ARCTIC WOLF

TECH HEADS

The Healthcare Cybersecurity Checklist

The healthcare industry is a prime target of cybercriminals: Hospitals, clinics, nursing homes, and other providers hold rich sources of sensitive personal information. This data can be exploited or held "hostage" in increasingly prevalent ransomware attacks. By accessing patient-critical information and then withholding it from the provider, hackers threaten the operations and security of healthcare organizations and the privacy and safety of their patients.

77%

of healthcare organizations have been breached[1].

DATA BREACHES CAN CLOSE DOWN HOSPITALS, **WHICH DIRECTLY IMPACTS PATIENT CARE**

In addition, the industry suffers from its use of legacy systems and complicated IT infrastructures that frequently leave vulnerabilities for attackers to exploit. Data breaches can close down hospitals, which directly impacts patient care, and has even been shown to increase the number of fatal heart attacks in the U.S.

Amidst these growing challenges, healthcare providers need a solid, well-implemented strategy for cybersecurity that will not only protect patient and organizational data, but also help them take care of those in need.

Use this checklist to develop your cybersecurity strategy, step by step:

66%

of organizations say it's difficult to retain cybersecurity talent[2]

Create a Security-Conscious Workforce

While they have the best of intentions, people often use shortcuts to work more efficiently. In doing so, they frequently engage in sloppy practices—like keeping passwords on a sticky note stuck to their monitor. Creating a work culture that emphasizes cybersecurity is the best way to mitigate the risks and pitfalls that come from human error.

- **Implement an ongoing schedule for security training and education.** These activities must involve all workers, and include updates on known attacks and information about best-in-class security procedures, such as two-factor authentication and password managers.
- **Evaluate IT processes for complexity.** Keep ease-of-use in mind whenever you update or alter processes to avoid having users turn to insecure shortcuts.
- **Restrict access to data and applications.** Employees should only be able to access information needed to perform their job; this same rule applies for physical access.
- **Implement data usage controls.** Block unsafe actions like uploading data to the web, sending emails to unauthorized addresses, or copying to external drives.
- **Establish a password policy.** Such a policy should require regular password changes, not writing down passwords, and using strong passwords.

Inventory and Control: Hardware and Software Assets

You can't secure assets you don't know you have. Reducing your organization's attack surface starts by having a complete view of all devices on your network. This can be difficult in healthcare, where hospital IT organizations control the network, but individual medical departments purchase and maintain their own medical devices. That gives hackers opportunities to access hospital networks via unpatched medical devices and then steal patient records from internal systems.

- **Document and secure all devices that could access the network.** This includes medical devices, onsite hardware, and staff personal devices.
- **Ensure that guest networks run on hospital/clinic grounds.** Use these for patients and visitors.
- **Use inventory tools to keep up-to-date records.** This goes for all existing software and hardware.
- **Oversee all user access to the network.** Record authentication errors and unauthorized access, and sweep the network for unusual activity.
- **Quickly disconnect any detected unauthorized devices.** Your network must keep unauthorized devices out, as well as devices that run potentially dangerous software.

Continuously Analyze, Prioritize, and Manage Vulnerabilities

Monitoring for security risks is a central tenet of HIPAA (Health Insurance Portability and Accountability Act of 1996) requirements. The IT team must have 24x7 cybersecurity operations to effectively manage vulnerabilities, monitor and detect threats, and respond to malicious and risky activities in real time.

- ✓ **Identify vulnerabilities and prioritize what needs patching.** A risk-based approach to vulnerability management enables an organization to eliminate vulnerabilities in methodical fashion, starting with the most severe risks and then addressing others in descending order of severity.

Secure Hardware and Software Configurations on Mobile Devices, Laptops, Workstations, and Servers

Manufacturers design default configurations with user experience and ease-of-use in mind. Security tends to be an afterthought. Basic controls, old protocols, preinstallation of unneeded bloatware, and open ports are easy targets for cybercriminals.

Configuration needs don't stop when users get access to devices, as you'll need to watch continuously for changes when systems are patched or updated.

- ✓ **Train staff on anti-virus and anti-malware requirements.** They also must understand the process for implementing automatic software updates to ensure that vulnerabilities are patched safely.
- ✓ **Configure items before they're put into use.** Be sure to remove all default settings and passwords.

62%

of hospital administrators feel inadequately trained or unprepared to mitigate cyber risks[3]

Maintain, Monitor, and Analyze Logs

Without logs for analysis, attacks may go unnoticed and uninvestigated. That leaves the door open to additional attacks and untold potential damages. Most IT teams keep audit records for compliance purposes, but attackers know there are many organizations that lack the time or resources to review logs on a regular basis. This leaves hackers opportunities to access systems and data undetected.

- ✓ **Log, monitor, and analyze security risks.** All HIPAA-covered entities need to record and examine log activity and analyze the resulting log information.
- ✓ **Continuously monitor your environment.** Ensure you have an audit trail when an incident occurs.
- ✓ **Perform regular risk assessments.** This helps identify weak points in the system.
- ✓ **Be ready to report.** Use managed vulnerability assessment services to gain an understanding of your organization's IT security posture and risk profile.

Back Up Data Offsite

In ransomware attacks, cybercriminals steal data and offer to return it only upon payment of a ransom. A second cache of critical data is essential to avoid having to pay this ransom, and also enables data recovery in the event of a natural disaster or system failure.

- ✓ **Maintain a current, flexible, secure, and speedy process to access data at all times.** Organizations need a recovery solution that allows them to recover data and bring applications back online as seamlessly as possible.
- ✓ **Ensure HIPAA compliance.** It must extend to your offsite data backup and recovery partner.
- ✓ **Consider cloud and physical backup solutions.** Develop a backup schedule that takes the frequency of update needs into account.

Stay on Top of HIPAA Compliance

HIPAA compliance deserves its own security strategy. All healthcare providers covered by HIPAA must be ready to show how they protect sensitive personal information and how they are prepared to report any data breaches to relevant authorities.

- ✓ **Ensure data protection tools and policies are implemented and followed.** That way you can demonstrate compliance with regulations when audited.
- ✓ **Hire a data protection officer and establish written contracts with external partners.** This will ensure compliance across your organization.
- ✓ **Record all data breaches.** You'll need to, where necessary, report these to relevant authorities. Or look to integrate with a partner who will document and report on vulnerabilities and breaches.

$6.5 MILLION

The average cost of a data breach in the healthcare sector.[4]

TAKE THE NEXT STEP TO **BETTER SECURITY**

The bottom line? Security isn't a project at your healthcare organization, it's a process.

Arctic Wolf® can help. Discover how the security operations experts can help you check off the items on your healthcare security list in the most comprehensive, secure, and affordable way possible.

Contact us to schedule a demo and learn more about how we help healthcare organizations keep their data—and that of their patients—secure.

ABOUT ARCTIC WOLF

Arctic Wolf® is the market leader in security operations. Using the cloud-native Arctic Wolf® Platform, we provide security operations as a concierge service. Highly trained Concierge Security® experts work as an extension of your team to provide 24x7 monitoring, detection, and response, as well as ongoing risk management to proactively protect systems and data while continually strengthening your security posture.

For more information about Arctic Wolf, visit arcticwolf.com.

Sources

1 2018 Thales Threat Report
2 ISACA
3 Black Book Market Research
4 Ponemon Institute

ARCTIC WOLF

TECHHEADS

SOC2 Type II Certified

AICPA SOC

ISO 27001 CERTIFIED
CYBERGUARD COMPLIANCE

Contact Us

techheads.com
1-503-639-8542