# Reducing the Risk Of a Cyber Crisis

JARRETT KOLTHOFF, GCFA, CISSP

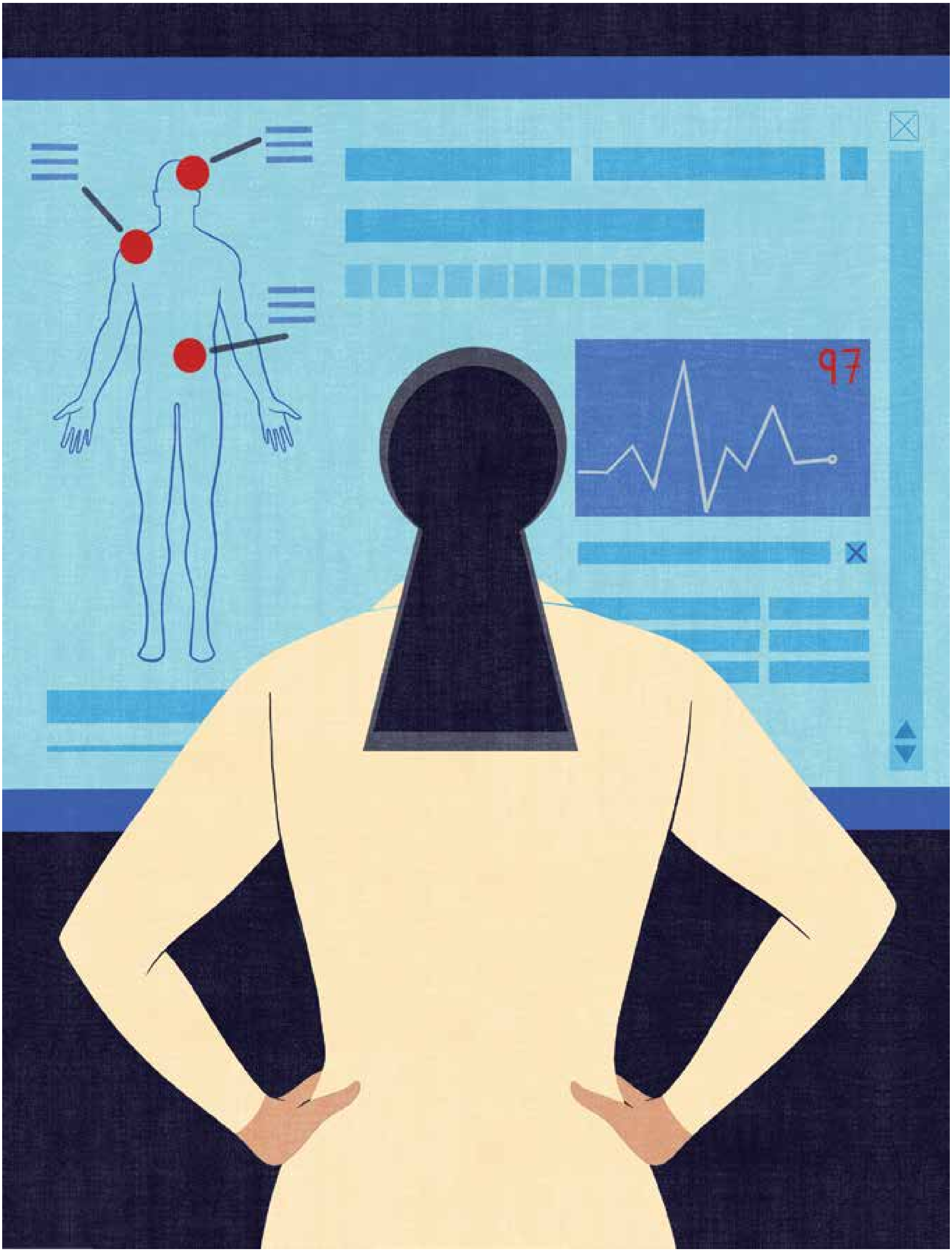
A true crisis facing health care in America stems from cyber criminals, who target the health care industry with greater frequency than any other sector of the economy. Protecting information is vital. Patients rely on the medical establishment not only for care, but for survival. The amount of sensitive personal data stored by America's medical establishment is vast.[1] Combine this personal data with detailed financial information and you have a treasure trove of assets that can be easily marketed on the "dark net," (the portion of the internet not open to public view) in such a fashion that virtually anyone, anywhere can purchase them for a few cents per file.

According to specialty insurer Beazley, 41% of all cyber incidents tracked by the company in 2018 occurred in the health care field. Of particular concern, 34% of all ransomware attacks and 27% of all business email compromises were carried out on health care providers, with business email compromise attacks skyrocketing by a whopping 133% from 2017 to 2018.[2] (A ransomware attack generally involves locking or taking a victim's electronic data, then demanding a ransom to restore access to it.)

When it comes to ransomware, organized cyber criminals and sophisticated hackers have narrowed their focus, with a significant concentration on small and medium-sized organizations, because they are commonly underfunded and poorly prepared for a cyber incident. According to Beazley's statistics, 71% of ransomware attacks tracked were perpetrated against small and medium-sized organizations, with an average ransom demand and/or payment of just over $116,000.[3]

With threats escalating and the severity of cyberattacks mounting, the calls for greater accountability and preparedness will most likely result in higher fines and even individual lawsuits seeking punitive damages which could be crippling to the health care industry as a whole. When personal information is disclosed, routine steps like credit monitoring are not satisfactory to those who have experienced harm from a breach. In some cases following a security breach, there have been lawsuits seeking damages similar to those sought in some malpractice cases. Consequently, substantial measures need to be taken to minimize cyber-risk within health care, including the implementation of practices to prevent breaches, precise strategic and tactical planning, and procedures to be followed in the event of breach.

According to specialty insurer Beazley, 41% of all cyber incidents tracked by the company in 2018 occurred in the health care field.


97

### INVOLVING THE BOARD

Before delving into breach prevention and mitigation measures, let's look at why organizations have to designate cybersecurity as a priority. The boards of directors and executive teams of every health care operation in the United States need to place cybersecurity on par with patient care in terms of importance. Without proper cybersecurity in place, patient care and safety are at serious, often mortal risk.

Once cyber criminals have accessed a health care organization's networks, operating systems and controls, the opportunity for harm escalates on an alarming scale. Medications and dosage levels can easily be changed and altered. MRIs, CAT scans and X-rays can be manipulated to show tumors, blockages, fractures and other conditions where they do not exist. Life support equipment can be reprogrammed or terminated, resulting in patient deaths.

**A board member with cybersecurity training and/or background is no longer a luxury, but an absolute necessity for every hospital and health care-related business.**

A board member with cybersecurity training and/or background is no longer a luxury, but an absolute necessity for every hospital and health care-related business. Cybersecurity has now surpassed malpractice as the most serious and significant threat to medical operations and medical liability. A single cyber incident could inflict catastrophic financial damages and also permanently erode brand value, brand trust and patient confidence, resulting in millions, even billions, of dollars in long-term losses.

Some boards may hesitate at "bringing the geeks to the table." But without board oversight and a cybersecurity champion on the board, cyber criminals and cyber terrorists may seek out and target your organization first, assuming a greater probability of vulnerabilities and gaps in your infrastructure.

### COMPLIANCE EQUALS COMPLACENCY

There are various federal and state cybersecurity protocols that organizations need to follow, including HIPAA health care data privacy and security requirements. But most regulations are loosely worded, leaving room for substantial individual interpretation of rules and application of standards.

Compliance standards simply cannot keep pace with the constant changes and shifts in how cyber criminals attack companies and organizations, particularly in the health care field. The moment compliance standards are written and released, they're instantly outdated, making cybersecurity all the more challenging.

As laws change, individual board members now can be held personally and fiscally accountable for losses resulting from cybersecurity practices that are not deemed to be "reasonable and prudent." This fact alone should be motivation for cybersecurity standards that go beyond compliance, but there are still boards and organizations that don't pay enough attention to these issues until they're faced with a significant cyber incident.

Boards and executive teams must prioritize cybersecurity as part of an organization's overall risk assessment strategy. Then they can determine the amount of risk exposure they are willing to accept in relation to cost of protection, prevention and the potential for loss across a number of different categories.

### HIRE CYBERSECURITY EXPERTS

In-house information technology departments and security departments at most health care facilities are stretched to the limit in terms of personnel, budget and workload. There's always something that needs to be done and a minor emergency that needs to be remedied. So adding cybersecurity onto these groups' responsibilities may be an undue burden.

Keeping up with the latest changes and developments in how cyberattacks are executed is a full-time job. Staying abreast of evolving cyber crime methods with the implementation, monitoring, tracking and updating required by an effective cybersecurity operation may be too big a task to handle with in-house staff. To make matters even more difficult, attracting and retaining top-level cybersecurity engineers to work at the level required by health care providers becomes expensive and time consuming. Some organiza-

tions may need to support their in-house departments with the expertise of outside cybersecurity experts.

### TACTICS TO HELP PREVENT A BREACH

In addition to the big-picture issues to consider, there are some street-level tactics that can help prevent a breach. Some of the ideas presented here are for information technology teams, while other items require only simple changes.

**Incorporate a dedicated "update and patch" team.** For larger operations, hiring a dedicated team that handles only updates and patches is money well spent. Given the number of computers, devices and types of equipment in the average hospital or large-scale organization, updating and patching can't be handled part-time. From updating and patching, to the overwhelming task of tracking every piece of software and equipment, to monitoring update notices, the work of a dedicated update and patch team will quickly become one of the most valuable functions in your organization.

**Create a cybersecurity culture.** Cybersecurity is everyone's responsibility, not just the members of a team or a committee or a department. Everyone in your organization is impacted by cybersecurity so everyone should also be part of the solution, not part of the problem.

Get everyone involved and excited. Offer recognition and rewards to those who provide ideas or create programs for improving cybersecurity at the employee level. Keep people aware. And provide avenues for education and for making employees realize their value in the process of organizational security. A simple weekly email blast, a monthly newsletter and intranet postings, along with regular recognition events are a great way to keep your organization cyber safe and to let employees know that you value how they're making a difference.

**Get everyone involved and excited. Offer recognition and rewards to those who provide ideas or create programs for improving cybersecurity at the employee level. Keep people aware.**

**Create departmental-level cybersecurity teams.** Depending on the size of your organization, have an executive-level cybersecurity team or leader, such as a chief information security officer, communicate weekly or bi-weekly to departmentally-based teams to share the latest on cybersecurity. Don't make it all nuts and bolts tech talk, as that could get repetitive and even boring. Consider including updates on how cyberattacks were stopped, or a new way to help secure patient care equipment, or little things every employee can do to help keep data and patients safer. By communicating and sharing, you can keep cybersecurity top-of-mind and reinforce its importance.

**Provide a personal benefit to employees during cyber training.** Consider offering cybersecurity training at a mealtime and provide a meal for employees. The cost of food is small, compared to what a single incident response would cost.

**Practice. Practice. Practice.** All the theoretical planning you do as part of your cybersecurity program is useless until its tested in a real-world environment. For your front-line IT and cybersecurity teams, call in your cybersecurity provider and host tabletop exercises on how to stop a simulated cyberattack. Once you see your strategies and tactics in action, you can evaluate, improve, change and even overhaul your procedures. Finding out what works and what doesn't is much better in practice than when you're actually being attacked.

A 2017 Privacy and Security Awareness Report showed that 78% of health care employees showed some lack of preparedness with common privacy and security threat scenarios.[4] That's why employers should practice cyber emergency drills, similar to fire drills. Create a variety of possible scenarios and have employees practice emergency protocols.

### STEPS EMPLOYEES CAN TAKE

There are a myriad of little things employees can do to help prevent breaches:

**Protect personal and mobile devices.** Mobile devices are your most vulnerable point of entry. With personal smartphones and tablets used to regularly access networks, all employee devices should be registered, protected with encryption and antivirus software, and more, depending on your facility. Through a mobile device manager, an organization can register and protect even personally owned devices. Work to make mobile devices as safe as possible.

**Be password strong.** Stolen passwords are an easy gateway for cyber criminals to breach your system. Stress that employees use strong passwords with a long variety of characters, numbers and symbols. Use verification techniques for added security when someone is accessing work accounts, such as multi-factor authentication with security questions and out-of-band notifications for logins. Have employees change passwords regularly. And finally, make the sharing of passwords a violation of work policy with appropriate consequences. Passwords should never be shared.

**Limit access.** Everyone doesn't need access to everything. Strictly limit access to sensitive data and information that doesn't apply to an employee's job description. Software, apps and other additions to your network should be handled only by designated information technology team members, not random personnel. And for vendors requiring network access, issue restricted access and time-limited credentials based on exactly what the vendor needs to complete the work.

**Teach proper cyber hygiene.** Most people have never been taught good cyber hygiene. Placing sensitive information in emails or leaving personal data in email attachments are just two easy ways to open doors that can allow criminals to steal information. Encourage employees to keep only critical immediate data on their computers and devices. Everything else can be backed up or stored on the cloud.

**Backup, backup, backup.** Keep information backed up in multiple places for added security. Backup offline on multiple devices. Backup on the cloud and backup in designated areas of the organization's networks. An independent backup free from malware or ransomware could be the ticket to saving valuable assets that might not otherwise be recoverable.

## WHAT TO DO IF YOU DISCOVER A BREACH

Most breaches aren't discovered for an average of 18 months. Once you become aware of a breach, time is of the essence. The faster you move, the less damage you face. But you have to do everything right from the beginning. Here's what you should do first:

**Enlist your cybersecurity provider immediately.** Dealing with a breach is not a do-it-yourself project. Asking anyone but an expertly trained cyber engineer to mitigate a breach is akin to asking a pastry chef to disarm a nuclear warhead. Expert incident response is critical to ending your breach quickly and effectively, so leave it to professionals.

**Don't turn off computers, networks or systems.** Most malware has built-in "kill switches" that can trigger when equipment is shut down in a manner meant to end a breach. The result can lead to permanent destruction of networks, systems and data. Call in the pros and let them do what they do best, or you could face catastrophic loss.

**An independent backup free from malware or ransomware could be the ticket to saving valuable assets that might not otherwise be recoverable.**

**Quarantine all devices, networks and systems.** Respond to a breach as you would to a highly contagious communicable disease. Nothing new comes in or goes out in terms of information technology. Until you determine the point of breach, what you're facing and how to eliminate the chance of the malware spreading to uninfected equipment, you need to quarantine everything, including personal devices used by staff and vendors, who have network and system access.

**Enlist your legal and communications teams.** Once you've been breached, you want to share accurate information and mitigate damage on multiple fronts. Bring in your legal representative to make sure you release information in compliant fashion and to the proper authorities and agencies. Once that happens, you'll have strict protocols to follow. Have communications ready to handle informational or news releases to necessary parties and the media, if needed.

Always stay one step ahead of what is required by law and manage the situation. Even more importantly, always present yourself professionally and keep the interest of outside parties impacted by the breach at the forefront of everything you do.

**Have digital forensics at the ready.** After your

cybersecurity partner mitigates the breach, call in the digital forensics team. It's critical to learn as much as possible about the breach, where and how it occurred, damages caused and how much data and other assets may have been stolen.

## CONCLUSION

It's disheartening that health care, an industry based on helping those in greatest need, has become a prime target for criminal enterprises. Many of us live with a false sense of security when it comes to health care cyber crime. We use personal devices, laptop and desktop computers, and various types of equipment dependent on information technology networks or systems when we're working. The natural assumption is that "we're all protected" by someone, somewhere, who has responsibility for making sure criminals are "locked out." But in reality, we are all just as responsible for cybersecurity in our own way as those with cybersecurity as part of their job function. The better we all plan, prepare and respond will lead to improved safety not only for the health care industry, but for the patients who place their lives in our hands every day.

**JARRETT KOLTHOFF** is the chief executive officer of St. Louis-based SpearTip Cyber Counterintelligence.

### NOTES

1. For more information, see Karim Abouelmehdi, Abderrahim Beni-Hessane, Hayat Khaloufi, "Big Healthcare Data: Preserving Security and Privacy," *Journal of Big Data* 5, no. 1 (2018), https://link.springer.com/article/10.1186/s40537-017-01107.
2. "Beazley Breach Briefing," Beazley website, March 21, 2019, https://www.beazley.com/news/2019/beazley_breach_briefing_2019.html.
3. "Beazley Breach Briefing."
4. Elizabeth Snell, "78% of Healthcare Workers Lack Data Privacy, Security Preparedness," Health IT Security website, Feb. 6, 2018, https://healthitsecurity.com/news/78-of-healthcare-workers-lack-data-privacy-security-preparedness.

JOURNAL OF THE CATHOLIC HEALTH ASSOCIATION OF THE UNITED STATES www.chausa.org

HEALTH PROGRESS®