BRIEF

Solutions for Common Healthcare Cybersecurity Risks

SecureWorks®

Healthcare organizations continue to experience a rise in cyber attacks and are unprepared to defend themselves. But even those organizations that don't have the budget and security professionals needed to protect their networks can still defend themselves by pairing up with a cybersecurity company that works around the clock to block, identify, contain, and eradicate cyber threats.

Nearly 90 percent of healthcare organizations surveyed incurred a data breach in the past two years, and nearly half (45 percent) had more than five data breaches in the same time period.[1] That data comes from an independent Ponemon survey that included 91 covered entities and 84 business associates. Another survey, the HIMSS Analytics Quick HIT Survey: Ransomware, conducted in April 2016, revealed that as many as 75 percent of U.S. hospitals surveyed admit they could have been hit with ransom malware. In addition to paying the costs stemming from a breach, healthcare organizations have had to pay fines for violations of the Health Insurance Portability and Accountability Act (HIPAA) involving compromises of electronic protected health information (ePHI). The U.S. Department of Health and Human Services' (HHS) Office for Civil Rights has obtained more than $16 million in settlements from five entities alone. To protect their data, organizations need to conduct a risk assessment to identify assets and their values, the impact of potential threats, and controls needed to mitigate risks. SecureWorks stands ready to help with that — and more. This paper includes some of the most common threats that healthcare organizations face, as well as some of the healthcare information security solutions that SecureWorks provides to help protect your data and patient information.

Risk:

Ransomware attacks

Because most healthcare organizations focus more on meeting compliance requirements rather than on securing their networks, threat actors are highly successful attacking them with ransomware. Small and large hospitals alike have suffered ransomware attacks and many have paid the demanded ransom after their staffs were forced to work offline. However, even after paying the ransom, some hospitals have not received the key to decrypt their files.

Solutions:

SecureWorks iSensor Intrusion Prevention System, Advanced Endpoint Threat Detection and Advanced Malware Protection and Detection

- **iSensor Intrusion Prevention System (IPS)** service protects your network from harmful traffic, including ransomware, that has passed through your firewall. iSensor IPS is a fully managed service that helps you eliminate malicious inbound and outbound traffic around the clock without the burden of device or signature management. Lightening the load on your IT and security staff, the service includes configuration and implementation, 24x7 monitoring and analysis of security events, unmetered support from SecureWorks' certified security experts, and on-demand security analysis and reporting. iSensor IPS helps you comply with regulations to protect your network from threats that are seeking your sensitive data, and provides comprehensive reporting to demonstrate the effectiveness of your security controls.
- **The Advanced Endpoint Threat Detection (AETD)**

service warns you when your endpoints have been compromised and accelerates remediation efforts by pinpointing exactly which systems were compromised, how they were compromised and how you can repair them. Since threat actors often reside in networks hours or days before releasing ransomware, AETD can help you remove threat actors before your data has been damaged.

- **The Advanced Malware Protection and Detection (AMPD)** service provides an extra layer of defense against emerging zero-day threats. Security analysts rapidly analyze and accurately diagnose zero-day threats, and provide focused guidance to speed your response and threat removal. AMPD protects against and detects command-and-control traffic, infection vectors like web drive-by download attacks, and inbound malicious emails. AMPD integrates with other security technologies like firewalls and intrusion prevention solutions to provide dynamic rule updates.

Risk:
Spending hours or days re-imaging computers that were not affected by a network breach

An average of 33 percent of endpoint re-images or remediations are performed without knowing whether the endpoint is truly infected, according to Ponemon's March 2016 study, *The State of Malware Detection and Prevention.*

Solution:
Advanced Endpoint Threat Detection – Red Cloak™

- **Advanced Endpoint Threat Detection (AETD) – Red Cloak** lets you know exactly which computers have been infected so you only spend time re-imaging those computers.

Risk:
Employees who use unauthorized ("rogue") applications that are not being updated and patched

Solution:
SecureWorks Risk Assessments

- A SecureWorks risk consultant can help you assess your network, and can recommend ways to tighten your internal controls and better secure your network.

Risk:
Failing to meet HIPAA requirements and to adequately secure your network

Solution:
SecureWorks Consulting Services

- The Health Insurance Portability and Accountability Act (HIPAA) Security Rule requires that covered entities conduct a risk assessment to ensure compliance with HIPAA's administrative, physical and technical safeguards. A SecureWorks HIPAA consultant can help you conduct a risk assessment, create a roadmap to meet your risk tolerance and strategic goals, and provide you with the best options to help prevent a data breach.

Risk:
A skill shortage threatens your security

For the past four years, information security/cybersecurity topped the list of skills shortages. In 2015, 28 percent of organizations claimed to have a shortage of cybersecurity skills, according to *Cybersecurity Skills Shortage: A State of Emergency by IT analysts at the Enterprise Strategy Group (ESG).*[2] The shortage is growing. The February 2016 ESG brief reveals that 46 percent of organizations say they have a shortage of cybersecurity skills. Organizations need cybersecurity experts who can perform functions that cannot be automated, such as analyzing devices for various alert and threat activities, thoroughly examining and understanding logs, and knowing how to remediate threats.

Solution:
Managed Security Services

- **SecureWorks Managed Security Services (MSS)** acts as an extension of your organization, providing you with 24x7 access to people, processes and technology, closing the loop of your security operations center support. Our information security services cover networks on premises and in the cloud. Services include 24x7 monitoring of networks and endpoints, managed endpoint security services, vulnerability management, threat hunting services, actionable threat intelligence and log management. As a global Managed Security Services Provider (MSSP) with more than 4,300 MSS customers around the globe, SecureWorks delivers advanced data analytics and security insights via our Counter Threat Platform (CTP), which acts as an early warning system to deliver dynamic intelligence and valuable context regarding the intentions and actions of cyber adversaries.

Risk:

Moving data to the cloud

Solution:

Cloud Security Services

- Our cloud security services detect and block emerging threats in the cloud. Upon detection of threat patterns, the SecureWorks Counter Threat Operations Center is notified, and a team of advanced security analysts deconstruct the event and provide actionable remediation guidance. Whether you use public, private or hybrid cloud computing architectures, the SecureWorks Incident Response and Management team can support cyber incident response assessments and threat investigations. Prior to an incident the team can help you develop a Computer Security Incident Response Plan (CSIRP).

Risk:

Hackers who break into medical devices, such as MRI machines, X-ray machines and drug infusion pumps, creating safety and privacy issues

Solution:

SecureWorks Network Security Solutions

- Using our tools, or working with our professionals, we can help you scan your software and hardware devices, including medical devices, for vulnerabilities. Although only medical device manufacturers can access their own operating systems, we can help you create a plan for implementing controls if you find vulnerabilities.

Risk:

Attackers who use malware to exploit a vulnerability in your software or operating system

Solutions:

Vulnerability Management Services, Intrusion Detection System/Intrusion Prevention System, Advanced Malware Protection and Detection, and Advanced Endpoint Threat Detection

- Vulnerabilities within networks, web applications and databases emerge every day, caused by software defects and misconfigurations that open the door to threat actors. Finding vulnerabilities relies on the accuracy of internal and external scan audits in environments on-premises and in the cloud. Helping you to satisfy compliance requirements and safeguard your critical data, our dedicated vulnerability management analysts provide you with continuous visibility into your environment so your security team can work on more strategic priorities.
- In addition to using firewalls around your segregated networks, you need to have an Intrusion Detection System/Intrusion Prevent System (IDS/IPS) to detect or block malware that gets through the holes left open in your firewall. SecureWorks finds that approximately 80 percent of malware bypasses firewalls, as well as antivirus technologies and other intrusion protection systems, because those technologies aren't updated often enough to recognize the latest malware signatures. While SecureWorks can monitor any IDS/IPS you use, we also offer our own proprietary hosted IDS/IPS, the iSensor, which we update each day with new countermeasures to block the latest threats seen by monitoring more than 4,300 networks around the world. However, there is nothing that will block all threats, so as soon they enter your network you need to be aware of them. Advanced Malware Protection and Detection (AMPD) and Advanced Endpoint Threat Detection (AETD) will detect malicious traffic that bypasses traditional security technologies and will alert a SecureWorks analyst, who will quickly analyze the threat activity and provide removal guidance.

Risk:

A threat actor who hacks into a user's computer

Remember that a threat is a "who" not a "what." Threats enter network computers in a variety of ways. An employee might inadvertently click on a malicious attachment or a malicious link found in an email or on a web page. Or, a threat actor might access an employee's computer remotely using stolen login credentials.

Solutions:

Advanced Endpoint Threat Detection, Advanced Malware Protection Detection, 24x7 Network Monitoring

- **Advanced Endpoint Threat Detection (AETD):** AETD continuously detects threat actor activity on endpoints (laptops, workstations and servers) so organizations can detect and respond to threats in their environments. As soon as our targeted threat tripwires are triggered — which could be the moment that malware is launched on a machine, credentials are stolen from a domain controller, or forensic countermeasures are deployed — AETD notifies the SecureWorks Senior Intrusion Analyst team to immediately conduct an investigation. Continuous monitoring enables our analysts to investigate not only the event, but what happened before and after it. This allows network defenders to answer key questions about how the attackers got in, what they did inside the network and how they were removed.
- **Network Monitoring 24x7:** SecureWorks monitors network and endpoint event logs 24x7 to note malicious activity as it occurs so you can remove attackers from your network as soon as possible. The objective is to stop threats before they can execute the attacker's mission of gathering and exfiltrating data.
- **Advanced Malware Protection Detection (AMPD):** AMPD combines a network appliance with SecureWorks' own threat intelligence and analysts, providing an early-warning system that protects organizations from web- and email-based attacks. By monitoring activity at the network level, AMPD detects files and activities that appear to be suspicious, including those that have bypassed endpoint solutions. An isolated sandbox, which emulates an end user device, automatically runs each suspicious file to determine its security status. If the file is found to be malicious, AMPD provides information on the malware's actions. Gathering as much detail as possible by viewing network traffic and analyzing sandboxed files, SecureWorks detects malicious activities and files, identifies what is likely happening in the network, alerts the organization and provides actionable intelligence to help remediate the threat.

Risk:

Attackers who have breached your network and remain undetected

One-third of organizations surveyed in the Ponemon Institute's study *2014: A Year of Mega Breaches* discovered two or more years after the incident that their networks had been breached. Ponemon's 2016 study *The State of Malware Detection & Prevention* found on average it took respondents 170 days to detect an advanced attack, 39 days to contain it and 43 days to remediate it. The longer a threat lingers in your network, the more risk for data, ePHI and financial loss.

Solution:

SecureWorks Targeted Threat Hunting Service

- Targeted Threat Hunting (TTH) engagements should be conducted at least semi-annually and more often if you see anomalous behaviors or suspect a threat might be in your network. In an April 2016 SANS survey, *Threat Hunting: Open Season on the Adversary,* responses from 494 participants revealed that 52 percent of those surveyed said threat hunting found threats that had previously been undetected. A Targeted Threat Hunting engagement provides a deep inspection of your networks and endpoints to identify indicators of attacker presence. To make your environment more resilient, security experts will provide recommendations for your security architecture, instrumentation and controls, and they will provide guidance on removing any found threats.

Risk:

An affiliated doctor or business associate gets hacked and an attacker moves into your network

Solution:

SecureWorks Counter Threat Operations Center

- By having your network and endpoints monitored 24x7, as soon as anomalous activity begins, the SecureWorks Counter Threat Operations Center (CTOC) is notified and begins researching the issue. If the activity is deemed to be a threat, your organization will be notified immediately and will receive remediation guidance.

Risk:

Undetected vulnerabilities on patient portal web applications that allow a hacker to access the patient database

Solution:

Vulnerability Management and Scanning Services

- Continuously scan web apps to discover and log vulnerabilities and website misconfigurations.
- Create reports on business objectives defined by your organization to drive remediation of critical and high-risk vulnerabilities. Since vulnerabilities are constantly changing, we will create a framework-based program for you to address any vulnerabilities that exist now or will exist in the future. SecureWorks will provide two separate reports — one for the technical IT team and one for the management team — explaining the current security posture and the steps needed to remediate vulnerabilities.
- Conduct web app testing at least quarterly and after any code change on the application to verify that there are no invalid redirects, that the workflow of the system is working correctly and that the app is not vulnerable to common attacks like SQL injections and Cross Site Scripting.

Risk:

A threat actor is detected inside your network or has shut it down with a DDoS attack

Solution:

Computer Security Incident Response Plan Development

- SecureWorks will work with your executives, directors and IT teams to help develop a Computer Security Incident Response Plan (CSIRP) that will include legal, regulatory and compliance reporting requirements, as well as suggestions for handling likely breach scenarios. Once the plan has been developed, we will conduct tabletop exercises, giving the main players in your organization their responsibilities and the experience needed to successfully handle a breach.
- Should a breach ever occur, SecureWorks can help you minimize damage and preserve evidence for legal action. We can also help your compliance, privacy and legal teams make sense of the breach's impact so your organization can meet its obligations.

For more information, call **(877) 838-7947** to speak to a SecureWorks security specialist.

www.secureworks.com

[1] Ponemon Institute, *Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data,* May 2016

[2] Oltsik, Jon, et al., Enterprise Strategy Group, *Cybersecurity Skills Shortage: A State of Emergency,* February 2016