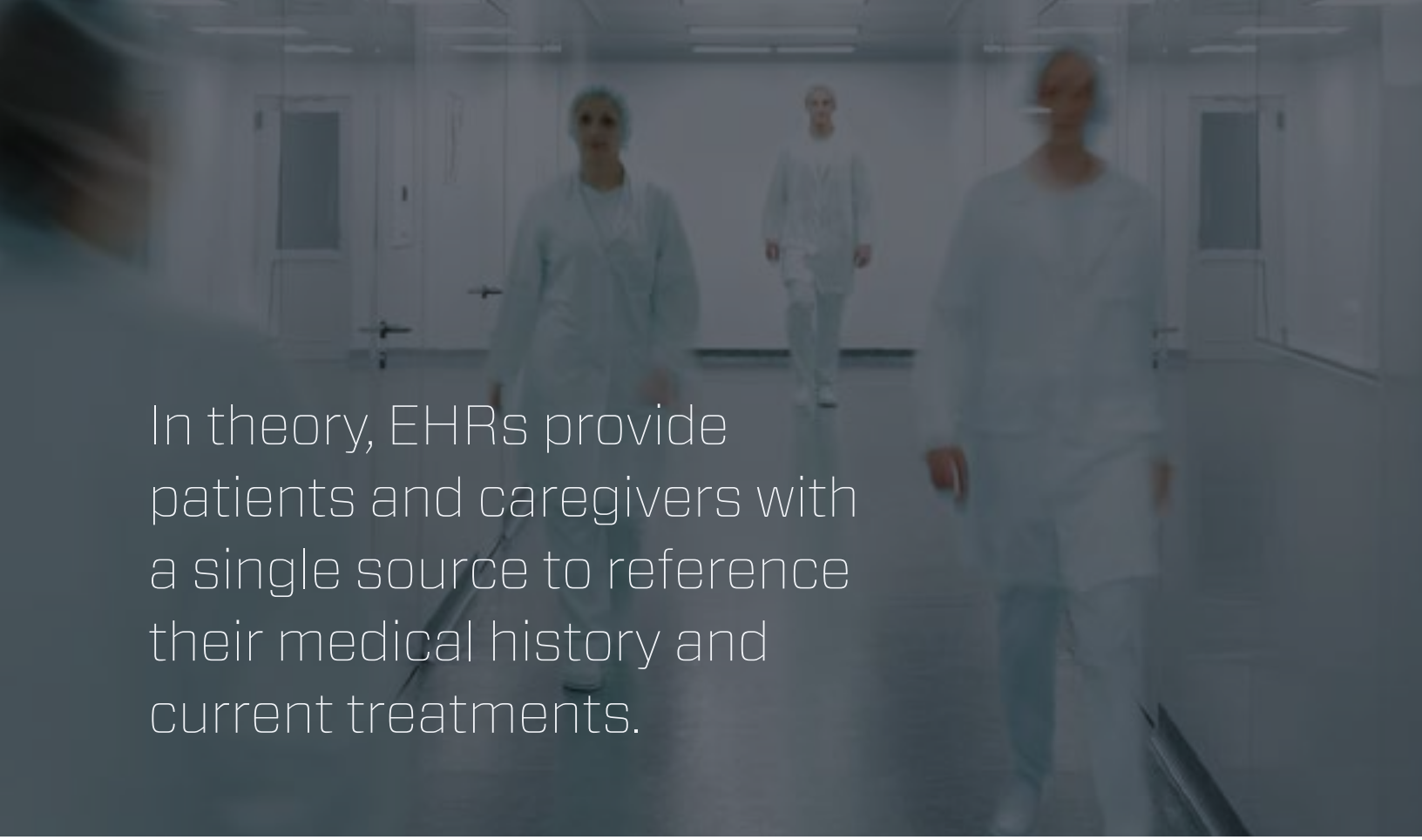
BlackBerry | CYLANCE

WHITE PAPER

A Devastating Assault on Healthcare

HITECH, Compliance, and the Growth of the Ransomware Economy



Introduction

The Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 encouraged the migration of personal health information (PHI) to electronic health records (EHRs). As part of the U.S. Government's 2009 economic stimulus package, HITECH provided incentives for transitioning offline patient data into Internet-accessible electronic records. Unfortunately, the increased act of adopting digital records attracted cyber criminals who responded by launching a historic number of assaults on the healthcare industry.

In theory, EHRs provide patients and caregivers with a single source to reference their medical history and current treatments. They eliminate many of the patient care mistakes which occur due to human error, such as illegible handwriting. They also provide healthcare administrators a holistic picture for each patient, resulting in more efficient care.

Moving patient data from paper records to EHRs makes it considerably more accessible. This increased accessibility benefits patients and caregivers. It also provides new opportunities for threat actors. Cyber criminals able to compromise healthcare systems may resell patient information, hold data for ransom, or commit identity theft.

The expanded availability of patient data has fueled a meteoric rise in cyber attacks. A 2018 CSO report states that healthcare suffers twice as many cyber attacks as other industries. These attacks exact a heavy toll through system downtime, operational delays, and patient care disruptions. Specifically, ransomware has proven especially troublesome for healthcare providers.

Ransomware, typically delivered via a phishing email, seeks out and encrypts critical files on the host system and any connected devices. Once encryption is complete, the victim usually receives on-screen instructions for submitting a payment to obtain a decryption code. This ransom is typically made with cryptocurrency, which provides the malware author with an untraceable form of instant payment.

Ransomware attacks often lead to dramatic financial losses. The ransom paid to hopefully regain data is one cost. Other associated costs include notifying patients of the data breach, regulatory investigations, civil litigation, significant system upgrades, and machine restorations. Revenue is also lost from turning away patients who cannot be processed or treated during a breach.

One of the costliest and most disruptive by-products of a ransomware PHI breach is a judgment by the U.S. Department of Health & Human Services (HHS). If the HHS rules that a HIPAA compliance violation has occurred, a healthcare organization can be fined up to $1.5 million per year.

Ransomware, Technology, and Healthcare Trends

A report published by the Institute for Critical Infrastructure Technology outlined a number of threat predictions. It foresaw an increase in attacks and new exploitations of unattended vulnerabilities previously claimed by adversaries. Specifically, the report defined healthcare as one critical area where ransomware attacks will wreak havoc on America's critical infrastructure. In addition, researchers at IDC Health Insights predicted that in 2016, cybersecurity breaches would touch one in three public health records.

The world witnessed a staggering increase in ransomware attacks against the healthcare industry in 2016. Several large hospitals were hit with malware. The attacks threatened the well-being of patients and jeopardized the hospital's ability to protect their PHI.

Recent trends in ransomware, healthcare, and technology are converging to help cyber criminals find a wealth of victims.

New and Evolving Variants

Locky ransomware began to surface early in 2016. It was used to shut down three Prime Healthcare Services hospitals in California and disrupt services at several of their affiliate locations. The malware moved through vulnerable systems, scrambling and renaming files. Victims were prompted to purchase the decryption key by paying the threat actors with bitcoins. In April 2016, the FBI issued a warning regarding another ransomware infection, Samsam. This ransomware was behind an attack on 10 hospitals in the Baltimore and Washington, D.C., area. Samsam is unique because it focuses on servers instead

High-Profile Ransomware Attacks on Hospitals

Hospital	Attack Date	Response	Ransom Demanded
Hollywood Presbyterian Hospital	February 2016	Ransom paid	40 Bitcoins ($17,000)
Methodist Hospital (Henderson, KY)	March 2016	Ransom paid	Undisclosed amount
Prime Healthcare Services, Inc. (Chino Valley Medical Center, Desert Valley Hospital, and Alvarado Hospital Medical Center with service disruptions in other locations)	March 2016	Hospital systems shut down by Locky ransomware	Undisclosed
MedStar Health (10 hospitals in Maryland, Washington, D.C.)	March 2016	Hospital systems infected by Samsam ransomeware; system interfaces of hospital immediately shut down; no ransom paid	45 Bitcoins ($18,500)
Kansas Heart Hospital	May 2016	Ransom paid; second ransom not paid	Undisclosed amount

While healthcare organizations work ardently to improve their cyber risk strategies, the challenge is daunting. An increasingly sophisticated community of ransomware authors, driven by the growth in financial incentives, continues to develop complex and evolving threat vectors.

The typical healthcare environment is a perfect storm of vulnerabilities, making it attractive to ransomware attacks.

of end-users. These are only two examples of how new and evolving ransomware exploits a growing landscape of threat vectors.

Ransomware-as-a-Service
Some ransomware attacks come from highly skilled programmers, but thanks to the proliferation of ransomware-as-a-service, novice cyber criminals are finding success as well. Ransomware specialists now offer their code and expertise online to novice attackers for a nominal fee or a cut of any ransom obtained. Ransomware-as-a-service puts advanced malware tools into the hands of anyone willing to pay, offering them the opportunity to profit from cyber crime.

The Internet of Things and Shrinking Platform Immunity
As the Internet of things (IOT) grows, the expansion of ransomware into previously untouched platforms creates new vulnerabilities. Gone are the days when Windows environments were the only platforms at risk of a cyber attack. Ransomware now plagues the users of Android devices, Linux, and Apple's OS software for Macs.

Medical Technology Velocity
Hospitals and healthcare systems face the risk of cyber attacks disabling life-saving equipment and systems. Medical device manufacturers may compromise on risk management practices to meet stringent production demands. This problem is further complicated by reliance upon a complex global supply chain and vendor network which may sacrifice device security for product launch expediency.

Increasing Supply of Cryptocurrency
The growing availability and use of anonymous digital cryptocurrency makes it difficult for law enforcement agencies to track ransom payments. This allows cyber criminals to demand increasingly hefty ransoms without fear of being discovered.

Why Healthcare?

The typical healthcare environment is a perfect storm of vulnerabilities, making it attractive to ransomware attacks.

Value of PHI
The goal of a healthcare ransomware attack is often to hold personal health information hostage for payment or to sell it to third parties. PHI data is more valuable on the black market than personal information from financial institutions.

PHI is also valuable to cyber criminals in creating a market for multiple secondary transactions. As published by the FBI Cyber Division, cyber criminals sell personal health information on the black market. Each electronic health record commands a rate of $50, compared to $3 for a stolen social security number or $1.50 per credit card number.

Large healthcare systems are particularly vulnerable to attacks. This is due to the siloed nature of their systems.

Sense of Urgency

Healthcare organizations are obligated to maintain the integrity of patient care environments and preserve accurate medical records. This obligation acts as a powerful incentive to return the environment to its original state following a cyber attack. This sense of urgency by healthcare providers to return to normal operations provides a strong advantage to the perpetrators of ransomware attacks.

In some industries, the ability to restore data from previous system backups is sufficient to return the business to an operational state. However, the fluid nature of healthcare operations requires immediate access to dependable real-time data. Backup data only a few minutes old can potentially put patients at risk.

HIPAA Penalty

When hospitals lose control of their data, they risk violating HIPAA regulations, specifically the HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414. This rule requires HIPAA-covered entities and associates to provide notification following a breach of unsecured PHI.

Older and less sophisticated strains of malware encrypt the PHI data, never moving it from the server or desktop environment. Unauthorized parties, including the threat actors, cannot view it. However, more sophisticated attackers can access the data, and may sit dormant for long periods of time before taking action. In such cases, the burden of proof is on each healthcare organization to determine whether the threat actors viewed or accessed PHI data. Such activity would enable the ransomware author to potentially download or view it. The HHS Office for Civil Rights is currently investigating over 400 HIPAA cybersecurity breaches affecting 500 or more individuals.

The healthcare industry is not alone in its responsibility to ensure the protection of sensitive and private health information. Any company in possession of health-related information about employees falls under the same HIPAA compliance scrutiny. For example, a Sony Pictures cyber attack affecting possible HIPAA-related corporate records resulted in a class action lawsuit and undisclosed settlement with 50,000 employees.

Complexity

Large healthcare systems are particularly vulnerable to attacks. This is due to the siloed nature of their systems. Hospitals often use diverse technologies created by numerous independently managed vendors. This technological diversity adds to the complexity of securing healthcare organizations.

Ransomware Payments

Several high-profile ransomware attacks on hospitals have resulted in the victims paying tens of thousands of dollars to cyber criminals. Their ransom payments led to multiple new attacks on these same organizations. In addition, the success of these ransomware attacks serves to embolden the cyber criminal community.

The Lack of Preparation

There is a quote that circulates frequently among enterprise workers: "A lack of planning on your part does not constitute an emergency on my part." In the case of cybersecurity prevention, nothing could be further from the truth. The healthcare industry's lack of focus on cybersecurity allowed several emergencies which are well documented by both the media and HHS.

An ABI Research study on cybersecurity and healthcare states that:

> *"The healthcare sector is ill-prepared for the new cyberage. Hospitals, clinics, trusts, and insurers are constantly under attack from malicious online agents. The value of personal health information, made more easily available with the convergence to electronic health records, is ten times that of financial data such as credit card numbers. Medical identity theft and fraud are on the rise, and healthcare providers are struggling to cope, with the past 2 years seeing hundreds of instances of data breaches leaking millions of personal records. And yet the industry spends very little on cybersecurity, comparatively to other regulated critical industries. ABI Research calculates cybersecurity spending for healthcare protection will only reach US$10 billion globally by 2020, just under 10% of total spend on critical infrastructure security."*

48%

of respondents said their organizations have experienced a security breach involving the loss or exposure of patient information in the last 12 months.

Healthcare organizations tend to have serious gaps in their cybersecurity. Some well-known weaknesses include phishing emails and fake URLs which trick employees into disclosing login information or downloading malware. Another common security issue is vulnerable servers which are not regularly patched. Without proper protection, medical devices and industrial control networks can be maliciously accessed with potential impact to life-saving systems.

The Lack of Security Awareness Training

A survey conducted by the Healthcare Information and Management Systems Society revealed that 64% of respondents experienced a phishing-related security incident within their organization. Healthcare professionals, while highly specialized in their clinical disciplines, are not generally well trained in security awareness. The report indicates otherwise savvy people click on links due to sophisticated impersonation techniques. Consider a clever phishing email that looks as if it comes from a familiar vendor like LabCorp with the subject Patient Results Available. The email appears exactly like a legitimate LabCorp email and raises no red flags. The link in the email takes the recipient to a perfectly spoofed copy of the login page on LabCorp.com. When the recipient tries to log in, his or her credentials are stolen. Now threat actors can log in to LabCorp and access PHI from the healthcare organization's patient rolls.

An Ounce of Prevention

In February 2016, the Ponemon Institute released the results of its State of Cybersecurity in Healthcare Organizations study. According to researchers:

- Healthcare organizations average one cyber attack per month
- 48% of respondents said their organizations have experienced a security breach involving the loss or exposure of patient information in the last 12 months
- Only half indicated that their organization have an incident response plan in place

With findings like this, the solution to healthcare's cybersecurity crisis seems obvious. Benjamin Franklin said, "By failing to prepare, you are preparing to fail." Healthcare decision makers currently have the opportunity to hardwire their enterprises with next-generation endpoint protection solutions. Smarter endpoint solutions and implementing a prevention-first strategy would likely result in a significant drop in cyber attacks over the coming 12 months.

Board members, C-level executives, and IT security specialists are responsible for taking the appropriate steps toward implementing effective cybersecurity solutions. In parallel, employees must be trained to identify phishing events and address them in a way that reduces security risk.

BlackBerry Cylance: Killing the Cyber Kill Chain

The healthcare industry faces several challenges that traditional antivirus (AV) and endpoint detection and response (EDR) solutions fail to address:

- Traditional AV/EDR solutions allow zero-day threats and other attacks to successfully compromise endpoints before effective counter-measures are crafted
- IT analysts spend significant time testing and deploying updated signatures and software, limiting their ability to address other business-critical needs
- End-users experience significant system performance decreases as additional security layers demand more resources
- Security teams have limited visibility into the environment, resulting in the misallocation of resources during incident response
- Many security solutions rely on a set of products that require significant time to deploy, configure, and maintain

BlackBerry Cylance solves these issues by putting artificial intelligence in command of cybersecurity. BlackBerry Cylance delivers a machine learning model trained to identify malicious executables in milliseconds, on-device, even when the specific executable has never been seen before. This means that BlackBerry Cylance's flagship product, CylancePROTECT®, can detect and prevent known, unknown, and zero-day payloads with 99.1% efficacy. Independent testing from SE Labs has proven that CylancePROTECT holds an average predictive advantage of 25 months over major malware families. This means the 2015 AI model was able to identify and prevent a threat which did not exist until 2017, over two years after the model had been trained and deployed.

Benefits of BlackBerry® Cylance® Security Products and Services

CylancePROTECT offers many benefits in addition to prediction-based threat prevention, including:

- **AI-Driven Malware Prevention:** CylancePROTECT uses field-proven AI to inspect any application attempting to execute on an endpoint before it executes.
- **USB Device Usage Policy Enforcement:** This capability allows IT administrators to control which devices can be used in their environment.
- **Script Management:** CylancePROTECT has built-in script protection, meaning organizations maintain full control of when and where scripts are run in their environment.
- **Memory Exploit Prevention:** When an attacker attempts to escalate privileges, undertake process injection, or make use of an endpoint's memory inappropriately by other means, CylancePROTECT will identify and prevent it immediately.
- **Application Control for Fixed-Function:** Application Control provides the ability to ensure fixed-function devices are in pristine state continuously, eliminating the drift that may occur over time when devices are left unmanaged.
- **Zero-Day Payload Prevention:** Using patented machine learning models, CylancePROTECT prevents attackers attempting to exploit a zero-day with a malicious payload from being successful

Complementing CylancePROTECT, BlackBerry Cylance's EDR product, CylanceOPTICS™, provides:

- AI-driven incident prevention
- Distributed search and collection
- Consistent cross-platform visibility
- Root cause analysis
- Enterprise-wide threat hunting
- Fast incident response
- Dynamic threat detection
- Remote forensic investigations
- Automated response

CylanceOPTICS deploys machine learning models which run locally on the endpoint. These security agents record system behavior and monitor system resources for anomalous activity. Enabling endpoint self-monitoring results in increased protection from a variety of threats ranging from living-off-the-land attacks to malicious user activity.

Breaking the Kill Chain

Advanced cyber attacks are planned and executed in a very similar manner, seldom straying from a high-level process map known as the Cyber Kill Chain. The only variable is the amount of technical or personnel resources cyber criminals spend on each attack stage. The seven steps of the Cyber Kill Chain are:

- Reconnaissance
- Weaponization
- Delivery
- Exploitation
- Installation
- Command and Control
- Actions

It's important to understand each aspect of the Cyber Kill Chain and have tools and techniques in place to uncover attacker activity at each step.

Reconnaissance: Attackers may attempt to identify users via social engineering, and look for IP addresses, emails, and other information that may enable them

to gain access to the environment. Ensure that users are vigilant in keeping company-related information secure with reoccurring training and simulated social engineering attacks.

Weaponization: Weaponization of websites, documents, and files is a preparatory step often performed in isolation and is therefore undetectable to potential victims.

Delivery: CylancePROTECT will identify and prevent malicious files before they can execute, thereby disrupting the Cyber Kill Chain at the delivery stage.

Exploitation and Installation: The robust memory protection and script/macro control features of CylancePROTECT also prevent the exploitation and installation phases of the kill chain from completing.

Command and Control: CylanceOPTICS will recognize and respond/report suspicious resource use when a threat seeks out a command and control server.

Actions: CylancePROTECT stops threats during pre-execution, ensuring that the action phase never completes. CylanceOPTICS can alert security teams to the malicious use of system resources or automatically respond by shutting down resource-based or fileless attacks.

Healthcare Wins with BlackBerry Cylance

BlackBerry Cylance provides healthcare organizations effective, lightweight, and easy-to-use security products and specialized security services. Healthcare organizations can implement a prevention-first cybersecurity strategy by using advanced AI-based security agents to predict and block threats. BlackBerry Cylance agents update semi-annually and do not require deep system scans which bog down endpoint and network performance.

Healthcare companies benefit from adopting BlackBerry Cylance's prevention-first cybersecurity strategy in the following ways:

- Better patient care as technological resources are freed from the demands of layered security and can refocus on the core business
- Increased compliance with privacy regulations like HIPAA, GDPR, HITECH, and PCI-DSS
- Improved security for medical devices providing patient care
- Greater visibility into the technological environment leading to early detection of vulnerabilities and threats
- Simplified security stack

There is a popular misconception in the healthcare industry that money used for cybersecurity competes with funding for treating patients and saving lives. This belief fails to recognize that a secure and resilient technological environment is a force multiplier for healthcare providers. Money spent protecting data, securing medical devices, and bringing organizations into compliance with privacy regulations is money spent improving patient lives.

For more information about new cybersecurity technologies that can secure healthcare and other organizations, visit www.cylance.com.

About BlackBerry Cylance

BlackBerry Cylance develops artificial intelligence to deliver prevention-first, predictive security products and smart, simple, secure solutions that change how organizations approach endpoint security. BlackBerry Cylance provides full-spectrum predictive threat prevention and visibility across the enterprise to combat the most notorious and advanced cybersecurity attacks, fortifying endpoints to promote security hygiene in the security operations center, throughout global networks, and even on employees' home networks. With AI-based malware prevention, threat hunting, automated detection and response, and expert security services, BlackBerry Cylance protects the endpoint without increasing staff workload or costs.

+1-844-CYLANCE
sales@cylance.com
www.cylance.com

MKTG-18-1117 20190529