSPITAL THREATS

“potentially affected,” a spokeswoman told the Associated Press. CCRM did not respond immediately to a request for comment.

Similar attacks hit several hospitals in the U.S. in the past year, including the Hollywood Presbyterian Medical Center in February 2016. It reportedly paid hackers a ransom of \$17,000 in bitcoin for the release of its electronic medical records and system. These hacks represent a problem in the health care industry that [has increased](#) fourfold over the past year and is only expected to get worse.

In 2016, 328 U.S. health-care firms reported data breaches, up from 268 in 2016, [according to the 2017 Healthcare Breach Report](#) released by data protection company Bitglass this week. Customers of Kroll’s Cybersecurity & Investigations have even found hackers using stolen information to get medical procedures, said Brian Lapidus, leader of identity theft and breach notification practice at Kroll’s Cybersecurity & Investigations.

An 85-year-old woman received an explanation of benefits that she had gotten a nose job. It turned out someone else had claimed the procedure on her insurance using stolen information.

One 85-year-old woman alerted them that she had received an explanation of benefits document in the mail stating she had gotten a nose job. It turned out someone else had claimed the procedure on her insurance using stolen information.

“This is an outcome where it starts getting dangerous,” Lapidus said. “Someone could have a more extreme procedure, like having their kidney taken out, for example, and now that is on your medical record and affecting your care.”

Other risks include being blackmailed due to sensitive diagnosis information included in health records or having prescriptions falsified. In 2015, Congress established the Health Care Industry Cybersecurity (HCIC) Task Force to address the growing risk of cybersecurity incidents in the industry and help their responses to them.

The latest health-care ransomware attack, which happened last April, targeted technology company Greenway Health and [affected 400 of its clients](#). A statement on the [company’s website](#) two weeks after the incident said an attempt to restore functionality to affected customers is “nearing completion.” (A company spokesman/spokeswoman said it wasn’t commenting on the incident). In 2016, [three other hospitals](#) were hit with ransomware in Kentucky, Arizona, and California.

So what can be done? In the report released this week, the task force called on federal regulatory agencies to standardize the “complicated patchwork of laws” affecting the health care industry’s cybersecurity. Still, it recognizes the need to continue to add features like electronic medical records and update the health care system in the U.S., as it “cannot deliver effective and safe care without deeper digital connectivity,” the report said.

“If the health care system is connected, but insecure, this connectivity could betray patient safety, subjecting them to unnecessary risk and forcing them to pay unaffordable personal costs,” the report said. “Our nation must find a way to prevent our patients from being forced to choose between connectivity and security.”

Health care breaches continue to happen, Lapidus said. “They’re going to continue to happen because there is a treasure trove of information at those institutions,” he said. “You can use personal health care information to open new credit cards, get payday loans, file fraudulent tax refunds and get prescriptions.” That’s because health institutions have what he calls the “holy trinity” of personal information: name, social security number, and date of birth. They also have more personal details that make such hacks even more risky than a typical retail breach, including prescription information and diagnoses.

Meanwhile, consumers need more literacy around health-related hacks, Lapidus said. Some people know the Internal Revenue Service [won’t email or call them](#) about taxes due to increased knowledge around such scams in recent years, but many don’t understand whether a doctor might call asking for a social security number or credit card information. Patients who receive such calls should hang up and call the doctor back at the main office number to ensure they are not being scammed.

Hospitals around the world also must prepare themselves for increasing attacks on a case-by-case level, Lapidus said, by educating their staff about the risks of phishing emails—where hackers pretend to be a legitimate service to get someone to open a link. They should also have a cohesive plan in place to respond when attacks do happen. “The job of a hospital is to service its patients and when they lose access to patients [via their medical records] that ability is precluded,” he said.

HOSPITAL THREATS

Airstrikes on hospitals in Yemen

Source: https://en.wikipedia.org/wiki/Airstrikes_on_hospitals_in_Yemen



A Saudi Arabian-led [military intervention in Yemen](#) began in 2015, in an attempt to influence the outcome of the [Yemeni Civil War](#). Saudi Arabia, spearheading a coalition of nine Arab states, began carrying out airstrikes^[1] in neighboring Yemen and imposing an aerial and naval [blockade](#) on 26 March 2015, heralding



a military intervention code-named Operation Decisive Storm^[2], [translit.](#) *Amaliyyat `Āṣifat al-Ḥazm*). More than 70 health facilities in Yemen have been destroyed by a series of airstrikes conducted by the Saudi Arabian-led [coalition](#) since March 2015. Many of these have been public health hospitals staffed or supported by [Doctors Without Borders](#) (MSF).^[3] Critics of the assaults say the airstrikes are war crimes in violation of the protections of health care facilities afforded by the [internationally recognized rules of war](#) and have called for independent investigations.^[4] Many other civilians targets, including schools^[5] in Yemen are also bombed by the Saudi-led coalition.^{[6][7][8][9][10]}

The UN accused the Saudi-led coalition of "complete disregard for human life".^[11]

Timeline

- ◆ [1.1 October 2015 - Saada airstrike](#)

HOSPITAL THREATS

- ◆ [1.2 December 2015 - Taiz airstrike](#)
- ◆ [1.3 January 2016 - Razeh district airstrike](#)
- ◆ [1.4 August 2016 - Abs district airstrike](#)
- ◆ [1.5 June 2018 - Airstrike on cholera treatment center in Abs](#)

Dramatic rise in attacks on UK hospital staff

Source: <https://www.hsj.co.uk/workforce/exclusive-dramatic-rise-in-attacks-on-hospital-staff-/7022150.article>

April 2018 – Physical attacks on NHS staff working in acute hospitals rose steeply last year, according to exclusive research by *HSJ* and Unison.

Attacks against hospital staff rose by 6 per cent between 2015-16 and 2016-17

The year 2016-17 was the first when information on staff attacks was not collected nationally, following the abolition of NHS Protect.

HSJ submitted freedom of information requests to all NHS trusts and received responses from just over 75 per cent. The research revealed sharp increases in attacks on staff working for acute trusts, but also a levelling off in assaults within mental health settings.

The work is part an *HSJ* [special report](#) sponsored by Unison, which explores the reasons behind the rise in violence and the variation across NHS trusts.

The responding trusts' data showed 56,435 reported physical assaults on NHS staff in 2016-17. Extrapolating numbers from this sample to cover the whole NHS in England, this suggests there were an average of just over 200 reported physical assaults on NHS staff every day.

When measured per 1,000 staff (to account for

growth in the NHS workforce), reported attacks rose by 6 per cent between 2015-16 and 2016-17. The absolute increase between the two years was 9.7 per cent.

Commenting on the findings, Sara Gorton, head of health for Unison, said: "This report reinforces what we suspected. The number of violent assaults is rising. Yet worryingly the collection of data about assaults, and the criminal or civil sanctions that should follow, are simply not happening in a robust or consistent manner. It's very difficult for trusts to know if they are doing well in protecting their staff when there are no figures they can compare to. Staff and patient safety needs to be paramount within the NHS. It can never be acceptable for staff to feel that regular assaults are simply 'part of the job'.

"The data worryingly shows a strong correlation between trusts that have higher deficits and those where violent assaults have increased. In workplaces that are struggling financially, there are likely to be staff shortages and longer waiting times for patients – all leading to pressures on patient services and increased stress for individuals... It's shocking that when assaults are on the increase, the government has decided to look the other way."

Across the 104 acute trusts covered by the research there were 18,720 reported physical attacks on staff during 2016-17 – 180 per organisation on average. This represents a rise of 3,251 on 2015-16, or 21 per cent.

On an "assaults per 1,000 staff" basis, the 2016-17 increase for these 104 trusts was 16.7 per cent.

In reviewing this data, two associations stand out strongly.

The first is in trusts which are performing poorly against the referral to treatment elective care target. Trusts whose year end performance was under 90 per cent saw an average 36.2 per cent increase in reported attacks. Trusts in this cohort include Lancashire Teaching Hospitals Foundation Trust and Hull and East Yorkshire Hospitals Trust.

The second association is financial balance. The 26 trusts, all but one acutes, reporting a deficit higher than £20 million for the 2016-17 financial year experienced an increase in reported attacks of 23.1 per



HOSPITAL THREATS

cent on 2015-16. Trusts in this cohort include North Bristol Trust and University Hospitals of Leicester Trust.

Contrastingly, at the 37 trusts (22 of which were acutes) reporting a £5 million plus surplus at year end assaults increased by just 1.5 per cent.

Levels of violence against staff working in mental health trusts remain much higher than elsewhere in the service. Across the 39 mental health trusts covered by the research there were 33,820 reported physical assaults in 2016-17; 867 per organisation on average.

However, mental health trusts do appear to be having some success in preventing the situation from worsening. In the 20 dedicated mental health trusts surveyed, there were 17,360 violent assaults in 2016-17: an increase of 825 (or 5 per cent) on 2015-16. In the 19 combined mental health and community trusts, there was an increase of 249 or 1.5 per cent.

However, when analysed on an "assaults per 1,000 staff" basis across these 39 trusts, the level of attacks was broadly in line with those recorded in 2015-16.

Other significant differences from the average 9.7 per cent increase in reported attacks included assaults up by:

- 25.7 per cent in specialist trusts – albeit from a very low base;
- 21.5 per cent in dedicated community trusts;
- 15 per cent in organisations employing more than 4,000 staff; and
- 14.5 per cent in ambulance trusts.

Trust responses

Karen Partington, chief executive of Lancashire Teaching Hospitals FT, said, "We have been working with staff to encourage all untoward incidents to be recorded, so better reporting is a factor in this increase. However, we are also seeing more acutely unwell and elderly patients, who may unintentionally assault staff as a result of their medication or condition.

"Staff welfare is really important to us, and in the past year we have introduced a range of measures to protect them, including increased security, conflict resolution and breakaway training, mental health and learning disability nurses on our wards, traumatic incident support service, and counselling. We also investigate every incident to ensure action can be taken to prevent recurrence. We are continuing to work with staff on our wards to see what further action we can take to safeguard them at work."

Nick Howlett, health and safety services manager at University Hospitals of Leicester, said: "It is very disappointing to see such a rise in assaults. We take all such threats against our staff very seriously and will not tolerate disruptive, insulting or violent behaviour. We have made great strides this year in our overall security management.

"We have increased our training provision as well as the number of security officers, and will shortly have our third local security expert. We also continue to work in collaboration with local organisations and Leicestershire Police on a number of initiatives and are beginning to see the benefits of this."

►► Hull's response can be found within the [full report](#).

Disaster preparedness in French paediatric hospitals 2 years after terrorist attacks of 2015

By Guillaume Mortamet, Noella Lode, Nadia Roumeliotis et al.

Source: <https://adc.bmj.com/content/early/2018/06/01/archdischild-2017-314658>

Abstract

Objective We aimed to determine paediatric hospital preparedness for a mass casualty disaster involving children in both prehospital and hospital settings. The study findings will serve to generate recommendations, guidelines and training objectives.

Design and setting The AMAVI-PED study is a cross-sectional survey. An electronic questionnaire was sent to French physicians with key roles in specialised paediatric acute care.

Results In total, 81% (26 of 32) of French University Hospitals were represented in the study. A disaster plan AMAVI with a specific paediatric emphasis was established in all the paediatric centres. In case of a mass casualty event, paediatric victims would be initially admitted to the paediatric emergency department

HOSPITAL THREATS

for most centres (n=21; 75%). Paediatric anaesthesiologists, paediatric surgeons and paediatric radiologists were in-house in 20 (71%), 5 (18%) and 12 (43%) centres, respectively. Twenty-three (82%) hospitals had a paediatric specialised mobile intensive care unit and seven (25%) of these could provide a prehospital emergency response. Didactic teaching and simulation exercises were implemented in 20 (71%) and 22 (79%) centres, respectively. Overall, physician participants rated the level of readiness of their hospital as 6 (IQR: 5–7) on a 10-point readiness scale.

Conclusion Paediatric preparedness is very heterogeneous between the centres. Based on the study findings, we suggest that a national programme must be defined and guidelines generated.

Hospitals: Soft Target for Terrorism?

By H. De Cauwer, Francis Somville, Marc Sabbe and Luc JM Mortelmans

Prehospital and disaster medicine: the official journal of the National Association of EMS Physicians and the World Association for Emergency and Disaster Medicine in association with the Acute Care Foundation 32(1):1-7 · December 2016

Source: https://www.researchgate.net/publication/311529181_Hospitals_Soft_Target_for_Terrorism

Abstract

In recent years, the world has been rocked repeatedly by terrorist attacks. Arguably, the most remarkable were: the series of four coordinated suicide plane attacks on September 11, 2001 on buildings in New York, Virginia, and Pennsylvania, USA; and the recent series of two coordinated attacks in Brussels (Belgium), on March 22, 2016, involving two bombings at the departure hall of Brussels International Airport and a bombing at Maalbeek Metro Station located near the European Commission headquarters in the center of Brussels. This statement paper deals with different aspects of hospital policy and disaster response planning that interface with terrorism. Research shows that the availability of necessary equipment and facilities (eg, personal protective clothing, decontamination rooms, antidotes, and anti-viral drugs) in hospitals clearly is insufficient. Emergency teams are insufficiently prepared: adequate and repetitive training remain necessary. Unfortunately, there are many examples of health care workers and physicians or hospitals being targeted in both political or religious conflicts and wars. Many health workers were kidnapped and/or killed by insurgents of various ideology. Attacks on hospitals also could cause long-term effects: hospital units could be unavailable for a long time and replacing staff could take several months, further compounding hospital operations. Both physical and psychological (eg, posttraumatic stress disorder [PTSD]) after-effects of a terrorist attack can be detrimental to health care services. On the other hand, physicians and other hospital employees have shown to be involved in terrorism. As data show that some offenders had a previous history with the location of the terror incident, the possibility of hospitals or other health care services being targeted by insiders is discussed. The purpose of this report was to consider how past terrorist incidents can inform current hospital preparedness and disaster response planning.



Source: https://www.hudson.org/content/researchattachments/attachment/291/dworkin_white_paper.pdf



Sick Islamic State terrorists could pose as MEDICAL WORKERS to attack HOSPITALS

Source: <https://www.express.co.uk/news/world/622187/belgium-france-brussels-paris-hospitals-manuel-valls-paris-attack-isis-jihadis>

November 2015 – Belgian authorities fear the savage terror group could be planning a Paris-style massacre in hospitals in Brussels – and government ministers have warned emergency services that terrorists could slip in undetected by impersonating them.

HOSPITAL THREATS

Reports have suggested hospital chiefs have been advised to ensure uniforms cannot be stolen and to update emergency plans and lists of doctors and senior staff.

The startling news comes after a dozen full-body protective suits were stolen from locked store in a Paris hospital – leading to speculation that a chemical or biological attack could be imminent.

Details of the theft emerged last Thursday – on the same day French prime minister Manuel Valls suggested the country could be at risk from such an attack.

He said: “There may also be a risk of chemical and bacteriological weapons” used by attackers.

Europe remains on high alert in the aftermath of the devastating attacks which killed 130 in Paris on November 13th.

French intelligence services are said to have alerted German police about a potential attack in Hannover last Tuesday – a warning which saw Germany’s footballers have a friendly match cancelled.

Spooks said terrorists could use an official vehicle packed with explosives – such as an ambulance, security car or TV van – to gain entrance to the city’s HDI Arena.

Brussels’ schools and underground network reopened today – having been on lockdown since a terror alert on Friday – and France remains in a state of emergency.

Belgian troops are patrolling the streets following a warning that ISIS terrorists were ready to launch an attack in the city.

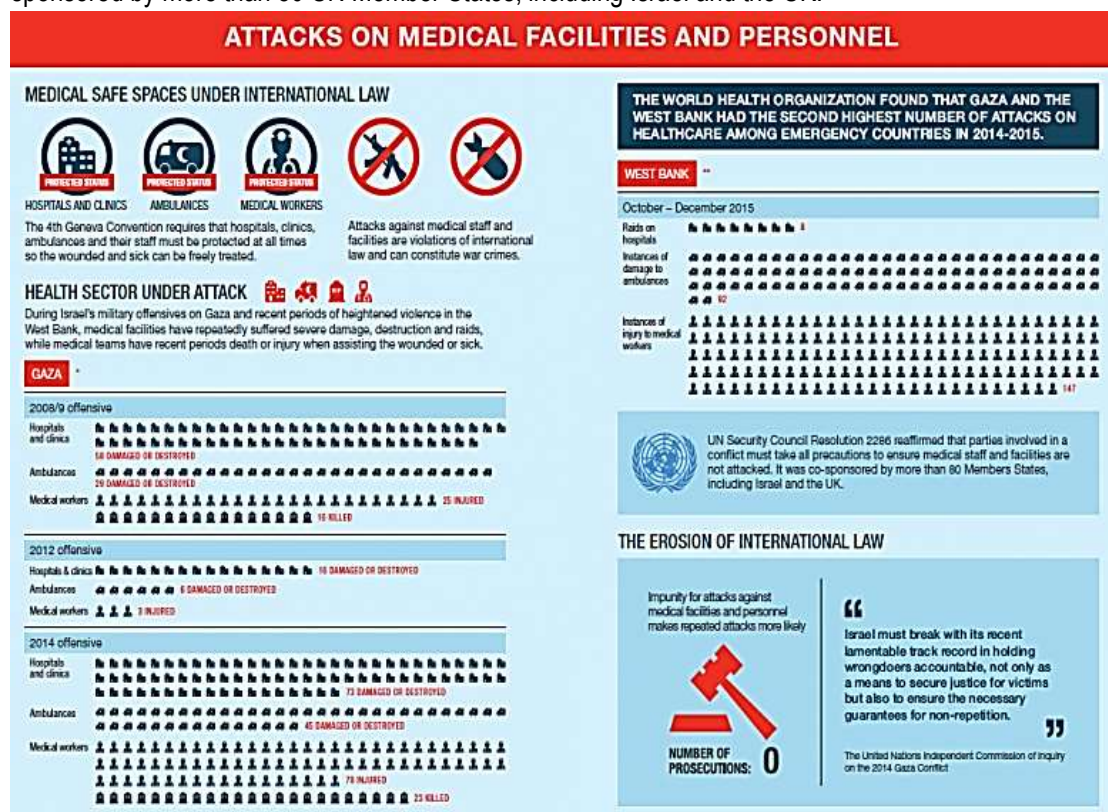
And police from both countries are tracking Paris masterminds Salah Abdeslam, 26, and Mohamed Abrini, 29.

Infographic: Attacks on medical facilities and personnel in the West Bank and Gaza

Source: <https://www.map.org.uk/news/archive/post/627-infographic-attacks-on-medical-facilities-and-personnel-in-the-west-bank-and-gaza>

October 2017 – The Fourth Geneva Convention requires that hospitals, clinics, ambulances and their staff be protected at all times during conflict so that the wounded and sick can be freely treated. Attacks against medical staff and facilities are violations of international law and can constitute war crimes.

These principles were reaffirmed last year by UN Security Council Resolution 2286, which was co-sponsored by more than 80 UN Member States, including Israel and the UK.



HOSPITAL THREATS



Nevertheless, 147 hospitals and clinics, and 80 ambulances, have been damaged or destroyed in military offensives on Gaza since 2008. 145 medical workers – most of them ambulance drivers – have also been injured or killed. The largest number of these incidents came during the 51-day attacks between July – August 2014.

Hospital Staff Fear for Their Lives Amid Sweden's 'Bloody Summer'

Source: <https://sputniknews.com/europe/201709131057346278-sweden-gang-shootings/>

September 2017 – Gone are the days when Sweden was considered one of the world's safest countries. The everyday situation in Sweden has become so dangerous that even personnel at Swedish hospitals have to fear for their lives.

Gang members barging in with guns, knife-fighting in the waiting rooms and shooting victims dumped near entrances have all become the harsh reality of the emergency department at Malmö Hospital, Swedish national broadcaster [SVT](#) reported.

"We have been attacked with knives and have seen people with guns. We put our lives at risk," an anonymous security attendant told SVT.

By the personnel's own admission, the emergency room in Malmö has become one of the city's most dangerous places, alongside the Central Station and the People's Park, with an abundance of threats and firearms and an overall atmosphere of hostility.

According to new regulations, the area must be now manned with at least two security guards. They admit that, there should be "at least four," since personnel are forced to intervene against "dangerous people" at least several times a week.

"It's only a matter of time before a shotgun pops up in the waiting room," an anonymous guard told SVT. The problem, however, is not just the violence itself, but the fact that the authorities deny the very existence of it. For instance, the section head of the Malmö police district, Per Wihlborg, said he was "totally satisfied" with security during a recent visit. According to personnel, this response was the most "laughable" thing they have heard, [SVT](#) reported.

Meanwhile, the number of [gang shootings](#) in Sweden has skyrocketed in recent months. This summer alone, which has been dubbed "bloody summer" by Swedish media, has seen 81 shootings, left 46 injured and 11 dead. The summer months account for about 40 percent of all shootings that have occurred in 2017, which the Swedish daily grimly summarized as "a shooting per day."

"Before 1990, there were about 4 gang murders a year in this country. After 1990 it hovered between 8 and 13 until 2015, and then it jumped to 30 a year," Gunnar Appelgren of the Stockholm Police told [Svenska Dagbladet](#).

The situation is worst in the metropolitan areas of Stockholm, Gothenburg and Malmö, which incidentally has been hailed as Sweden's "most multicultural city."

After having long kept the lid on the perpetrators' nationality for [ethical reasons](#), the Swedish media have earlier this year begun to digress from their former norms.

In May, a survey by the Swedish daily [Dagens Nyheter](#) indicated that immigrants account for 9 out of 10 shootings in Sweden. Out of a 100 people involved in shootings and attempted murders, 90 had at least one foreign-born parent. The vast majority of them had their roots in the Middle East and North Africa, in countries such as Iraq, Iran, Lebanon, Turkey, Somalia and Eritrea.

In late June, the tabloid daily [Expressen](#) published a survey of organized crime in Stockholm. Of 192 gang criminals, an overwhelming majority of 94.5 percent had at least one foreign-born parent. Bosnia, Lebanon, Somalia, Syria and Turkey were reported as the most recurrent countries of origin.

HOSPITAL THREATS

Earlier this year, the Swedish government counted at least 61 [no-go areas](#) with rampant crime, up from 55 last year. Swedish National Police Commissioner Dan Eliasson pleaded the government for assistance in tackling the problem, venturing that without help the country's over 5,000 hardened criminals could easily subvert society's social contract.

Earlier this week, the Swedish government said it would like the Customs Administration to perform more border checks to throttle the smuggling of arms and drugs. Next year's budget, 115 million SEK will be allocated for that purpose. In total, the agency will receive an extra 500 million SEK until 2021. At the same time, however, its staff might be reduced by 100 employees, [SVT](#) reported.



Risks to emergency medical responders at terrorist incidents: a narrative review of the medical literature

By Julian Thompson, Marius Rehn, Hans Morten Lossius, and David Lockey

Crit Care. 2014; 18: 521.

Source (full paper): <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4422304/>

Abstract

As the threat of international terrorism rises, there is an increasing requirement to provide evidence-based information and training for the emergency personnel who will respond to terrorist incidents. Current major incident training advises that emergency responders prioritize their own personal safety above that of the 'scene and survivors'. However, there is limited information available on the nature of these threats and how they may be accurately evaluated. This study reviews the published medical literature to identify the hazards experienced by emergency responders who have attended previous terrorist incidents. A PubMed literature search identified 10,894 articles on the subject of 'terrorism', and there was a dramatic increase in publications after the 9/11 attacks in 2001. There is heterogeneity in the focus and quality of this literature, and 307 articles addressing the subject of scene safety were assessed for information regarding the threats encountered at terrorist incidents. These articles demonstrate that emergency responders have been exposed to both direct terrorist threats and environmental scene hazards, including airborne particles, structural collapse, fire, and psychological stress. The emphasis of training and preparedness for terrorist incidents has been primarily on the direct threats, but the published literature suggests that the dominant causes of mortality and morbidity in responders after such incidents are the indirect environmental hazards. If the medical response to terrorist incidents is to be based on evidence rather than anecdote, analysis of the current literature should be incorporated into major incident training, and consistent collection of key data from future incidents is required.

...

Chemical hazards

Despite the Chemical Weapons Convention, which came into force in 1997 and which forbids the possession, development, and use of chemical weapons, chemical terrorism remains a threat. Countries that possessed chemical weapons undertook to destroy them, but several states, including Iran, Iraq, Libya, and Israel and its neighboring countries, did not accede to the convention [\[37\]](#). Even without state support, non-governmental groups or even individuals can successfully manufacture chemical weapons and may remain undetected by government intelligence agencies. Some chemical agents are used in a controlled environment in industry or agriculture and do not require illicit manufacture. Consequently concerns have been expressed regarding the accessibility of agents such as organophosphates and the vulnerability to attack or theft of chemical establishments [\[38,39\]](#).

In conflict and peacetime, there have been numerous chemical incidents with large numbers of casualties. There have been multiple attempts by terrorists to harness the lethal effect of such agents, but despite generating widespread fear, these attempts have met with limited success to date [\[37\]](#). Secondary contamination of medical personnel treating contaminated victims is seen to occur in accidental incidents, and one study identified 17 medical personnel injured in this way over a 3-year period in the US [\[40\]](#).

The 1994 sarin nerve agent attacks by the Aum Shinrikyo cult in Matsumoto and Tokyo, Japan, claimed the lives of 19 people and injured over 6,000 [\[41-55\]](#). Health-care workers suffered secondary contamination in both incidents; 18 were affected in Matsumoto [\[46\]](#) and 245 in Tokyo [\[44,46,48,51\]](#).

HOSPITAL THREATS

Identification of the chemical agent was delayed, and contaminated patients were treated on the scene and in the hospital by staff without appropriate PPE. Consequently, secondary contamination of medical staff occurred; in one report, 13 of 15 doctors involved in resuscitating a patient became symptomatic, 6 of whom required atropine [47]. Follow-up of victims after this sarin attack demonstrated chronic decline of psychomotor and memory function at 7 years [43] and high levels of post-traumatic stress disorder (PTSD) at 10 years [56]. The lessons learned from these incidents have informed chemical terrorism preparedness across the world [57].

Biological hazards

Biological warfare (but not research into defense or protection against biological agents) was outlawed by the Biological Weapons Convention in 1972. Biological weapons are biological toxins or infectious agents such as bacteria, viruses, fungi, or parasites intended to kill or incapacitate and have been widely used throughout history [37,58]. With the exception of some rapidly acting toxins, biological agents usually present only hours or days after exposure with non-specific 'flu-like' symptoms before organ-specific diseases become apparent [58]. The risk presented by biological agents can be classified by their individual pathogenicity, infectivity, latency, lethality, transmissibility, and virulence. The US Centers for Disease Control and Prevention categorize agents depending on the threat that they may pose to national security because of their dissemination, person-to-person transmission, high mortality rates, potential for social disruption, and need for public health preparedness. The Category A (highest priority) organisms are rarely seen in the US and include anthrax, botulism, plague, smallpox, tularemia, and viral hemorrhagic fever [59]. Category B agents are more commonly encountered and include food-and-water safety threats such as *Salmonella* species, *Escherichia coli* 0157:H7, and *Vibrio cholerae*. Ricin is the Category B agent most frequently encountered in the US, can be easily prepared from castor beans, and has been used in 'white powder' letters. Although such acts have been largely criminal in nature rather than true bioterrorism and are frequently hoaxes, such incidents pose a potential threat to emergency medical responders [60]. Successful terrorist use of biological weapons is extremely rare, and one source suggests that only two confirmed terrorist biological attacks have harmed humans [61].

Between October and December 2001, widespread fear was caused across the US by a series of letters containing anthrax spores that were sent to government buildings. Five people died from anthrax, 13 contracted disease, and many thousands were exposed and took preventative antibiotics. Health-care personnel were not specifically targeted, although other emergency services required to deal with suspicious packages were exposed to risk [62].

The difficulty in identifying biological attacks is apparent from the *Salmonella typhi* outbreak in The Dalles, Oregon, in 1984 when 751 citizens were affected [63]. Only 1 year later did it emerge that the Rajneeshee cult had intentionally contaminated water and salad bars in an attempt to influence a local election result. Similarly, when the Aum Shinrikyo cult was investigated in the wake of the 1995 Tokyo sarin subway attacks, it was discovered that they had built three laboratories to culture *Bacillus anthracis*, botulinum toxin, and *Coxiella burnetii* and carried out nine undetected biological weapon attacks between 1990 and 1993 [58,64].

Secondary biological threat has been identified as a consequence of exposure to contaminated biological material in explosive incidents. Following the London bombings of 7 July 2005, bone fragments from other victims were found embedded as biological foreign bodies within the soft tissues of five patients at one receiving hospital [65]. Similar events have occurred in suicide bombings in Israel and in conflict zones against US military personnel, and protocols have been established for post-exposure interventions to prevent infection with hepatitis B and C, HIV, or tetanus [66-68].

Radiation

Nuclear detonation by terrorists is perceived to be unlikely given the state-sponsored level of technology required to develop or deploy a device [37]. A 'dirty bomb' or radiological dispersal device (RDD) is a more likely scenario [69]. Radiation sources are routinely used in science, industry, and medicine and could be used by terrorists to create an RDD. Concerns have been compounded by the low level of security surrounding these sources, and there is documented evidence of multiple missing sources [70-72].


A very small amount of radioactive energy can cause serious biological damage. External radiation is primarily gamma radiation that has no mass, travels long distances in air, and penetrates shielding. Alpha

HOSPITAL THREATS

and beta particles represent the dominant risk if a radioactive substance has entered the body. Alpha particles consist of two neutrons and two protons, and although they can travel up to 3 cm in air, they cannot penetrate skin but are extremely dangerous if ingested or inhaled. Beta particles are electrons that can penetrate approximately 5 mm in skin and 3 cm in air [73].

In recent decades, there have been multiple radiation accidents, including incidents at nuclear power stations and the accidental misuse of scientific radiation sources [37,74]. The single non-accidental incident using radiation identified in the medical literature is an assassination that occurred in London in 2006, when Alexander Litvinenko was poisoned with polonium-210. The single victim is alleged to have unknowingly ingested an alpha source and died 22 days later suffering from multiorgan failure as a result of radiation. Despite the limited size of this polonium-210 source, the potential scale of the radiation contamination was illustrated by the 664 individuals from 52 countries who were considered at risk of exposure following this single incident [75].

Conclusions



Current major incident training emphasizes the importance of personal safety but is unable to provide an evidence-based analysis of the scene hazards encountered at terrorist incidents. There is a need to refine safety guidance for emergency medical responders in light of the experience from the thousands of international incidents that occur each year. The medical literature represents an incomplete and inconsistent record of the global burden of terrorist incidents but reports a diverse range of threats at previous incidents. Interestingly, while the **direct terrorist threats of CBRNE constitute the principal focus of major incident training and the predominant fears of responders**, the conventional scene hazards of building collapse, airborne particles, and mental health sequelae continue to cause greater harm to emergency responders. If the medical response to terrorist incidents is to be based on evidence rather than anecdote, analysis of the current literature should be incorporated into major incident training. Of critical importance is the need to improve data collection from major incidents so that the emergency response can develop an evidence-based approach to saving the lives of victims and responders in the future.

Developing operating models for severe violent attacks in emergency hospital environment

By Partanen, Henna

2017 Leppävaara, Finland

Source: https://www.theseus.fi/bitstream/handle/10024/125092/Thesis_PartanenHenna_SecurityManagement.pdf?sequence=1

This thesis and development project of facing severe acts of violence in emergency hospital environment has been made in cooperation with the Helsinki and Uusimaa Hospital District. The intention of this thesis was to develop approaches for facing severe violent attack in emergency hospital environment. Because already existing guidelines wanted to be clarified and developed, one approach was chosen for the thesis, which is suitable for most acts and by this decreases the number of guidelines and simplify actions during the attack. The subject is relatively marginally studied in Finland and most of the used guidelines and existing studies concern mental and minor physical violence facing hospital personnel, which is very widely recognized both in Finland and globally.

The theoretical background is limited to only particularly severe acts of violence, which may result in loss of life or interruption of the operation. Such acts may be, for example active shooter or bomb attacks. Practically the work was limited to consider only emergency hospitals, which constitutionally everyone has the right of access. By this was achieved diverse operating environment, which still has similar features, and selected approach is jointly suitable for all environments. The methods used were literature review and expert interviews. The literature review materials were mainly foreign research articles of severe violence in hospital environment and articles based on the chosen approach. Finnish literature studies of the general workplace violence as well as safety culture and security management literature and studies were used. Expert interviews were carried out in interface of open and theme interview, to get as much as possible authority point of view for the selected approach and development proposals for the development of hospital safety and security. The theme interview frame was formed by the chosen

HOSPITAL THREATS

approach and the end was carried out as an open interview. The study indicates that, even though physical and mental violence towards hospital personnel is generally known, the threat of severe violence is still marginally researched presumably because it has hardly taken place in Finland. However, specialists familiar with the subject are aware of the possibility and acknowledge the need to develop operational models. Clear operating procedures, which are suitable for more than one possible situation, are easy to understand for layman and minimize the possibility of incorrect operation. Safety and security management, training, as well as communication and information are methods to develop hospitals safety and security in order to maintain the target level of safety, and to improve the safety culture.

Norwegian health authority hacked, patient data of nearly 3 million citizens possibly compromised

Source: <https://www.helpnetsecurity.com/2018/01/18/norwegian-health-authority-hacked/>

January 2018 – Hackers have breached the systems of the Southern and Eastern Norway Regional Health Authority (Helse Sør-Øst RHF), and possibly made off with personal information and health records of some 2.9 million Norwegians.

What's known about the breach

The breach was [announced](#) on Monday by the authority.

The first to notice that something was amiss was HelseCERT, the Norwegian healthcare sector's national information security center, which detects unwanted events and traffic and reports them to affected actors. HelseCERT notified Hospital Partner HF, the company responsible for all ICT operations in Helse Sør-Øst RHF.

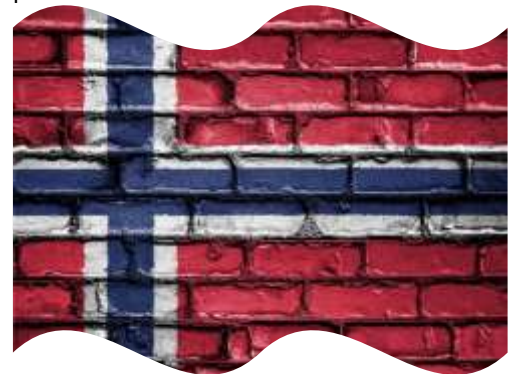
Cathrine M. Lofthus, the CEO of the Southern and Eastern Norway Regional Health Authority, said that measures have been taken to limit the damage caused by the breach, but that it hasn't affected patient treatment or patient safety.

"The event is handled according to established emergency preparedness routines and in collaboration with HelseCERT (Norwegian Helsenett SF) and NorCERT (National Security Authority) as well as other expertise. A number of measures have been implemented to remove the threat and further measures will be implemented in the future," the authority said.

Norway's police, military intelligence and its National Security Authority are investigating the breach, but it's still unknown if the attackers managed to access and exfiltrate patient data.

"Due to pending investigations, there is not much information available about the breach itself. Still, it is said to involve a serious foreign actor, with speculations pointing to a state actor," Kai Roer, CEO at Norwegian security culture company CLTRe, told Help Net Security.

Helse Sør-Øst RHF says that "the threat actor is an advanced and professional player."



Speculations

Norwegian public health care is divided into several regions, and the Southern and Eastern Norway Regional Health Authority covers the counties of Akershus, Aust-Agder, Buskerud, Hedmark, Oppland, Telemark, Vest-Agder, Vestfold, Østfold, and Oslo (the country's capital).

Health records found here will most probably include that of government and secret police employees, military and intelligence staff, politicians and other public individuals.

Nyvoll Nygaard, an adviser with the Norwegian Police Security Service, [said](#) that it's possible that someone working for a foreign state aimed to collect information that may harm fundamental national interests relating to the community infrastructure.

But, it could just as easily turn out that the attackers were merely after data they can sell on to the highest bidder.

"The healthcare sector is known to be a target for hackers, and the healthcare sector in Norway is no exception. 2,8 m patient records lost is equal to half of Norway's total population, and as such must be considered a major breach," Roer noted.

HOSPITAL THREATS

Assaults against medical staff grow in Italy's hospitals

Source: <http://www.lastampa.it/2018/07/02/esteri/assaults-against-medical-staff-grow-in-italys-hospitals-DIWGjVHTBeRV9gPD04TLrI/pagina.html>

July 02 – In Rome and Udine self-defense courses are given to doctors and nurses, while in Palermo the staff rely on the army's watch. This is because in two out of three health facilities, physical assaults occur against medical staff. There is also severe overcrowding in emergency rooms at a national level, and from Rome down the hospitals are on red alert because “the frustration of patients increases when there are more shortages of staff and beds,” explains the health union.

Five hours for one visit

In Italy, two out of three doctors are assaulted. According a poll by Anaaio Assomedi (oversees medical and health professionals) from June 2018, 65% of doctors were victims of assault — for 66.19% verbal, 33.81% physical. The violence occurs mostly in the South of Italy (72.1% in specialised departments; 80.2% in ER). And the figures are getting worse from month to month. According to a survey by SIMEU (Società Italiana di Medicina d'Emergenza-Urgenza), 63% of First Aid responders have reported at least one incident of violence in the last year. In an attempt to halt further escalation, the Italian Doctor's Union has put forward to the Senate Health Committee a petition of 35,000 signatures with a package of proposals that includes “the transformation of the public health worker” and “sanctions for the Local Health Services that do not guarantee surveillance in psychiatric services and outposts of 118”. The secretary general of the Italian Doctor's Union, Pina Onotri, describes the situation of a “multiplier effect”, that is, “cuts to the emergency room, less accessible services, increased patient dissatisfaction, police forces under the staff and more psychiatric patients without assistance”. She herself, had a flower vase flung at her by woman going through a nervous breakdown. And the more crowded the emergency room gets, the more frequent the attacks on health workers become. This includes the four- to five-hour wait for a physician in the large cities, and up to 60 hours for hospitalization. In Rome, on an average day, 40 patients out of 144 patients at the Policlinico Casilino are waiting for a bed, at Umberto I 49 out of 124, at Gemelli 49 out of 128, and at San Camillo-Forlanini, 50 out of 143.

In First Aid services, one third of a thousand patients is waiting for hospitalization, and half of the staff on duty must neglect the emergencies to assist the patients on stretchers (there's been a decrease in beds by 24% in the last decade). Again, only 80% of Italy's hospitals offer First Aid assistance — a total of 12,000 doctors and 25,000 nurses. Beyond the long wait, the alcohol abuse, drug addiction and mental disorders trigger additional violent behavior. Assaults are growing, although at a slower pace, among Sert staff, psychiatric clinics and geriatric services. Statistics reveal that 90% of nurses report being physically or verbally assaulted or having witnessed assaults on their colleagues, while 35% of health personnel suffered physical violence and 52% witnessed it. Add to that, 31% of the attackers needed medical treatment, with prognosis in 30% of cases from 5 to 15 days. In 90% of the episodes, health workers did not report the violence suffered (neither verbal or physical).

In First Aid services, one third of a thousand patients is waiting for hospitalization, and half of the staff on duty must neglect the emergencies to assist the patients on stretchers (there's been a decrease in beds by 24% in the last decade). Again, only 80% of Italy's hospitals offer First Aid assistance — a total of 12,000 doctors and 25,000 nurses. Beyond the long wait, the alcohol abuse, drug addiction and mental disorders trigger additional violent behavior. Assaults are growing, although at a slower pace, among Sert staff, psychiatric clinics and geriatric services. Statistics reveal that 90% of nurses report being physically or verbally assaulted or having witnessed assaults on their colleagues, while 35% of health personnel suffered physical violence and 52% witnessed it. Add to that, 31% of the attackers needed medical treatment, with prognosis in 30% of cases from 5 to 15 days. In 90% of the episodes, health workers did not report the violence suffered (neither verbal or physical).

An underestimated phenomenon

In the US, out of the 5 million health workers, there are 2,637 physical attacks a year, or 8.3 per 100,000 hospital workers. **In Italy, 1,200 attacks of violence were reported this year — but it represents only a fraction of the actual assaults. And it's clear why:** In Rome, four First Aid hubs are without a permanent police station (Santo Spirito, Ophthalmic, San Filippo Neri, Cto), five have public security offices with 6 hours of daily work (Sant'Eugenio, San Giovanni, Pertini, San Camillo, Sant'Andrea), two



HOSPITAL THREATS

have police surveillance from 8 am to 8 pm (Umberto I, Policlinico Tor Vergata), and only one has private supervision (Ospedale Grassi di Ostia). Those who are most likely to raise their hands or their tone of voice are: the patients waiting in line (50% of cases), relatives (21%), relatives and patient together (11%), other escorts (10%), general users of the Emergency Room (8%).

Ripple Effect: How Hurricanes and Other Disasters Affect Hospital Care

Source: <https://labblog.uofmhealth.org/industry-dx/ripple-effect-how-hurricanes-and-other-disasters-affect-hospital-care>

September 2017 – On a typical day, hospitals can be chaotic.

But when a natural disaster hits, occupancy rates — and stress levels of health care workers — can be pushed to the limit. Both represent significant barriers to optimal care.

The aftermath of hurricanes Irma and Harvey underscore the need for health care facilities to plan for the worst.

“If you’re not prepared for sudden surges in demand for acute and emergency care, then you will compromise not only the incoming disaster patients but also existing emergency department and hospitalized patients,” says [Mahshid Abir, M.D., M.Sc.](#), an assistant professor of emergency medicine at the University of Michigan and director of the Acute Care Research Unit at the U-M [Institute for Healthcare Policy and Innovation](#).

Storm-related injuries aren’t the only reason for the influx of patients presenting to emergency departments and hospitals, however.

Abir and [Sue Anne Bell, Ph.D., M.S.N., FNP-BC](#), a U-M clinical associate professor of nursing, published a study in August affirming that natural disasters can set off a chain reaction of medical issues among patients, leading to increased hospitalization rates.

The study, in [Annals of Emergency Medicine](#), compared the first 30 days of Medicare claims data from southeastern ZIP codes affected by a deadly rash of tornadoes on April 27, 2011, with claims data from the rest of the year.

After excluding the first three days after the disaster — when weather-related injuries were most likely — hospitalizations rose by 4 percent during the post-tornado period, the same increase seen during the 72 hours after the storm.

Even a single-digit percentage increase can have major implications: “It translates to hundreds of additional hospital admissions,” says Bell, whose research focuses on disaster preparedness and response.

Prior work by Abir and U-M researchers also showed [increased hospital length of stay](#) in the weeks after a mass-casualty incident.

Which is why hospitals must anticipate a range of risks surrounding storms — from medication shortages and mental health needs to nonfunctioning home medical equipment due to power outages.

Abir and Bell spoke more about their work:

How can a natural disaster affect a hospital’s ability to offer care?

Abir: Many hospitals already function at near or maximum capacity. Imagine being hit with a surge of critical patients or those with exacerbation of chronic disease. There’s only so many resources to go around.

If an area is flooded or at risk of flooding, facilities will evacuate. That happened in Texas with Harvey. In Florida, they have pre-emptively evacuated hospitals and nursing homes.

When transferring evacuated patients to alternate facilities, it is key to utilize electronic health records to make patient records available to receiving facilities where possible. You have to create the full picture of a patient’s health for the receiving facility to preserve continuity of care. Otherwise, you’re starting from scratch.

Your study found that hospitalization rates still rise even after disaster-related injuries are excluded. Why?

Abir: One of the things that happens after a disaster, particularly if it involves a rush to evacuate, is that patients leave medications behind. Maybe the pharmacies are closed. That can lead to an exacerbation

HOSPITAL THREATS

of chronic diseases such as diabetes and asthma. Others might lose power to operate home medical devices such as ventilators. Undoubtedly, that may lead to increased hospitalizations.

Bell: People often hear these dire warnings on the news, and then the storm might take a last-minute turn. That could make them reluctant to evacuate. There's always some inherent uncertainty with a disaster, but one of the best ways for an individual to protect his or her health and relieve a burnt-out health care system is to heed the warnings of authorities.

How might those seeking care after a disaster differ from other patients?

Bell: These people face enormous challenges. It's possible they've lost homes, they don't know where their loved ones are, they could have left pets behind. They're also going back to a completely uncertain future. And there's plenty of evidence to show that patients with baseline mental health issues experience the stress of a disaster even more.

Abir: There's a saying that disasters don't discriminate. It couldn't be further from the truth. Yes, disasters affect everyone, but vulnerable individuals — those with lower socioeconomic status, mental health issues, older individuals, children, pregnant women — are generally more challenged. More and more preparedness approaches are taking vulnerable populations into account.

What lessons can facilities take from your research?

Bell: Lack of access to dialysis is a big problem. After Harvey, a number of dialysis centers closed. [Dr. Abir's](#) and [other prior research](#) helped elucidate the need to have people dialyzed before the storm, bridging the gap until resources were more stable.

What role do health care coalitions play in disaster response?

Bell: A health care coalition is a group of state, local and hospital-based administrators working together to think critically about preparedness and what they can do to pool resources in a time of disaster. For example, in Michigan, we have a clear plan to share access to ventilators.

Abir: They are set up differently in states across the U.S. Ultimately, they work with various stakeholders across the health care system — including dialysis vendors and pharmacies — and other key stakeholders in the private sector, faith-based groups, to help build community resilience and share resources during emergencies.

Although the goal is to build relationships that can be leveraged during emergencies, a lot of coalitions now recognize that a situation doesn't have to be catastrophic to share information and resources to meet community needs.

How might the increased workload after a natural disaster affect health care employees?

Abir: Moving forward, we need to screen for and address the stresses these providers may experience. Some hospitals have offered mental health services for staff in the aftermath of mass-casualty incidents. I think it's a really important issue, but I don't think we're quite there yet. Health care providers are patient-first, rightly so. But in order to provide the best care, we need to take care of ourselves and each other. This is especially true in the stressful aftermath of disasters.

Bell: Being able to identify signs of mental health distress among providers is important. Those little things might include debriefing in a safe space with colleagues, taking a few minutes out to do some deep breathing and focusing on individual and immediate needs. That is often overlooked on a daily basis, but it becomes even more important when you're in a disaster situation.

The impact of floods in hospital and mitigation measures: A literature review

By N A Yusoff, H Shafii and R Omar

IOP Conference Series: Materials Science and Engineering, Volume 271, conference 1

Source: <http://iopscience.iop.org/article/10.1088/1757-899X/271/1/012026/pdf>

Abstract

In late December 2014, the flood was most significant and largest recorded specifically in the Kelantan, Malaysia. It was considered to be a "tsunami like disaster" in which 202,000 victims were displaced and causing widespread collapse of public infrastructure. Flooding of hospital results in interruption of business, loss of infrastructure, such as electrical power and water supplies, increased difficulty in providing routine medical and increased patient admissions and nursing care for patients with chronic diseases, such as renal failure, diabetes, cancer, cystic fibrosis and mental illness. The aimed of this

HOSPITAL THREATS

paper to identify the best of measures for reduce the risk of flood in hospital. Method of this paper uses the previous study result. Several related previous study can be used as measures to mitigation flood risk in Malaysian hospitals. Early stage research of related studies hope to help add more information to assist researchers in reducing the risk of flooding in hospital. The findings with proper pre-event preparation framework for mitigation flood risk of hospitals, the continuing medical services can be provided to patient especially during emergency.

The importance of disaster management and impact of natural disasters on hospitals

Conference Paper: The 6th World Construction Symposium 2017, At Sri Lanka.

By Payam Salamati and Udayangani Kulatunga

Source: https://www.researchgate.net/publication/318128263_THE_IMPORTANCE_OF_DISASTER_MANAGEMENT_IMPACT_OF_NATURAL_DISASTERS_ON_HOSPITALS

Abstract

The purpose of this research is to study and explore the importance of hospitals in natural disaster events and identifying some impacts on the hospitals in natural disaster events. A disaster is an unforeseen event, which can overwhelm the capacity of the affected people to manage its impact. Many people are periodically exposed to natural disasters in their life, and most disasters, or more correctly hazards that lead to disasters, cannot be prevented. However, their effects can be mitigated. Disaster management efforts aim to reduce or avoid the potential losses from hazards, assure prompt and appropriate assistance to the victims of a disaster, and achieve a rapid and effective recovery. It is crucial that hospitals remain safe and functional during and after disasters. Health facilities at all levels deserve special attention in the case of natural disasters as they must continue the work of current patient treatment within their facilities and provide care for persons injured by the disaster event. Disaster management becomes even more important for hospitals as the health sector has been particularly vulnerable to the damage caused. For this study, secondary information was retrieved from the Internet on sudden-onset natural disasters in different parts of the world. This study found some barriers and deliverables for disaster managers that can mitigate the risk of a natural disaster's impact on a hospital. Accordingly, this paper evaluates the importance of disaster management for hospitals and the challenges that need to be considered during the disaster response.



Source: <http://usir.salford.ac.uk/43939/1/SSE070213f.pdf>

ENISA – Smart Hospitals

Source: <https://www.enisa.europa.eu/publications/cyber-security-and...hospitals/.../fullReport>

In recent years, many pervasive systems for healthcare have been proposed, discussed and sometimes realised. Pervasive healthcare is highly multifaceted, with many applications focusing on interoperability with the legacy hospital assets, the “traditional hospital”, the security and privacy of sensitive information and the usability of end users. The notion of smart hospitals is introduced when Internet of Things (IoT)

HOSPITAL THREATS

components are supporting core functions of a hospital. Collaboration among various stakeholders, numerous interconnected assets and high flexibility requirements do not only lead to complexity and dynamics but also to blurred organisational boundaries. Due to the great number of significant assets at stake (patient life, sensitive personal information and financial resources) information security is a key issue for smart hospitals.

Threats to smart hospitals are, however, not limited to malicious actions in terms of their root cause.



Human errors and system failures as well as third-party failures also play an important role. The risks that result from these threats and corresponding vulnerabilities are typically mitigated by a combination of organisational and technical security measures taken by smart hospitals which comprise good practices. With respect to organisational measures, compliance with standards, staff training and awareness raising, a sound security organisation, and the use of guidelines and good practices are particularly relevant. Relevant technical measures include network segmentation, asset and configuration management, and network monitoring and intrusion detection. However, manufacturers of information systems and devices used in smart hospitals have to take certain measures too.

Among them are, for instance, building security into products from the outset, adopting secure coding practices and extensive testing.

Based on the analysis of documents and empirical data, and the detailed examination of attack scenarios found to be particularly relevant for smart hospitals, the study proposes key recommendations primarily for hospital executives. Namely hospitals should:

- Establish effective enterprise governance for cyber security
- Implement state-of-the-art security measures
- Provide specific IT security requirements for IoT components in the hospital
- Invest in NIS products
- Establish an information security sharing mechanism
- Conduct risk assessment and vulnerability assessment
- Perform penetration testing and auditing
- Support multi-stakeholder communication platforms (ISACs)

The study also makes recommendations for industry representatives in order to enhance the level of information security in smart hospitals. Namely industry players should:

- ◆ Incorporate security into existing quality assurance systems
- ◆ Involve third parties (healthcare organisations) in testing activities
- ◆ Consider applying medical device regulation to critical infrastructure components
- ◆ Support the adaptation of information security standards to healthcare



Threats to urban public hospitals and how to respond to them

By Alan Sager, Ph.D.

Professor of Health Services and Co-Director, Health Reform Program, Health Services Department, Boston University School of Public Health

Source: <https://www.bu.edu/sph/files/2015/05/Threats-to-Urban-Public-Hospitals-DC-General-Medical-Staff-30-Mar-011.pdf>

Since the 1930s, decade after decade, urban hospitals that serve lower-income patients and minority patients (African-Americans or Hispanic-Americans) have been substantially more likely to close, even after controlling for number of beds, whether the hospital is a teaching hospital, efficiency of the hospital, and other factors.

I've examined all hospitals (some 1,200) open at any time since 1936 in 52 U.S. cities—all of the large cities and most of the mid-sized ones. Fully 54 percent of hospitals have remained open in census tracts with 1990 minority population shares under 20 percent, but only 33 percent of hospitals have remained open in hospitals with minority shares over 80 percent.

HOSPITAL THREATS

If we map hospitals and their closings in several cities, we can see how this works out for people. These maps of St. Louis, Washington, Detroit, and Brooklyn succinctly summarize hospital survival over time in relation to demography.

When we look at public hospitals alone, in these 52 cities, we find that there were 73 public hospitals with 48,000 beds in 1936 and 53 public hospitals with only 24,000 beds in 1996. Public hospital beds dropped from almost one-third of the total beds in those cities in 1936 to about one-seventh of the beds in 1996. (Please refer to chart at end of document.)

►► Read the full paper at source's URL.

Top 10 IT Threats to Healthcare Security

Source: <https://www.arrowsolutionsgroup.com/blog/top-10-threats-healthcare-security>

2017 was the year when relentless cyber-attacks happened in the healthcare industry. Who will ever forget the catastrophic WannaCry malware that caused problems to different hospitals all over the United Kingdom? The thing is that this incident is not isolated and that the healthcare industry is known to have the worst cybercrime incidence of all sectors. In fact, the cost of a breach in the healthcare security is \$380 per capita. Below are the top 10 security threats that the healthcare industry should watch.

Ransomware and Other Malware

Malware poses a severe problem in the healthcare industry. It is essential to take note that the healthcare industry works in an intricate and interconnected network of information. Malware and ransomware can cause the inaccessibility to information within the industry. The WannaCry attack, for example, forced hospitals to shut down because they could not access the records of their patients.

Phishing

Phishing emails pose threats to the personal data and information stored in a particular healthcare setting. They start out as innocent emails that are embedded with malware. Once you open it, it releases the malware that can phish for data such as login credentials to access vital patient information.

Insider Threats

Insider threats can be carried out by patients as well as staff and can either be accidental or intended. According to the 2017 HIMSS survey, experts found out that insider threats pose as much as 75% of the cyber threats in the healthcare industry.

Increased Use of Cloud Computing

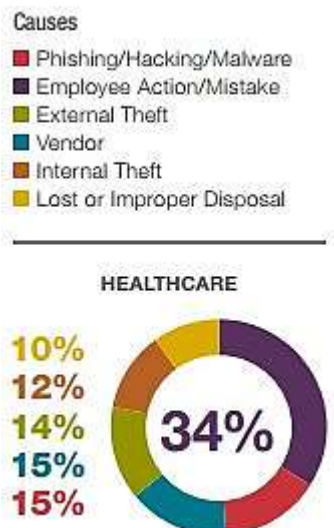
Online security in cloud computing is often compromised. And while the use of cloud computing in the healthcare industry is projected to rise to 20.5% by 2020, little is done when it comes to online security. Protecting the data during transit across different web services does require not only robust encryption methods but also efficient authentication.

Internet of Things Attacks

Recently, the healthcare industry has embraced the [Internet of Things](#) to improve the patient experience. While it is done to improve the patient outcomes, IoT poses threats as the data stored can be stolen by hackers. Hackers can make the data can be inaccessible or skewed, and this can disrupt the treatment of patients.

Weak I.T. Healthcare Security Providers

The TRICARE breach is a perfect example that the supply chain in the healthcare industry is weak and, at the most, negligent. This led to the exposure of 4.6 million patient records. The problem is that a variety of suppliers within the healthcare industry provide poor service regarding cybersecurity. Hopefully, with more focused I.T. healthcare professionals, this can change.



HOSPITAL THREATS

Authentication Issues

Many massive breaches within the healthcare industry are caused by authentication issues. Using weak passwords can be dangerous. This is the reason why two-factor, as well as risk-based authentication, are popular as they offer a higher degree of mitigation against phishing and security attacks.

Legacy Apps Still Being Used

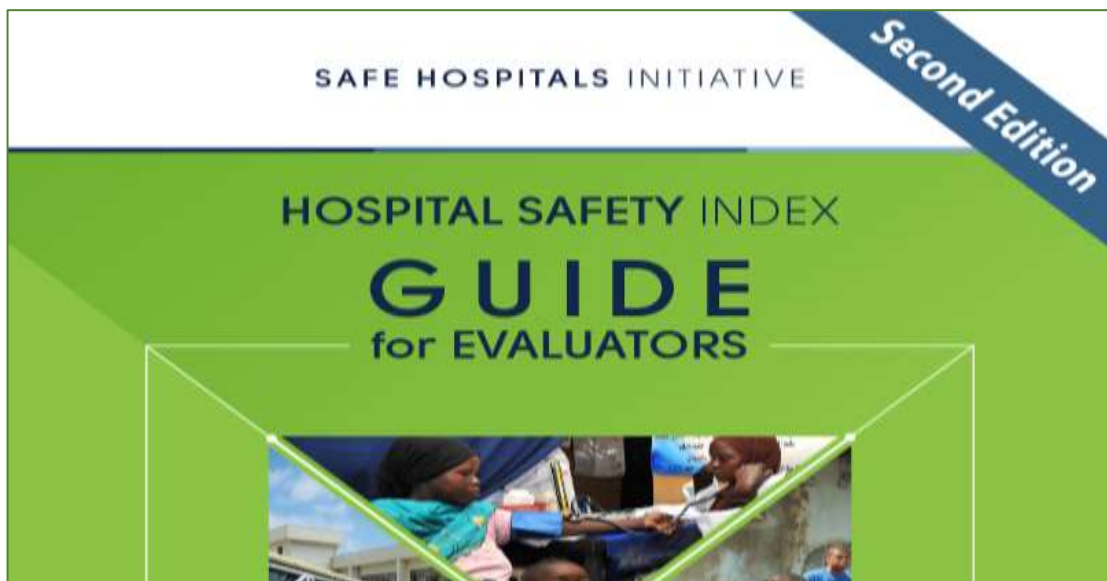
Many hospitals are still using legacy apps or old apps to preserve the data of their patients. However, using legacy applications give cybercriminals a significant opportunity to take advantage of the vulnerability of old operating systems and structures.

Poor Funding Affecting Security

Many hospitals are up against poor funding regarding cybersecurity. The thing is that robust security programs cost money for both training and implementation. Unfortunately, not too many hospitals are keen on spending money on high-end security infrastructure. But the constant cyber-attacks within the healthcare industry should change their minds.

Poor Security Awareness Program

Security is a problem for everyone within the organization. While most hospitals are using technology to integrate information, employees are not fostering a culture of security. They still use weak passwords and seem not to be careful in opening emails. This is a big problem, and a habitual problem is often hard to correct. Hospitals and medical practices must find ways to build more awareness about security and its importance in the workplace.



Source: http://www.who.int/hac/techguidance/hospital_safety_index_evaluators.pdf

Smart Hospitals – Part 1: Designing the future

By Dimitrios Gontzes

Source: https://www.optimityadvisors.com/Smart_Hospitals_Part1

The term “smart hospital” might sound like another *buzzword* that businesses use, but the idea behind it is solid and, given the digital technology advances, very tangible. The introduction of Internet of Things, the development of sophisticated software and the need for more personalised care are pushing “traditional” hospitals to transform in terms of interoperability and legacy systems. The Smart mantra can be summarised in a simple question: “How do we leverage real time information to achieve clinical excellence and enhanced patient experience?” That’s essentially what Smart Hospitals are trying to answer.

HOSPITAL THREATS

In this two part blog I will first lay out what a Smart Hospital is and define the assets that form the starting point for implementation. The second part will focus on the benefits to the healthcare system, the inherent security and data protection dangers and the ways to protect organisations from them. First things first. According to the European Union Agency for Network and Information Security (ENISA),



a smart hospital is a hospital that relies on optimised and automated processes built on an ICT environment of interconnected assets, particularly based on Internet of things (IoT), to improve existing patient care procedures and introduce new capabilities. The overarching objectives of a smart hospital are to provide enhanced patient care including remote medical care, enable efficient patient and medical information flow and boost diagnostic, surgical and organisation intelligence capabilities while ensuring patient safety and cyber resilience.

The key to unlocking the Smart capabilities lies in the assets of a hospital. It may be too obvious, but **networking equipment** such as Wi-Fi and routing protocols are essential components that ensure connectivity throughout the hospital premises. **Networked clinical information systems and medical devices** are the heart of a smart hospital and the first step to implementation. Clinical information systems should be able to connect with each other as well as with medical devices to seamlessly exchange information. Wearable medical technologies and mobile devices can provide real time precise health data and enable further remote health care and connection with healthcare professionals. The ability to track and authenticate patients, staff and devices is also of paramount importance in a smart hospital. **Identification systems** may include tags, Radio Frequency Identification (RFID), CCTV cameras, biometric scanners and others. The foundation of a smart hospital relies on the effective co-operation of this triumvirate.

But we should not stop here. These assets generate a lot of data – data that can inform healthcare professionals about the status of a patient and, when analysed from an operational perspective, can provide valuable insights into the organisation's performance and patients' experience. Therefore, smart hospitals must have ways to **analyse, protect and store** this data and translate them into valuable information (see [blog](#)). Finally, **mobile client devices** (e.g. emergency apps) and **remote care systems** (tele-monitoring, medical equipment for drug distribution) can enhance the reach of care make the right information available to staff and patients.

So, here you have it, the Smart Hospital broken down into assets. But what is the value of this transformation to the organisation and to patients? And equally importantly, what are the risks and protective measures of a smart ecosystem? Join me at my next blog and you will find out.

Smart Hospitals – Part 2: Managing the Inherent Cyber Security Risk

By Dimitrios Gontzes

Source: https://www.optimityadvisors.com/Smart_Hospitals_Part2

Becoming a Smart Hospital is not a utopic state. In my previous [blog](#), I described what a Smart Hospital is and how tangible its defining assets are. In fact, hospitals are inevitably moving in this direction – they adopt new technologies and systems to enable them to respond to the increasing customer demands, achieve greater efficiencies and better react to regulatory standards and disruptive risks. Hospitals are also expected to experience great benefits from using an interconnected network of systems and devices – increased healthcare reach (through tele-health, tele-monitoring), cost and time savings, and enhanced

HOSPITAL THREATS

quality of care. Furthermore, Smart Hospitals are likely to bring improvements in the areas of patient safety, medical and surgical abilities, and customer experience.

Smart Hospitals, however, seem to carry an inherent danger – the cyber security risk.

Cyber security has always been a hot topic for healthcare organisations. The data they handle is considered very [sensitive](#) and the use of devices or other technologies can have a direct impact on the health of individuals. This issue becomes even more important with the introduction of networked systems and the Internet of Things (IoT). Why? Because a system is as resilient as its weakest component. And



in this world of increasing interconnectedness and numbers of IoT devices, the number of attack vectors will increase and so will vulnerabilities. In addition, as is often the case with healthcare organisations, new technologies connect with legacy systems that may remain inadequately protected. The unprecedented speed of technological innovation may also result in out-dated malware detection mechanisms, unrealistic organisation policies and lack of standard device configurations which can further weaken an organisation's defences.

So, what are the types of cyber threats a modern hospital faces and what are the consequences?

According to a survey conducted by [ENISA](#), the most critical threat to the organisation's operation, staff and patients is the threat of malicious attacks. A malicious attack is a deliberate action by individuals or organisations and may include malware such as viruses and ransomware, network or device hijacking, theft of data or physical devices, medical device tampering, Denial of Service attacks (DoS) and others. Most of the time, there is a financial motive for these attacks. Hackers can take control of systems and devices, steal patient data or equipment and sell them to the highest bidder or even hold operational data hostage, demanding a ransom for their release.

The most likely threats however seem to stem from human errors. Exceptionally disruptive in a smart hospital setting are the medical system configuration errors, the patient or physician errors and the unauthorised access controls. Take the infusion pump case for example. Generally, hospitals make sure that such devices are configured in a way to prevent over-infusion of drugs but create back doors for specialised staff in case of an emergency. If the device is not configured with such access controls, patients and individuals can tamper with the device and the drug delivery protocol, which might have deadly consequences. Other threats that prove troublesome to a hospital's operations are system failures such as software and device failure and supply chain failure particularly with third party service providers and suppliers. Such errors and failures can be critical as they pose an immediate danger to the patient's health. In addition, they may also affect the hospital's everyday operations and therefore its profitability and reputation.

When it comes to managing security risk and breaches, there are a few tried and tested practices. First stop, a cyber security risk assessment. What are your weakest points, what are the threats of these vulnerabilities and what is the likelihood of a breach and its potential impact? Moving to protection measures, technological solutions such as anti-malware software, regular backups, firewalls and data encryption techniques are the most commonly used. Particularly effective is the architecture measure of dynamic network segmentation where system components that are more susceptible to cyber-attacks are separated from critical components of the network. Management of assets and standard configuration protocols can minimise human errors and make the detection of malicious activity more effective. An organisation should certainly not rely solely on its technological measures. Internal security policies, distinct roles and access controls, frequent penetration testing and security audits as well as comprehensive awareness and training courses can strengthen a hospital's resilience and minimise these cyber risks.

HOSPITAL THREATS

The future of healthcare is undeniably here. It is digital, networked, personal and collaborative. There are great benefits in embracing the technological revolution but one must be protected against its dangerous artefacts.

Dimitrios Gontzes is a Data Science Consultant and Machine Learning & Data Engineer.

Insider Threats at Hospitals

INFOSEC Institute

Source: <https://resources.infosecinstitute.com/insider-threats-at-hospitals/#gref>

Insider threat is an umbrella term for a number of different malicious acts carried out against an organization by someone inside that organization. It covers a gamut of actions, from angry employees deleting sensitive records to state sponsored espionage carried out via someone close to the organization, and everything in between. According to PWC in their "[Global State of Information Security 2016 Report](#)," 63% of security incidents can be attributed to current or former employees.

The types of insider threats can be broken down into several categories:

1. Intentional, e.g. sabotage, data theft
2. Unintentional, e.g. loss of data via lost devices, accidental disclosure of data, improper disposal of records

The reasons for insider attacks include:

- Revenge – disgruntled employee, dissatisfied with job or manager
- Competition – to use intellectual property to start their own business
- Financial – to sell data online or to a third party who may use the data in a number of ways, such as reselling through the black market

Insider threats are much more heavily cloaked than external threats by the organization suffering them. This could be due to the very sensitive nature of an internally initiated breach. Because of this, companies avoid the use of the law, preferring to deal with the issue, quietly. PWC in their report on [managing cyber risks](#), stated that:

"75% of respondents to the US cybercrime survey said they did not involve law enforcement or bring legal charges in compromises committed by insiders."

The same report found that insider cyber crimes were more costly than external cyber crimes. This may be due to insider threats taking longer to detect, after all, the actions are carried out by people allowed to perform those tasks. In a report by NATO [Cooperative Cyber Defense Center of Excellence](#) (CCDCOE), they found that the different types of insider threat actions had timelines associated with their execution. Sabotage, which was often enacted out of revenge, was a fast action, usually occurring on average 30 days after a contract was terminated. Theft of data and intellectual property was a longer term action, taking around 60 days to commit. Fraud, where data such as Personally Identifiable Information (PII) is modified or sold, is an ongoing concern. Exfiltration of information can occur over several months or even years before detection.

On a global level it is the USA that feels most under threat from insiders, with [92% of U.S. organizations](#) feeling vulnerable to this type of security issue.

How big is the problem of Insider threats in the healthcare industry as a whole and in hospitals?

The 2016 Verizon "[Data Breach Investigations Report](#)" (DBIR) points out that the healthcare industry is one of the top three sectors to suffer at the hands of an insider. We can look at the scale of the issue using the '[wall of shame](#)' hosted by the Department of Health and Social Services. This is a requirement of the Health Insurance Portability and Accountability Act (HIPAA) which mandates that a breach affecting over 500 individuals must be submitted to the authorities and be publically accessible. To view the extent of insider threats within health care providers (which included hospitals and associated health centers) the 'wall of shame' was filtered for the following variables:

1. The first 6 months of 2016
2. Healthcare providers only (which includes hospitals as well as medical care centers and doctors)
3. Theft or unauthorized disclosure of data
4. Electronic medical records (EMR)

HOSPITAL THREATS

The result was 8 breaches with a total of 81,432 EMRs. If I add to the filters all types of data, which includes sensitive information not in EMR format, then this figure jumps massively to 64 healthcare providers being breached and the data of almost 1 million individuals being compromised. Some examples of the bigger breaches include Public Health Trust of Miami-Dade County, Florida with over 24,000 EMRs lost and Eye Institute of Corpus Christi with almost 44,000 lost EMRs.

The whys and wherefores of health-related insider threats

Some further interesting facts that have come out of the 2016 DBIR include that internal threats are often initiated by outsiders. It outlines a picture of a typical insider threat: a disgruntled employee, usually with privileged access credentials, but less likely to be someone in a management role. The reasons behind the attacks are most likely financial or espionage. When you consider that the [average healthcare salary](#) of a nursing aide is around the \$28K range, and for computer operators around the \$40K mark, if you have the mindset of a disgruntled or angry employee, you may well be easy prey for an external malicious source to take advantage of. But in a recent worrying twist to insider threats, [Gartner](#) has identified that the ease of use of the dark web is allowing it to be used as a direct medium for a disgruntled employee to upload and sell PII directly.

But why is the healthcare industry and hospitals such a prized target for insider breaches?

To answer this we need to look at some facts about data and our healthcare providers. Firstly Personal Health Information (PHI) is valuable. Where credit card details may fetch as little as [\\$5 on the dark web](#), a PHI record will fetch closer to \$363 according to the [Ponemon Institute and IBM](#). This is because data records within the health system contain personal data, such as social security numbers, that can be used for further cybercrime – it's like the gift that keeps on giving. Cybercriminals can take the rich data from an Electronic Medical Record (EMR) and use it for a number of further criminal activities, for example, to buy drugs and medical equipment. The IRS breach of 2015 was successful because health records gave enough information to allow fraudulent tax claims to be made in real people's names. Secondly, the theft of health data, especially that stolen by insiders which is difficult to detect, means that the data has a longer life span. Unlike stolen credit cards, which can be swiftly cancelled, PHI has a long lifetime, and great re-use possibilities.

Some examples of hospital based insider threats

Hospitals are a busy, multi-dimensional community. The vast majority of people who choose to go into healthcare as a career do so because they are genuine and caring human beings. However, like any organization, hospitals have a variety of people to manage, which can include less than scrupulous ones. Some insider threats, like the first in our list here, are on the edge of what is malicious and what is just plain lack of privacy awareness. Others are organized attempts to extract as much personal data as possible, over long periods of time, and sell it on for profit.

Example 1: The first example is [Children's Healthcare of Atlanta, Inc. v. McCray](#). Sharon McCray was a senior audit advisor for [Children's Healthcare of Atlanta](#). McCray started to send healthcare records of patients from her corporate email to her home email on the day that she resigned. When caught, she told the hospital that she had emailed the data for "future employment reference."

Example 2: Another long term breach was found at the Florida hospital, who sent out a [notice to affected patients](#). They found that two hospital employees had printed out data sheets that contained patient personal data, including social security numbers, phone numbers, names and addresses. The breach had occurred over a two year period. The hospital believes that the PHI was being used to make fraudulent benefit claims from health insurers.

Example 3: Other insider breaches come under the banner of disgruntled employee. For example, an employee of Woodwinds hospital in Minnesota was sacked and, as retribution, took 200 pages of confidential information home. The now ex-employee said she was using the information to blow the whistle on the hospital who she believed had carried out a number of medical misconducts.

Example 4: The wider hospital network, including smaller facilities which offer assisted care, are not immune to insider breaches. Earlier this year, a worker at a facility for the elderly, [Holland Manor Eldercare in Maryland](#), used his privileged access on the network to steal patient data. He then used these data to fraudulently obtain credit cards. Again this was carried out over a 2 year period before being detected.

HOSPITAL THREATS

What mitigation strategies exist to control insider threats

Insider threats are extremely difficult to detect because of the nature of the problem – a breakdown in trust by otherwise trusted individuals. Unfortunately, the facts, such as those identified by the DBIR, mean we cannot just give blind trust to employees and the extended supply ecosystem. Because internal breaches are often carried out using normal modes of operation, we can't use traditional tools, like firewalls or antivirus software, to stop them. Instead we have to think like an insider and build a security strategy that can handle internal as well as external cyber security issues.

The Intelligence and National Security Alliance (INSA), in partnership with the Office of Homeland Security, the FBI and the Office of the Director of National Intelligence, have created an [Insider Threat Resource Directory](#). They have used over 200 insider threat profiles to create a framework which contains 13 guidelines for developing a strategy around insider threats. A key theme running through the guidelines is top down driven awareness. Security awareness and training which has leadership buy-in has greater success across the organization. Being driven at the executive level gives the program kudos and weight. Having security awareness programs that build upon the idea of trust, built into the very ethos of a hospital, may not prevent the small minority of rogue employees attempting to carry out a malicious act, but they will give the rest of the team the knowledge to spot and prevent the act occurring.

Self-policing of staff is an essential part of the overall insider threat strategy, but it is not the whole story. Technology can also play a part in thwarting insider data exfiltration attempts. Monitoring, combined with modern analytics, is an important tool in the security strategy kit. Using intelligence, such as the information gleaned from reports like DBIR, can help to focus energies on key areas of importance. For example, it was found that a likely time for an insider threat to take place was in the month after an employee has resigned, so this would be a good place to focus monitoring and analytics. Or as the DBIR has stated, it is those with access to sensitive data such as EMRs or other PII that are more likely to cause a breach, so focusing attention in those areas would be wise. The DBIR recommends that you:

“...monitor the heck out of their [employees] authorized daily activity, especially ones with access to monetizable data (financial account information, personally identifiable information (PII), payment cards, medical records).”

Perhaps the most difficult task in handling insider threats is striking a balance between tackling the threats and ensuring the trust of the vast majority of your workforce. If your strategy around insider threats is not carried out with the agreement and acceptance of the wider workforce, then it may backfire. This is where a well coordinated and inclusive security awareness program can really excel.



Source: https://www.ache.org/pdf/secure/gifts/Harrison_Chapter5.pdf

EU THREATS Project

Source: <http://www.threatsproject.eu/>

The THREATS project aims to increase the resilience of EU hospitals as critical infrastructure by improving their protection capability and security awareness against terrorist attacks. Its aims are:

- To develop a reliable method for assessing the risks and vulnerabilities of major EU health infrastructures to terrorist attacks;
- To prepare specific security and threat assessment models and tools applicable to the Health sector using other EU projects;
- To challenge these tools through application to the San Raffaele Hospital in Milan;



HOSPITAL THREATS

- To disseminate guidelines designed to optimize the preparedness of hospitals' healthcare infrastructures against terrorist attacks.

Cybersecurity in healthcare: A narrative review of trends, threats and ways forward

By Lynne Coventry and Dawn Branley

Source: <https://reader.elsevier.com/reader/sd/8387A31C0F3863C97094AFEB870B739C1ED9E37C92E567A32063BB14B550F0FD56F4C033714D947FCD5EAA7CF3F7F727> [full paper]

Abstract

Electronic healthcare technology is prevalent around the world and creates huge potential to improve clinical outcomes and transform care delivery. However, there are increasing concerns relating to the security of healthcare data and devices. Increased connectivity to existing computer networks has exposed medical devices to new cybersecurity vulnerabilities. Healthcare is an attractive target for cybercrime for two fundamental reasons: it is a rich source of valuable data and its defences are weak. Cybersecurity breaches include stealing health information and ransomware attacks on hospitals, and could include attacks on implanted medical devices. Breaches can reduce patient trust, cripple health systems and threaten human life. Ultimately, cybersecurity is critical to patient safety, yet has historically been lax. New legislation and regulations are in place to facilitate change. This requires cybersecurity to become an integral part of patient safety. Changes are required to human behaviour, technology and processes as part of a holistic solution.

The impact of flooding on the delivery of hospital services in the southeastern United States

By McGlown KJ and Fottler MD

Health Care Manage Rev. 1996 Summer;21(3):55-71.

Source: <https://www.ncbi.nlm.nih.gov/pubmed/8832278>

Abstract

A survey and three case studies were conducted of hospitals in Alabama, Georgia, and Florida affected by flooding in July 1994. Our findings suggest that the existence or quality of hospital or community plans for disaster did not seem related to the effect of the flood or the hospitals' response to flooding. Recommendations for preparation and problem avoidance in future flood disasters are provided.

Hospital responses to acute-onset disasters: a review.

By Milsten A

Prehosp Disaster Med. 2000 Jan-Mar;15(1):32-45.

Source: <https://www.ncbi.nlm.nih.gov/pubmed/11066840>

Abstract

INTRODUCTION: Hospitals the world over have been involved in disasters, both internal and external. These two types of disasters are independent, but not mutually exclusive. Internal disasters are isolated to the hospital and occur more frequently than do external disasters. External disasters affect the community as well as the hospital. This paper first focuses on common problems encountered during acute-onset disasters, with regards to hospital operations and caring for victims. Specific injury patterns commonly seen during natural disasters are reviewed. Second, lessons learned from these common problems and their application to hospital disaster plans are reviewed.

METHODS: An extensive review of the available literature was conducted using the computerized databases Medline and Healthstar from 1977 through March 1999. Articles were selected if they contained information pertaining to a hospital response to a disaster situation or data on specific disaster injury patterns. Selected articles were read, abstracted, analyzed, and compiled.

HOSPITAL THREATS

RESULTS: Hospitals continually have difficulties and failures in several major areas of operation during a disaster. Common problem areas identified include communication and power failures, water shortage and contamination, physical damage, hazardous material exposure, unorganized evacuations, and resource allocation shortages.

CONCLUSIONS: Lessons learned from past disaster-related operational failures are compiled and reviewed. The importance and types of disaster planning are reviewed.

Review article: evacuating hospitals in Australia: what lessons can we learn from the world literature?

By Rojek A and Little M

Emerg Med Australas. 2013 Dec;25(6):496-502. doi: 10.1111/1742-6723.12160. Epub 2013 Nov 13.

Source: <https://www.ncbi.nlm.nih.gov/pubmed/24224553>

Abstract

The creation of hospitals safe from disaster is an area of increasing public policy. The vulnerability of hospitals to damage and destruction during an event has profound implications for the health of a community. Although hospital evacuations do occur in Australia, their prevalence is unknown and what leads to a successful evacuation is poorly understood. This article reviewed the worldwide hospital evacuation literature to determine the prevalence of hospital evacuations and common precipitants for evacuation. Factors leading to safe evacuation and areas of ongoing challenge were identified. The findings highlight the need for more structured and detailed reporting of hospital responses to disaster. A number of lessons can be learned from hospitals that have experienced evacuation. Most critically, all hospitals must have a practised, detailed hospital evacuation plan existing before an impending threat. There are also areas for improvement in the areas of assessing the risk to the facility, communications, leadership, logistics, staffing and planning. These lessons should be included into comprehensive, detailed evacuation plans for all Australian hospitals, supported by a national framework that standardises planning and response.



Source: https://www.fema.gov/media-library-data/20130726-1609-20490-5010/577_ch3.pdf

The 2013 floods and Bundaberg Hospital

By Adrian Pennington (WBHHS Chief Executive)

Source: <https://www.health.qld.gov.au/widebay/media-releases2/january-march-2018/the-2013-floods-and-bundaberg-hospital>

WHEN I think back to the 2013 floods, it feels like an age ago and it feels like yesterday.

In January 2013 I'd been the Chief Executive of the fledgling Wide Bay Hospital and Health Service for less than a year, I was finding my job both challenging and rewarding, and my family and I were loving our new life in Bargara.

With well over three decades' experience in health care, I'd been involved in high-level disaster management in the UK before – including a fire in one of my British hospitals – but I'd never been involved in managing a disaster on the scale of that Bundaberg flood.

To this day, I've never seen a team of people pull together for the good of others the way I did during the several days the disaster was at its peak, and it makes me proud and emotional every time I think about it.

HOSPITAL THREATS



When the impacts of ex-Tropical Cyclone Oswald started to be felt in Wide Bay on Australia Day, it was the start of four days of an unprecedented emergency response, both for the region and for the health sector in Queensland.

By the end of January 29, all inpatients of Bundaberg Hospital would be evacuated and we had to manage service continuity to our isolated rural hospitals. For the first time in our history, all 11 WBHHS facilities had been cut off from each other.

An added responsibility in these situations is that disaster management protocols dictate the Chief Executive of the public health service takes responsibility for the management of all health facilities across the district – meaning I also had to make decisions about the movement and transfer of patients at the Mater and Friendly Society private hospitals, and local aged care facilities as needed.

When the Local Disaster Management Group (LDMG) was stood to, it unleashed a heady and relentless chain of events.

With Chief Operating Officer Debbie Carroll and then Manager of

Operational Services Gerard Devine by my side constantly, we maintained a punishing schedule. For three days we met every two hours with more than 20 specialist staff, constantly monitoring the information we were being given about river heights and doing our best to predict the potential impact on our services and our workforce.

A key part of emergency planning is to be thinking 24 hours ahead of the next trigger point. This included the closure and transfer of all patients to the Friendlies from the Mater – which was just as vulnerable as Bundaberg Hospital because of its proximity to the river.

We also cancelled all private surgery so beds could be made available for about 100 patients from the RSL Care Fairways nursing home. These patients needed to be transferred at an early stage to minimise the risk of simultaneous evacuations, should Bundaberg Hospital patients need to be moved.



HOSPITAL THREATS

The first Bundaberg Hospital patient areas at risk were the Rehab and Mental Health units, whose patients were transferred to alternate facilities in Brisbane and elsewhere. Patients in the Intensive Care Unit and babies in the Special Care Nursery were also transferred early and quietly – in part to mitigate risk



associated with a full evacuation, and in part to prevent any form of panic within the community.

Renal patients were individually prepared, and were transferred to appropriate accommodation to be managed nearby. Our dialysis team continued to function throughout the event.

Crucially, we also had to ensure the hospital provided emergency services at a time of catastrophic need within our community. We had made contingency plans to relocate our Emergency Department, which could be operational within five hours if necessary.

For Bundaberg Hospital, the critical operational issues during a time of flood are sewerage and power.

At a given level of flooding, the ability to pump sewage would be lost and therefore become dependent on the laws of gravity. Obviously a river level equal to the ground floor would mean serious clinical and infection issues, and we would have to close operations.

Our power is dependent on two sub-stations. The first, as predicted, was turned off at 9.5m. The second sub-station was at serious risk when the water levels in some places were in excess of 10m.

But there was a complication – the river levels experienced by the hospital were higher than what were being officially recorded. As debris was being carried down the Burnett River at a frightening volume and rate, the nearby Tallon Bridge was essentially acting as a dam as it caught the floating junk.

As a result, the water on our side of the bridge was rising fast and we had to manually amend Bureau of Meteorology predictions to derive the expected impact on our electricity supply. When all was said and done, we ended up being just 26mm away from the catastrophe that would have ensued if we had lost the second sub-station.

The decision to evacuate the remaining patients in Bundaberg Hospital en masse was made in the early hours of January 28, when the river reached 8.4m.

I'll never forget the moment I had to make that call. Throughout the past two days, the strain and pressure had been enormous. We had had to move some very sick and frail patients, and I was constantly concerned that the stress and upheaval of the situation would be too much for some to survive. Several of us hadn't slept since the disaster started and it was starting to take its toll.

But when the river reached that height and the predictions were for merciless rises of at least a metre more, there seemed little other option.

At one point, when it felt like I might have prevaricated, emergency physician and disaster management specialist Dr Mark Little asked me during that key LDMG meeting: "Ade, what are we going to do?"

HOSPITAL THREATS

I hesitated for a moment, feeling a great weight on my shoulders, but knew the answer. “Go,” I said. Planes, air force teams, ambulances and taxis were at the ready, effectively giving us 24 hours to execute the most professional evacuation of a hospital in Australia.

Hercules aircraft were called in at 2.10am and started arriving soon after. A stepped holding medical facility was established at Bundaberg Airport, and 135 patients were transferred to Brisbane hospitals on three flights. A further 10 were transferred by air ambulance to other supporting health facilities.

At the high point of the evacuation, somehow we managed to have at least two members of staff assisting every patient transferring.

The spirit of staff – many of whom had been personally affected by the flood – was overwhelming. Debbie and I hadn’t slept at all for three-and-a-half days but the adrenaline and morale of our staff kept us going. Once the evacuation was complete, many staff were stood down to take a well-earned rest – but there were still decisions to make.

We needed to decide what to do about the Emergency Department. Should we close it or stand ready for a speedy transfer, as per our contingency plans?

We decided to wait. Fortunately, a few hours later the river peaked and later in the day the levels finally started to fall.

The IT team was challenged by the need for the movement of our servers, but thought outside the box to deliver exceptional support, at one point using a mobile dental van as a portable server and communication centre.

Our Public Health team also provided exceptional support to the wider community, both during and after the flood event. There were many different issues facing the city due to the disaster, including water safety, sewerage issues, mosquitoes, mould and providing support to evacuation centres.

Throughout all this, I did what seemed like an unending stream of media interviews with journalists across the globe, as Bundaberg’s floods became an international news story.

Finally, it was time for me to have a break too. When I arrived home, I said little to my family and walked through to the bedroom. Sitting on the side of the bed, my wife placed a hand on my shoulder, which was my cue to unleash all that had built up. I sobbed uncontrollably for what seemed an eternity.

A long shower and 14 hours’ sleep later, I was ready to go again. To my amazement, many staff were already back on deck when I got to the hospital. “The Mud Army” (a new concept for me) had also kicked in, and the clean-up had begun.

Both staff and volunteers had the hospital site cleared within 24 hours.

I talk little of these events today, which is probably true of the wider team that managed the process. And, I must admit, whenever I hear heavy rain outside I find myself instinctively looking toward the river.

But looking back, our successes lay in constantly thinking ahead, in finding the right people for each job at hand, and in everybody pulling together to carry out their respective tasks, whether it was clinical, operational or administrative.

There were some things we learned, too. The biggest one is that I probably would have evacuated the hospital earlier if I had my time over.

We’ve now become like a well-oiled machine when it comes to disaster management. When the after-effects of Tropical Cyclone Debbie were bearing down on us last March, it was once again impressive to watch the way our teams prepared for a range of eventualities.

To this day I’m awestruck by two things about that 2013 flood.

The first was the dedication of our employees and the way they put our patients first, at a time many of them must have been worried about the wellbeing of their own families. As an essential service, healthcare workers are frequently called on to step up for their community, and we do it time and time again without question. The morale in our corridors was incredible.

The second was the community spirit in this city, and by the way we were surrounded by an army of volunteers who helped us so quickly get back on our feet after such a seismic event.

I cannot think of a better place to be.

HOSPITAL THREATS



Source: <http://blogs.harvard.edu/cybersecurity/files/2017/01/risks-and-threats-healthcare-strategic-report.pdf>

Cybersecurity has become a crucial issue for many organizations but also for private individuals. As well as for “regular” crime, anyone may become a target of ill-intentioned people, exploiting the vulnerabilities of information systems (IS) in any possible way. Healthcare organizations are some of the entities we trust the most and that hold the most sensitive information about us: name, date and place of birth, medical records, social security details, etc. Suffering from many flaws (low budget, lack of IT organization, excessive use of legacy systems...), healthcare actors have become easy targets for hackers, facing more and more pressure and threats from them.

This article aims at depicting the current state of cybersecurity in healthcare organizations as well as at understanding the main cyber threats they face and how these last ones could be addressed.

First of all, the stakes and risks associated to the healthcare environment will be presented. The different types of assets likely to be targeted will be reviewed as well as the profile of the potential attackers/threats and their objectives.

Then, **examples of attack scenarios** - that occurred in real life or pentests - will be studied in order to highlight the consequences they may have on healthcare IS.

Finally, the current state of cybersecurity in healthcare facilities will be portrayed and possible measures to enhance it will be discussed.



Source: <https://www.aha.org/system/files/2017-12/ahaprimer-cyberandhosp.pdf>

Cybersecurity has been a hot topic, both within the government and the private sector, for several years. However, the issue recently has taken on even greater prominence. Many organizations, from private media companies to the U.S. Department of Defense, recently disclosed cybersecurity intrusions. Private sector chief executive officers (CEOs) and general counsels have consistently identified cybersecurity threats as one of their top concerns. And in February 2013, President Obama issued an *Executive Order on Improving Critical Infrastructure Cybersecurity* with the goal of improving cybersecurity and reducing cyber threats to the nation’s “critical infrastructure sectors,” including the Healthcare and Public Health Sector. Despite the attention cybersecurity has received, not everyone knows what cybersecurity is or what it really means for American businesses, particularly for those in the critical infrastructure sectors referenced in the president’s executive order.


Hospitals and health care organizations fall into the Healthcare and Public Health Critical Infrastructure Sector under federal law and policy; the executive order uses the same critical infrastructure classifications when identifying the potential impact on the U.S. economy by cybersecurity threats. In

HOSPITAL THREATS

other words, the executive order and other government policies collectively identify hospitals' systems and assets as so vital to the U.S. that their impairment would severely threaten public health and safety.³ As a result, hospitals need to have an awareness of cybersecurity risks, as well as a clear understanding of what their cybersecurity responsibilities are (and how they might intersect with other statutory and regulatory requirements). This paper provides an overview of what cybersecurity is and addresses four questions that hospital leaders should consider when thinking about cybersecurity and how it impacts their organization:

1. Why should hospitals and hospital leaders care about cybersecurity?
2. What should hospitals do in response to the 2013 *Executive Order on Cybersecurity*?
3. How can hospitals best protect their assets and manage cybersecurity risks?
4. What are the roles of hospital leadership and how can leadership stay informed about cybersecurity threats to the hospital?

This paper is intended to make the cybersecurity issues specifically facing hospitals concrete, identifiable and actionable. It includes an appendix that provides an overview of the 2013 *Executive Order on Cybersecurity* and a glossary of the cybersecurity terms used in general discussions of cybersecurity and in this paper.

	
	Cyberwatch
Cyber Vulnerabilities and Risks in the Healthcare Ecosystem	
Executive summary	1
Key Findings	2
Vulnerability in the Healthcare Context	3
Reform of Healthcare Ecosystem	4
Medical Data at Risk	5
Healthcare Industry is an Attractive Target	5
Motivations Behind Cyber Attacks	7
Conclusions	9

Source: <https://objects.fi-1.nebulacloud.fi/messukeskus/wp-content/uploads/sites/492/2017/09/958c/CyberVulnerabilitiesandRisksintheHealthcareEcosystemKEYYT.pdf>

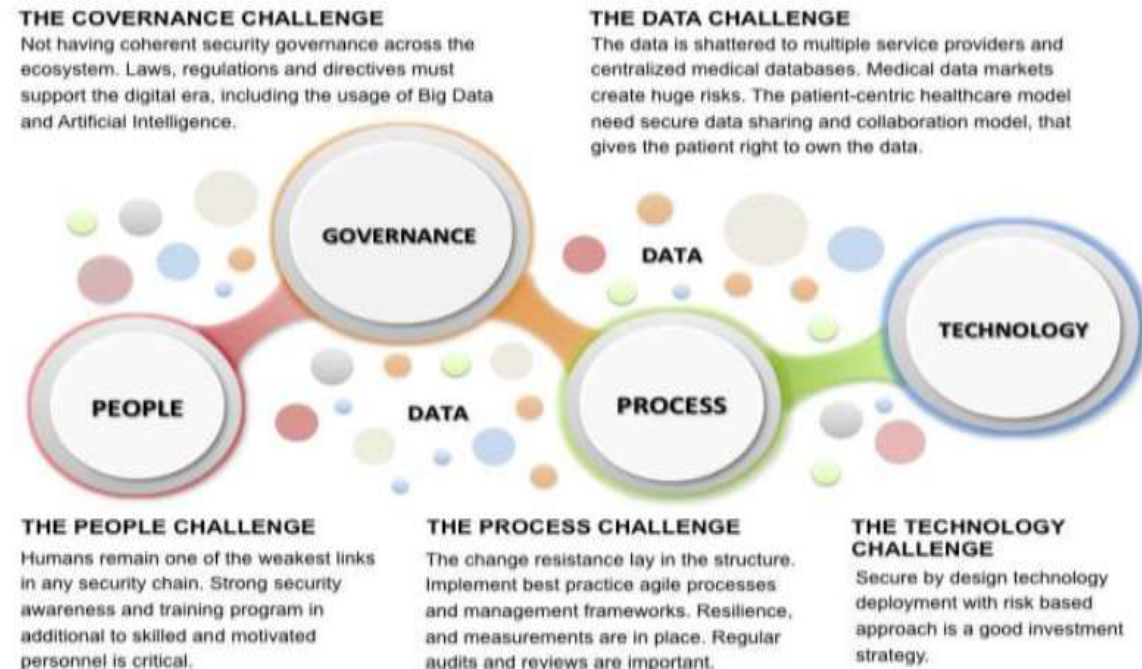
Critical infrastructure is the backbone of modern society. Healthcare infrastructure and services are part of critical infrastructure and they could even be called super critical, because well-functioning health care is needed in our everyday life but more importantly in every crisis situation. It should be part of the national plan of Critical Infrastructure Protection (CIP). Modern cyber-attacks are based on vulnerabilities – it is impossible to protect the healthcare ecosystem without knowing the vulnerabilities. The key question is do we know the vulnerabilities in our healthcare ecosystem, if not what should be done?

The aim of this document is to raise the awareness of the vulnerabilities in healthcare infrastructure and services for the decision maker in the healthcare industry and medical infrastructure as well as at the level of hospitals. All the involved parties should understand the risk and threat these vulnerabilities can create for the whole healthcare ecosystem. In the headlines, we have this as a rising risk in the light of some recent cyberattacks and data breaches. It is probably right to claim that cyber-attacks or data breaches are going to happen more and more in the near future. The question is when and at what cost? Lloyd's of London estimates that a major cyber-attack could cost as much as a super storm Sandy to the global economy, roughly \$53 billion.

To fully perceive the big picture and to be able to make reasonable decisions it is important to define vulnerabilities and risks in all levels of the ecosystem covering people, process, technology and data, and in addition governance, where the prerequisite for success or failure originally is laid down. Identifying the need for a common understanding of existing threats, regulations, standards, risks and complexities are essential for securing the healthcare ecosystem in the future. It is very much up to the national authorities

HOSPITAL THREATS

to decide who is overlooking the security of the whole healthcare ecosystem. A comprehensive situational awareness is needed to be able to prevent and protect cyber-attacks.



Picture 1: Vulnerability challenge in the healthcare ecosystem

Key Findings

- There is a great systemic challenge at hand. The patient-centered healthcare model is reforming the healthcare industry, which might have major effects on medical health data liabilities and patient's rights to own the data.
- For the leaders and decision makers it is a necessity to identify viable future scenarios, trends and changes to be expected, to form a common understanding of possible threats and risks related to them. Lawmakers and decision makers are to set the direction for the future of healthcare ecosystem. Better awareness is needed at all levels across the board.
- There needs to be a pointed organisation and person in charge having responsibility for cyber security in the healthcare industry, hospitals as well as in every organisation in this sector.
- Sufficient resources allocated to comply regulations and standards; competent people, modern and agile processes utilizing security by design technologies. Well trained and competent people are crucial for minimising the risks.
- New technological threats and vulnerabilities will arise. Resilience and quick recovery from any reasonable situation should be emphasised.

Security threats categories in healthcare information systems

By Ganthan Narayana Samy, Rabiah Ahmad and Zuraini Ismail

Universiti Teknologi Malaysia, Malaysia

Health Informatics Journal. 2010; 16(3) 201–209

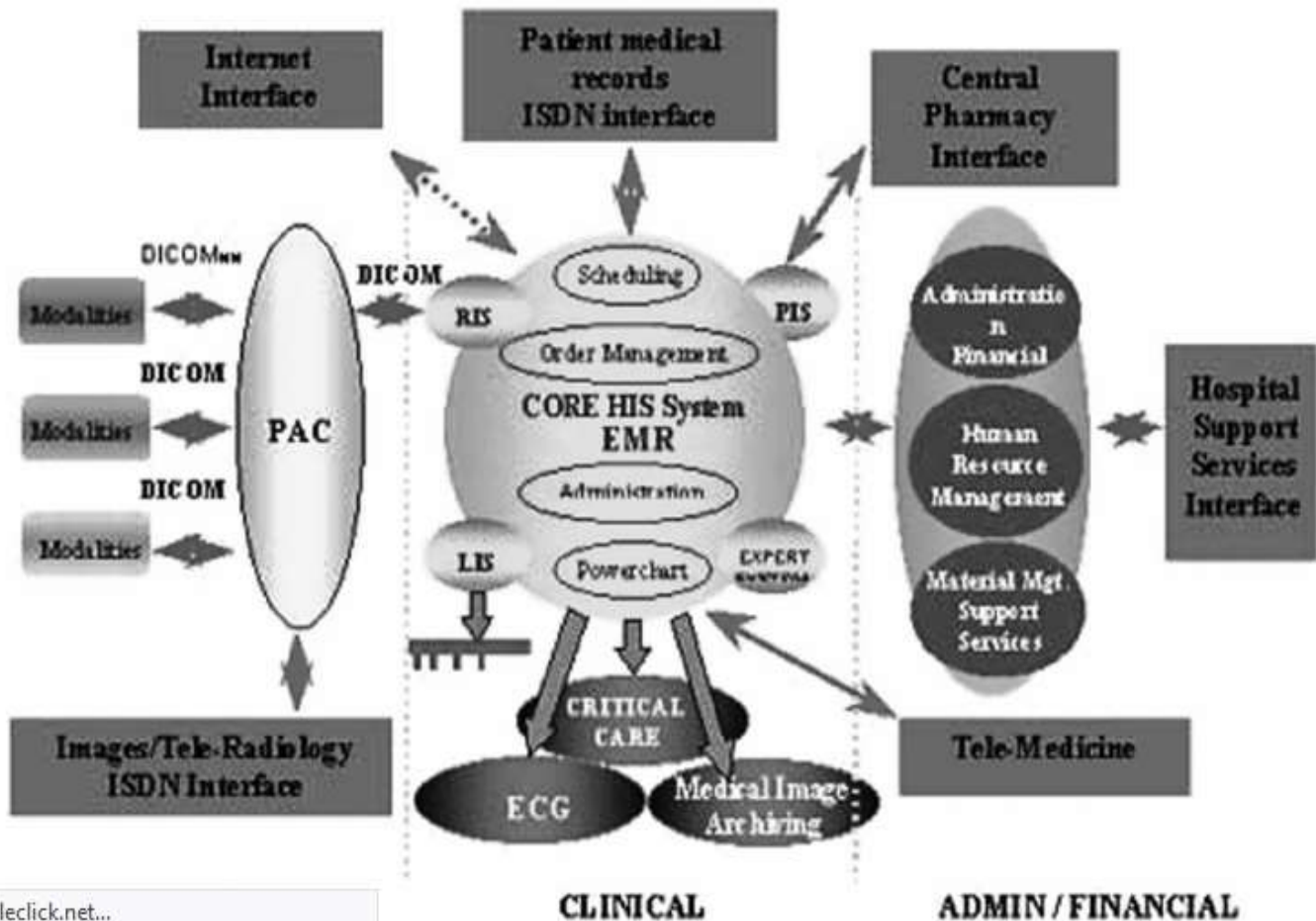
Source: https://www.researchgate.net/publication/47300369_Security_threats_categories_in_healthcare_information_systems

This article attempts to investigate the various types of threats that exist in healthcare information systems (HIS). A study has been carried out in one of the government-supported hospitals in Malaysia. The hospital has been equipped with a Total Hospital Information System (THIS). The data collected were from three different departments, namely the Information Technology Department (ITD), the Medical Record Department (MRD), and the X-Ray Department, using in-depth structured interviews. The study identified 22 types of threats according to major threat categories based on ISO/IEC 27002 (ISO

HOSPITAL THREATS

27799:2008). The results show that the most critical threat for the THIS is power failure followed by acts of human error or failure and other technological factors. This research holds significant value in terms of providing a complete taxonomy of threat categories in HIS and also an important component in the risk analysis stage.

TOTAL HOSPITAL INFORMATION SYSTEM



The Total Hospital Information System (THIS) is an integration of clinical, administrative, and financial systems. The clinical side comprises the Hospital Information System and the Picture Archiving Communication System (PACS). The Hospital Information System is composed of various applications such as person management, scheduling, order management, and clinical documentation. The administration and finance system forms a back end which is integrated with the Hospital Information System so that any chargeable procedures or tests performed on the patients will automatically trigger the generation of bills. With PACS, the system is also interfaced with the various X-ray machines. Figure 1 shows the current THIS key components.



Source: <https://synoptek.com/wp-content/uploads/Healthcare-Security-Booklet-Final.pdf>

HOSPITAL THREATS

From the contents of Synoptek report

The curious doctor and a USB stick

Target: a 400 bed community hospital

Outcome: Stolen social security numbers and medical records

How did they do it?

Attackers entered a community hospital dropping malware-laced USB thumb drives where staffers might tend to pick them up. Before the drop, the attackers disguised the USB drives by labeling them with the hospital's logo.

Within 24

hours, a curious doctor had picked up the USB drive and plugged it into their computer. This type of malware can download and install itself off of a USB drive, take control of the device, and grant control to a remote attacker. The attack quickly spread undetected across the hospital's internal network.

How could this have been prevented?

A study by the University of Illinois found that 48% of people DO plug-in unknown USB drives they find on the ground. Not only do many people plug in USB devices, they connect them quickly. 20% of the connected drives were connected within the first hour and 50% were connected within 7 hours. This means that the window of time available to detect that this attack is occurring is very short. CIO and CSO magazines report only 29% of organizations say their employees (at all levels) are very aware of cyber risks.

The report also found that in 37% of cyber attack incidents, employee error was the cause of the security breach. By investing in an end-user cyber security training program The curious doctor and a USB stick this hospital's staff would have been educated and aware of the threat that unknown USB drives pose.

The cost per record breached is \$355



A Cyber Security Risk Assessment of Hospital Infrastructure including TLS/SSL and other Threats

Millar, S. (2016). A Cyber Security Risk Assessment of Hospital Infrastructure including TLS/SSL and other Threats. Queen's University Belfast.

Source: https://pure.qub.ac.uk/portal/files/125120790/StuartMillar13616005_ACyberSecurityRiskAssessmentOfHospitalInfrastructure_TLS.pdf

Cyber threats traditionally target governments, financial institutions and businesses. However, of growing concern is the threat to healthcare organizations. This study conducts a cyber security risk assessment of a theoretical hospital environment, to include TLS/SSL, which is an encryption protocol for network communications, plus other physical, logical and human threats. Despite significant budgets in the UK for the NHS, the spend on cyber security appears worryingly low and many hospitals are wide open to attack. This paper concludes that major change, led nationally by the UK government, is needed to make cyber security a major priority in the NHS, without diluting long-standing values of service provision to patients.

HOSPITAL THREATS

Cyber Risk Management in the Finnish Healthcare Sector

University of Tampere

Master's Thesis

January 2018

Author: Hanne Hellstén

Supervisor: Lasse Koskinen

Source: <https://tampub.uta.fi/bitstream/handle/10024/102897/1518709273.pdf?sequence=1&isAllowed=y>

Advances in technology and digitalization have been widely adopted by Finnish healthcare organizations. This development has led to improvements in the efficiency and outcomes of patient care, but has also exposed healthcare providers to new kinds of risks.

Cyber risks are becoming an increasingly common occurrence in the health care sector, and can lead to serious consequences for patients and organizations alike. The significance of cyber risks within healthcare has been projected to grow, as internet-enabled applications and medical devices become increasingly ubiquitous in the industry.

Cybersecurity Toolkit for Rural Hospitals and Clinics

January 2018

Source: https://www.maine.gov/dhhs/mecdc/dlrs/rhpc/documents/Cyber_Toolkit.pdf

Cybercrime and Other Threats Faced by the Healthcare Industry

Mayra Rosario Fuentes

Forward-Looking Threat Research (FTR) Team

Source: <https://www.trendmicro.com/content/dam/trendmicro/global/en/security-intelligence/research/reports/wp-cybercrime-&-other-threats-faced-by-the-healthcare-industry.pdf>

HOSPITAL THREATS



Source: http://www.vm.gov.lv/images/userfiles/Nozare/E-veseliba/20170602_eHealth_Security_ENISA_Athanasios_Drougkas.pdf

Post-earthquake functionality of critical facilities: A hospital case study

S. Youance & M.-J. Nollet

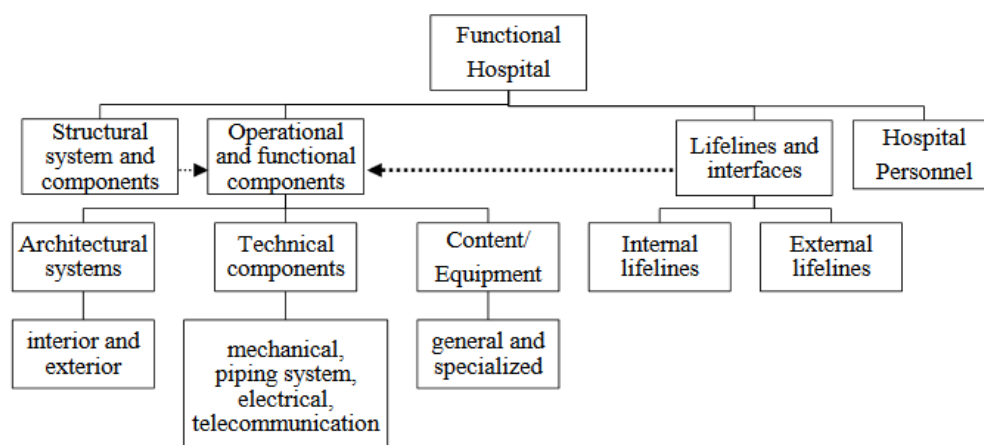
Department of Construction Engineering, École de technologie supérieure, Université du Québec

G. McClure

Department of Civil Engineering and Applied Mechanics, McGill University

Source: https://www.iitk.ac.in/nicee/wcee/article/WCEE2012_2287.pdf

This paper investigates the post-earthquake functionality of hospital buildings in Montreal, Canada by taking into account the interdependencies between the structural framework and the various nonstructural components and lifeline services. Health care facilities are classified as post-disaster systems in most



Functional components of a hospital

building codes and are therefore required to be fully operational and safe during and after an earthquake. The main objective of this research is to develop a comprehensive methodology to evaluate the post-earthquake functionality of individual hospital facilities, in opposition to existing methodologies used in “urban scale” models. The hospital used as a case study is a complex built in 1954. It is described through its logical functionality scheme including a simple consideration of the lifeline services at this stage of the

HOSPITAL THREATS

research. The seismic vulnerability of each group of components (structural, nonstructural and interfaces with utilities) is evaluated in terms of resistance and functionality according to Canadian standards.

Earthquake Spectra Vol 27, Issue 3, pp. 617-634, 2011.

Earthquake Induced Structural and Non-structural Damage in Hospitals

Nebil Achour¹, Masakatsu Miyajima², Masaru Kita² and Andrew Price¹

The Sichuan (China) and L'Aquila (Italy) earthquakes again highlighted the question of our preparedness for natural hazards. Within a few seconds an earthquake can demolish many buildings, destroy infrastructure, and kill and injure thousands of people. In order to reduce the impact of earthquakes on human life and prepare hospitals to cope with future disasters, this paper discusses earthquake related damage to healthcare facilities. It investigates the damage to 34 healthcare facilities in seven countries caused by nine earthquakes between 1994 and 2004, in order to determine common and specific issues. The investigation shows that structural and architectural damage tended to be different and specific to the situation, while utility supplies and equipment damage were similar in most cases and some common trends emerged.

Source: https://www.researchgate.net/publication/274246886_Earthquake-Induced_Structural_and_Nonstructural_Damage_in_Hospitals



A collection of papers





Safe Hospitals

Documents available on the web

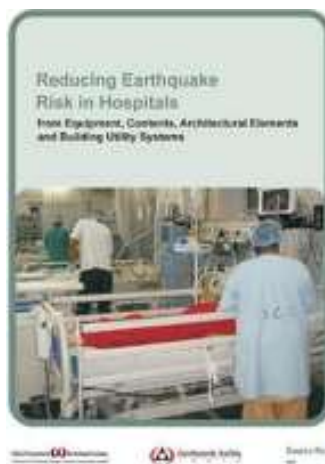
This catalogue is available in electronic format at
www.who.int/hac/events/safe_hospitals_info.pdf

See also the Hospitals Safe from Disasters web site at www.safehospitals.info/

Source: http://www.who.int/hac/events/safe_hospitals_info.pdf

Hospital Safety Manual

Source: https://docs.wixstatic.com/ugd/08dab1_0125e46ba28c4f479e403c53822f2665.pdf



GeoHazards International and reinsurer Swiss Re created this manual to show how to reduce hospital damage and losses from items that fall, rupture or topple during earthquakes.

It offers clear instruction how to identify hazards and brace medical equipment and supplies, contents, architectural elements, and building utility systems.

Damage to these items in past earthquakes has caused deaths, injuries, loss of building function, and economic loss, even when the building structure itself was essentially undamaged.

HOSPITAL THREATS

Guidelines for Hospital Emergency Preparedness Planning

Source: http://asdma.gov.in/pdf/publication/undp/guidelines_hospital_emergency.pdf

The GoI-UNDP Disaster Risk Management Programme is a national initiative to reduce vulnerabilities of communities in some of the most hazard prone districts of India (169 districts and 17 states). The Programme aims to contribute to the social and economic development goals of the National and State Governments, enabling them to minimize losses to development gains and to reduce their vulnerability to natural disasters. Urban Earthquake Vulnerability Reduction Project (UEVRP), a sub-component of the DRM Programme, essentially aims at strengthening capacities of communities, urban local bodies and administration in mitigation, preparedness and response in 38 cities in India. These cities have been chosen on the criteria of being located in Seismic Zones III, IV or V, with more than half a million population.

Health and Hospital systems are the most critical units of the Emergency Support Function. "Guidelines for developing Hospital Emergency Management Plan" intends to support the hospitals to formulate their own "all hazard" emergency plans in accordance with their manpower and infrastructural resources that will meet the demands of medical care more effectively during disasters/emergencies.

This document would guide in developing integrated Hospital Plans that are consistent with the city or community disaster management plans. Emphasis is laid on strengthening the functioning, coordination and response for an enhanced pre-hospital and hospital care.

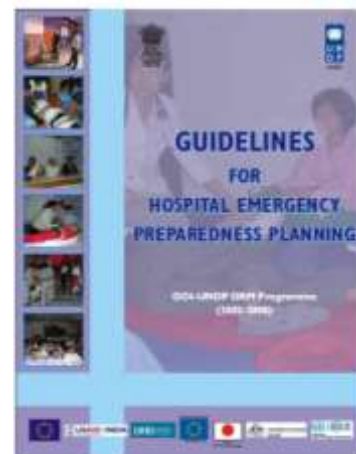
It is ensured that these guidelines are in accordance with the "National Disaster Management Guidelines for Medical Preparedness and Mass Casualty Management" brought out by National Disaster Management Authority (NDMA).

The **first chapter** provides an overview of Disaster Management, concepts of hospital emergency planning, and issues of coordination and networking both for pre-hospital and hospital care.

The **second chapter** covers the principles and the steps involved in hospital planning.

The **third chapter** presents the templates for developing the actual plan for different levels of health facilities from secondary to tertiary and the teaching hospitals.

Vital inventories, tables and charts, job cards etc. form a part of the annexes.



The preparedness of hospital Health Information Services for system failures due to internal disasters¹

Cheens Lee, Kerin M Robinson, Kate Wendt and Dianne Williamson

Abstract

The unimpeded functioning of hospital Health Information Services (HIS) is essential for patient care, clinical governance, organisational performance measurement, funding and research. In an investigation of hospital Health Information Services' preparedness for internal disasters, all hospitals in the state of Victoria with the following characteristics were surveyed: they have a Health Information Service/Department; there is a Manager of the Health Information Service/Department; and their inpatient capacity is greater than 80 beds. Fifty percent of the respondents have experienced an internal disaster within the past decade, the majority affecting the Health Information Service. The most commonly occurring internal disasters were computer system failure and floods. Two-thirds of the hospitals have internal disaster plans; the most frequently occurring scenarios provided for are computer system failure, power failure and fire. More large hospitals have established back-up systems than medium- and small-size hospitals. Fifty-three percent of hospitals have a recovery plan for internal disasters. Hospitals typically self-rate as having a 'medium' level of internal disaster preparedness. Overall, large hospitals are better prepared for internal disasters than medium and small hospitals, and preparation for disruption of computer systems and medical record services is relatively high on their agendas.

Source: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.498.8381&rep=rep1&type=pdf>

HOSPITAL THREATS

Assessment of disaster preparedness among emergency departments in Italian hospitals: a cautious warning for disaster risk reduction and management capacity

By Matteo Paganini, Francesco Borrelli, Jonathan Cattani et al.

Scandinavian Journal of Trauma, Resuscitation and Emergency Medicine; December 2016, 24:101

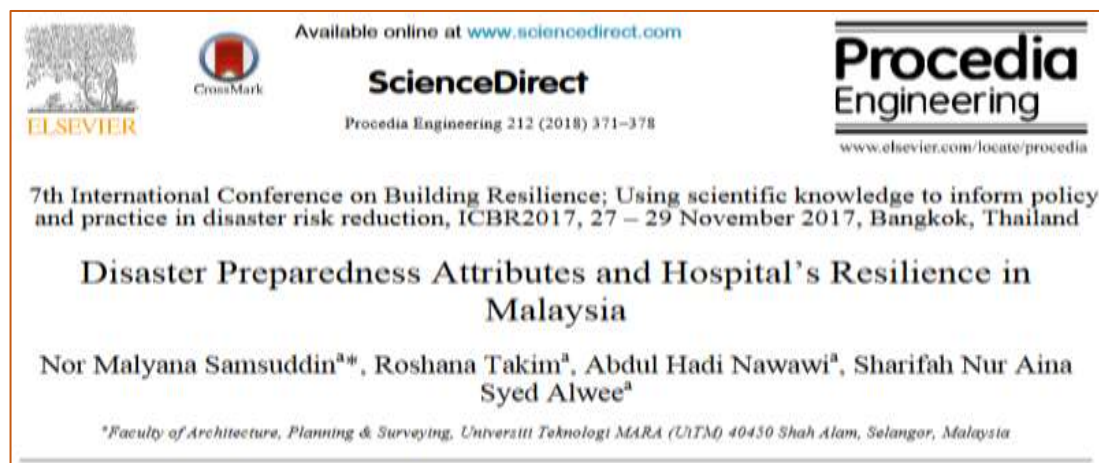
Source: <https://link.springer.com/article/10.1186/s13049-016-0292-6>

Study hypothesis: Since the 1990s, Italian hospitals are required to comply with emergency disaster plans known as Emergency Plan for Massive Influx of Casualties. While various studies reveal that hospitals overall suffer from an insufficient preparedness level, the aim of this study was to better determine the preparedness level of Emergency Departments of Italian hospitals by assessing the knowledge-base of emergency physicians regarding basic disaster planning and procedures.

Methods: A prospective observational study utilized a convenience sample of Italian Emergency Departments identified from the Italian Ministry of Health website. Anonymous telephone interviews were conducted of medical consultants in charge at the time in the respective Emergency Departments, and were structured in 3 parts: (1) general data and demographics, (2) the current disaster plan and (3) protocols and actions of the disaster plan.

Results: Eighty-five Emergency Departments met inclusion criteria, and 69 (81 %) agreed to undergo the interview. Only 45 % of participants declared to know what an Emergency Plan for Massive Influx of Casualties is, 41 % believed to know who has the authority to activate the plan, 38 % knew who is in charge of intra-hospital operations. In Part 3 physicians revealed a worrisome inconsistency in critical content knowledge of their answers.

Conclusions: Results demonstrate a poor knowledge-base of basic hospital disaster planning concepts by Italian Emergency Department physicians-on-duty. These findings should alert authorities to enhance staff disaster preparedness education, training and follow-up to ensure that these plans are known to all who have responsibility for disaster risk reduction and management capacity.



Source: <https://ac.els-cdn.com/S1877705818300614/1-s2.0-S1877705818300614-main.pdf>

Disaster resilience hospital (DRH) is the hospital's ability to resist, absorb, accommodate and recover from the effects of a hazard in a timely and efficient manner. DRH includes the preservation and restoration of the hospital's essential basic structures and functions. Resilience (i.e. robustness; redundancy; resourcefulness; and rapidity) could be achieved through enhancement of preparedness attributes in terms of structural, non-structural and functional measures. However, over the past few years there is a growing body of evidence to show that the impacts of disasters are affecting negatively towards public hospitals in Malaysia. It is believed that to a certain extent the preparedness attributes of hospitals towards disaster resilience are insufficient. Hence, the purpose of this paper is twofold: to investigate the hospital preparedness attributes and resilience indicators; and to establish relationship of preparedness attributes towards hospital's resilience. Cross-sectional survey was conducted among twenty six (26)

HOSPITAL THREATS

Malaysian hospitals' staff. A total 243 preparedness attributes (structural- 21; non-structural-107; and functional-115) and 23 resilience indicators (robustness- 5; redundancy-5; resourcefulness-6; and rapidity-7) were subjected to non-parametric Spearman Correlation. The results revealed that 17 preparedness attributes and 23 resilience indicators are rated 'very critical' by the respondents by which human resources & training and ability to adapt in a timely manner are ranked first. In addition, non-structural preparedness presented greater strength of correlation towards robustness; redundancy; and resourcefulness. On the contrary, the functional attributes showed higher correlation towards rapidity. The results could serve as indicators for the public hospital's stakeholders in Malaysia to improve its preparedness and enhancing its resilience..

Hospital Disaster Readiness: Why Are We Unprepared?

Source: <http://www.ceep.ca/publications/HospitalDisasterReadinessWhyAreWeUnprepared.pdf>



Source: <https://www.urban.org/sites/default/files/publication/50896/411348-Hospitals-in-Hurricane-Katrina.PDF>

MEDICAL PRACTICE

JTS Chan 陳德勝
RSD Yeung 楊世達
SYH Tang 鄧耀鏗

Hospital preparedness for chemical and biological incidents in Hong Kong

香港醫院應付生化事件的準備

The risk of mass exposure to toxic substances has increased steadily during the twentieth century due to the expansion of industry and the deliberate development and use of agents of chemical warfare. Although Hong Kong is considered a relatively safe place, hoax anthrax attacks have occurred since 17 October 2001. People who have been seriously injured by hazardous materials have a greater chance of recovery without complications when appropriate emergency treatments are provided. Recognition and identification of hazardous materials, assessment of the conditions, decontamination, and protection of staff and facilities are important elements in the formulation of a contingency plan. The objective of this article is to outline the efforts of the Hong Kong Hospital Authority in formulating a hospital response to incidents involving hazardous materials.

Source: <http://www.hkmj.org/system/files/hkm0212p440.pdf>

HOSPITAL THREATS

Hospital Emergency Evacuation Toolkit



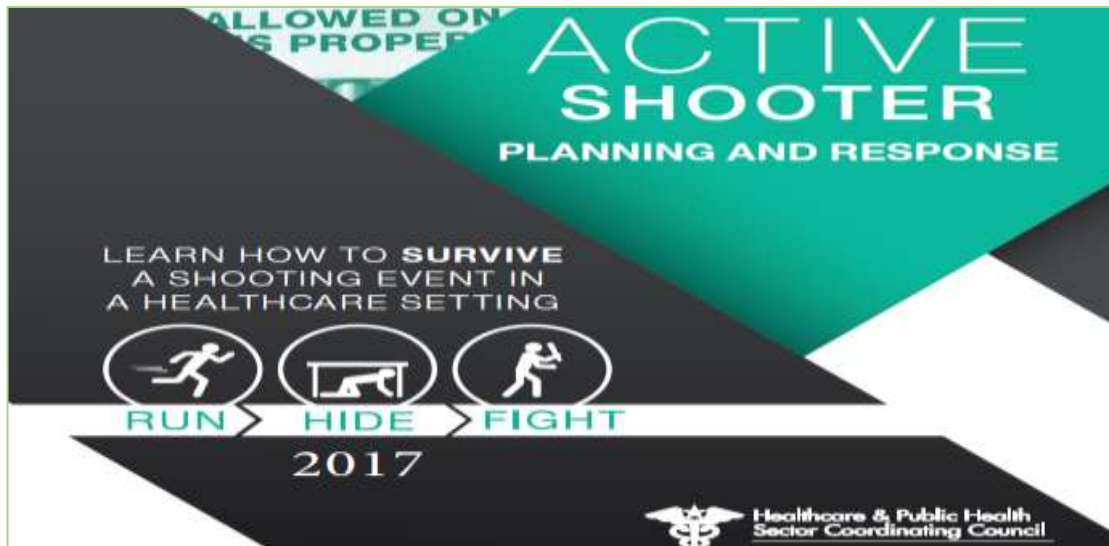
Source: <http://www.floridahealth.gov/programs-and-services/emergency-preparedness-and-response/healthcare-system-preparedness/discharge-planning/documents/%20evac-toolkit.pdf>



Medical Waste

By William A. Rutala, PhD, MPH and C. Glen Mayhall, MD;
The Society for Hospital Epidemiology of America

Source: <https://www.shea-online.org/images/guidelines/med-waste92.pdf>



Welcome to the third edition of Active Shooter Planning and Response in a Healthcare Setting. When our project began in 2013, we knew that while there were resources to address a public active shooter event, there was no guidance to address an active shooter event that occurs inside a healthcare facility. We gathered experts from the public and private sector, and discussed and debated the difficult questions of patient, visitor, and personal safety, duty to act, and abandonment. We also committed to regular updates of this guidance, to incorporate lessons learned, new tactics, and feedback.

This new edition brings additional information on warm zone operations (providing care in an area wherein a potential threat exists, but it is not direct or immediate, law enforcement tactics, unified command, and psychological support.

This guidance was produced and updated by the Healthcare and Public Health (HPH) Sector Coordinating Council (SCC). The HPH Sector Critical Infrastructure Protection (CIP) Partnership brings together leaders in business and government to prepare for and protect against all hazards facing the Sector. The CIP framework focuses on protecting HPH organizations *themselves* during a disaster, so that they may focus on their mission of saving lives. The partnership identifies and prioritizes the most critical elements of the Nation's HPH infrastructure, shares information on risks facing that infrastructure, and implements activities to protect the Sector. The HPH Sector partnership consists of a Government Coordinating Council (GCC) of government partners and the SCC of private sector partners. These two groups come together through two joint working groups and six subsectors to address issues of mutual concern. All

HOSPITAL THREATS

public and private sector members of the HPH Sector with a role in the HPH Sector's homeland security mission are invited to take part in one or more of the joint working groups. More information is available at: <http://www.dhs.gov/critical-infrastructure-sectorpartnerships>

Active shooter events in a healthcare setting present unique challenges: a potentially large vulnerable patient population, hazardous materials (including infectious disease), locked units, special challenges (such as weapons and Magnetic Resonance Imaging (MRI) machines (these machines contain large magnets which can cause issues with firearms, or remove it from the hands of law enforcement), as well as caregivers who can respond to treat victims.

There is no single method to respond to an incident, but prior planning will allow you and your staff to choose the best option during an *active shooter* situation, with the goal of maximizing lives saved. The best way to save lives is to remove potential targets from the shooter's vicinity. We address some difficult choices that will need to be made in this document.

We hope as you read, review, and implement your own plan, you will provide feedback to our team, so this continues to be a living document, providing the latest information and guidance to our healthcare community. Feedback may be sent to scott.cormier@medxcelfm.com. Thank you for all the work you do in keeping our patients, staff, and visitors safe.

We also encourage you to review the healthcare active shooter video produced by the MESH Coalition. MESH, Inc. is an innovative non-profit, public-private coalition located in Marion County, Indiana (Indianapolis) that enables healthcare providers to respond effectively to emergency events, and remain viable through recovery. For more information on the coalition, please use <http://www.meshcoalition.org>.



Active shooter/violent intruder incidents in healthcare settings

Source: <https://www.phca.org/wp-content/uploads/2016/09/Session+NandU+Pigeon+Tues.pdf>

Active shooter in the emergency department: A scenario-based training approach for healthcare workers

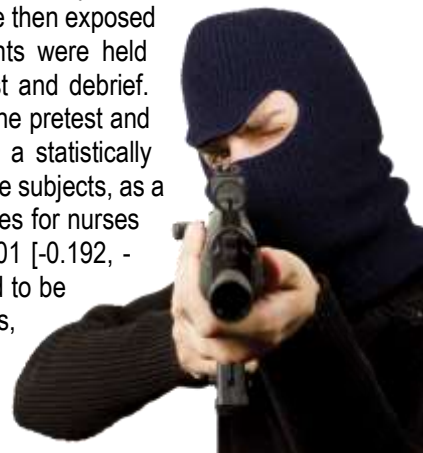
By Joseph G Kotora, Terry Clancy, Lauren Manzon and Mark A Merlin

American journal of disaster medicine. 2014; 9(1):39-51

Source: https://www.researchgate.net/publication/261517596_Active_shooter_in_the_emergency_department_A_scenario-based_training_approach_for_healthcare_workers

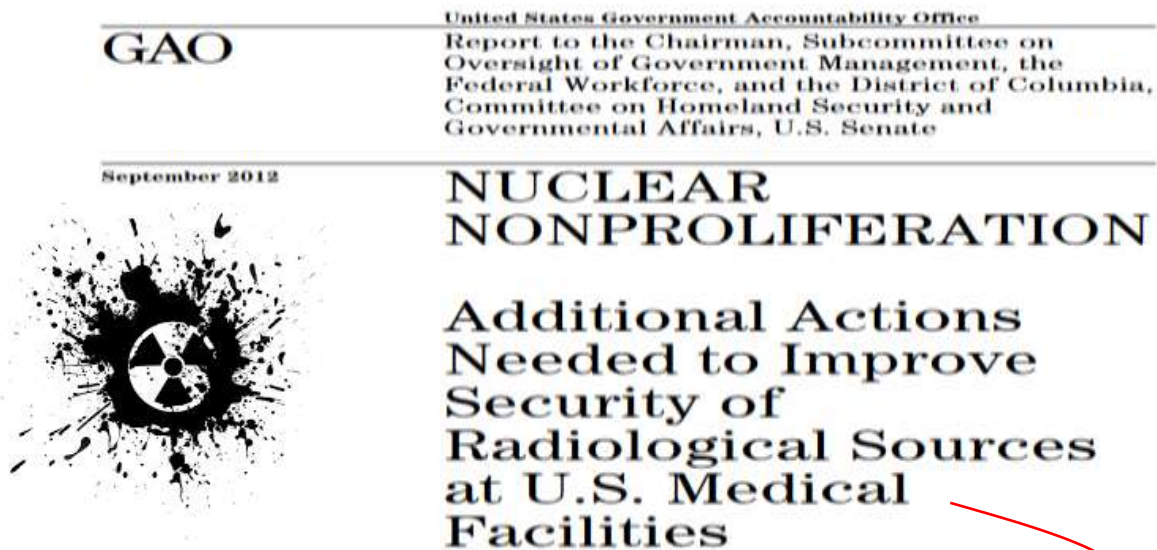
An active shooter in the emergency department (ED) presents a significant danger to employees, patients, and visitors. Very little education on this topic exists for healthcare workers. Using didactic and scenario-based training methods, the authors constructed a comprehensive training experience to better prepare healthcare workers for an active shooter. Thirty-two residents, nurses, and medical students participated in a disaster drill onboard a US military base. All were blinded to the scenarios. The study was approved by the institutional review board, and written consent was obtained from all participants. Each participant completed a 10-item pretest developed from the Department of Homeland Security's IS:907 Active Shooter course.

Participants were exposed to a single active shooter scenario followed by a didactic lecture on hostage recovery and crisis negotiation. Participants were then exposed to a scenario involving multiple shooters. Many of the participants were held hostage for several hours. The training concluded with a post-test and debrief. Paired Student's t-test determined statistical significance between the pretest and post-test questionnaire scores. Paired Student's t-tests confirmed a statistically significant difference between the pretest and post-test scores for the subjects, as a whole ($p < 0.002$ [-0.177, -0.041]). There was no difference in scores for nurses ($p = 1$ [-1.779, 1.779]). The scores for resident physicians ($p < 0.01$ [-0.192, -0.032]) and medical students ($p < 0.01$ [-0.334, -0.044]) were found to be significant. Didactic lectures, combined with case-based scenarios, are an effective method to teach healthcare workers how to best manage an active shooter incident.



HOSPITAL THREATS

A must read report



Source: <https://www.gao.gov/assets/650/647931.pdf>

Hospitals threatened by theft of radiological material

By Greg Freeman

Source: <https://www.ahcmedia.com/articles/78645-hospitals-threatened-by-theft-of-radiological-material>

The Government Accountability Office (GAO) recently issued a warning to hospitals about the risk of the theft of radiological materials, which could be used to make a dirty bomb. Experts caution that the presence of radiological materials in a hospital brings a significant obligation to provide security.

Nearly four out of five hospitals across the country have failed to put in place safeguards to secure radiological material that could be used in a dirty bomb, according to the report, which identifies more than 1,500 hospitals as having high-risk radiological sources. Only 321 of these medical facilities have set up security upgrades, according to the GAO review, which found some surprising lapses of security in 26 hospitals.

At one facility, a device containing potentially lethal radioactive cesium was stored behind a door with a combination lock. The combination was written on the door frame.

The National Nuclear Security Administration spent \$105 million to complete security upgrades at 321 of more than 1,500 hospitals and medical facilities that were identified as having high-risk radiological sources, the report says. The upgrades include security cameras, iris scanners, motion detectors, and tamper alarms.

While it is not known that terrorists have stolen radiological material from hospitals, there have been suspected incidences of "probing" in which criminals seek to determine a hospital's security weaknesses. A series of incidents in 2005, in which people posed as inspectors from The Joint Commission to gain access, was attributed to terrorists planning attacks on hospitals, looking for radiological material, and assessing hospitals' capacity for emergency response.

Hospitals' ability to protect radiological material is likely to vary greatly, says **Bryan Warren**, CHPA, senior manager for corporate security at Carolinas Healthcare System in Charlotte, NC, and president of the International Association for Healthcare Security and Safety in Glendale Heights, IL. Larger hospitals with a robust security program probably have policies and procedures in place that will at least make radiological theft difficult, he says. "But if the plant operations and maintenance people are handling security, they are likely not even aware of the issue, much less acting in a proactive way to protect this material," Warren says. "Unfortunately, being a smaller hospital does not mean you won't have radiological material."

HOSPITAL THREATS

Help is available

Hospitals can improve their radiological security by working with the Global Threat Reduction Initiative (GTRI) in the federal Office of Defense Nuclear Nonproliferation, Warren says. GTRI helps identify, secure, remove, and/or facilitate the disposition of high risk vulnerable nuclear and radiological materials around the world that pose a threat to the United States and the international community. *(For information on contacting GTRI, see the [resource](#) at the end of this article.)*

"GTRI has been working with hospitals for a number of years to help protect any kind of radiological materials so that the bad guys can't get it and turn it into a dirty bomb," Warren says. "Once hospitals are aware of it, they can get a preliminary analysis of their infrastructure to see if they have enough radiological source material to pose a threat, and what they can get through this federally funded program to protect it."

Once a hospital requests assistance, GTRI sends a survey team to a site assessment concerning radiological materials, Warren explains. Most of the resources and assistance are provided at no charge to the hospital. The free aid can include surveillance equipment and other physical improvements to security.

"They also will train your staff and first responders from your local jurisdiction," Warren says. "They will pay for everything to send you to Oak Ridge, TN, for some very intensive training to mitigate the risk at your facility."

More than just high-grade at risk

The GAO report was not surprising to Zachary Goldfarb, EMT-P, CHSP, CHEP, CEM, principal with Incident Management Solutions, a company in Uniondale, NY, that helps hospitals and other organizations prepare for and respond to emergencies. Radiological material in hospitals has been a primary concern for homeland security professionals after the 2001 terrorist attacks, Goldfarb says.

Hospital risk managers should realize that terrorists might be interested not only in high-grade radiological material such as cobalt, Goldfarb says. That type of material is found in fewer facilities, but many hospitals have less radioactive substances that still could be a target, he says.

"For years we've been building scenarios that involve mixing low-level radioactive source material, like medical waste, with a bomb," Goldfarb says. "The real objective of a dirty bomb could be accomplished with low-level medical waste because if any radiation, even at a very low level, were detected after an explosion, it would be the first time for this country. It would create the intended effect of scaring the daylights out of many, many people."

Personal info of 1.5m SingHealth patients, including PM Lee, stolen in Singapore's worst cyber attack

Source: <https://www.straitstimes.com/singapore/personal-info-of-15m-singhealth-patients-including-pm-lee-stolen-in-singapores-most>

July 20 – In Singapore's worst cyber attack, hackers have stolen the personal particulars of 1.5 million patients. **Of these, 160,000 people, including Prime Minister Lee Hsien Loong and a few ministers, had their outpatient prescriptions stolen as well.**

The hackers infiltrated the computers of SingHealth, Singapore's largest group of healthcare institutions with four hospitals, five national speciality centres and eight polyclinics. Two other polyclinics used to be under SingHealth.

At a multi-ministry press conference on Friday (July 20), the authorities said PM Lee's information was "specifically and repeatedly targeted".

The 1.5 million patients had visited SingHealth's specialist outpatient clinics and polyclinics from May 1, 2015, to July 4, 2018.

Their non-medical personal data that was illegally accessed and copied included their names, IC numbers, addresses, gender, race and dates of birth.

No record was tampered with and no other patient records such as diagnosis, test results and doctors' notes were breached. There was no evidence of a similar breach in the other public healthcare IT systems.

HOSPITAL THREATS

Health Minister Gan Kim Yong and Minister for Communications and Information S. Iswaran both described the leak as the most serious, unprecedented breach of personal data in Singapore.

Mr Gan apologised to the affected patients, saying: "We are deeply sorry this has happened."

Mr David Koh, chief executive of the Cyber Security Agency of Singapore, said that "this was a deliberate, targeted and well-planned cyber attack".

"It was not the work of casual hackers or criminal gangs," he added.

In the light of the attack, all of Singapore's Smart Nation plans, including the mandatory contribution to the National Electronic Health Record (NEHR) project - which enables the sharing of patients' treatment and medical data among hospitals here - have been paused.

Specifically, mandatory contribution to NEHR is now on hold until further notice.

Mr Iswaran, who is also Minister-in-Charge of Cyber Security, will [convene a Committee of Inquiry \(COI\)](#) to conduct an independent external review of the incident. Retired district judge Richard Magnus will chair the committee.

Initial investigations showed that one SingHealth front-end workstation was infected with malware through which the hackers gained access to the data base. The data theft happened between June 27, 2018, and July 4, 2018.

SingHealth has imposed a temporary Internet surfing separation on all of its 28,000 staff's work computers. Other public healthcare institutions will do the same.

Unusual activity was first detected on July 4 on one of SingHealth's IT databases. Security measures, including the blocking of dubious connections and changing of passwords, were taken to thwart the hackers.

On July 10, the Health Ministry, SingHealth and the Cyber Security Agency of Singapore were informed after forensic investigations confirmed that it was a cyber attack. A police report was made on July 12.

No further data has been stolen since July 4.

All patient records in SingHealth's IT system remain intact and there has been no disruption of healthcare services.

SingHealth will be contacting all patients who visited its specialist outpatient clinics and polyclinics from May 1, 2015, to July 4, 2018, to notify them if their data has been stolen. An SMS message will be sent to all patients over the next five days.

Patients can also access the Health Buddy mobile app and SingHealth website to check if they are affected by the breach. They can also check [using this link](#).

Mr Iswaran said that "we must get to the bottom of this breach".

"We must not let this derail our Smart Nation services... it is the way of the future," he said, taking a longer-term view of the projects.

Even though a thorough review of Smart Nation projects will be conducted, he stressed that Singapore has paused but not halted these projects.

The Ministry of Health has directed a thorough review of the public healthcare system to improve cyber security, and all public and private healthcare institutions have been advised to take cyber-security precautions.

