The State of **Cybersecurity** in Healthcare: Still Much Ground to Cover
Jeffery Daigrepont specializes in healthcare automation, system integration, cybersecurity, operations, and deployment of enterprise information systems for large integrated delivery networks and medical practices. His particular interests deal with data migrations, vendor contracting, strategic IT planning and optimization, security and compliance.

Christopher Kunney provides strategic, enterprise-wide solutions that address the current issues faced by health systems, including governance, meaningful use, PPACA, HITECH Act, HIPAA, EMR Adoption, CMS quality measures, and HIEs. An experienced IT leader, he has demonstrated an ability to build peak-performing teams and achieve cross-functional business objectives that effectively integrate within the clinical setting.

Terry J. Wilk’s expertise spans the full range of information technology (IT) executive oversight—from strategic planning, IT governance and organizational design, vendor selection / negotiations, complex IT system implementation, crisis management, and operational turnarounds. Mr. Wilk partners with executives, physicians, and staffs to effectively use IT to address unprecedented pressures and change.
## Contents

<table>
<thead>
<tr>
<th>Page</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Introduction</td>
</tr>
<tr>
<td>5</td>
<td>Cybersecurity Breaches on the Rise</td>
</tr>
<tr>
<td>8</td>
<td>External Attacks</td>
</tr>
<tr>
<td>11</td>
<td>Insider Threats</td>
</tr>
<tr>
<td>14</td>
<td>Cybersecurity and Today’s Healthcare CIO</td>
</tr>
<tr>
<td>19</td>
<td>Third Party Vendors</td>
</tr>
<tr>
<td>23</td>
<td>Privacy and Security Risk Analysis</td>
</tr>
<tr>
<td>28</td>
<td>Penalties</td>
</tr>
<tr>
<td>31</td>
<td>The Impact on Covered Entities</td>
</tr>
<tr>
<td>34</td>
<td>In Conclusion</td>
</tr>
<tr>
<td>36</td>
<td>Sources</td>
</tr>
</tbody>
</table>
News breaks daily about cybersecurity breaches across all industries, with the latest report appearing to top the previous event in expanse and damages. Healthcare organizations are not immune to the same threats facing other industries, though the losses from exposure may exceed other business entities due to the nature of the information. The state of cybersecurity in healthcare is improving, but there is still lots of ground to cover in order to have robust protection.

Cybersecurity in healthcare is critical to patient safety. Attacks on patient information, medical devices, and a hospital’s information systems and operations can have serious consequences. Disrupting the delivery of services, putting patients at risk for medical identity theft, and possibly endangering the lives of individuals who have a medical device are a few of the possible repercussions.

The Health Insurance Portability and Accountability Act (HIPAA) security rule requires that covered entities conduct a **security risk analysis** (SRA) of their healthcare organization. In the following pages, we address the problem of cybersecurity breaches, sources of threats, the CIO’s responsibilities, working with third-party vendors, and conducting privacy and security risk analyses. The information will help your organization take proactive steps to gain ground in developing and maintaining a strong cybersecurity posture. There’s much catching up to do.
Cybersecurity breaches on the rise
Healthcare cybersecurity is a growing concern, as evidenced by the steady rise in hacking and IT security incidents over the last few years. Many healthcare organizations have struggled to defend their network perimeter and hold cybercriminals at bay. Now more than ever, healthcare providers have to protect multiple connected medical and non-medical devices. Additionally, the number of Internet of Things (IoT) devices that are integrated into the healthcare industry has skyrocketed. Data is the new currency, and cybercriminals will stop at nothing to gain access to this valuable commodity. These offenders are developing more sophisticated methods and techniques to attack healthcare organizations and increase their chances to cash in this data by holding it at ransom or selling it on the black market.
The **2019 HIMSS Cybersecurity Survey** provides valuable insight into the information security experiences and practices of U.S. healthcare organizations experiencing hackings and compromises. Over 160 U.S.-based health information security professionals were polled, and the findings reflect the following:

- **A pattern of cybersecurity threats and experiences is discernable across U.S. healthcare organizations.** Significant security incidents are a nearly universal experience in U.S. healthcare organizations with many of the events initiated by bad actors, leveraging email as a means to compromise the integrity of their targets.

- **Many positive advances are occurring in healthcare cybersecurity practices.** Healthcare organizations appear to be allocating more of their information technology (IT) budgets to cybersecurity.

- **Complacency with cybersecurity practices can put cybersecurity programs at risk.** Certain responses are not necessarily bad cybersecurity practices but may be an early warning signal about potential complacency seeping into the organization’s information security practices.

- **Notable cybersecurity gaps exist in critical areas of the healthcare ecosystem.** The lack of phishing tests in certain organizations and the pervasiveness of legacy systems raise grave concerns regarding the vulnerability of the healthcare ecosystem.
External attacks
According to the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (DHS), approximately 15% of healthcare providers reported a data breach due to a hacking of hospital IT systems in the past 24 months. The remaining victims were other types of healthcare organizations, such as physician practices, ambulatory surgical centers, mental health facilities, rehabilitation facilities, and others. Further, approximately 2/3 of non-acute and vendor organizations reported experiencing a security incident in the past 12 months.
Unfortunately, many healthcare organizations have been slow to respond to cybersecurity threats and generally lag behind other industries in prevention. Even though cybersecurity budgets have begun to increase, and new cybersecurity technologies are being purchased, healthcare entities still struggle to thwart attacks and keep their networks secure proactively.

SOURCE: HIMSS 2019 Cybersecurity Survey
Insider threats
In addition to cybersecurity attacks from external actors, healthcare organizations continue to deal with challenges inside their organizations. Securing healthcare data and managing an effective cybersecurity program can be daunting. According to a recent Verizon Data Breach Investigation Report, 58% of healthcare PHI breaches are caused by insiders\(^2\). The report went on to state that healthcare was the only industry where internal actors are the greatest threat.
Healthcare data is primarily used internally but shared with a wide variety of individuals in order to facilitate the coordination and delivery of care. This activity is complicated to accomplish in and of itself, and to also secure the data while ensuring access to those who need it adds a layer of complexity. Even with the increased transition to electronic health record (EHR) systems, paper records are causing data security problems, according to the Verizon study. Hard copy documents were the assets most often involved in security incidents.

"Healthcare organizations, therefore, should consider instituting an effective risk management program that invests in comprehensive data breach detection measures."

This program would include table-top exercises and reviewing Internet of Things (IoT) security as just a few prevention and detection requisites. Additionally, it is mandatory for healthcare leaders to ensure that internal staff has adequate cybersecurity training and resources needed to ensure the appropriate precautions are taken to protect sensitive data from compromise by internal and external bad actors.
Cybersecurity and today’s healthcare CIO
Among other regulatory compliance requirements, cybersecurity continues to be top-of-mind for healthcare chief information officers (CIOs), chief information security officers (CISOs), executives and Boards. Healthcare entities continually face the challenge of balancing tightly-secure, protected health and financial information with providing easy authorized access within and across the organization including external entities.
As CIOs seek ways to achieve this delicate balance, they are trying to move from a reactive to a proactive position in several key areas, including the following:

<table>
<thead>
<tr>
<th>SECURITY AREA</th>
<th>CONSIDERATIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Perimeter Security</td>
<td>Also known as a de-militarized zone (DMZ), perimeter security addresses the boundary between the private, locally-managed and owned side of a network, and the public and externally-managed network such as the Internet. The DMZ is one of the highest security risks that must be continually assessed, tested, and addressed.</td>
</tr>
<tr>
<td>EHR System Security</td>
<td>EHR vendors have included various forms of security to protect unauthorized access to their systems. CIOs must ensure that their EHR system(s) security works in harmony with their network perimeter security to avoid negatively impacting an authorized user from accessing the system or degrading EHR system performance. This harmony should be assessed and verified each time a change or upgrade is made to the EHR system or the network perimeter.</td>
</tr>
<tr>
<td>End User Authentication</td>
<td>We have seen a continual rise in the number of legitimate users logging on to an organization’s wired or wireless network to access protected health information. This escalation increases the amount of network traffic to monitor for unauthorized access. CIOs need assurance that all log-in attempts are monitored and acted upon accordingly. Some CIOs have implemented a single-sign-on (SSO) solution to control and resolve these issues. Whatever solution is deployed, organizations must test, document, and resolve authentication issues continually.</td>
</tr>
<tr>
<td>User Identity</td>
<td>More organizations are implementing a virtual desktop infrastructure (VDI) in their EHR environments. It often becomes difficult to capture and audit user identities in these environments, which further raises security risks.</td>
</tr>
<tr>
<td>Internet-of-Things (IoT)</td>
<td>We are seeing an exponential number of items (devices) becoming computer-based and linked to the Internet. IoT devices such as biomedical, security cameras, and HVAC systems must be identified, continually monitored for security risks, and managed.</td>
</tr>
</tbody>
</table>
Merely complying with privacy, security, and confidentiality regulations is no longer enough. Violating these regulations often result in tens or hundreds of thousands of dollars in fines, not to mention potential destruction of an organization’s information assets, an adverse patient outcome, or negative publicity. CIOs must proactively secure and monitor their networks, applications systems, and data while conducting periodic security audits.
As the number and complexity of IT systems, devices, and users grow over time, forward-thinking CIOs are welcoming third-party advisors to conduct ongoing security audits, analyses, and penetration tests using human interaction with specialized automated tools to conduct and report on these security activities. The existence and compliance with updated privacy and security policies are under closer scrutiny along with employee behavior and habits in complying with these policies. Additionally, updated cybercrime and security education and training must be implemented on an ongoing basis.

CIOs are expected to develop and implement a cyber defense strategy to protect their healthcare organizations and patient information. Those CIOs who openly assess their vulnerabilities, prioritize their actions, and continually monitor and manage their security risks are best positioned to help their organizations grow efficiently, effectively, and safely.
Third-party vendors
If dealing with your own security threats wasn’t a big enough challenge, you must also ensure all your business associate (BA) partners are compliant. Many organizations mistakenly assume a signed business associate agreement (BAA) is enough for ensuring that third-party vendors are compliant and responsible for their own breaches. While having a BAA is a critical first step, it is insufficient in and of itself. There are three common misconceptions when it comes to the BAA:

- The third-party vendor or person doing work for the hospital/practice is not storing PHI data; therefore, they are not considered a BAA. This presumption is false. If they have access to data, they qualify as a BA and must sign a BAA.

- All third-party vendors use encryption and offer a privacy statement. Again, false. They still have access to the data, and encryption is not always a 100% safeguard.

- All third-party vendors use encryption and offer a privacy statement. Again, false. They still have access to the data, and encryption is not always a 100% safeguard.
Many security breaches happen as a result of primary vendors using unknown, down-the-chain resources who are not directly contracted with the hospital/practice. In some cases, these are individuals who may come from staffing agencies and/or work as freelancers. They will usually be unaware of policies or standards. They carry no insurance and would have no means of protecting anyone if they cause a breach, so there would be little to no recourse.
Further, they may not even be in the United States. Therefore, here are several tips to reduce security threats when working with third-party vendors:

- All subcontractors must be preapproved. Under no circumstances can any vendor use subcontractors without prior permission.
- Vendors must disclose all existing subcontractors and require each to sign the BAA provided by the hospital/practice and present proof of insurance. If covered under the primary vendor’s insurance policy, require evidence.
- All vendor contracts should require provisions about cybersecurity breaches. Specifically, the vendor must be responsible for their mistakes and the cost to remediate the issue.
- The BAA should have a breach notification requirement mandating the vendor notify of any incidents.
- There should be a data return policy and/or destruction requirement upon termination of a vendor’s contract.
- System access should have a start and end date. Most systems today allow for setting an expiration date.
- Require the right to audit and inspect adherence to these policies at any time.
- Have vendors provide evidence of their own security risk analyses, compliance certifications, and proof of staff privacy training.
- Revisit policies and the BAA after each major upgrade, new release, and version change as these events are when new contractors are often introduced.
- Consider adopting contract management software to help manage and track key dates and documents as these BAAs are updated annually.
Privacy and security risk analysis
The Health Insurance Portability and Accountability Act (HIPAA) Security Rule requires that covered entities conduct a security risk analysis (SRA) of their healthcare organization. A risk analysis helps your organization ensure it is compliant with HIPAA’s safeguards. A risk analysis also helps reveal areas where your organization’s protected health information (PHI) could be at risk.
In 2013, the Final Omnibus Rule updated the HIPAA Security Rule and Breach Notification clauses of the HITECH Act. The new regulations further extended the requirement to conduct a HIPAA risk analysis to business associates, and also increased the amount a covered entity or business associate could be fined for non-compliance with HIPAA regulations.

The failure to conduct a HIPAA risk analysis can be costly. The severity of fines for non-compliance with HIPAA has historically depended on the number of patients affected by a breach of PHI and the level of negligence involved. Fines are now issued in the lowest “did not know” HIPAA violation category. The federal government says there is little excuse for not knowing that organizations have an obligation to protect PHI.

The Office of Civil Rights (OCR) has the responsibility to provide guidance to regulated entities about conducting risk analyses. *Guidance on Risk Analysis requirements under the HIPAA Security Rule* describes nine essential elements a risk analysis must incorporate, regardless of the risk analysis methodology employed.
These elements are as follows:

**Scope of the Analysis.** All ePHI that an organization creates, receives, maintains, or transmits must be included in the risk analysis. (See 45 C.F.R. § 164.306(a).)

**Data Collection.** The data on ePHI gathered using these methods must be documented. (See 45 C.F.R. §§ 164.308(a)(1)(ii)(A) and 164.316(b)(1).)

**Identify and Document Potential Threats and Vulnerabilities.** Organizations must identify and document reasonably anticipated threats to ePHI. (See 45 C.F.R. §§ 164.306(a)(2), 164.308(a)(1)(ii)(A) and 164.316(b)(1)(ii).)

**Assess Current Security Measures.** Organizations should assess and document the security measures an entity uses to safeguard ePHI. (See 45 C.F.R. §§ 164.306(b)(1), 164.308(a)(1)(ii)(A), and 164.316(b)(1).)

**Determine the Likelihood of Threat Occurrence.** The Security Rule requires organizations to take into account the likelihood of potential risks to ePHI. (See 45 C.F.R. § 164.306(b)(2)(iv).)
Determine the Potential Impact of Threat Occurrence. The Rule also requires consideration of the “criticality,” or impact, of potential risks to confidentiality, integrity, and availability of ePHI. (See 45 C.F.R. § 164.306(b)(2)(iv).)

Determine the Level of Risk. The level of risk could be determined, for example, by analyzing the values assigned to the likelihood of threat occurrence and resulting impact of threat occurrence. (See 45 C.F.R. §§ 164.306(a)(2), 164.308(a)(1)(ii)(A), and 164.316(b)(1).) The risk calculation process is taken from the National Institute of Standards and Technology (NIST) 800-30.

Finalize Documentation. The Security Rule requires the risk analysis to be documented but does not require a specific format. (See 45 C.F.R. § 164.316(b)(1).)

Periodic Review and Updates to the Risk Analysis. The risk analysis process should be ongoing. In order for an entity to update and document its security measures “as needed,” which the Rule requires, it should conduct continuous risk analysis to identify when updates are needed. (45 C.F.R. §§ 164.306(e) and 164.316(b)(2)(iii).)
Penalties
HIPAA was established in 1996, with an annual cap of $25K for all violations of an identical provision. Over the last two decades, only a few revisions have been made to the civil monetary penalties (CMP) limits.

On April 26, 2019, a new structure for HIPAA violation CMP was announced by the OCR. As a result of this change, the financial risk of HIPAA breach violations for covered entities that can demonstrate updated security risk management plans, policies, and procedures for sensitive patient data were significantly reduced.
KEY CHANGES IN HIPAA/HITECH CMP
ANNUAL LIMITS

TIER 1 – No Knowledge – Annual limit reduced from $1.5M to $25K

TIER 2 – Reasonable Cause – Annual limit reduced from $1.5M to $100K

TIER 3 – Willful Neglect – Corrected - Annual limit reduced from $1.5M to $250K

TIER 4 – Willful Neglect – Not Corrected - Annual limit unchanged at $1.5M

2009 ANNUAL LIMITS (HITECH)

<table>
<thead>
<tr>
<th>Capacity</th>
<th>Minimum Penalty/Violation</th>
<th>Maximum Penalty/Violation</th>
<th>Annual Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tier 1 - No Knowledge</td>
<td>$100</td>
<td>$50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Tier 2 - Reasonable Cause</td>
<td>$1,000</td>
<td>$50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Tier 3 - Willful Neglect</td>
<td>$10,000</td>
<td>$50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Tier 4 - Willful Neglect</td>
<td>$50,000</td>
<td>$50,000</td>
<td>$1,500,000</td>
</tr>
</tbody>
</table>
The impact on covered entities
Organizations that maintain thorough and well-documented HIPAA compliance and risk management programs reduce their risk of financial exposure to civil monetary penalties from HHS/OCR. Preserving the appropriate privacy and security documentation necessary to satisfy compliance with the key HIPAA security rule is critical. This also includes conducting a security risk analysis (SRA) to help covered entities avoid the fourth and highest-level of liability for “willful neglect – not corrected.”

"The SRA should be performed at least annually, and should include an assessment of the covered entity’s technology infrastructure and information security policies and procedures."

The SRA should consist of a remediation plan to outline the actions that will be undertaken to address any weaknesses in the organization’s security program. The use of risk analysis and risk management tools, such as the ones leveraged by us at Coker Group, can be effective resources in assessing and managing any gaps identified through the SRA process. Risk analysis tools can provide a method of documenting each recognized risk event or vulnerability point in the organization, including those with business associates. They also serve as a repository of your organization’s security remediation efforts and can be used as evidence in the event the covered entity is subject to an audit from the Office of Civil Rights (OCR). This detailed documentation validates that a covered entity has an effective risk management program in place and may help to prevent the “not corrected” status associated with the $1.5m annual limit.
Also, OCR has stated that it will be actively auditing organizations that do not report any breaches. Therefore, covered entities with the most accurate security risk analysis and comprehensive breach detection program will reduce the likelihood of the imposition of fines and penalties as a result of a security audit or breach.
In conclusion
The findings of the 2019 HIMSS Cybersecurity Survey suggest that healthcare organizations’ cybersecurity initiatives are moving in the right direction with some degree of uniformity. However, we still have a long way to go in comparison to other industries. While the progress is positive, budgets allocated to cybersecurity are still inadequate to deal with all the emerging cybersecurity threats that most healthcare organizations face. Moreover, the lack of knowledgeable cybersecurity personnel also continues as a detriment to progress.

Legacy systems and lack of staff awareness continue to present a problem in need of innovative approaches. On the whole, healthcare organizations are moving in the right direction, but bad actors continue to stay one step ahead in the game.

Coker Group and its partners have developed a comprehensive and cost-effective approach to conducting a security risk analysis that meets the nine essential elements as required by The Office of Civil Rights (OCR). For additional information on Coker’s comprehensive cybersecurity risk analysis, contact us at 800.345.5829 or email info@cokergroup.com
Sources


3. A “business associate” is a person or entity, other than a member of the workforce of a covered entity, who performs functions or activities on behalf of, or provides certain services to, a covered entity that involves access by the business associate to protected health information.

4. “Business Associate Agreement.” Covered entities must ensure that they have a current HIPAA business associate agreement in place with each of their partners to maintain PHI security and overall HIPAA compliance. These partnerships are known as business associate agreements (BAAs).

