CYBERSECURITY ADVICE FOR PHYSICIANS AND HEALTHCARE LEADERS

ACKERMANN MARKETING & PR

smart strategy, creative thinking

Cybersecurity Advice for Physicians and Healthcare Leaders

As the consumerization of healthcare allows patients to think more about the value of their care, efficiency of service becomes an even greater priority when deciding where to receive care. Physician groups, dentists, and hospital networks are being driven to evaluate the quality of service, in addition to their number one priority – quality of care. In the pursuit of this expanded "service" purview, healthcare providers and physicians are evaluating the balance of quality, efficiency and security. Quality has always been a top priority for healthcare providers, and efficiency has moved into a close second position. Now, security is proving to gain ground in the minds of both healthcare executives and consumers.

Cybersecurity is not a new consideration, but its importance and likelihood of impact on healthcare organizations is growing at a rapid pace. At the Sword & Shield EDGE2017 Security Conference in Knoxville, Tenn., Maj. Gen. Brett T. Williams, former head of U.S. Cyber Command, offered a wake-up call to all businesses: "You have a 100% chance of being attacked." While all businesses hope attacks come later rather than sooner, preparation is no longer an option.

Healthcare has risks associated with the cybersecurity industry that most other businesses do not. Hospitals and physician practices collect payment and patient information that require significant security, as well as the HIPAA and PCI regulatory requirements. For those reasons, how do healthcare providers balance the cost pressures of their daily operations, the value of patient care, and investing in security measures that prevent patient data from escaping to the black market?

Ackermann met with a group of cybersecurity experts to offer key advice to healthcare organizations, from prevention to crisis response.

A look at the Numbers

60% of small companies are unable to sustain their business six months after a cyber attack.
- U.S. National Cybersecurity Alliance

$65 BILLION Global healthcare cybersecurity spending will exceed $65 billion cumulatively over the next five years. (2017-2021) - *Cybersecurity Ventures*

$3.62 MILLION Average cost of a security breach in 2017, according to IBM Security/ Ponemon.

88% of all ransomware attacks in U.S. industries last year were carried out on the healthcare industry.
- Solutionary, an NTT Group security company

Unique Value and Unique Risk

All private data is valuable. Businesses gain efficiencies of scale by interconnecting data. However, these two elements open the door for cyber risk that is unique to healthcare organizations. Data within healthcare organizations have attributes which make hospitals extraordinarily attractive targets for hackers. One of the reasons the healthcare industry is at a high risk for a cyber-attack is because of the wealth of patient information healthcare providers maintain. Patient records include permanent information such as Social Security numbers and birthdates.

Not only does this type of patient data have a longer shelf-life, it is worth much more than the amount of credit card information on the dark web. In a 2015 study by Trend Micro, health information and medical records sold on the dark web for an average of $59.80 each and Social Security numbers sold for $55.70 each, while payment records were valued around $36.00 each. If a credit card is stolen, the thief is likely to use it immediately and frequently before the cardholder notices and cancels the card. Social Security information cannot be canceled, leaving this information available to identity thieves for as long as they have access to it.

Not to mention, cybersecurity can now play a role in drug addiction. If obtained through a data breach, patient records can then be sold on the black market for access to prescriptions. When the Man Alive, Inc. Lane Treatment Center, a non-profit substance abuse and mental health facility in Baltimore was recently hacked with ransomware, patient information including names, dates of birth, social security numbers, and drug dosages were stolen.

> "The higher the number of individuals and organizations involved with patient records, the higher the risk of a breach and lower amount of control directed by the provider"

Another element that creates unique risk within the healthcare industry is the number of people, departments, network connected machines, and vendors that have access to patient records. It is important to be aware of the number of people who may have access to patient files.

"Any provider involved in treatment payment and operations can access a patient's protected health information," said Karen Clark, Chief Information Officer at OrthoTennessee. "The more individuals and organizations involved with patient records, the higher the risk of a breach and lower amount of control directed by the provider."

Regardless of the number of vendors involved, patients will likely still hold the primary provider responsible for any breach of trust. For local physician practices, security is uniquely exposed by front line staff. Phishing issues should be a part of regular communication and employees should constantly be aware of them. A third-party vendor working for TRICARE was transporting patient information when he was robbed. The thief's acquisition included patient information full of birthdates, social security, and other permanent information.

> "Technology modalities that need approval through the FDA have a very slow process, setting hospital technology four to six years behind."

Healthcare devices are also at risk. Bill Dean, Senior Manager at LBMC Information Security, explains that vendors are developing high-tech devices but have put security on the backburner. "Security is usually the last aspect considered in the medical device manufacturing process," said Dean. " A single medical device connected to a provider network could put the entire network at risk." Dean explains that if breached, the result of this risk could potentially include control of medical devices in the wrong hands and potential threats to patient care.

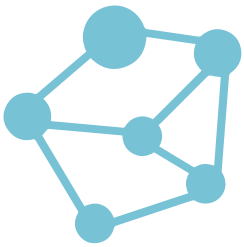
Another major risk unique to healthcare is the rate at which hospital technology gets approved, according to Chris Lyons, Senior Security Consultant at Sword & Shield Enterprise Security, Inc. Lyons explains that, "technology modalities that need approval through the FDA have a very slow process, setting hospital technology four to six years behind technology used by hackers." In an article in HIPAA Journal, Itamar Kandel interviewed doctors and healthcare providers about their opinion on why healthcare technology moves slower than other industries. The number one answer revolved around safety. When other kinds of businesses test new technology and it fails, they can lose money and time. If a business in the healthcare industry tries new technology and it fails, they could lose lives. Although justifiably driven by patient health, by the time certain devices are approved, the technology used by cyber hackers has already advanced, thus leaving healthcare providers in a constant state of catch-up and potential danger.

"Unfortunately, with the rise of breaches comes the chance that patients may become more reluctant to share certain information with their medical providers," said Eliza Scott, Esq., an attorney and former Security Consultant at Oak Ridge National Lab and Y-12 National Nuclear Security Complex. "This may lead to unintended consequences during diagnosis and treatment. When patients stop trusting the integrity of their information, they may choose not to share important medical history."

Another growing risk is the mobile clinician. All industries are adapting to the growing trend of a remote workforce; however the sensitivity of healthcare data makes secure access even more important. Consider a doctor on her lunch break who decides to review patient records from a nearby coffee shop. It is likely she will utilize the coffee shop's WIFI, which will undoubtedly expose her to being hacked.

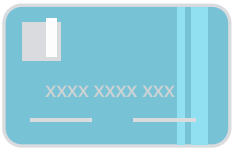
What's Compromised?

Medical Records



Interconnected Devices

Phishing



Payment Information

HIPPA Compliance

Remote Access

Efficiency vs. Security

There are certain trends in technology and patient service that are shaping the intersection of healthcare and cybersecurity, one of which is the need for speed. Patients expect quicker service, and hospitals are searching for ways to scale costs. In some ways, security is being traded for efficiency.

"When records were on paper," said Paul Sponcia, "someone had to break-in and then haul boxes of records away."

It was also inefficient for staff and physicians to access, but now it is at our fingertips. "It comes in waves," says Bill Dean. "At first, security was seen as making people less productive but now it's necessary." Dean suggests we are entering the second phase of this tension between efficiency and security. "While efficiency is convenient and important to a physician, it is also convenient for a hacker."

In the spirit of efficiency, an entire market of Electronic Health Records (EHR) software makers have emerged and now become a basic requirement of managing patient data in any modern healthcare facility.

On the other side, EHR systems "potentially compromise the security of millions of patient records," according to Ian Hennessey and Dan Swanson, attorneys at London Amburn. "The theft of one employee's laptop can "cost an organization its reputation, patient trust and large sums of money,"said Hennessey and Swanson, "Although beneficial overall, EHRs have shown to be more attractive to cyber criminals because they are able to access the information of millions of patients. Moving these files can also cause a loss of data."

Leadership Prioritization

"Cybersecurity is a risk management issue, not an IT issue," says Karen Clarke. "Healthcare providers should be thinking of cybersecurity the same way a company thinks about employee lawsuits, competition, regulatory changes and malpractices."

Businesses who take cybersecurity seriously are dedicating the time and resources of key leaders within the organization to ensure preparedness. "The biggest gauge of commitment to cybersecurity I see when discussing how to get started in cyber defense is when I ask how involved the board or executive team is as it relates to cybersecurity," adds Bill Dean. "Is it part of their risk management plan? If I hear silence, alarms start to go off."

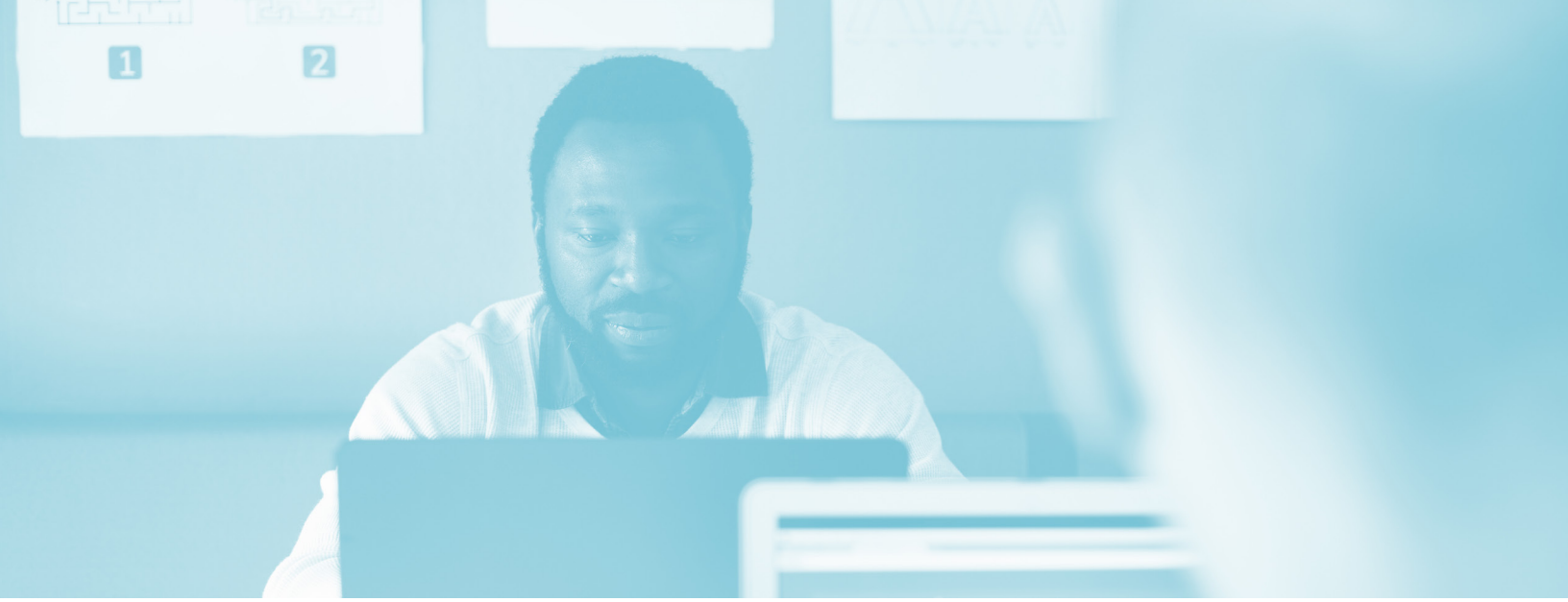
In fact, most healthcare companies are taking prevention matters seriously. A 2014 KMPG study found that 86% of providers had invested in cybersecurity during the previous 12 months.

While leadership buy-in is important, true commitment means dedicating staff to it specifically. As for the smaller hospitals, Dean explains there is no longer an option to avoid making investments in cybersecurity prevention measures.

Interconnected Devices

As the "internet of things" connects data and networks to physical devices, cyber risk must be considered. With more interconnected devices comes the risk of access to hack into those devices. New equipment is being introduced to hospitals that are all interconnected to the same IT network, making it easier for an attack. Karen Clarke has witnessed medical device vendors leave default passwords for ease of future services. "Without proper protocols, this default setting is often neglected, thus providing easier access for hackers," added Clarke.

"The feasibility of hacking a pacemaker or network-connected life-saving device may very well be the next level of threats that have to be addressed," says Hennessey and Swanson. Fitness trackers and smartphones contain increasing amounts of personal, health and biometric data that could be attractive to hackers. Offsite EHR companies are not completely safe from targeting. When working with those services, Swanson and Hennessey suggest groups work with their IT vendor to come up with the solutions that best fit their circumstances. "The closer the companies work together, the better understanding they will have of their cybersecurity plans and precautions."



Preparedness

"Even with the most prepared companies, there is no perfect privacy or security plan," says Eliza Scott. Breaches can occur in any company. However, it is important to have a plan when it does occur. Scott suggests considering a technical, legal, and/or public relations firm to design a plan that best fits your company. The group should meet regularly to be sure the best plan is in place. Do not expect to handle it alone.

Typically, organizations believe they are already doing everything they can, when in reality there is much more to be aware of. Paul Sponcia offers five of the most common weaknesses that healthcare organizations frequently downplay:

1. Visibility and commitment from the top, including shareholders
2. Lack of risk management, policies and procedures
3. Incident Response and Disaster Recovery plan and testing
4. Minimal investment in technology
5. Lack of information security awareness training

So where do smaller healthcare providers begin? For starters, federal, state, and local resources are available. The Department of Homeland Security, Department of Health and Human Services, Food and Drug Administration, Office of Civil Rights, the Federal Bureau of Investigation, and the Secret Service all offer free resources such as alerts, guidelines, and scans of software to contribute to the protection and prevention of cybersecurity breaches. In fact, Karen Clark suggests calling the FBI for specific training and situation readiness.

As technology evolves, HIPAA should as well. Swanson and Hennessey point out, "HIPAA did not contemplate that doctors would look at patient records on their phones or that a hospital emergency room would text x-ray images to a radiologist."

"The HIPAA Privacy and Security rules require all healthcare organizations to develop a plan to protect their patient records," according to Swanson and Hennessey. This means HIPAA requires them to have firewalls, passwords, and a plan to respond in case of a breach. However, as technology progresses, HIPAA will need to adapt as well. Eventually, new rules and regulations will need to be put in place. HIPAA does require the breached organization to provide notice to any patient who may have had their information hacked. Fines and penalties can occur for an organization after a breach, especially if proper protocols were not in place to begin with. For example, Multi-State Billing Services had to pay the state of Massachusetts $100,000 because of a data breach related to identity theft and fraud.

When forming a plan, do not just "set it and forget it" as Eliza Scott puts it. Organizations who put cybersecurity in place but do not actively test and monitor it are prone to breaches. After forming boards and hiring people to specialize in a potential breach, remember to take action and be prepared.

Swanson and Hennessey note, "a failure of facilities to keep their policies current regarding technology is a severe weakness and because of the growth of technology, policies created 15 years ago are no longer applicable when dealing with a breach." Something like a lost or stolen cellphone or USB drive could now potentially cost a healthcare provider millions of dollars in mitigation expenses and fines. This type of issue would not have been addressed in policies created 10 to 15 years ago.

"The greatest threats to hospitals may be the individual user," warns Paul Sponcia. "End users are the ones who typically make the mistakes which create the backdoors for data to be exfiltrated. An institutional priority must be set within the organization in order to allow individual employees to identify risks."

Not only should the IT staff be up-to-date and well aware of cybersecurity actions taken, but other members of the staff should be as well. Staff should be conscious of potential threats via email or password hacking. Companies should go as far as sending out phishing tests to test employees.

Respond Effectively

When a breach is initially detected, the most important steps come next. To respond effectively, it is necessary to get in touch with technical, legal and communications teams. Eliza Scott suggests, "Get the technical team on site immediately to mitigate further problems and start determining what has happened and look for technical solutions."

Swanson and Hennessey add, "ignoring the problem or delaying action will only disadvantage the healthcare provider and may be considered bad faith by any investigator, should the Office of Civil Rights investigate."

In considering a response, federal and state requirements set the primary course of must-do actions. According to federal requirements, if a breach occurs, the healthcare provider has at most 60 days to provide notice to patients.

"The Health Insurance Portability and Accountability Act is the most well-known federal statute containing requirements governing the protection of patient information," says Eliza Scott. "Depending on the type of organization, the Family Educational Rights and Privacy Act may also apply. Generally, the requirements relate to informing patients about how their information may be administered, forming an appropriate security plan or policy, when and with whom information can be shared, and notifying patients in the event of a compromise of their information."

Consumers have unique engagement requirements, but state governments require explicit notifications. For example, Tennessee Governor Bill Haslam recently added two new requirements to the state's breach notification laws, one confirming a 45-day response timeline related to breach discovery and notification.

While patient notification is a requirement in some cases, it is important to remember that patients are now informed consumers, so it may be necessary to go above and beyond. Outbound phone calls, in-person information sessions and other more personal engagement go a long way in reinforcing trust between the organization and the consumer. For example, both New York-based Kaleida Health and Delaware-based Medical Oncology Hematology Consultants offered free credit monitoring to all patients whose records were involved in cyber breach incidents in 2017.

Prevention and Response Tips

Every organization in the healthcare industry is susceptible to cyber threats. Patient data is the most valuable, private type of consumer data, and smaller organizations are usually the most attractive prey. Prevention requires investment, prioritization and specific strategies, and even then, there is no silver bullet to ensure 100 percent immunity. If a breach does happen, it is imperative for healthcare organizations to respond according to both federal and state law, but also according to the growing demand for trust between the organization and the modern informed consumer.

The good news is that there are significant resources available to businesses of all sizes. Prevention and response training experts abound, and basic prevention measures are becoming more affordable every year. Investments in cyber threat prevention and response are now becoming a critical part of enterprise risk management. While most physician groups and hospitals are rightly focused on patient health, this new challenge for organizations will cause a shift in thinking to also require a focus on patient data health.

If your business is part of the growing healthcare ecosystem, here are some basic takeaways to avoid playing with cyber fire:

Prevention

- Plan for a worst-case scenario
- Practice that scenario a few times a year
- Be sure the staff is aware of the plan and train them accordingly
- Set up new passwords and firewalls
- Encrypt data and back it up both onsite and offsite
- Create a risk management team specifically for technical issues

Action

- Find experts who specialize in cyber threats
- Act quickly and wisely
- Get predetermined team to meet immediately
- Engage legal council to understand your liability
- Inform staff and outside stakeholders

Response

- Notify patients and outside parties as required by law
- Keep in contact with media relative to damage control and new prevention plans
- Meet with legal team to ensure everything that should have been done is taken care of
- Maintain trust and accountability with patients with ongoing communications
- Ensure consistent communication with patients and stakeholders

Ackermann Marketing and PR is a 36-year-old, full-service marketing and communications firm headquartered in Knoxville, TN. With long-term strategic thinking as its specialty, Ackermann helps businesses grow through the planning and execution of public relations, digital strategy, product marketing, brand identity, advertising, crisis communication and media training.

Strategic Planning	Public Relations
Product Marketing	Brand Identity
Digital Strategies	Advertising

Sotiria security comms

Sotiria Security Comms is a worldwide group of full-service PR/comms agencies with a mandate to provide both cyber and physical security organizations with specialist security communications consultancy services. Ackermann is the only US member firm of Sotiria.

SPECIAL THANKS TO:

Chris Lyons - Sword & Shield Enterprise Security

Dan Swanson - London Amburn Attorneys at Law

Ian Hennessey - London Amburn Attorneys at Law

Bill Dean - LBMC

Karen Clark - OrthoTennessee

Paul Sponcia - The IT Company

C. Eliza Scott - Attorney and Former Security Consultant at Oak Ridge National Lab and Y-12 National Nuclear Security Complex

Tommy Smith - Ackermann Marketing & PR