FREQUENTLY ASKED QUESTIONS:

CYBERSECURITY IN HEALTHCARE

What are the top 3 security challenges facing healthcare organizations?

Healthcare companies are increasingly being targeted by cybercriminals and face many information security challenges. Of these, the top three proven to be the most disruptive to business in the first half of 2016 are:

- **Ransomware:** A type of malware designed to block access to a computer system until a sum of money (or ransom), is paid. Ransomware has become highly sophisticated and effective detection and response against attacks requires continuous monitoring.

- **Phishing:** An attempt to obtain sensitive information such as user names, passwords, and credit card details for malicious reasons, by posing as a trustworthy entity in an email or other electronic communication.

- **Data breach/leak:** A major security incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen, or used by an unauthorized entity.

What makes an organization vulnerable to these security threats?

A combination of people, process and technology make companies susceptible to these security threats.

- **People:** Good people with inadequate cybersecurity training failing to recognize possible threats may unknowingly cause as much damage as people with malicious intent.

- **Process:** Having a documented process for prevention and incident response is critical to immediately detecting and responding to security threats. If an organization doesn't have an incident response plan in place or if there are gaps in the plan, they can easily be exploited by attackers.

- Technology: Security products are like a bike that needs constant uphill pedaling. When you stop pedaling the bike stops. Having the right combination of products, expertise, and services is critical to combating sophisticated attacks.

How should companies plan for security staffing?

The rule of thumb is to have 1 FTE for every 300 employees. If a company already has a dedicated IT team, roughly 10% of that IT team should be focused on security. To run a full time 24/7 security operations center (SOC), Gartner estimates it requires 8–10 FTEs including additional management staff and architects. A more affordable alternative to this scenario is to outsource part of your security team — this also provides the benefit of getting different vantage points from inside and outside of the company.

What makes Arctic Wolf's 24/7 SOC-as-a-Service unique?

Arctic Wolf's 24/7 SOC is staffed with more than 25 security engineers and analysts, management staff, and a security architect to serve more than 60,000 users. The SOC analyzes roughly 3.5 Billion events a day through best-of-breed technologies such as machine learning, big data analytics, forensic capability, security intelligence, threat feeds, perimeter and application monitoring, and other ITIL framework tools. The goal is to collect and analyze all of the machine data through various tools to get different vantage points. If an organization needs similar capabilities but cannot afford to have a dedicated team and the extensive technology required, they might consider outsourcing their SOC at a fraction of the cost to a managed detection and response (MDR) company like Arctic Wolf.

Is it necessary to choose between best-of-breed or working with a single security vendor?

Effective cybersecurity requires specialized tools for each use case which often, but not always, means working with multiple vendors. This can help correlate security events through multiple devices to get different vantage points. A good example of this is the common recommendation to have Anti-Virus, Firewall, and Content Filters from different vendors. Using a single tool for security and operations may cause conflict of interest apart from false positives.

What about developing a security training program for employees?

The best place to start is annual basic training for employees that covers all aspects of the top 3 security threats facing healthcare organizations (ie: what you need to know about cybersecurity threats and prevention). Train employees on how to recognize and respond to threats so they understand their role in helping to recognize and prevent attacks. Hold a training refresher every six months to update employees on new learnings and threats. Send all employees quarterly reminders in the form of tips and tricks and best practices to conduct business securely so security is regularly front of mind.

Have specialized trainings for people that have external email responsibilities such as sales, marketing, or customer support on email and Phishing attacks. Develop regular company-level best practices such as sending some test emails to see vulnerable users who can be re-trained. Drop some USBs around in the office to see who plugs into their computers, manage a training dashboard, and have some fun and learn with training gamification. If you don't have expertise or resources to develop, manage and measure security training effectiveness, this is something that can be outsourced to the security experts at Arctic Wolf Networks.

Will legacy systems and old medical devices prevent healthcare organizations from de ploying effective cybersecurity measures?

There are some business cases that prevent security and IT teams from upgrading certain systems and devices. For these organizations you can use strong role-based, access-control mechanisms. Check to see who has what kind of access to which systems or devices. The IT team should lookout for patches and updates to OS and if vendors are still available, check with them to understand best security practices. Conduct regular security audits. See if you can avoid Internet connectivity on those systems. If the systems should have Internet connectivity, put a Firewall between them and other legacy systems/ IT. Good anomaly detection capabilities also help improve quick response to incidents. Have a proper incident response (IR) plan and have the IR team prepared through fire drills.

How can investment in cybersecurity training and incident response planning show value in tight budget situations?

Senior management needs to be made aware of the security risks facing an organization so they can make a case for IR enhancements to their executive boards. This can be done by providing data on attempted attacks, mitigated incidents, and recent breaches or cyberattacks covered in the media. Another way to provide convincing and unbiased metrics is to engage a third party managed detection and response service provider to evaluate and manage your response plan. Arctic Wolf's affordable SOC-as-a-Service installs in minutes and starts continuously monitoring and analyzing your environment to ensure proactive detection and response to threats. Response management and reporting provides hard data on attempted breaches, mitigated incidents and cost-savings from less time and resources spent on data analysis and chasing false positives.

Contact us
arcticwolf.com
1.888.272.8429
ask@arcticwolf.com