Mature Information Risk Management Programs

Prevent avoidable data breaches with multidisciplinary teamwork

By Bob Chaput, MA, CISSP, HCISPP, CRISC, CIPP/US

Chief Audit Executives do not need to be reminded that data breaches are increasing in scope and severity every month. As the nexus of risk management, governance and control processes, internal auditors can have a strategic influence on the effectiveness of a healthcare organization's cybersecurity program.

Bob Chaput is the CEO of Clearwater Compliance, LLC. and is widely recognized for his extensive and in-depth knowledge of healthcare compliance and cyber risk management. As a leading authority on safeguarding health data, Chaput has supported hundreds of hospitals and health systems to successfully manage healthcare's evolving cybersecurity threats and ensure patient safety. You can contact him at *Bob.Chaput@clearwatercompliance.com.*

The many aspects of enterprise risk management include preventing fraud and abuse, meeting safety and credentialing standards and weighing the prudence of mergers and acquisitions. However, information risk management (IRM) is quickly rising to the top of the list.

Many organizations claim they are unable to fund an IRM program because of competing priorities that include technical debt—the significant investment they have already made in electronic health records (EHRs) and billing systems that need continuous updating. Even sufficiently funded organizations often do not know where all their protected health information (PHI) resides and, therefore, where all the risks to that information lie.

Most healthcare organizations have taken an ad hoc approach to data security, fixing problems after they arise. However, it is far wiser to take a proactive, multidisciplinary approach to IRM.

Ten startling facts

Although many Chief Audit Executives (CAEs) are familiar with the grim findings below, a surprising number of their colleagues in the C-suite and on the board would be startled to learn about these realities.

Criminal attacks are now the leading cause of data breaches

For the second year in a row, according to a study published in May 2016 on privacy and security of healthcare data,[1] 50 percent of healthcare organizations reported that the nature of the breaches were criminal attacks. The *2016 Cost of a Data Breach* study[2] also found that criminal attacks accounted for 50 percent of data breaches. In addition, the study noted that automated malware attacks caused security incidents at 78 percent of healthcare organizations.

[1] Co-sponsored by ID Experts and the Ponemon Institute: www.ponemon.org/blog/sixth-annual-benchmark-study-on-privacy-security-of-healthcare-data-1

[2] Co-sponsored by IBM and the Ponemon Institute

Hackers are learning how to monetize patients' personal data

"The healthcare industry is being hunted and hacked by the elite financial criminal syndicates that had been targeting large financial institutions until they realized healthcare databases are more valuable," says Tom Kellerman, former Chief Cybersecurity Officer at Trend Micro, an internet security firm.

Ransomware attacks are increasing rapidly

Hackers are now demanding sizeable payments from hospitals in order to unlock data that's been encrypted. The Gartner Group reports that ransomware attacks in the U.S. quadrupled last year. According to Solutionary, a cybersecurity firm, hospitals are the targets of an astonishing 88 percent of ransomware attacks.

Hospital hackers often have IP addresses linked to countries such as Iran, North Korea, China and Russia. Ransomware is frequently demanded in Bitcoin, and according to the FBI, paying the ransom doesn't always guarantee that you will get your data back.[3]

Medical identity theft continues to be a nightmare

According to Medical Identity Fraud Alliance, medical identity fraud is the "fastest-growing identity fraud, affecting more than 2 million people annually in the United States."[4] Millions of Americans have been victims of medical identity theft, and the majority of victims pay more than $13,000 to resolve the matter.

Employees are often the weakest link

It is important for hospitals to alert and educate all colleagues about the many ways—online and analog—that data can be compromised, including:

- *Malicious insiders* – In that same study conducted by the Ponemon Institute and ID Experts, 13 percent of the healthcare organizations surveyed reported that the criminal attacks were due to a malicious insider.[5]
- *Careless, untrained or distracted employees* – According to an article on the Forbes website, more than two-thirds of all hacks are caused by social engineering or phishing techniques.[6]
- *Inadvertent employee errors* – This includes everything from losing a laptop containing unencrypted patient data to using an unsecured wifi hotspot. Fifty percent of the breaches of more than 500 records on the HHS Breach Portal were due to loss or theft of unencrypted laptops, thumb drives, servers and other portable electronic devices.[7]
- *Snooping* – Although the number of records breached remains well below the 500 level each year, unauthorized access to the medical records of celebrities, family members, neighbors and friends leads to many firings and regulatory penalties at hospitals nationwide.
- *Non-electronic breaches:*
  - Photocopiers, multi-function printers and computers that have not been scrubbed of confidential data before resale or disposal
  - Voicemail systems: Voice recordings for quality purposes and care-related messages left by providers are considered PHI
  - Closed circuit TV systems: If the system captures a person entering what is clearly a healthcare facility, that is considered PHI and must be protected
  - Loss of analog records: Improper disposal of paper records, radiology images, etc.

[3] www.fbi.gov/news/stories/incidents-of-ransomware-on-the-rise

[4] http://medidfraud.org/wp-content/uploads/MIFA-Wisdom-Paper-Exec-Summary.pdf

[5] www.ponemon.org/blog/sixth-annual-benchmark-study-on-privacy-security-of-healthcare-data-1

[6] www.forbes.com/sites/laurashin/2017/01/04/be-prepared-the-top-social-engineering-scams-of-2017/#92ceeb67fec1

[7] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

In short, all assets that "create, receive, maintain or transmit" PHI—whether paper, electronic, voice or video—must be monitored in an IRM program.

Business Associates risk is your responsibility

Business Associates (BAs) are responsible for 19 percent of reported breaches greater than 500 records, but for 40 percent of the number of breached records.[8] Covered entities (hospitals, providers and payers) are now responsible for contractually ensuring that their business associates are safeguarding data and are reporting data breaches properly.

Device tampering is a huge patient safety issue

St. Jude Medical recently issued security updates to fix hackable pacemakers.[9] Johnson & Johnson issued a warning to diabetic patients that their insulin pump is vulnerable to hacking.[10] A growing number of hackers are not interested in the resale of health data, but are instead intent on tampering with medical devices and altering health records. Studies show that it is relatively easy for digital intruders to change the dosages and medications in patient health records. It is just as easy to reprogram infusion pumps, defibrillators and even surgery robots.

Custom cyber-insurance is a must

Unless properly amended, cybersecurity insurance may not cover the cost of system remediation, lawsuit defense, regulatory fines, and business interruption. According to a recent Reuters report, insurers will no longer write cybersecurity policies exceeding $100 million in industries that have already incurred large data breaches.

In healthcare, annual cybersecurity premiums can exceed $500,000, with deductibles as high as $500,000. As a result, some healthcare organizations are considering cyber-liability lines of insurance within their captive insurance programs to help cover the costs of crisis management, special call centers, credit monitoring, legal fees and more.

More six-figure penalties for incomplete risk assessments

Many healthcare organizations fail to understand that risk assessments are not optional.[11] The HealthITSecurity website reported:

> *"All too often we see covered entities with a limited risk analysis that focuses on a specific system such as the electronic medical record or that fails to provide appropriate oversight and accountability for all parts of the enterprise," OCR Director Jocelyn Samuels said in a statement. "An effective risk analysis is one that is comprehensive in scope and is conducted across the organization to sufficiently address the risks and vulnerabilities to patient data."*[12]

Most healthcare organizations have taken an ad hoc approach to data security.

Nearly 75 percent of all OCR resolution agreements and corrective action plans to date cite a failure to conduct an accurate and comprehensive risk analysis.

To date, 11 hospitals and health systems have had to pay $2 million or more (an average of $3.4 million) in OCR settlement agreements related to risk analysis and management. In the 39 settlement cases involving ePHI, 35 organizations (a staggering 90 percent) had failed to conduct an accurate and complete HIPAA Risk Analysis.[13]

Most data breaches are preventable

All employees need to be educated about the organization's policies and procedures concerning data security: access control, minimum necessary access, safeguards, incident reporting and mitigation, sanctions for violations, password protection, and phishing-attack avoidance, to name a few. Staff training needs to be more extensive than a brief online tutorial about HIPAA—and needs to be specific to the employee's role and responsibilities.

Need for a comprehensive solution

Healthcare organizations cannot remedy the data security problems outlined above with ad hoc solutions. An organization-wide IRM program is needed that does not fixate on the threat du jour and only on today's information assets.

A good place to start is with the audit and compliance committees, which can assess the organization's risk tolerance and unique circumstances. These committees can

[8] *Ibid.*

[9] www.washingtontimes.com/news/2017/jan/10/st-judge-pacemaker-company-issues-security-updates/

[10] www.reuters.com/article/us-johnson-johnson-cyber-insulin-pumps-e-idUSKCN12411L

[11] §164.308 (a)(1)(ii)(A) *Risk analysis* (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.

[12] http://healthitsecurity.com/news/lack-of-risk-assessment-key-in-uwm-750k-hipaa-settlement

[13] www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/

then bring other departments and senior leadership into the process by implementing three critical components:

- *The National Institute of Standards and Technology (NIST) Cybersecurity Framework (What to Monitor)* – This combines current standards, guidelines and best practices to reduce cybersecurity risk.
- *The NIST IRM Process (How To Do It)* – The NIST Information Risk Management Process that is documented in NIST SP 800-39 provides detailed steps for framing, assessing, responding to and monitoring risks.
- *Robust maturity model* – This component demonstrates the organization's commitment to continuous process improvement and to a maturity model that ensures proper implementation and ongoing optimization.

Many healthcare organizations fail to understand that risk assessments are not optional.

Implementing the NIST Framework + NIST Process + Maturity Model solution requires a fresh look at:

1. *Governance* – IRM needs to be a "team sport," not just the sole responsibility of an IT or compliance department.
2. *People* – This approach requires a cross-functional team that includes people from many departments, including internal audit, legal, risk management, finance, compliance, IT, quality and operations.
3. *Process* – An organization cannot "checklist" its way to effective IRM. Using a HITRUST or ISO checklist often creates a false sense of compliance, but they are certainly not secure.
4. *Technology* – It is no longer possible to manage an IRM program on paper. It takes a comprehensive software platform to achieve desired results.
5. *Engagement* – There needs to be an organization-wide culture of information risk awareness that starts with C-suite leaders and trustees. According to an HIMSS analytics study in December 2016 for Symantec, only 34 percent of health systems have regular IRM reports at board meetings.

Five Action Items for CAEs

1. Make sure that cybersecurity risk gets formally integrated into the organization's audit plan.
2. Make IRM a "team sport," encompassing many departments (clinical, quality, internal audit, legal, risk management, IT, compliance, etc.), plus active involvement from the C-suite and board.
3. Lobby to make IRM discussions an agenda item at every board meeting.
4. Educate colleagues on the advantages of implementing the NIST Framework + NIST Process + Maturity Model approach rather than simply using controls checklists.
5. Estimate the potential cost of a data breach in your organization by using the American National Standards Institute's (ANSI) free online tool called The Financial Impact Of Breached Health Information.*

*https://webstore.ansi.org/phi/

CAEs: Catalysts for change

When the confidentiality, integrity and availability of vital health data are imperiled, the organization as a whole is in serious jeopardy.

For too long, information risk management has been unfairly relegated to just a single department such as IT or compliance. Because of CAEs' integral role in risk management, they can help foster the multidisciplinary teamwork that is required. They can insist that cybersecurity risks are formally integrated into the organization's audit plan. And they can take the lead in educating their colleagues about the escalating risks in data security—and the need to abandon checklists in favor of a comprehensive IRM solution.

It is wise to take a proactive, multidisciplinary approach to IRM.

Audit committees and hospital boards already have strong relationships, so CAEs can be instrumental in convincing trustees to make data security an agenda item at each board meeting. Vigilance and teamwork can go a long way toward helping healthcare organizations avoid the gigantic costs and reputational damage arising from preventable data breaches. **NP**