Future Proof Your Healthcare Organization with an Information Security Management Program

By Chandragupta Gudena, Merritt Neale and Mike Seiser

Data breaches, malware and other security hacks are on the rise across healthcare organizations. Happening in parallel is the adoption of new technology like the cloud, artificial intelligence, and patient engagement tools that seek to increase efficiency, improve data accessibility and drive down cost. While these advancements offer many benefits, if appropriate security measures aren't established from the start, they leave healthcare organizations vulnerable to cyberattacks that expose patient data, impact an organization's brand reputation and result in millions of dollars in losses, essentially eliminating all potential cos cost savings these technologies promise.

Instead of simply reacting to these cybersecurity threats, take a proactive approach by applying findings from your security risk analysis to the creation of a comprehensive security management program that mitigates risk and addresses vulnerabilities before they are exploited.

Build Your Program Off the Analysis

While a security risk analysis is a federal requirement for a number of compliance areas such as Health Insurance Portability and Accountability Act (HIPAA) or Federal Information Security Modernization Act (FISMA), it can be foundational in mitigating cybersecurity attacks regardless of compliance mandates. However, they're only as valuable as what you put in. Simply checking the boxes on the assessment doesn't make your healthcare organization any more secure, nor does creating information security management policies that align to the analysis but doing little to enforce them.

A thorough analysis that covers your entire organization and all areas of information management and enabling technologies will identify where vulnerabilities lie and their degree of severity. This gives you a clear picture of what needs to be improved and how quickly you need to react, which can be incorporated into a information security management program. Just like it's critical to do something with your security risk analysis results, the same is true with the framework for your program. You must use it as a platform to address gaps and vulnerabilities in your organization. This involves aligning policies, processes, technology and people.

As part of your security management program, consider the following:

- **Don't just write a policy, enforce it.** Put policy measures in place and hold staff accountable to them. Many organizations have written policies, but they don't enforce them. As a result, those in the organization have little incentive to follow them, leaving the organization at risk.
- **Optimize your existing security technology investments.** A common response to a security breach is an investment in cyber security technology. While technology is essential for mitigating a breach, it's not the solution. For information and cyber security technology solutions to deliver on their promise, they must be well designed, well implemented and well established as part of a continuous improvement process, especially as organizations integrate new technologies and processes into the organization. To ensure this occurs put staff in roles where they are managing your technology-related risk otherwise these investments won't have as much of an impact or benefit as they should.
- **Empower your chief information security officer (CISO) with decision-making authority and align them to compliance:** A CISO's role sits at the intersection of IT security and risk management. This is vastly different than the role of a chief information officer who's focused on getting new or changed IT services to customers cheaper and faster with ever increasing gains in technology efficiencies. And at times these roles don't see eye to eye, especially when security protocols hinder process improvements or time to market. However, it's common for a CISO to report to the CIO—making it difficult for a CISO to optimally perform their job. An alternative reporting approach is to more closely align a CISO with those responsible for compliance, regulations or enterprise risk management.
- **Hire security analysts.** Instead of having existing IT staff responsible for managing security technology and managing the information security management program, dedicate individuals strictly to audits, policies, procedures and managing your security program. This will allow them to focus on monitoring data. generated by technical controls and make sure security protocols (e.g. cyber and internal controls) are implemented correctly without having the added complexity of day-to-day security control operations.
- **Engage physicians, nurses and staff in continuous improvements.** Ensure that staff know why information management security policies and procedures are in place. By giving them a better understanding of why they're required to perform certain security measures that may seem redundant or laborious you can instead gain buy in. At the same time, by listening to their feedback, you can identify areas of improvement.

Implement the Program

As you put your information security management program in place, take the following steps to drive sustainable results:

- **Communicate results of your security risk analysis to leadership and the board to get funding.** Share the results along with your plan to move forward with your leadership and board. Then request funding to make improvements just like you would do for funding for any other program. It's important to emphasize that this is a continuous, long-term investment and it is separate from the funding of other technologyrelated projects.
- **Communicate with your staff.** Keep them closely engaged along your cyber security journey. Share the security risk analysis results, the framework that you've put in place, new initiatives that you're launching to mitigate risk and seek their feedback. This will increase engagement around the policies you've put in place.
- **Implement the program and seek continuous improvement.** Once you've established a path forward, execute on it and periodically reassess progress. If new technologies are implemented, proactively address potential security gaps at the

outset and address them during implementation. If compliance or other regulatory changes occur, quickly reassess and understand your gaps.

As technology becomes more vital to managing healthcare operations and improving health outcomes, organizations cannot afford a hack or data breach. These security incidents are not only expensive to address, but they negatively impact your brand reputation. A comprehensive security management program should strike a delicate balance between mitigating risk and allowing people to do their jobs effectively. It should use your risk analysis as a critical foundation for building the program which will increase security at your organization today and propel your organization into the future.

Key Takeaways

As you take a proactive approach to information security and develop your security management program:

Think differently.

Prioritize breach prevention rather than focusing solely on reactive cyber security strategies.

Plan differently.

Frame a security risk analysis as more than just a box that must be checked, but as a way of building a strong and mature security foundation.

Act differently.

Leverage a risk assessment framework, develop a program and invest in people, process and technology to establish an information security management program that supports a strong business today and future growth.

HURON

huronconsultinggroup.com