IDC Health Insights

White Paper

Providing Outside-In and Inside-Out Protection Against Ransomware and Other Intensifying Cyberthreats

Sponsored by: Fortinet

Lynne Dunbrack
July 2016

EXECUTIVE SUMMARY

Healthcare organizations are under siege by cybercriminals with the intent to do harm and extort money from their victims. The profile of cybercriminals has evolved from "script kiddies" and rogue individuals who wanted to see how far they can infiltrate a company's IT infrastructure to a more sophisticated, well-funded, and organized effort backed by syndicated crime rings and nation-states motivated by financial gain or committing espionage. Cybercrime is becoming more strategic and directed, with specific organizations coming under attack. In the case of ransomware, healthcare organizations in particular are being targeted because the healthcare industry is a 24 x 7 business that cannot tolerate any downtime in its mission-critical applications. Key findings include:

- Many of the same major trends that promote the widespread deployment of healthcare IT solutions are also making healthcare organizations more vulnerable to cybersecurity threats. These trends include electronic health record (EHR) deployment to qualify for meaningful use incentives, data aggregation and health information exchange to support population health initiatives, and consolidation of healthcare organizations to create economies of scale and competitive advantage.
- In 2015, the industry saw a shift from unintentional breaches – the inadvertent disclosure of protected health information like a laptop left behind in a coffee shop – to intentional cyberattacks committed by organized crime rings and nation-states. Financial gain is a major motivator for committing these crimes.
- Threat vectors are evolving, increasing in number and scope of attack. Threat vectors include social engineering, phishing and spear phishing, drive-by downloaders, and compromised Web sites. Attacks are becoming more insidious. Today's high-profile malware includes ransomware, which encrypts critical system files, rendering them inaccessible until a ransom for the key to unlock the files is paid.
- Attack surfaces are becoming increasingly borderless in a connected healthcare environment, with proliferating mobile and Internet-connected medical devices.
- Conventional firewalls are only as good as their cybersecurity signature libraries. Next-generation firewalls that further segment valuable IT assets provide essential protection from the inside out.
- Today's cyberattacks are more advanced and persistent. The increasing volume of phishing attacks and high-profile security breaches inside and outside the healthcare industry is creating a heightened demand for security products and services.
- No single security technology will provide adequate protection against cyberattacks. Healthcare organizations need to invest in a balanced portfolio of advanced persistent threat protection technologies that prevent, detect, and mitigate breaches.

IN THIS WHITE PAPER

This IDC Health Insights White Paper is sponsored by Fortinet and examines the broader security issues of the "Internet of Threats," high-profile malware such as ransomware, phishing attacks, and the use of vulnerable medical devices as a launchpad for these attacks. This White Paper is based on briefings with Fortinet and interviews with Fortinet customers, as well as IDC Health Insights' security and compliance research. The objective of this White Paper is to educate healthcare organizations about the new borderless threat vectors and how to mitigate the risk of a cyberattack.

THREAT VECTORS ARE EXPANDING IN SCALE AND INTENSITY

Healthcare organizations are increasingly under attack, experiencing thousands of threats on a daily basis. At least 100 of these attacks are potentially dangerous, and 10 are so serious that they warrant calling in law enforcement agencies to investigate. In 2015, the industry saw a shift from unintentional breaches to intentional cyberattacks committed by organized crime rings and nation-states. 36 hacking and IT incidents affecting 93 million individuals were reported in 2015 to the U.S. Department of Health and Human Services, up from 1.8 million individuals in 2014. Approximately 295,000 individuals' health records were breached in 2015 because of theft and loss compared with 7.1 million in 2014.

Healthcare organizations are more susceptible to being attacked by cybercriminals, in part because they perceive that healthcare organizations are soft targets because of their reputation of poor security relative to other industries. Also, more sensitive health information is available today than ever before in an electronic format as a result of widespread deployment of electronic health records to achieve meaningful use incentives and new care delivery and reimbursement models that require greater data aggregation for analytics and health information exchange across the enterprise. Healthcare databases aggregate valuable financial, insurance, and demographic data that is increasingly targeted by nefarious intruders that seek to commit both financial and healthcare identity theft. Consequently, healthcare organizations are increasingly at risk of targeted and highly sophisticated attacks.

Ransomware: A Targeted Threat Vector Exploiting Vulnerable Servers

Threat vectors are also evolving, increasing in number and scope of attack. They range from phishing and spear phishing to high-profile malware, such as ransomware. In many cases, the primary vector is a phishing email with a link or attachment that is malicious. The user clicks on it, and the malware is downloaded and executed. Older ransomware variants, such as CryptoLocker and TelsaCrypt, relied on unsuspecting users to click on a link in an email or visit an infected site. Today's ransomware is more insidious, targeting known vulnerabilities in unpatched Web servers to penetrate the network. Hospitals are being targeted by cybercriminals because they need round-the-clock access to mission-critical applications. Furthermore, cybercriminals are well aware that patch management is an ongoing challenge for understaffed healthcare IT organizations, especially as it relates to patching embedded systems in medical devices.

One such example of the new family of ransomware is SamSam (also known as Samas, Samsa, Kazi, and RDN/Ransom), which exploits known vulnerabilities in JBoss Application Servers by using JexBoss, an open source penetration testing tool. Once access to the network has been established, the malware can move laterally through the network to compromise additional machines. Other tools can be used to collect credentials and other information on the networked computers and encrypt multiple Windows systems. Cybercriminals then extort their victims to pay them a ransom to unlock the files. In recent ransomware attacks, a hospital in California and a hospital in Maryland paid $17,000 and $18,500, respectively, in bitcoin to obtain the keys to decrypt their locked systems.

The real impact of ransomware beyond the extortion payment is the very risk of adversely affecting daily operations, patient care, and safety. A Kentucky hospital declared an "internal state of emergency" and placed a scrolling red alert on its home page, advising visitors that it had limited access to Web-based communications and electronic communications. When vital systems are locked, staff must revert to using manual, paper processes, which can create delays in accessing critical patient information and potential patient safety risks because electronic error checking is not available. Younger staff may never have been taught how to use paper charts. In some instances, hospitals that were infected with ransomware had to divert patients without life-threatening conditions arriving by ambulance to other hospitals and cancel patient appointments because they didn't have access to their health records. Delay in receiving care and diversion not only affect patient care but also have a financial impact on the infected healthcare organization.

The situation has become so severe, with nearly a dozen U.S. hospitals affected by ransomware since the beginning of 2016, that the Federal Bureau of Investigation issued a confidential urgent "FLASH" message about SamSam ransomware. In addition, the agency released Indicators of Compromise (IoC) for the SamSam threat so that healthcare organizations could monitor themselves. The U.S. Department of Homeland Security (DHS), in collaboration with the Canadian Cyber Incident Response Centre (CCIRC), released its own alert on March 31, 2016, "to provide further information on ransomware, specifically its main characteristics, its prevalence, variants that may be proliferating, and how users can prevent and mitigate against ransomware."

The situation has become so severe, with nearly a dozen U.S. hospitals affected by ransomware since the beginning of 2016, that the Federal Bureau of Investigation issued a confidential urgent "FLASH" message about SamSam ransomware.

Internet of Threats: Expanding Attack Surfaces Are Increasingly Borderless

Today's digital hospitals connect more devices to the network than ever before. Clinicians use their own or hospital-provided mobile devices to access their patients' health information. Bedside telemetry sends alerts regarding the vital signs of patients to their clinicians' mobile devices and routine readings to the patients' electronic health records. Medical imaging machines have long been connected to remote servers over the Internet for monitoring and servicing by their manufacturers. Patients are sent home with connected weight scales, pulse oximeters, and blood pressure cuffs to monitor their vitals and detect complications while recovering at home. Healthcare organizations are piloting the use of wearables for consumers and smart glasses and smartwatches for clinicians. In addition to connected clinical devices, photocopiers as well as HVAC and other operational systems are also connected to the Internet. With all these connected devices, the attack surface is growing exponentially and becoming increasingly borderless.

Proliferating connected devices will require more firmware updates, mobile device patching, and network connections that need to be secured. Managing the ever-increasing number and variety of devices will further tax already overburdened healthcare IT organizations. "How do you make these devices, that you don't own or control, secure for your environment?" questioned a security engineering manager from a large, nationally ranked integrated healthcare system interviewed by IDC Health Insights. Once an advanced persistent threat makes it past perimeter defenses in a flat network, it becomes relatively easy for cybercriminals to infiltrate the network because internal traffic is deemed "trusted." Successful attacks could take days to weeks to months to be detected. Cybercriminals know this and will continue to exploit vulnerable endpoints to obtain access to more valuable IT assets and sensitive health and financial information.

"How do you make these devices, that you don't own or control, secure for your environment?" questioned a security engineering manager from a large, nationally ranked integrated healthcare system.

Vulnerable Endpoints: Exploiting Medical Devices to Launch an Attack

Medical devices are increasingly connected to the network and interconnected with healthcare IT systems. Securing medical devices is inherently complex. Medical devices are often vulnerable because of poor security practices, such as lack of system hardening and hard-coded or default passwords. Their embedded software is often not reliably patched and, in some cases (e.g., Microsoft XP), is no longer supported. Cybercriminals can exploit these vulnerabilities to gain access to the healthcare organization's network. This type of attack is referred to as "medjacking."

While the exploitation of medical devices is increasingly becoming a concern for healthcare chief information security officers (CISOs), most healthcare organizations have been slow to adequately protect interconnected medical devices. According to an IDC Health Insights survey, only 9.6% of respondents indicated that they had integrated medical devices into their enterprise security architecture, and 10.6% of respondents said they had not yet begun this process. An industry report confirmed that medical devices, including insulin pumps, heart monitors, and picture archiving and communication systems (PACS), have been used by cybercriminals as a means of gaining access to healthcare organizations' networks. In three separate cases, medical devices were infected with malware, enabling the cybercriminals to move laterally within the healthcare network to access protected health and other sensitive information. Malware found on the devices included ransomware, Conficker, Citadel, and Zeus. While the malware could have been used to compromise the operations of the medical devices themselves or take remote control of the devices, it would appear that the malware was used only to provide backdoor access to the hospitals' networks.

According to an IDC Health Insights survey, only 9.6% of respondents indicated that they had integrated medical devices into their enterprise security architecture, and 10.6% of respondents said they had not yet begun this process.

Since most medical devices are closed systems, they are not routinely scanned by the IT security team and are often maintained by the biomedical engineering team, with no access or input from IT security. The U.S. Food and Drug Administration (FDA) has issued warnings indicating "as medical devices are increasingly interconnected, via the Internet, hospital networks, other medical devices, and smartphones, there is an increased risk of cybersecurity breaches, which could affect how a medical device operates." Specifically, in a 2013 alert, the FDA noted that attacks "could be initiated by the introduction of malware into the medical equipment or unauthorized access to configuration settings in medical devices and hospital networks." According to the security engineering manager, "There are manufacturers that hide behind the Federal Drug Administration rulings and claim

that they can't make changes to the *underlying* OS or systems because they would have to run the product through the clearance process again. Medical device manufacturers need to be responsible for what they are doing."

HOW HEALTHCARE ORGANIZATIONS CAN PROTECT THEMSELVES AGAINST CYBERATTACKS

Protection from the Outside In: Advanced Threat Protection

Conventional firewall protection is no longer enough. Conventional firewalls cannot adequately protect IT systems from new threats that do not exist in their signature base, nor can they keep pace with the new volume of malware. Firewalls are only as good as their cybersecurity signature library. Thus a multilayered security approach provided by an advanced persistent threat protection framework is required to:

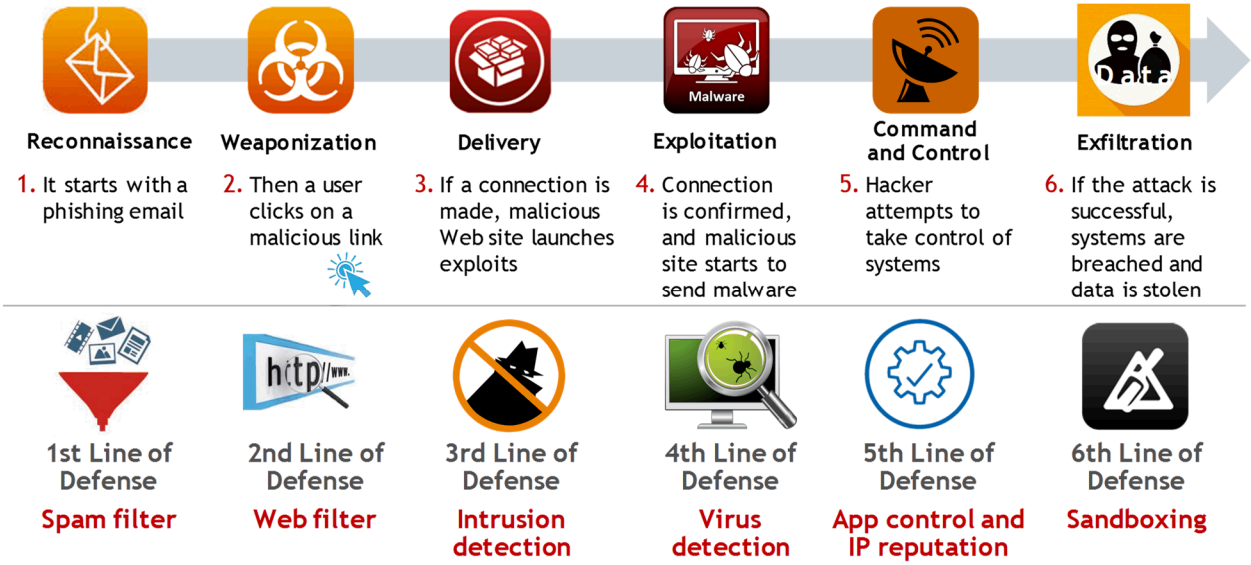
- **Prevent intrusion by acting on known threats or information.** Healthcare organizations must use a layered approach to prevent network access. Next-generation firewalls contain multiple layers of defense, including antispam and Web filtering, intrusion and antivirus protection, application controls, and IP reputation technologies, that protect against known threats.
- **Detect previously unknown threats.** Cybercriminals are constantly evolving how they will attack their targets to exploit zero-day vulnerabilities. Advanced persistent threat detection technologies, such as sandboxing, create an additional layer of protection by helping identify and isolate unknown threats to ascertain whether they contain malware before letting them through to the network.
- **Mitigate damage by responding quickly to potential incidents.** Time is of the essence when it comes to cyberattacks. The challenge for healthcare organizations is that cybercriminals can be stealthy, operating reconnaissance and data exfiltration unnoticed on a compromised network for months before detection. Many healthcare organizations simply do not know how to adequately respond to a breach because today's malware is so much more complex and can evade security controls.

In many ways, ransomware is like any other technology market. Because it is highly profitable for cybercriminals, more players are entering the market. More revenue opportunities from extorting victims are funding development, resulting in more variants of ransomware that make it harder for signature-based antivirus tools to keep up. These new variants are essentially undetectable by those tools and are capable of wreaking serious havoc as they spread through the network.

Security professionals often refer to breaking the *kill chain* (a term that originated from the military concept of an attack) to describe a targeted attack on IT resources that consists of reconnaissance, weaponization, delivery, compromise/exploitation, command and control, and exfiltration. Figure 1 depicts an attack starting with a phishing email, with advanced network security technology providing multiple lines of defense to thwart the attack, thereby breaking the kill chain.

FIGURE 1

Breaking the Kill Chain with Advanced Network Security Lines of Defense



Source: IDC Health Insights, 2016

Advanced threat protection technology is one approach to disrupt the kill chain to thwart or at least slow down the attack to enable the security team to respond before more damage is done. Education is another. "We try to preach that a lot. Be aware of your surroundings. Understand what you are doing and who you are seeing in front of you, in your email, and when you're online. Security is everybody's responsibility," emphasized the security engineering manager.

Real-Time Threat Intelligence: Actionable Insight Enhances Advanced Threat Protection

Many unknown cyberthreats adapt to risk and security measures. Healthcare organizations need access to actionable threat intelligence for up-to-date protection at every security layer and enforcement point. Sandboxing suspicious network traffic enables security teams to identify previous unknown threats and share this threat intelligence with the broader security community. Security technology should be integrated such that threat signatures ascertained during sandboxing, for example, are shared with firewalls and other advanced network security technology.

Threat intelligence services provided by security technology companies collect massive quantities of threat information from around the world and use Big Data and analytics technology to decipher patterns and look for anomalies in user behavior and network traffic. This actionable insight helps IT organizations detect threats earlier in the kill chain and remediate them quicker. Consequently, security moves from being reactive to proactive to, ultimately, predictive as real-time threat intelligence continues to improve, enabling security professionals to counteract potential attacks before they happen.

Benefits of Advanced Threat Protection

Using a three-pronged approach for advanced threat protection, healthcare organizations can thwart cyberattacks and mitigate the potential risk of serious damage to the infrastructure, expensive privacy and security breaches, and loss of reputation and consumer confidence in the ability of the organizations to adequately protect their sensitive health information. When properly deployed, advanced threat protection can provide the following benefits:

- **Broader security coverage.** Advanced threat protection offers broader security coverage and reduces complexity by providing security across a wide range of attack vectors — mobile devices, endpoints, networks, and email — from a single console.
- **Protection against known and unknown threats.** Stronger prevention measures reduce the number of successful breaches, avoiding the expensive and time-consuming effort of detecting and mitigating advanced persistent threats. Sandboxing technologies create an additional layer of protection by helping identify and isolate unknown threats to ascertain whether they contain malware before letting them through to the network.
- **Collection of threat intelligence from millions of sensors and threat information sharing.** The global distribution of millions of sensors found in various products and solution sets enables the collection and dissemination of threat intelligence in near real time to real time across multiple threat vectors — Web, network, file, and message. This enables security insights to be delivered across products and solution sets, as well as across customers and industries.

Protection from the Inside Out: A New Class of Firewall

The first line of defense has always been (and will continue to be) firewalls at the perimeter. However, "hard on the outside, soft on the inside isn't going to work anymore," commented the security engineering manager interviewed for this White Paper. If the perimeter defense is successfully breached in a spear phishing attack whereby the user is duped into sharing his/her credentials, the attacker will essentially have unfettered access to endpoints and devices connected to the network. The proliferation of access points combined with advanced persistent threats calls into question the reliance on flat network architectures. Once an advanced persistent threat makes it past perimeter defenses (north-south movement) in a flat network, it becomes relatively easy for cybercriminals to traverse the network (east-west movement) because internal traffic is deemed "trusted." Successful attacks could take days to weeks to months to be detected.

Next-generation firewalls are designed to protect the network at the perimeter, stopping detected threats from entering the network. Internal segmentation firewalls (ISFWs), a new category of firewalls, are designed to protect the network from the inside out, providing an additional layer of protection to stop threats from spreading once inside the network. ISFWs further segment internal networks, creating virtual fencing around valuable IT assets. An apt analogy is locking the front door to protect the house (security at the edge) but also locking up jewelry and other valuables in a home safe to protect them in the event a thief breaks down the door or enters through an open window. ISFWs complement conventional firewall and unified threat management technology. ISFW is not a replacement technology.

An ISFW has three key characteristics:

- **Performance.** Wire speed, multigigabit network performance
- **Security.** Continuous "inside out" protection against advanced threats through integrated security functionalities
- **Platform.** One scalable and versatile security platform with a consolidated management console for end-to-end network visibility and control across all segmentation deployment scenarios

The ISFW can then be placed at strategic points along the network in front of servers that contain protected health information or cloud-based Web applications, thereby quickly providing visibility to the traffic flowing in and out of the IT asset. "Internal network segmentation is all about threat analytics and getting that information to where you can on the desktop, security devices, and network devices and identifying the users on the network and what they are doing," stated the security engineering manager.

"Internal network segmentation is all about threat analytics and getting that information to where you can on the desktop, security devices, and network devices and identifying the users on the network and what they are doing," stated the security engineering manager.

Benefits of Internal Segmentation Firewalls

When properly deployed, internal segmentation firewalls provide the following benefits:

- **Protect valuable IT data assets with strategically placed ISFWs.** The value of health information, which can be used to commit medical fraud, is surpassing the value of social security and credit card numbers on the black market, thereby increasing the attractiveness of stealing health information. According to an April 2014 FBI bulletin, a patient health record is valued at $50 compared with $1 for a social security number or a credit card number. Cordoning off servers that store protected health information mitigates the risk of an expensive breach that violates HIPAA.
- **Ensure continuous operations.** Many healthcare settings are 24 x 7 operations, requiring round-the-clock access to mission-critical clinical applications. In extreme situations, lack of access to essential patient health information could mean the difference between life and death. Thus uptime, network performance, and reliability are critical considerations when downtime is not an option. Segmenting the network into zones helps prevent it from being brought down in the event of an attack that adversely affects network operations.
- **Protect vulnerable access points.** Networked medical devices are often vulnerable endpoints because of poor security practices, such as hard-coded or default passwords, lack of system hardening, out-of-date patch level, and the absence of cybersecurity tools. They present challenging exposure profiles to cyberthreats. The more common threat is collateral damage from malware. Similar to protecting data assets, strategically placed ISFWs can protect vulnerable access points.
- **Mitigate risk of publicly accessible networks.** Most healthcare organizations provide guest networks for patients and their family members, visitors, and clinicians who may have admitting privileges but are not employed directly by the hospital. Other open networks readily available include third party-provided WiFi offered by a coffee shop or restaurant colocated in the healthcare organization. ISFWs enable the healthcare organization to monitor and segregate these networks without having to have complete control over them.
- **Help achieve meaningful use privacy and security requirements.** Protecting patient health information from unauthorized disclosure along with protecting the confidentiality, integrity, and availability of the health information is a core requirement for qualifying for the Medicare and Medicaid electronic health record incentive programs. ISFWs limit the movement of malware that has compromised user credentials by preventing access to protected health information and other sensitive data and help reduce the impact of malware on the IT infrastructure overall.
- **Provide an additional layer of protection from business associates.** New care delivery and reimbursement models and meaningful use requirements for health information exchange require new levels of care collaboration and data exchange between entities. Some of these entities may be owned, and some may be loosely affiliated business associates whose security controls are not the most rigorous. An organization is only as secure as its weakest link. ISFWs further enhance a healthcare organization's security position.

- **Sequester successful attacks.** Traditional firewalls are designed to protect the perimeter from attack. Should an attack be successful, such as when credentials are compromised as a result of a phishing attack, the internal segmentation firewall restricts the east-west movement of the attack along the network, essentially blocking it from doing more damage and accessing its target.

Complex Healthcare Environment Requires an Integrated Security Approach

Today's healthcare IT environment has grown increasingly more complex as a result of multiple mergers and acquisitions, rapid deployment of EHRs and other clinical systems to meet federal mandates and avoid financial penalties, and responding to new care delivery and reimbursement models established by the Patient Protection and Affordable Care Act (PPACA). A greater acceptance of cloud computing and SaaS-based solutions has accelerated the acquisition of new applications by line-of-business (LOB) buyers. To complicate matters, LOB buyers of this shadow IT have given little thought to how these new applications will fit into the healthcare organization's overall security infrastructure. All too often, IT becomes aware of these newly acquired systems when a request for data integration between new systems and legacy systems is submitted or a routine scan is performed.

No one security technology will provide adequate security protection across the enterprise. Healthcare organizations need to think differently about security and move beyond investing in a series of point solutions to protect data, applications, networks, Web sites, mobile devices, and workloads moved to the cloud. Acquiring separate security technology for each of these domains sets up the possibility of security gaps that can be exploited by cybercriminals. Instead, healthcare organizations should consider a multilayered holistic approach to security and install an integrated suite of security technology, including advanced network security and ISFW, to both thwart and continue to detect the threat actors focused on stealing the data that resides in their network. New security solutions should be integrated with existing security functions and management consoles.

BEST PRACTICES

"It's only going to get worse," stated the security engineering manager interviewed for this White Paper. "If someone wants to get into an environment, they are going to find a way." Healthcare organizations must protect themselves from not only the outside in but also the inside out. Understanding the healthcare organization's risk profile is an important first step. A comprehensive cyberthreat assessment will identify technical, physical, and administrative vulnerabilities. As the old adage goes, an ounce of prevention is worth a pound of cure. But healthcare organizations also need to be able to detect potential threats and be poised to respond swiftly when attacks are successful. The following are recommended best practices for protecting healthcare organizations against cyberattacks:

- **Educate users that security is everyone's responsibility.** Preventing malware from being inserted onto the network in the first place is an important step in establishing a strong security posture. Many attacks start with phishing or spear phishing attempts to steal user credentials. Cybercriminals have become very adept at social engineering and creating phishing emails that look remarkably like legitimate emails. Mock phishing attacks can identify where more training about what a suspicious email or link looks like is required.
- **Identify where the most valuable assets are stored.** One of the first steps to protect the healthcare organization against cyberattacks is to identify the assets that would be attractive to cybercriminals. While this recommendation may seem obvious, many healthcare organizations have hundreds to thousands of applications in their product portfolio that have never been rationalized. Critical IT and

data assets most attractive to cybercriminals should be segregated behind strategically placed ISFWs that provide an additional level of network protection. In addition, these firewalls provide better visibility for detecting exploits sooner, thereby helping minimize damage and reduce remediation costs by enabling security teams to respond to breaches faster.

- **Take a multilayered, holistic approach to security.** Healthcare IT organizations have historically relied on security point solutions to protect IT infrastructure, cloud services, and mobile devices. They should consider a holistic approach to security and install an integrated suite of security technology, including ISFWs, to both thwart and continue to detect the threat actors focused on stealing the data that resides in their network. New security solutions should be integrated with existing security functions and management consoles.
- **Include all devices and device types in the cyberthreat assessment.** Interconnected medical devices and RTLS create more access points that need to be secured and managed. The increased use of connected health technologies has resulted in an ever-expanding attack surface. Any device that is connected to the network or can be accessed remotely should be evaluated for its potential to be exploited by cybercriminals. In addition to clinical devices, connected devices can include lab and pharmacy equipment, printers, photocopiers, HVAC, and other operational systems.
- **Accelerate recognition and remediation of an attack to minimize business disruption.** Cyberattacks are typically not "smash and grab" type attacks. Instead, cybercriminals infiltrate their targets, often using phishing email to lure users to open a link or attachment that has embedded malware that then installs itself on the computer and multiplies itself by installing additional malware on the computer and creating backdoors to ensure continued access in the event that the first malware is noticed and removed. Once inside the network, the criminals have access to other systems, can steal user credentials and certificates, can explore the systems for sensitive information, and can then exfiltrate that data. By impersonating legitimate users and covering their tracks, the criminals can put off detection for long periods of time. ISFWs provide additional visibility into network traffic and can quarantine suspicious content, applications, and traffic for further analysis until the activity has been deemed safe.
- **Segregate medical devices and other valuable IT assets.** It's one thing if claims administration systems are compromised. To be sure, it's a hassle to have some downtime and reimage systems. But should it happen in radiology, and the CT or MRI machine has to be taken offline, the clinical safety and revenue implications are significant. Patient lives could be at risk if cybercriminals were able to take over control of a medical device and adjust radiation doses unbeknownst to clinicians. Major outages might require that patients be diverted to other hospitals if the attacked hospital couldn't provide the level of care necessary for the number of beds it has using a paper-based system. Medical devices should be segregated to create secure zones, network traffic should be deeply inspected, and sandboxing should be deployed to quarantine any suspicious traffic.
- **Move from reactive to proactive to real-time security.** Automated risk assessment and threat detection will enable predictive analytics and help identify breaches in real time to proactively mitigate cyberthreats before significant loss occurs. A holistic approach to analytics will facilitate detecting "slow and low" threats that emerge over time.
- **Deploy a balanced combination of advanced threat protection technologies.** Security threats are rapidly evolving. It is not sufficient to prevent access from known threats. Healthcare organizations need strong detection technology to identify and isolate potential threats for evaluation. In the event an attack is successful, automated and assisted incident response capabilities enable a swift response, thereby limiting the damage incurred during the breach.

- **Be hypervigilant about installing security patches.** While it can be a daunting task to keep up with security patches, it is imperative that these known vulnerabilities be addressed, thereby reducing the potential attack vectors for malware and ransomware.
- **Perform and test regular backups of key systems.** Guidance from the United States Computer Emergency Readiness Team recommends that organizations affected by ransomware not pay the ransom because doing so will only serve to perpetuate this lucrative crime. Regular, comprehensive backups can help limit the exposure to ransomware and expedite the recovery process should the healthcare organizations be locked out of critical systems. These backups should be kept offline so that they are not also compromised in the ransomware attack.
- **Use security products based on extensive security intelligence.** Cybercriminals are notorious for sharing strategies and tools they use to infiltrate computer systems and evade detection. Healthcare organizations similarly need to leverage the threat intelligence gathered by security service providers in real time to detect cyberthreats, most of which are unknown, targeted, and adaptive to risk and security measures. Look for products that have been certified by third-party testing and certification companies for IT security.

PARTING THOUGHTS

The healthcare IT environment is inherently complex. Healthcare organizations exist in a bimodal IT and business world as they migrate from legacy systems to 3rd Platform technologies while shifting from fee-for-service to value-based care delivery and reimbursement models. The resulting digital transformation with its data consolidation and proliferation of connected devices – mobile, medical, imaging, and monitoring, to name a few – creates an expanding attack surface and a nearly borderless environment. Healthcare organizations will need an advanced persistent threat framework to prevent, detect, and mitigate cyberattacks. Advanced network security, including next-generation firewalls that internally segment networks to protect valuable IT assets, and security intelligence are essential tools in the security professional's arsenal to thwart cyberattacks.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.935.4445
Twitter: @IDC
idc-insights-community.com
www.idc.com