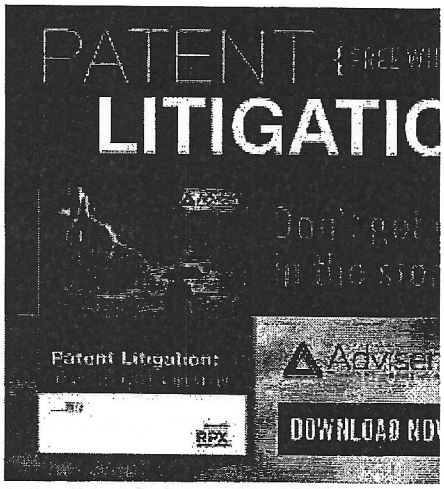
Advisen Healthcare Front Page News - Friday, June 30, 2017

DOWJONES Newswires℠

Cyberattack forces West Virginia hospital to scrap its computer systems

Publication Date: **06/29/2017**
Source: **Dow Jones News Service**
By Melanie Evans



Princeton Community Hospital in rural West Virginia will scrap and replace its entire computer network after being struck by the cyberattack paralyzing computers globally.

The cyberattack, known as Petya, froze the hospital's electronic medical record system early Tuesday, leaving doctors unable to review patients' medical history or transmit laboratory and pharmacy orders, said Rose Morgan, the hospital's vice president of patient care services.

Officials were unable to restore services, and found there was no way to pay a ransom for the return of their system. So, after consulting with the Federal Bureau of Investigation and cybersecurity experts, officials made the decision to replace the system.

Now, doctors, nurses and other hospital staff are adjusting to what will be days of working off paper forms to record vital signs, order medications and scribble notes.

"There is a lot more paper visible up on our units than there used to be," Ms. Morgan said. "It was a bit of organized chaos at first. Now we've hit our stride."

Nurses reverted to two-foot-long paper templates for patient records known as flow sheets, she said.

Employees from human resources and finance, who can't work without computers, have stepped in to ferry doctor's orders from one hospital department to another, deliver prescriptions or shuttle billing records. The pneumatic tubes that typically whisk materials throughout the hospital fell silent in the attack. The tube system is connected to the hospital's computer network.

The Petya attack disrupted operations at major corporations including Merck & Co. and A.P. Moeller-Maersk A/S and at least two other U.S. hospitals owned by the Heritage Valley Health System in Pennsylvania.

Surgeons at the Heritage Valley Hospital in Beaver, Pa., canceled elective surgeries Tuesday and Wednesday, but the Heritage Valley hospitals and emergency rooms remained open.

Heritage Valley continued to make progress restoring its clinical and ancillary care systems Thursday, a spokeswoman said. Regarding whether the system was able to pay a ransom, she said, "Even if we wanted to pay, it is our understanding the [internet service providers] have blocked communication with the attackers."

At Princeton Community Hospital, new hardware will replace existing infected computers and servers. Backup records will be used to restore patient files after technology staff screen the backup files to be sure they aren't infected by the malware, Ms. Morgan said. Officials hope to have the network rebuilt by the end of next week.

It isn't yet known how much it will cost and how much the hospitals' cyber insurance and business-continuity insurance will cover. The nonprofit hospital, which ends the fiscal year on June 30, finished last year with a slim 3.5% operating margin on revenue of $139.1 million.

The cyberattack almost left Princeton Community Hospital without even paper templates, which were stored on a computer file, to be printed. No one could access the file, Ms. Morgan said. Fortunately, her administrative

assistant, Linda Cunningham, had an archive of paper templates that she had printed and saved in a binder, Ms. Morgan said.

Doctors and nurses continued to care for more than 100 patients who were being treated in the hospital Thursday, according to Ms. Morgan. Surgeries continued as scheduled. Four uninfected computers can access the hospital's electronic medical record data using an uncompromised guest network, but the records can only be viewed, she said.

The emergency room continued to accept patients with life-threatening conditions, but diverted other ambulances between Tuesday morning and Thursday morning.

The emergency room reopened to all patients Thursday morning, Ms. Morgan said.

Write to Melanie Evans at Melanie.Evans@wsj.com

Advisen Healthcare Front Page News - Thursday, May 25, 2017

How ECMC got hacked by cyber extortionists

Publication Date: **05/20/2017**
Source: **Buffalo News (NY)**

May 20--It was 2 a.m. Palm Sunday. Computer screens across Erie County Medical Center flashed white with bright red words: "What happened to your files?"

The ransom demands began with hot pink text.

"Step1: You must send us 1.7 BitCoin for each affected PC OR 24 BitCoins to receive ALL Private Keys for ALL affected PC's."

Hackers had encrypted the hospital's files and wanted the current equivalent of $44,000 to provide a key to unlock them.

By 3:30 a.m., the medical center, while still assessing the damage and risks to private patient information, had shut down all its computer systems as a precaution.

It was a potentially crippling move that forced one of the region's major healthcare institutions to go low-tech.

Now, after six weeks of around-the-clock efforts to reconstruct its systems, ECMC is closer to normal operations. Officials say no patient data was compromised. But the cyberattack left a lasting impression, magnified by a growing epidemic of computer attacks, including the global ransomware extortion that disabled hundreds of thousands of computers this month.

"What's happening is a form of terrorism like an attack on critical infrastructure," said Thomas Quatroche, president and chief executive officer of the 602-bed hospital and 390-bed long-term-care facility on Grider Street. "It's a call to action to view cybersecurity the way we do law enforcement, to raise the profile of the issue."

The medical center follows a protocol for computer issues and uses regular downtimes for parts of its system to practice. But no one expected a disruption as long or extensive as this.

ECMC's network would go dark for weeks. But in the hours after the attack, hospital managers had a decision to make: Should they pay the ransom?

The morning of the attack

By 5:30 a.m., the hospital called in cybersecurity consultant GreyCastle from Troy and worked to notify top managers.

"For the first few minutes when I learned what happened, I was in a state of disbelief," said Dr. Jennifer Pugh, associate chief of service for emergency medicine. "Then my reaction changed to anger. This is our Level 1 trauma center. It felt like a direct attack."

Quatroche assembled his management team by 9:30 a.m. to organize a response.

"My first thought was to let people do what they have to do. We needed to identify what was going on and get going using paper," he said.

Many businesses quietly pay ransoms. But one of the first decisions made at ECMC, with advice from GreyCastle and law enforcement authorities, was to refuse to do that.

Among the reasons:

ECMC had access to a tape backup to restore files, as well as HealtheLink, the regional system for sharing health information electronically among hospitals and doctors. The hospital outfitted critical departments, such as the emergency room and intensive care, with borrowed laptops with ad hoc internet access. Through HealtheLink, doctors and nurses could view patient records that existed up to the date of the attack.

Officials also voiced concern that the perpetrators might not provide the key after getting the money. And even with a key to decrypt the system, how could they be certain everything was OK?

"A part of it also was about the integrity of the organization," said Quatroche, acknowledging that the hospital will likely bear a high cost for recovering from the ransomware attack.

He said ECMC increased its cybersecurity insurance coverage in November and, in the context of the small margins generally of hospitals in New York State, remains in a good position financially -- with stable patient volumes and a balance sheet about $2 million ahead of expectations for the year as of March.

"Whether to pay or not is a very individual thing," Quatroche said. "If you have no backup, you have no choice."

A week earlier

Ransomware commonly spreads by conning a person to click a link or download an email attachment that looks like a message from a friend or institution, such as a bank requesting verification of a password. Attackers also search the internet for vulnerabilities -- systems without updated software security patches, for instance.

This case was different. Officials believe hackers used an automatic program that anti-virus software could not recognize to exploit a hospital web server accessible remotely that should have been configured differently to prevent an incursion. The hackers then applied "brute force" computing -- trying millions of character combinations to identify a relatively easy default password to gain entrance into the hospital's system.

Officials believe the hackers randomly accessed the ECMC server about a week before the ransom notes arrived using a variant of ransomware known as SamSam.

Once they had breached the perimeter, it's believed a person then logged in and manually searched files. The intruders then encrypted files in a way that made it more difficult to recover data before they issued the ransom note.

"This attack was in our top 10 percent in terms of sophistication, and the manual intervention with someone poking around was unusual," said Reg Harnish, chief executive officer of GreyCastle Security, the Troy cyber-security consultants hired to assist the hospital.

SamSam, which targets vulnerabilities in servers to infiltrate computer networks, is responsible for other attacks, including a major ransomware incident last year at 10-hospital Medstar Health in Maryland.

Harnish said he does not believe the hackers knew they had hit a large hospital until they searched ECMC files and, after discovering the business of their victim, demanded more money than typical in ransomware attacks.

The decision not to pay the ransom came quickly on April 10. Restoring the system, computer-by-computer, would take weeks.

After the attack

In its response, ECMC turned back to paper charts and face-to-face messaging -- easier said than done in any modern hospital that has come to rely on a complex array of integrated computer systems to run every major aspect of the organization, from patient records and communications to bed tracking and image archiving to lab reports and finances.

Quatroche said the hospital managed the crisis with changes that proved bumpy at times and foreign to many staff members too young to have experienced work life before the internet age.

"Our people were tested, and it blew me away. They have been resourceful, and have rallied around each other and the patients," he said. "There also was a silver lining in that we learned that having administrators do rounding through the hospital is something we need to do more of in the future."

According to a timeline provided by ECMC officials, here is how the restoration unfolded in the weeks after the ransom notes first surfaced on Sunday, April 9:

* April 10: The hospital began to obtain laptops, some of them from the Kaleida Health hospital system. The roll out started with the emergency department and critical

care, and included wireless hot spots to access the Internet.

* April 19: The attack affected more than 6,000 computers at the hospital, all of which had to be wiped clean and re-distributed in phases starting on this day, with the emergency department and critical care areas given priority. The computers worked in view-only mode.

* May 5: Doctors could begin to upload their progress notes into the electronic medical record. Nurses in the emergency room could do electronic documentation again.

* May 8-10: Computer-order entry worked again, initially in the emergency department, allowing physicians to communicate with radiology, the lab and other departments. Desktop computers continued to return to their stations.

* May 12: Electronic prescribing came back online.

Harnish praised ECMC's response and characterized its cybersecurity as similar to the average hospital, but noted that just about every business needs to step up efforts to prevent attacks from increasingly resourceful criminals.

"There was nothing negligent or out of the ordinary," Harnish said. "They quickly identified the issue and escalated. That was important. They had done disaster preparedness. There was muscle memory, and people worked well as a team to deal with this instead of finger-pointing."

The identity of the perpetrators, who can easily mask their computer activity, remains unclear, according to ECMC officials. An investigation traced the ransomware to computer connections in such countries as Brazil and the Netherlands, but hasn't determined a point of origin.

What happened at ECMC reflects a global ransomware crisis. On average, more than 4,000 ransomware attacks have occurred daily since Jan. 1, 2016, disrupting hospitals and businesses, a 300 percent increase over the approximately 1,000 attacks per day in 2015, according to the FBI.

Weeks later

In addition to GreyCastle, ECMC has received assistance from an assortment of computing firms, including Microsoft, Cisco, Symantec and Meditech, its electronic medical record vendor. ECMC staff came in on their days off. Information technology personnel from Kaleida Health and the Catholic Health system also helped.

Officials said they expect most systems to be running normally later this week, although work remains to be completed in outpatient clinics.

The focus on the emergency department reflects its importance. More than 80 percent of ECMC's admissions come through the emergency room, and it serves as the region's Level 1 trauma center for adults badly hurt in motor vehicle crashes, industrial accidents and acts of violence.

The emergency department never went on diversion to send patients elsewhere. As in other areas of the hospital, doctors, nurses and other staff found workarounds.

They charted patients on paper, information that will have to be entered eventually into the electronic medical record. They viewed X-rays on old light boxes instead of computer screens. Clerical staff ferried samples and reports back and forth to the lab.

"It was like a blast from the past," said Pugh.

New York State required electronic prescribing in 2016, so some veteran doctors brought in their unused paper prescription pads from home. ECMC rushed an order of stamps for other doctors to use on generic prescription pads.

"One of the key things that got us through this is we have a plan in place and we practiced," Pugh said.

The aftermath

The attack highlights the risks of a connected world.

"This is a people problem, not a technological one," said Harnish, referring to the fact that most incidents arise from inadvertently introducing malicious software into a computer through a scam email. "We want things to be easy and fast. But we also need to develop a culture of security to minimize those risks."

William Pelgrin, co-founder of CyberWA, a security consultant, said organizations must adopt "good cyber hygiene," routinely taking such steps as using strong passwords, backing up data and limiting access to networks.

There is no way to guarantee 100 percent protection, but individuals and businesses can improve the defenses in their control, he said.

"Security is not just for the IT department. We all have a responsibility, and should be held accountable," said Pelgrin, also a co-founder of the Global Cyber Alliance and former president of the Center for Internet Security.

Quatroche said one of the lessons learned is that hospitals like ECMC must alter their thinking about cyber security. Among other steps, the medical center plans to tighten access to the internet.

"Technology is important," Quatroche said. "But there is a tradeoff between convenience and security that requires people to work differently."

Advisen Healthcare Front Page News - Thursday, September 28, 2017

Ransomware in health care: An insurance-based analysis

Publication Date: **09/26/2017**

Source: **Mondaq Business Briefing**

By Ms Kristen Psaty and Christina Terplan

The medical field recognizes a standard pre-procedure verification process called a "time-out" that occurs prior to any invasive procedure requiring patient consent. This is an element of the Universal Protocol and includes a deliberate pause in activity among all members of the treatment team and a checklist review of patient demographic information, medical history, and medical procedure details. The Universal Protocol has been a mandated practice in all hospitals accredited by the Joint Commission since 2004.1 It is formally endorsed as an industry best practice, with National Time-Out Day recognized annually at the behest of the Association of Perioperative Registered Nurses2 with support from the World Health Organization.3 The standard procedure is mandated as a way to prevent egregious medical errors, including wrong person or wrong procedure surgery.

Compliance with the time-out procedure is dependent on the health team's access to patient medical records. Increasingly, patient medical records are created, stored, and accessed by medical professionals in electronic form. In fact, in 2015, 87 percent of all U.S.-based physicians reported use of electronic medical records (EMRs).4 An EMR is a digital version of a patient medical chart containing a patient's medical history, including

information on patient allergies, current medications, lab results, and diagnosis, as well as basic demographic information, including home address, personal phone number, and personal point of contact information.5 A patient EMR might also include details such as medical diagnoses, date of birth, and Social Security number.

Exploiting Extreme Duress: The Explosion of Ransomware in the Health Care Field

Imagine, then, you are a physician administering care or a surgeon preparing to operate when suddenly your health care facility's computer systems become inaccessible. This scenario, which is becoming increasingly common, was the case in recent global ransomware attacks, Petya and WannaCry, in which attackers were able to specifically exploit a vulnerability in Microsoft Windows software.6 Ransomware is frequently installed when a user clicks a URL link or opens an attachment sent via email from a malicious threat actor. The ransomware then encrypts device files on both computer devices and entire networked servers, making them inaccessible to users, including health care professionals who require access to provide patient care.

The WannaCry attack struck more than 30 facilities in England's vaunted National Health Service.7 The immediate result was chaos. Physicians and staff had to put together and store makeshift files with paper and pen, and some hospitals told patients not to come to emergency centers unless their conditions were urgent.8 In Jakarta's Dharmais Hospital, Indonesia's biggest cancer center, hundreds of people packed waiting areas, unable to receive treatment as a result of the WannaCry ransomware incident.9 In India, EMRs in the state-run Berhampur City Hospital were encrypted by WannaCry, seriously disrupting e-medicine services.10 In the United States, the Petya virus affected health care, hitting Heritage Valley Health Systems, a Pennsylvania health care provider, and its hospitals in Beaver and Sewickley, Pennsylvania, and forced operations to be canceled.11 Also in the United States, for the first time on record, there were even several reports, acknowledged by device manufacturers, that the WannaCry malware had infiltrated connected, Internet of Things (IoT) hospital medical devices and rendered them inoperable.12

Business email loss accompanying ransomware. Successful ransomware attacks often include a human

element. As a result, ransomware has become embedded in an accompanying phishing-threat landscape.13 Ransomware phishing emails contain a malicious link or file that attackers must induce recipients to click or open in order to unleash the accompanying ransomware.14 Increasingly, these attacks rely on soft targeting by functional area. In contrast to broadly disbursed email scams, soft targeting focuses on a category of individuals based on their role within an organization.15 Furthermore, these can even include attacks specifically tailored to and directed toward specific employees.16

One plausible ransomware scenario also includes additional business email loss arising from a fraudulent wire instruction request. For example, an email might arrive from an individual pretending to be a vendor of the hospital, requesting that future payments be transferred to a new account number. In a soft-targeted phishing attack, a threat actor would create an email resembling an email from the accounting manager of the vendor and send a request to the hospital accounting department coordinator, requesting that the wire transfer information be updated administratively, perhaps explaining that the vendor was consolidating accounts, and including an attachment with the new account information. The authenticity of these fraudulent wire request emails can appear deceptively convincing due to spoofed email domains, replicated signature lines and letterheads, and other personal details gathered in online research. Accordingly, an unsuspecting hospital staff person may open the attachment and change the payment destination so the next time a payment from the hospital is transferred, be it a few hundred or several million dollars, it falls into the hands of cyber thieves.

From an insurance coverage perspective, this type of phishing loss is complex and unsettled, frequently leaving room for coverage gaps under many policies. While these losses often resemble traditional theft of property, crime and bond insurers have contested coverage for the payment amounts because they result from the "authorized" acts of unsuspecting employees.17 Computer-fraud coverage has similarly been contested. Most recently, the U.S. District Court for the Northern District of Georgia held in a decision related to computer fraud coverage, *InComm Holdings, Inc. v. Great American Insurance Co.*, released on March 16, 2017, "That a computer was somehow involved in a loss does not establish that the wrongdoer 'used' a computer to

cause the loss. To hold so would unreasonably expand the scope of the Computer Fraud Provision, which limits coverage to "computer fraud." The court, which accepted Great American's declination of coverage in a loss scenario that included an exploitable coding error in the insured's computer systems, further explained that "[l]awyerly arguments for expanding coverage to include losses involving a computer engaged at any point in the causal chain—between the perpetrators' conduct and the loss—unreasonably strain the ordinary understanding of 'computer fraud' and 'use of a[ ] computer.'"18 The *InComm Holdings* court cited another recent decision from the U.S. Court of Appeals for the Fifth

Circuit, *Apache Corp. v. Great American Insurance Co.*, which also found that the mere use of computers in the business email loss fraud was insufficient for computer fraud coverage. The court reasoned that computer fraud coverage, which required that the covered loss result "directly from the use of any computer to fraudulently cause a transfer," did not apply because a computer was but one step in a process leading to the authorized payment to fraudulent accounts.19 Business email loss coverage falls short in other areas as well, including forgery coverage. In a loss scenario where an accounting firm employee received a phishing email requesting a $94,280 wire transfer of client funds to a Malaysian bank, the Ninth Circuit upheld a denial of forgery coverage under a "forefront portfolio policy," finding that "[u]nder a natural reading of the policy, forgery coverage only extends over the forgery of a financial instrument."20 The court reasoned in its March 9, 2017, decision in *Taylor & Lieberman v. Federal Insurance Co.*, "Here, the emails inducting [the insured] to wire money were not financial instruments like checks, drafts and the like."21

However, specific coverage for this type of business email loss is becoming available from some carriers as an endorsement to cyber insurance policies.22 This coverage may be found under certain types of cyber crime endorsements to cyber policies, and it can include coverage provisions for financial fraud or phishing attacks. These policies provide for loss, including public relations expenses, arising from the insured's receipt of misleading or deceptive communication from a third party purporting to be an employee, client, or vendor of the insured, directing or requesting a transfer of funds.

Rise of cyber policies. Since 2000, the U.S. cyber insurance market, developed in response to Internet- and privacy-based loss, has grown from about 10 insurers providing stand-alone cyber insurance policies to at least 50.23 These stand-alone cyber insurance policies provide specialized first-party and third-party coverage for loss arising from coverage events such as computer security failure, data breaches, and other cyber incidents. Sales of these policies are projected to grow exponentially, with annual gross written premiums expected to increase from $2.5 billion to $7.5 billion in the next three years.24 The quick development and relative immaturity of the cyber insurance marketplace has resulted in a lack of uniformity among policies and a wide range of available coverage.25 Compounding these variables is the swift and relentless evolution of cyber loss, resulting in uncertainty about future exposure in stand-alone policies and a climate ripe for potentially contentious coverage disputes.26

Ransomware and Cyber Coverage

Despite the unsettled coverage arising from business email loss, many cyber policies contemplate the specific losses arising from ransomware and the ensuing fallout. Once the unsuspecting hospital employee clicks the malicious attachment sent by the hypothetical vendor, a catalyst for ransomware infection has been initiated, unrolling a multitude of complex and potentially contentious issues within the context of cyber insurance coverage. The use of ransomware enables cyber pirates to extort ransom fees from organizations by holding data "hostage" in exchange for payment. There is evidence that hospitals are increasingly becoming the target of ransomware attacks.27 Indeed, the health care industry was the second-most targeted sector for ransomware attacks, comprising 15 percent of total reported incidents in 2016.28

Extortion demand coverage and limitations. In the immediate wake of a ransomware attack, a health care facility must first grapple with whether or not to pay the extortion demand. Factors many entities must consider include the amount of the demand, the type of ransomware involved, and the accompanying reasonable or demonstrated likelihood that the threat actors involved will provide the encryption key if paid. Also included is the type of information rendered inaccessible and the relative importance of the information to critical health care

functions. The ransom, typically demanded in Bitcoin, a form of decentralized digital cryptocurrency, is usually a relatively small amount. For example, the 2017 WannaCry ransomware demand remained below $600,29 while the demand paid in 2016 by the Hollywood Presbyterian Medical Hospital reached $17,000.30

Currently, cyber extortion payment coverage is an available option under many insurers' cyber policies. This coverage includes payment of the ransom demand amount and, in some cases, also provides assistance in procuring the Bitcoin necessary to complete the ransomware transaction. Service-oriented cyber insurance policies have immediate response programs integrated into coverage, mobilizing computer consultants skilled at negotiating with cyber extortionists and experienced with converting large quantities of capital into Bitcoin necessary to effectuate extortion payments. Acquiring large amounts of Bitcoin, unlike traditional currency, is often difficult given the distribution and mining constraints on the cryptocurrency. Accordingly, some companies are beginning to keep reserves on hand in case of future ransomware attacks.31 Still, the decision to pay a demand can be a complex one and is frequently constrained by many elements of the policy.

Many cyber policies contain provisions excluding loss, such as a cyber extortion payment, arising from acts of terrorism or foreign enemies. Attribution of cyber attacks is generally very time-intensive and costly but not impossible. Attribution scenarios might also include attacks voluntarily claimed by terrorist groups or hacktivists. Other cyber extortion coverage constraints include sub-limits of coverage, extortion demand-to-damage ratio of loss thresholds, and specialized reporting provisions. As the Internet continues to become the forum for friction across geopolitical lines, it is conceivable that cyber coverage disputes over terrorism exclusions may arise.

If a hospital decides not to pay the extortion demand, it will likely incur extensive data recovery costs to regain access to information, including patient EMRs. Many cyber policies also include coverage for a hospital's costs to restore or re-create information contained on encrypted files as a result of a ransomware attack. The cost to restore such data is dependent on hospital information backup procedures; however, oftentimes these costs are

exponentially higher than the ransom demand and take valuable time.

Covered breach response costs. Whether or not a hospital elects to pay the ransom amount, it will ultimately have to handle the issue of data breach response and attending legal obligations. Due to the large amounts of sensitive information usually handled by the health care industry, these costs can quickly add up, totaling $6.2 billion in the United States annually.32 Fortunately, many cyber policies contain standard breach response coverage provisions.

Typically, immediate computer forensic investigation is necessary to determine the details of the incident and the scope of information affected. This involves conducting a thorough analysis to piece together what computer events transpired, who was involved, and the relative timeline of events to make a breach determination.33

Also critical to the breach response phase is the help of privacy legal counsel to determine the extent of reporting obligations facing a health care institution. At the federal level, the U.S. Department of Health and Human Services has given guidance to entities covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA),34 including hospitals and health care facilities, stating that ransomware incidents should be treated as a security incident for response and reporting purposes.35 Depending on the residency of affected patients, a health care facility may also be required to comply with the disparate and evolving body of state-level breach laws now implemented in 48 states, with the most recent addition of New Mexico's state breach laws on the books in May 2017.36 State laws have widely differing notice obligations and requirements. Most states offer a safe harbor that does not require reporting of encrypted data. However, effective July 1, 2016, Tennessee's breach notice definition was amended to include the loss of not only unencrypted data but also certain types of encrypted data, subject to complex technical encryption protocol thresholds.37 Understandably, the costs to evaluate and respond to breach notice requirements for a health care facility, especially a regional or specialized treatment facility with patients from different states, can quickly add up. These types of computer forensic and privacy legal breach investigation fees are typically eligible as covered costs under available stand-alone cyber policies.

In the likely event a health care institution is under a breach notification obligation, which involves informing all individuals (including patients, employees, patient emergency contacts, and anyone else whose personal health or sensitive information had been compromised, depending on the jurisdiction) and the amount and type of information involved, stand-alone cyber policies first-party coverages will also typically include coverage for notification costs. Notification costs, which averaged $560,000 per health care breach incident in 2016, often include fees for printing and mailing notice letters to individuals—many applicable health care breach statutes mandate breach notice by mail, as well as setting up temporary call centers to respond to or answer questions from notified individuals about the incident.38 Coverage for costs to enroll affected individuals into credit or identity theft monitoring programs, as is sometimes mandated by law, is also not uncommon among typical coverage portions of cyber policies. While this coverage is generally helpful in responding, further repairs and fallout can prove costly as well.

Business interruption loss—A complicated analysis in a health care scenario. According to the 2016 Cost of a Data Breach Study by IBM and the Ponemon Institute, a health care facility suffers an average of $113 million in lost revenue per reported data breach.39International law firm DLA Piper, which experienced at least 10 days of information technology disruption as a result of WannaCry in June and July of 2017, is already estimated to have suffered millions in business interruption.40 Stand-alone cyber policies also typically provide coverage for business interruption loss. Business interruption coverage generally compensates a breached entity for lost income and extra expenses incurred as a result of a computer or technology interruption, as might accompany a ransomware incident.

This coverage varies greatly between different insurers' cyber policies. Some models include a waiting period that typically requires substantial disruption for a requisite number of hours—waiting periods in the range of 8–12 hours are common. Under this approach, coverage is available only for business interruption events that extend beyond the waiting period. Accordingly, if a hospital has a 12-hour waiting period and its computer systems were affected by an attack for only 10 hours, then the business interruption coverage would not be triggered. Other models use a monetary scheme that requires a

quantifiable loss in excess of some fixed amount before coverage kicks in. Still other models use both a waiting period and a monetary retention.

In a hospital ransomware scenario, business interruption coverage is difficult to calculate. The loss that is easiest to establish arises from the hospital's own commercial activity. For instance, the lost revenue of hospital operation sub components, such as the hospital cafeteria or gift store, may be easy to demonstrate.

More difficult calculations might include loss resulting from temperature-controlled medication spoilage as a result of electronic-temperature monitoring disruption arising from a computer security incident. Other loss arising from a hospital's inability to take in new patients during a ransomware scenario or loss affecting a nonprofit hospital is similarly difficult to account for.

Costly fallout. Further fallout includes class action costs to respond to third-party privacy claims and resulting settlements. The largest data breach settlement in history has recently been agreed to for $115 million dollars. This was in response to a cyber attack of health insurer Anthem Inc., resulting in the theft of the personal information belonging to 78 million health plan members.41 In addition, some policies can include special provisions for costs associated with regulatory investigations or penalties.

Looking Forward—Connected Health Care Devices and the Shifting Scope of Exposure

There is an increasing number of Internet-connected end points being introduced into the hospital environment as part of the Internet of Things (IoT) expansion, potentially further complicating cyber coverage analysis as it pertains to hospital ransomware scenarios. These medical devices include things like Internet-connected bandages capable of detecting blood clots, talking thermometers, and automated infusion pumps that deliver medication or nutrients.42 Many believe malicious actors responsible for health care cyber attacks will increasingly look to exploit the vulnerabilities associated with these connected devices.43 WannaCry ransomware resulted in encryption of medical devices, rendering Bayer Medrad radiology equipment inaccessible to health care professionals. A Bayer spokesperson confirmed that it had received at least two reports from customers in the

United States of Windows-based device-level ransomware, noting that operations at both sites were restored within 24 hours.44 The success of medical device encryption may be a watershed moment for the health care threat landscape and the attending cyber insurance policies involved.

The first potential area of contention related to IoT medical device loss includes the scope of defined terms; namely, whether networked devices are part of a health care facility's computer systems for purposes of cyber coverage. The definition and scope of computer systems, if construed to include connected devices, could open coverage up to medical device interruption. If the devices are not found to be part of a hospital's computer systems, they may be challenged as part of the hospital's network for purposes of recovering in the event of a cyber disruption.

Second, the use of connected medical devices will likely further complicate business interruption analysis. For example, some connected devices may derive primary value from their ability to generate medical data. These devices enable wireless transfer, storage, and display of clinical data, which may have value to a hospital in a variety of ways, including for grant purposes, research use, or even direct sale.45

Finally, third-party claims will presumably become more complex as a result of enhanced hospital connectivity. Namely, claims related to the negligent provision of patient medical care as a result of technology business interruption could conceivably arise. It is important to note that many cyber insurance policies include provisions excluding loss arising from bodily injury. However, as medical devices and care become more interconnected, it is easy to imagine a paradigm in which the responsibility to provide adequate patient care extends beyond physicians to include, to some degree, hospital information technology staff. For example, hospitals can be held liable for medical equipment failure under various theories. Hospitals can be liable for negligence or medical malpractice if they fail to maintain medical equipment properly. Likewise, hospitals can be liable for failure to properly train their personnel in using the equipment. If the failure to properly train personnel in using medical equipment leads to the negligent operation of the equipment, the hospital may be liable. Moreover, in the future, if the network that the connected devices operate

on is not properly maintained, perhaps negligence and even malpractice within the scope of network security will arise, separate and apart from failure to maintain the medical equipment itself.

This type of loss might ultimately challenge the relevant exposure under the network security coverage provided by cyber policies. One example might include a cause of action for medical negligence or malpractice against hospital information technology staff. For example, in 2015, the U.S. Food and Drug Administration issued a safety communication, warning of cyber security vulnerabilities present in certain IoT- connected drug infusion pumps, resulting in the discontinuation and market recall of the device.46 The pumps were directly related to patient care and could have put a patient at physical risk if tampered with. On the other hand, if the vulnerabilities had not been present in the drug pump, but were instead in the hospital's internal network, it is plausible that the facility could have faced allegations that the physician and the information technology staff are, to some degree, both responsible for providing care. More imminently plausible, however, are cases involving poor patient care resulting from an inability to access necessary patient medical records.

Conclusion and Recommendations Proposed preventive measures.

Although the insurance market has quickly grown up around stabilizing the toppling effects of current cyber threats, including the robust coverage for contemplated ransomware loss, hospital ransomware scenarios are too serious and too egregious not to warrant specific preventive concern. As the recent string of ransomware attacks affecting hospitals worldwide has proved, ransomware affecting health care facilities effectively renders health care facilities unable to provide adequate patient care, targets vulnerable populations, induces chaos, and exploits a medical facility for payment, capitalizing on extreme duress. Solutions to stop this from happening must be advanced on a variety of fronts.

Internally, hospitals must take precautionary measures. One measure might involve warning vulnerable employees of soft-targeting threats and ensuring that checks are in place to prevent business email loss, investing in robust information security programs and implementing emergency backup plans. Future

responsibility to safeguard patient data may ultimately fall on health care providers as well. The Universal Protocol may require an amendment to require a "click-through step" related to ensuring patient electronic information safety.

Innovative approaches may also be necessary, including solutions from the technology sector such as physician keychains that store critical health information for patients currently being treated on backed-up devices that would be secure in the event of a ransomware attack.

Support from legislators and policy makers must also be enlisted to bolster cybersecurity. Collaboration between private and public sector stakeholders on threat-information sharing initiatives is a critical step. Developing information- sharing ecosystems, like nonprofit Information Sharing and Analysis Centers (ISACs), enables computer network owners to protect their facilities from cybersecurity threats.47 In addition, encouraging secure software construction through liability or penalties may be worth exploring. Today, the costs of insecure software, like the Microsoft Windows software exploited by WannaCry and Petya, are not borne by the vendors that produce it. Instead, these manufacturers are incentivized for quickly putting new features and operating systems into the market place every year.48 Allocating incentives, assessments, or some relative degree of liability to software manufacturers, who are best situated to address software security issues up front, could result in more secure software rollouts or the development of more robust software update processes.

Still, these measures are only best to prepare for and respond to egregious health care distress. Action to deter these extortion scenarios is also necessary. Consider the human impact, such as the experience of a 61-year-old man, due to undergo major heart surgery after months of waiting, left distraught when the WannaCry attack suspended medical treatment at his operating facility.49 A 50-year-old man, whose cancer treatment surgery was also canceled due to WannaCry said of the cyber pirates, "They should be hung, drawn, and quartered."50

Relevant deterrent penal measures to counteract hospital ransomware might include legislation based on either strict liability or criminal intent. Legislation could mandate strict liability penalties based on the type of information encrypted, such as EMRs or other specific types of personal health information, in an effort to deter hospital

ransomware. Additionally or alternatively, threat actors knowingly or purposefully soft-targeting hospitals with phishing and ransomware could be subject to criminal enhancement statutes. This type of legislation might be similar to gang enhancement legislation adopted in an effort to condemn especially reckless or dangerous behavior.51 As difficult as identification, prosecution, and enforcement of cyber crime may be, the existence of strict penalties may serve to deter the rise in health care targeting and send a strong signal that health care targeting, which impacts people, communities, and public health, is not acceptable.

Footnotes

1 Joint Comm'n, Universal Protocol for Preventing Wrong Site, Wrong Procedure, Wrong Person Surgery.

2 Press Release, Patient Safety Monitor, The Association of Perioperative Registered Nurses (AORN) Is Sponsoring National Time-Out Day June 23 to Highlight the Importance of Taking a Time Out Before Beginning a Surgical Procedure to Verify That the Procedure, Patient, and Site Are Correct(June 23, 2004).

3 World Alliance for Patient Safety, WHO Surgical Safety Checklist and Implementation Manual(World Health Org. 2008).

4 Practice Fusion, HER Adoption Rates: 20 Must-See Stats, Mar. 1, 2017.

5 HealthIT.gov, What Is an Electronic Medical Record (EMR)? (Sept. 22, 2016).

6 "Hospitals Increasingly Targeted by Ransomware," *Security*, Dec. 15, 2016; Nicole Perlroth, Mark Scott & Sheera Frenkel, "Cyberattack Hits Ukraine Then Spreads Internationally," *N.Y. Times*, June 27, 2017.

7 Frank Langfitt, "British Hospitals Among Targets of Global Ransomware Attack," *Nat'l Pub. Radio*, May 12, 2017.

8 Frank Langfitt, "British Hospitals Among Targets of Global Ransomware Attack," *Nat'l Pub. Radio*, May 12, 2017.

9 Jeremy Wagstaff, Reuters, Channel NewsAsia, May 15, 2017. http://www.channelnewsasia.com/news/singapore/wannacry-ransomware-attacks-hard-lessons-for-some-victims-8849716.

10 "City Hospital System Down, Officials Fear 'WannaCry' Attack," *Z News*, May 17, 2017; Chanchal Chauhan, "WannaCry Ransomware Attacks Berhampur City Hospital in Odisha; Demands $300," *India.com*, May 17, 2017.

11 Nicole Perlroth, Mark Scott & Sheera Frenkel, "Cyberattack Hits Ukraine Then Spreads Internationally," *N.Y. Times*, June 27, 2017.

12 Radiologysolutions.bayer.com, Information Technology Advisory—WannaCry Ransomware (May 26, 2017).

13 PhishMe, Q1 2016 Malware Review (registration required).

14 Fed. Bureau of Investigation, Public Service Announcement, Ransomware Victims Urged to Report Infections to Federal Law Enforcement (Sept. 15, 2016).

15 PhishMe, Q1 2016 Malware Review (registration required).

16 Mark Camillo, "Cyber Risk and the Changing Role of Insurance," 2 *J. Cyber Pol'y* 53–63, Mar. 27, 2017 (published online).

17 Alice Kyureghian, Benjamin Fliegel, Christina M. Shea& J. Andrew Moss, Reed Smith Client Alerts, Phishing in the Insurance Coverage Gap (Feb. 15, 2017).

18 David S. Wilson, John Tomaine & Chris McKibbin, "InComm: U.S. District >Court Holds That Computer Fraud Coverage Does Not Respond in Prepaid Debit Card Scheme," *Blaney's Fidelity Blog* (Blaney McMurty LLP), Mar. 22, 2017.

19 David S. Wilson & Chris McKibbin, "Apache Corporation: Fifth Circuit Holds That Commercial Crime Policy's Computer Fraud Coverage Does Not Extend to Social Engineering Fraud Loss," *Blaney's Fidelity Blog* (Blaney McMurty LLP), Oct. 24, 2016.

20 Judy Greenwald, "Chubb Not Liable for Accounting Firm's Fake Email Loss," *Bus. Ins.*, Mar. 10, 2017.

21 Judy Greenwald, "Chubb Not Liable for Accounting Firm's Fake Email Loss," *Bus. Ins.*, Mar. 10, 2017.

22 Kevin LaCroix, "The Growing Risk of Payment Instruction Fraud and Related Insurance Coverage Problems," *D&O Diary*, Apr. 10, 2016.

23 Yoav Leitersdorf, Ofer Schreiber & Iren Reznikov, "Cyber Insurance Is Changing the Way We Look at Risk," *Tech Crunch*, June 13, 2016.

24 PricewaterhouseCoopers, Insurance 202 & Beyond: Reaping the Dividends of Cyber Resilience(2015).

25 Andrea Wells & Stephanie K. Jones, "Growth in Cyber Coverage Expected as Underwriting Evolves," *Ins. J.*, Apr. 4, 2016.

26 Org. for Economic Co-operation & Development, Supporting an Effective Cyber Insurance Market: OECD Report for the G7 Presidency (May 2017).

27 Gillian Mohney, "Hospitals Remain Key Targets as Ransomware Attacks Expected to Increase," *ABC News*, May 15, 2017.

28 Jessica Davis, "Ransomware Accounted for 72% of Healthcare Malware Attacks in 2016," *Healthcare IT News*, Apr. 27, 2017.

29 Symantec, Ransom. Wannacry, May 24, 2017.

30 Richard Winston, "Hollywood Hospital Pays $17,000 in Bitcoin to Hackers; FBI Investigating," *L.A. Times*, Feb. 18, 2016.

31 Phil McCausland, "Companies Stockpiling Bitcoin in Anticipation of Ransomware Attacks," *NBC News*, May 18, 2017.

32 Erin Dietsche, "Healthcare Breaches Cost $6.2B Annually," *Becker's Health IT & CIO Rev.*, Jan. 19, 2017.

33 Kristin M. Nimsger & Michele C.S. Lange, Electronic Evidence and Discovery: What Every Lawyer Should Know Now, ch. 5, Computer Forensics (ABA Book Publishing 2009).

34 HIPAA addresses data privacy and security provisions for safeguarding EMRs and patient medical information.

35 U.S. Dep't of Health & Human Servs., Fact Sheet: Ransomware and HIPPA.

36 Davis Wright Tremaine LLP, Summary of U.S. State Data Breach Notification Statutes (2017).

37 Stephen Embry, "State Data Breach Notification Laws Just Got Crazier," *Your ABA*, May 2016; "Tennessee Adds Technical Requirements to Its Data Breach Notification Laws," *Nat'l L. Rev.*, Apr. 26, 2017; Thomas Ritter, "Tennessee Amends Its Breach Notification Law (AGAIN) and Reinserts the Encryption Safe Harbor," *ThompsonBurton.com*, Mar. 29, 2017.

38 Erin Dietsche, "Healthcare Breaches Cost $6.2B Annually," *Becker's Health IT & CIO Rev.*, Jan. 19, 2017.

39 Protenus, Cost of a Breach (white paper) (2016).

40 James Booth, "DLA Piper's Hack Attack Could Cost 'Millions'," *Am. Law.*, July 7, 2017.

41 "World's Largest Data Breach Settlement Agreed by Anthem," *HIPPA J.*, June 26, 2017.

42 Nile Lars, "Connected Medical Devices, Apps: Are They Leading the IOT Revolution—Or Vice Versa?," *Wired*; Ian Scales, "Smart Bandages to Use Real-Time 5G Connectivity," *TelecomTV*, 2017; Kim Zetter, "Hacker Can Send Fatal Dose to Hospital Drug Pumps," *Wired*, June 8, 2015.

43 Andrea Wells & Stephanie K. Jones, "Growth in Cyber Coverage Expected as Underwriting Evolves," *Ins. J.*, Apr. 4, 2016.

44 Thomas Fox-Brewster, "Medical Devices Hit by Ransomware for The First Time in US Hospitals," *Forbes*, May 17, 2017.

45 Nile Lars, "Connected Medical Devices, Apps: Are They Leading the IOT Revolution—Or Vice Versa?," *Wired.*

46 U.S. Food & Drug Admin., Cybersecurity Vulnerabilities of Hospira Symbiq Infusion System: FDA Safety Communication (July 31, 2015).

47 *See* National Council of ISACs.

48 Bruce Schneier, "Computer Security and Liability," *Schneier on Security*, Nov. 3, 2014.

49 Ellie Cambridge, Holly Christodoulou & Lizzie Parry, "NHS Cyber Attack 'Only Just Beginning' as Hackers Use 'Malware Atomic Bomb' to Turn Hijacked Machines into Infectious 'Zombies'.," *Sun*, May 14, 2017.

50 Ellie Cambridge, Holly Christodoulou & Lizzie Parry, "NHS Cyber Attack 'Only Just Beginning' as Hackers Use 'Malware Atomic Bomb' to Turn Hijacked Machines into Infectious 'Zombies'." *Sun*, May 14, 2017.

51 Nat'l Inst. of Justice, Office of Justice Programs, Gang Membership as a Prosecution Enhancement (Oct. 28, 2011).

The content of this article is intended to provide a general guide to the subject matter. Specialist advice should be sought about your specific circumstances.

Ms Kristen Psaty
Clyde & Co
The St Botolph Building
138 Houndsditch
EC3A 7AR
London
UK
Tel: 207876 5000
Fax: 207876 5111
E-mail: communicationsteam-global@clydeco.com
URL: www.clydeco.com