WEBINAR SUMMARY

December 3, 2020

black hat

Stopping Snake Oil with Smaller Healthcare Providers: Addressing Security with Actionable Plans and Maximum Value

Mitchell Parker, CISSP, CISO, Indiana University Health
Tim Vidas, Senior Distinguished Engineer, Secureworks

KEY TAKEAWAYS

- When done right, risk assessments can be used to develop effective risk management plans.
- COVID-19 has introduced additional risks to the healthcare industry and its data.
- The technologies and tools in use—and not in use—impact risk.
- The right processes and policies increase security.
- Secureworks solutions focus on what matter most to healthcare organizations.

in partnership with

Secureworks

OVERVIEW

Healthcare has been affected by ransomware, data breaches, and other types of hacks. In addition, during the COVID-19 pandemic, with more people working from home, the security risks to healthcare providers are further increased. Unfortunately, numerous "snake oil" companies have taken advantage of healthcare organizations' fears about security gaps by selling expensive and ineffective risk assessments.

But when done right, risk assessments can offer healthcare organizations significant value in assessing security risks and being used to help develop actionable risk management plans. Identifying and planning for the biggest, most costly, most likely risks allows providers to protect against and quickly respond to attacks, ensuring business continuity.

Secureworks provides a portfolio of software and services that include threat detection and response as well as vulnerability detection and prioritization. These solutions focus on meaningful, actionable communications.

CONTEXT

Mitchell Parker discussed the benefits of risk assessments and risk management plans, as well as some of the tools, technologies, processes, and policies healthcare providers need to take into consideration. Tim Vidas discussed challenges the healthcare industry has faced since the COVID-19 pandemic began, and shared recommendations for actionable and valuable incident response strategies.

KEY TAKEAWAYS

When done right, risk assessments can be used to develop effective risk management plans.

Risk assessments have a somewhat tarnished reputation among some healthcare providers. That's because some risk assessments have cost providers a great deal without delivering any value. But when done right by a knowledgeable company, risk assessments can give healthcare organizations the information and tools they need to develop risk management plans that create maximum value and immediate returns.

> Snake oil companies have provided risk assessments that cost smaller practices tens of thousands of dollars and don't deliver anything of value.
>
> *Mitchell Parker*

Tips for Conducting a Good Risk Assessment

- **Conduct the risk assessment internally** with outside help. Don't have an outside firm do all of the work. This helps organizations learn the business and know where its holes are.
- **Honestly report on the compliance status** within the company, as well as to the Office of Civil Rights (OCR) and the insurance company. This protects against additional issues, like insurance fraud, in the case of a data breach.
- **Use a quantitative assessment.** Indiana University Health evaluates and scores risk based on likelihood, impact, velocity, potential income loss, and reputational impact.
- **Include physical security risk** in the assessment, to ensure anything that is on a network connection or that protects data is in scope.

A good risk management plan focuses on the top 20% of the risks identified during the assessment phase; focusing on just the top 20% typically addresses 80% of the risk. This plan needs to have a set of methods and processes that will be used to address the risks. It should also include a communication plan and should assign accountable parties to all key tasks.

Additionally, policies and procedures required by the Health Insurance Portability and Accountability Act (HIPAA) need to be tied directly to risk and risk management plans.

Resources for Risk Assessment and Management

The following resources are beneficial for healthcare providers working on risk assessment and risk management plans.

- Information Security Policy Template from the US Department of Health and Human Services
- Healthcare Information Sharing and Advisory Center (H-ISAC), which provides content, mailing lists, and threat intelligence for healthcare organizations
- Health Sector Coordinating Council (HSCC), which provides significant guidance, content, recommendations, and coordination between members

COVID-19 has introduced additional risks to the healthcare industry and its data.

While initially the overall threat level in 2020 remained largely unchanged, the situation changed dramatically after COVID-19 emerged and a large portion of the workforce shifted to working remotely. When this occurred, the risks to systems and data increased, especially in the healthcare industry.

The pandemic has driven an increase in government-sponsored threat actors targeting research facilities to acquire or manipulate sensitive COVID-19 data, including treatment and vaccine information. COVID-19 has also overwhelmed healthcare providers, meaning they are less diligent in protecting protected health information (PHI).

Average daily rate of FBI-reported cybersecurity complaints per day	
Before the pandemic	1,000
After the pandemic	2,000-3,000

> We're seeing nation-state–level actors going after healthcare providers more than usual, typically related to COVID-19 treatment information, intellectual property, or misinformation-type campaigns.
>
> *Tim Vidas*

As the risks have increased, healthcare organizations can use risk assessments and risk management to come up with actionable and valuable incident response strategies.

10 Recommendations for Actionable, Valuable Incident Response

1. Use multi-factor authentication (MFA) as much as possible
2. Gain visibility into systems; use telemetry and ensure logs and audit trails include the information necessary to identify and prioritize threats
3. Plan for remote incident response, and practice incident response
4. Develop baseline configurations
5. Secure remote access
6. Update bring-your-own-device (BYOD) policies
7. Strengthen remote termination processes
8. Revise remote help desk processes
9. Plan for a secure transition to cloud services
10. Scale capacity for remote connectivity

Source: Secureworks Incident Response (Oct 2020). "Pandemic-Driven Change: The Effect of COVID-19 on Incident Response."

The technologies and tools in use—and not in use—impact risk.

When assessing risks and understanding how to best manage those risks, healthcare organizations need to look at which tools and technologies are used—and how they are used—in the organization. They also need to understand what new tools and technologies can mitigate existing risks; for example, using a password manager to track multiple account passwords.

Common tools and technologies to consider when assessing and mitigating risk

Tool/Technology	Consideration
Electronic medical record (EMR)	Maintenance of EMR systems is increasingly complex. Healthcare providers hosting their own systems should instead consider looking to health system providers to host and manage their system.
Password managers	Use password management technology to track the numerous incompatible logins healthcare users tend to have across systems, instead of easy-to-steal account information written on paper.
Payment Card Industry Data Security Standard (PCI-DSS)	Credit cards, not cash, are now the most common form of payment in most healthcare practices. Providers need to ensure they are compliant with PCI standards, as well as customer expectations like using the credit card chip instead of a credit card swipe.
Firewall security	Especially with the increase in remote access to systems during COVID-19, firewall security isn't always enough. Older appliances, open ports, and even remote desktop or virtual private network (VPN) don't offer the security that organizations need today.
Cloud-based backups	Most insurance companies require companies to store backups separately under a different set of credentials to ensure the backups are not subject to the same attack as the primary systems. Not only do cloud-based backups allow healthcare organizations to meet this requirement, but the average cloud provider has better security.
Secure email	Patients expect to be able to send and receive emails with providers. Secure providers, like ProtonMail, offer the encryption, mobile access, and simple secure portal that providers need and that patients expect without being prohibitively expensive.
Endpoint detection response (EDR)	Antivirus in healthcare does not stop malware from getting through. EDR integrates with security information and event management (SIEM) systems and analytics tools, enabling organizations to quickly identify problems.
Two-factor authentication (2FA)	2FA has stopped the majority of hack attempts, especially in healthcare where phishing attacks use compromised accounts.

The right processes and policies increase security.

When the right processes and policies are in place, overall security is improved across the business and its users. Good processes and policies to have in place include:

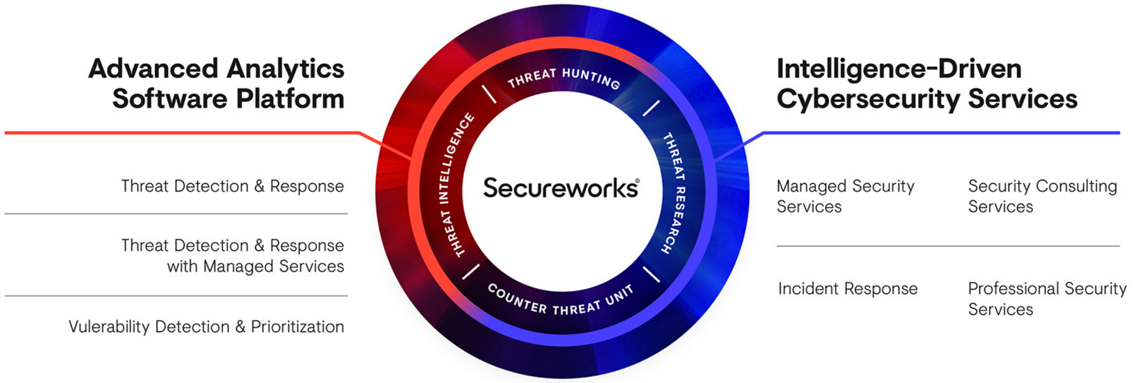
- Always be available and helpful. Team members must be available to respond to all customer requests.
- Have a callback policy to thwart attacks that rely on impersonation of trusted executives to coerce people into sending money. A trusted vendor relationship that encourages callbacks and confirmation decreases the likelihood that these types of social engineering attempts will be successful.
- Perform risk analysis of vendors, beginning with a good baseline and requirements. Example: Indiana University Health's vendor relations expectations and requirements.

Additionally, training that ties security policies directly back to actual jobs can have a positive impact on security. All policies should come with training plans, and training modules should be no more than three to five minutes.

Secureworks solutions focus on what matter most to healthcare organizations.

Secureworks' portfolio of software and services focuses on meaningful, actionable communications. From a software perspective, these solutions include threat detection and response (TDR) offerings, as well as vulnerability detection and prioritization (VDP). Secureworks combines intelligence-driven cybersecurity services with an advanced analytics software platform.

Figure 1: Secureworks takes a holistic approach to security with their cloud-native security analytics software and strategic services


Advanced Analytics Software Platform
Threat Detection & Response
Threat Detection & Response with Managed Services
Vulerability Detection & Prioritization
THREAT HUNTING
THREAT RESEARCH
COUNTER THREAT UNIT
THREAT INTELLIGENCE
Secureworks
Intelligence-Driven Cybersecurity Services
Managed Security Services
Security Consulting Services
Incident Response
Professional Security Services

BIOGRAPHIES

Mitchell Parker, CISSP, CISO

Indiana University Health

Mitchell Parker, CISSP, is the CISO at IU Health. Mitch has done a significant amount of work in researching the effects of cloud and distributed computing, network-based threats, compliance, and privacy and security requirements on connected health devices. Mitch works collaboratively with a number of EMR, infrastructure, and biomedical equipment vendors to improve their security postures and provide a better quality of service. He currently resides in Carmel, IN, with his wife, two children, and two cats.

Tim Vidas

Senior Distinguished Engineer, Secureworks

Tim Vidas is a Senior Distinguished Engineer at Secureworks working to foster innovation and help secure human progress. In the past, Tim has led the DARPA Cyber Grand Challenge infrastructure team, and overseen the digital forensics research group at CERT.

Tim earned highly esteemed DEF CON Black Badges for winning its Capture the Flag contest and is a member of The Shmoo Group, a nonprofit research think-tank comprised of security professionals from around the world. Tim holds a B.S. and an M.S. in computer science and a PhD in ECE from Carnegie Mellon University.