Cybersecurity risks: Are you prepared?

Maintaining a secure posture: How strong cybersecurity practices help keep organizations healthy

Now more than ever, cybersecurity threats continue to increase, specifically in the healthcare industry. Hackers can and will continue to wreak havoc in times of vulnerability because they thrive in chaos. Being proactive with a secure enterprise should always be top of mind for healthcare organizations.
Table of contents

Executive summary ............................................................................................................. 3
An increase in cyber attacks .............................................................................................. 3
Data protection is everyone’s responsibility ........................................................................ 4
How can health care organizations proactively prepare? .................................................. 5
Cerner serves as an extension of your team ......................................................................... 8
Closing .................................................................................................................................. 8
It is no surprise that attackers target the healthcare industry. Numerous factors have contributed to this increase, which include a global pandemic and the amount of sensitive data that is stored at healthcare organizations. A shift in mindset about who is responsible for a cybersecurity posture must occur. This responsibility does not fall solely upon the shoulders of the IT department. Instead, this is an enterprisewide effort. Having an effective cybersecurity program helps secure your enterprise and can be comprised of incident response planning, cybersecurity insurance, identity and access management, patch management, auditing strategies and robust training across the organization at a minimum.

**Increase in cyberattacks**

There are many factors that contribute when a health system has an insecure enterprise. Perhaps the largest risk is inadequate funding for enough headcount to handle expectations and workloads coupled with the work required for good cyber hygiene. Hackers thrive in chaos, targeting the most vulnerable during crisis situations, which makes the healthcare industry an easy target.

Even if a healthcare organization has the appropriate funding, the resources and technology requirements to build a world-class defense can be daunting. Technology alone can be enough to potentially drive a hospital into bankruptcy.

More recently the healthcare industry has been hit hard with the effects of the global pandemic, playing a large part in the increase of cyberattacks. When you couple a global pandemic with overworked, underfunded and understaffed IT teams, it can result in an environment where hackers thrive. Healthcare organizations have had to shift their mindset since March 2020.

The cyberattacks in the healthcare industry nearly
As illustrated above, cybersecurity impacts the entire health system and is everyone’s responsibility.

doubled in 2020, with 28% of all attacks tied to ransomware.¹ This resulted in one ransomware hacking group making over $123 million in profits.¹ Sadly, we are beginning to see the same trend in 2021. A few things to consider are:

- Health and well-being of employees
- Security controls established for remote workforce
- Cybersecurity best practices in employee homes
- Help desk equipped to facilitate requests now that the workforce is remote

**Data protection is everyone’s responsibility**

Healthcare organizations should not deprioritize cybersecurity as part of their business strategies. Cybersecurity not only falls within the purview of the IT department; the responsibilities lie within the entire health
system. The potential impacts of a security incident could affect the entire health system, IT, regulatory, clinical and finance.

Here are a few examples of departments that can be impacted when a cyber event occurs:

**IT department**
- Recovering from a ransomware event
- Value of the data being protected

**Regulatory department**
- Fines associated with a breach and exfiltration of data

**Finance department**
- Lost revenue determination
- Costs associated with employees' time lost

Healthcare C-suite executives now have an understanding of the impacts when a breach occurs. This will provide an executive the full picture of potential business risks and when the IT department plans and prepares a budget, the C-suite has better context.
How can health systems proactively prepare?

Incident response planning should be a health system’s top priority when preparing for a cybersecurity event. Development of an incident response plan does not require any additional technical investment; it simply defines a protocol your organization will follow using current technology and existing resources. While an established plan cannot prevent an attack from occurring, the worst time to make critical decisions is during a cyber event and with no plan. Hackers do not care about your business goals and objectives; they are more than happy to attempt attacks at the most inconvenient time, like during the middle of a major system upgrade.

Incident response planning is similar to practicing for a natural disaster. Healthcare organizations need to examine how to handle a digital disaster with the same mindset. Once the plan is established, the next step is to examine people, process, technology, risk, regulatory requirements and business continuity. Often times, organizations have the appropriate technology and it is a matter of adding the appropriate processes around those pieces of existing technology.

Sometimes health systems are lulled into a false sense of security simply because they have purchased cybersecurity insurance and expect that to cover any damages. Unfortunately, insurance may not be an adequate failsafe for organizations that haven’t proactively prepared for a cybersecurity event. Some insurance companies still hold the health system accountable for maintaining a secure posture, and there are reports of claims being denied due to poor prevention practices, failure to document preventative measures, third-party risks, errors and omissions.

One way to demonstrate a good security posture for insurance purposes is to have an incident response plan, keep it updated and exercise the plan twice a year to ensure it is current in the event of a security breach. Organizations that have a team dedicated to IR planning and tested the plan, realize $2M in average savings per data breach compared to those without an IR team or plan established.²

When used as part of a comprehensive, end-to-end approach, cybersecurity insurance is another step that healthcare organizations can implement to protect their enterprise. In the event of a breach, insurance can help health systems fix damaged computer systems or restore patient information that may have been compromised. Cybersecurity insurance comes in three forms:

- First-party written coverage
- Third-party written coverage
• Implicit cybersecurity coverage (non-affirmative cyber exposure)

On average, a healthcare data breach can cost an organization $7.13M, which is up from 10% from 2019. Approximately 80% of those breaches resulted in the exposure of personal identifiable information (PII), among the costliest to the breached organizations. Making sure they have coverage on patient health records, devices, equipment, etc. will help restore systems and technology.

In addition to IR planning and cybersecurity insurance, implementing an identity and access management (IAM) strategy is key for an effective program. Too often, firewalls tend to be the edge for security and safety from bad actors. There are too many instances where simple passwords are reused in several different systems, which gives a hacker access to numerous systems after uncovering only one of these passwords. All the age-old rules around IAM are more important than ever for healthcare organizations.

Organizations must take steps for an effective multifactor authentication strategy. Multifactor authentication should be treated as the new edge for a security best practice.

You can take steps for an effective multifactor authentication strategy for your organization;

1. Establish a password policy to address items like, but not limited to:
   • Meeting a character minimum
   • Using certain character types (mixed case, numerals and special characters)
   • Preventing users from choosing previously used passwords
   • Requiring passwords to be changed frequently

P2Sentinel™ 7 generates reports extremely fast, which makes the workflow more efficient, and provides a dashboard of tools that provide a snapshot of various activities in the EMR. These tools allow drilling down to the details of the aggregated data, as needed, such as monitoring access to high profile patient charts or excessive user activity by personnel role.

- Yvonne Walters, Privacy Officer & Compliance Specialist,
  Southwest General Health Center
2. Understanding all applications and their locations, including:
   - Determining which applications require multifactor authentication
   - Knowing cloud solutions so the IAM strategy extends for those services
   - Keeping an accurate inventory

Knowing the types of threats to protect against is critical. Vulnerability and Threat Management Process (VTM) should not be overlooked in a cybersecurity program. Establishing a process for any device on your network with an IP address can include; network devices, servers, PCs, laptops, medical devices, mobile devices, IoT devices, etc. By knowing where devices are located within your enterprise, software currency and vulnerability management will help drive how your VTM process is built.

Having a solid auditing strategy is a final, yet effective, strategy for a cybersecurity program. In today’s cyber environment, there are too many connected devices to review logs manually or by using a simple automation or a script. Implementing a security information and event management (SIEM) tool is an effective way to collect, correlate and act upon logs. To get the full effect of the SIEM tool, have it managed by a security operations center (SOC) to provide your environment with continuous 24x7 monitoring.

Implementing the SIEM tool is an effective first step to ensure you have a sound auditing strategy in place. Organizations tend to overlook the configuration of the logs collected. It’s important because it provides the details behind each log being collected. Understanding the entire lifecycle of each log tells you what network, VPN, active directory, application, cloud services, medical and mobile devices each user in your organization have accessed. To keep up with the demands of the everchanging IT landscape, healthcare organizations should review and baseline on a quarterly basis.

**Cerner is an extension of your team**

More than an electronic health record company, Cerner understands healthcare and cybersecurity and the importance of their correlation. Our aim is to improve your organization’s security posture. Cybersecurity experts act as an extension of your team, helping to meet compliance and regulatory requirements with a customized security strategy tailored to meet your organization’s unique needs and budgets.
Sources


About Cerner

We’re continuously building on our foundation of intelligent solutions for the healthcare industry. Our technologies connect people and systems, and our wide range of services support the clinical, financial and operational needs of organizations of every size.

Contact us for more information

- cybersecurity@cerner.com
- Cerner.com

2800 Rock Creek Pkwy.
North Kansas City, MO 64117