Raytheon | websense®

2015 Industry Drill-Down Report Healthcare

websense® SECURITY LABS™

TABLE OF CONTENTS

Executive Summary | **3**

Industry Overview | **4**

Key Research Findings | **5**

Valuable Data Targeted by Advanced Malware | **6**

Lack of Resources: Underfunded and Understaffed | **7**

A Global Challenge with Regional Issues | **9**

Connected Medical Devices and the Internet of Things | **11**

Conclusion | **12**

Methodology | **12**

Sources | **13**

EXECUTIVE SUMMARY

Modern medical care is delivered through an incredibly complex network of information technology systems connecting patients, doctors, nurses, pharmacists, technicians, administrators and accountants with electronic health records (EHR), connected medical devices and insurance companies. Driven by the need to improve patient outcomes and lower costs, the rush to embrace digital technology has created a complex network of connected devices, systems and entities where security may be an underfunded afterthought. Network security is further complicated when IT must balance protecting data from inappropriate access against the fact that lives could be lost if medical personnel cannot access the information they need, when they need it. Data thieves recognize both the incredible value of healthcare information and the vulnerabilities and security gaps which exist in this newly-connected world. This report explores the state of the healthcare industry security landscape, key research findings from the Raytheon|Websense® Security Labs™, and implications for providers and patients.

Industry Overview

» A look at the modern healthcare industry landscape.

Key Research Findings

» Key statistics with major implications for healthcare.

Valuable Data Targeted by Advanced Malware

» Healthcare records contain information which is up to 10x more valuable on the black market; data thieves use advanced malware to try to steal it.

Lack of Resources: Underfunded and Understaffed

» The further removed from the patient, the lower the priority.

A Global Challenge with Regional Issues

» Patient care is local, but records, devices and networks are global – with regional twists.

Connected Medical Devices and the Internet of Things

» Devices to monitor patients and administer medicine are connected and represent both an infection vector and a hacking target.

Conclusion

Methodology

Copyright © 2015 Raytheon Company.

INDUSTRY OVERVIEW

Hospital and health systems are critical infrastructure entities, absolutely essential for the functioning of a society and its economy. Increasingly, digital technology is used to gather, store and share patient information and other related data effectively and efficiently. Modern medical care is delivered through an incredibly complex network of information technology systems connecting patients, doctors, nurses, pharmacists, technicians, administrators and accountants with electronic health records (EHR), medical devices and insurance companies. When processes become digital and networked, functionality and connectivity generally have first priority, with security often seen as an afterthought. This is especially true in the healthcare industry.

The potential for criminal exploitation of healthcare information was well documented by the Cyber Division of United States' domestic intelligence, security and law enforcement agency, the Federal Bureau of Investigation (FBI) in an April 2014 Private Industry Notification.[1] This report emphasized that the healthcare industry is not as resilient to cyber intrusions as the financial and retail sector. Multiple factors contribute to this state of affairs, including a mandatory January 2015 deadline to transition to electronic health records (EHR), lax cybersecurity standards and more internet connected medical devices than ever before. Compounded by the fact that medical information can command up to 10 times more money on the black market than financial information, the FBI described the healthcare industry as "a rich new environment for cybercriminals to exploit." While the dates and names of government agencies vary from country to country, similar stories of increased risk are unfolding around the world.

Experts in the field agree. "The adversary is way ahead of us right now," said Jim Nelms, the Mayo Clinic's first Chief Information Security Officer, in recent remarks to media.[2] Lax security can have broad impacts. In the U.S., data loss carries the potential for fines and sanctions under the Health Insurance Portability and Accountability Act (HIPAA). In the worst case scenario, failure of the network to deliver accurate, timely and secure data critical to patient care can mean the difference between life and death. Whether reducing legal exposure or improving patient outcomes, there is a growing awareness in the healthcare industry for data systems to ensure privacy and security while providing reliability and functionality.

Keeping ahead of criminals is a challenge for security engineers and researchers; there is no such thing as one-size-fits-all security. To build security systems, it is important to understand who is being attacked, by whom, how and why.

Criminals often move to the easiest targets, and with retail and banking becoming more secure, healthcare networks became a prime target. In 2014, Raytheon|Websense reported that cyberattacks on hospitals had surged 600 percent.[3] This huge spike prompted our researchers to examine security trends in different industries and economic sectors, focusing on attack methodologies and techniques documented from real-world data to gain new insight into attack patterns.

Copyright © 2015 Raytheon Company.

Our first industry report, published in June 2015, focused on the financial service industry,[4] and yielded specific insights on the challenges facing banks and brokerages. This second report is focused on the healthcare services industry and includes attacks on devices, health records, medical treatment facilities and insurance providers.

KEY RESEARCH FINDINGS

» The healthcare industry is more than 200 percent more likely to encounter Data Theft and sees 340 percent more security incidents and attacks than the average industry.

» One in every 600 attacks in the healthcare sector involves advanced malware. In addition, healthcare is:

- 400 percent more likely to be impacted by advanced malware.
- 450 percent more likely to be impacted by Cryptowall.
- 300 percent more likely to be impacted by Dyre.
- 74 percent more likely to be impacted by phishing schemes such as FakeBank.

» The healthcare industry is 376 percent more likely to encounter Dropper Files, up from 200 percent in 2014.

- In the first half of 2015, more than 83 percent of Dropper incidents were seen in the healthcare sector alone.
  - A March 2015 spike comprised more than 90 percent of all Dropper incidents categorized in all industries.

Copyright © 2015 Raytheon Company.

VALUABLE DATA TARGETED BY ADVANCED MALWARE

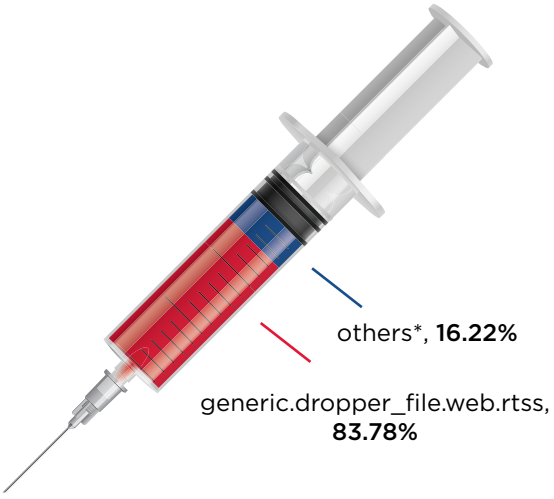
Healthcare records hold a treasure trove of data that is valuable to an attacker. No other single type of record contains as much Personally Identifiable Information (PII) that can be used in a multitude of different follow-up attacks and various types of fraud. Health records not only contain vital information on the identity of an individual (name, address, social security) but also often link to financial and insurance information. Access to PII allows an attacker to commit identity fraud, while the financial information can lead to financial exploitation. This is a logical and profitable secondary attack area for cybercriminals who have already dealt in stolen credit card data.

As a result, Raytheon|Websense Security Labs has identified that the healthcare industry sees 340 percent more security incidents and attacks than the average industry and is more than 200 percent more likely to encounter data theft.

The Health & Human Services' Office of Civil Rights (OCR) estimates that the personal health data of up to 30 million Americans has been compromised since 2009; in fact, as of September 15, 185 hacking or IT incidents involving unauthorized access to the personal health information of 500 or more individuals have so far been documented.[5] These numbers mirror results of a June 2015 Healthcare Information and Management Systems Society (HIMSS) survey[6] where two-thirds of the respondents had experienced a significant security incident, while 42 percent said there were too many threats to track.

Indeed, Raytheon|Websense Security Researchers identified ongoing fluctuations of attack patterns throughout 2014 and 2015. **The Dyre trojan, BrowseFox and different Dropper files have each taken a turn as the top type of threat encountered by the industry within the last six months alone (see Figure 1).** Most surprising, however, was the massive and outsized proportion of attacks that use of advanced malware to target sector. **One in every 600 attacks in the healthcare sector involves advanced malware.** With tens or hundreds of millions of security incidents and attacks every six months, the number of incidents involving advanced malware accumulates rapidly. **In fact, healthcare is four times more likely to be impacted by advanced malware than the average industry.**

Figure 1. Most popular threats in healthcare – last 6 months



*others: generic.lure.web.rtss - **0.15%**, generic.fraud.web.rtss - **0.19%**, necurs.backchannel_traffic.web.rtss - **0.24%**, kazy.backchannel_traffic.web.rtss - **0.26%**, fraudkit.fraud.web.rtss - **0.29%**, generic.threat.web.rtss - **0.29%**, generic.rsik.web.rtss - **0.31%**, generic.installer_page.web.rtss - **0.46%**, generic.obfuscation.web.rtss - **0.5%**, vawtrack.backchannel_traffic.web.rtss - **0.91%**, dyre.backchannel_traffic.web.rtss - **1.08%**, injection.black_seo.web.rtss - **1.09%**, generic.unsolicited_content.web.rtss - **1.35%**, generic.redirection.web.rtss - **1.4%**, sinkhole.backchannel_traffic.web.rtss - **1.44%**, mal_tds.redirection.web.rtss - **1.9%**, browsefox.backchannel_traffic.web.rtss - **2.88%**

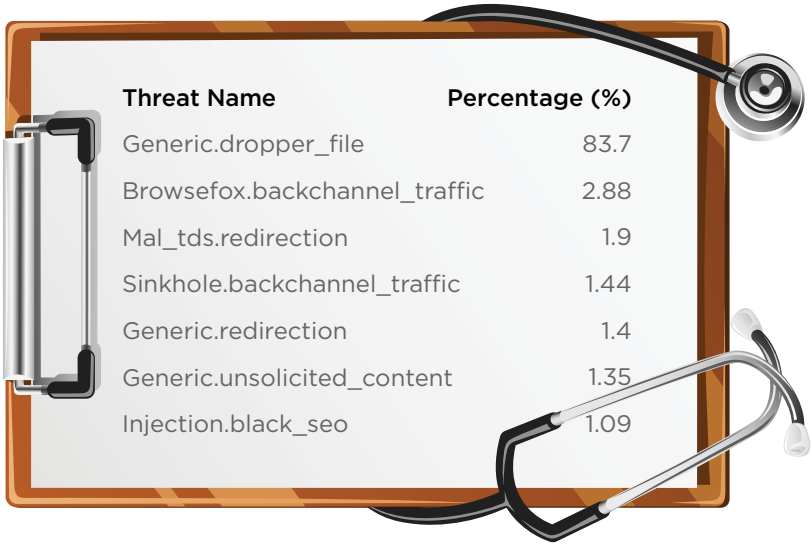
Copyright © 2015 Raytheon Company.

LACK OF RESOURCES: UNDERFUNDED AND UNDERSTAFFED

Many healthcare organizations lack the administrative, technical, or organizational skills necessary to detect, mitigate and prevent cyberattacks. Just 53 percent of executives at health care providers and 66 percent of health insurers said they are prepared to defend against attacks, according to a KPMG 2015 Healthcare Cybersecurity survey.[7] And although 74 percent of respondents in a 2015 Health Information Management and Systems Society (HIMSS) Leadership Survey[8] identified IT as critical to helping achieve patient care goals, an overwhelming majority of CIOs cite budget and resources as being major roadblocks to accomplishing objectives,[9] even as their role continues to increase in complexity.[10]

Healthcare organizations should be spending at least 10 percent of their IT budget on cybersecurity according to Lisa Gallagher of HIMSS,[11] yet the industry average is just 3 percent.[12] The American Hospital Association's (AHA) 2015 Most Wired Survey,[13] tracking hospital use of important cybersecurity measures, seems to all but confirm Gallagher's assessment, with statistics showing that while cybersecurity incident response is a top growth area among 79 percent of "Most Wired" hospitals, for all other hospitals surveyed that number is a meager 37 percent. Even as hospitals acknowledge concern about ongoing cyber risk, less than 40 percent have a plan to respond to an attack or data breach, according to the 2015 Travelers Business Risk Index.[14] Some hospitals have yet to implement[15] even basic preventative measures such as intrusion detection systems, infrastructure security assessments, remote data wiping of mobile devices, or encryption. Though not required under HIPAA or the Health Information Technology for Economic and Clinical Health (HITECH) Act, OCR estimates 60 percent of healthcare data breaches since 2009 could have been prevented through encryption.[16]

Figure 2. Top threats observed within healthcare – first half of 2015



Threat Name	Percentage (%)
Generic.dropper_file	83.7
Browsefox.backchannel_traffic	2.88
Mal_tds.redirection	1.9
Sinkhole.backchannel_traffic	1.44
Generic.redirection	1.4
Generic.unsolicited_content	1.35
Injection.black_seo	1.09

This absence of a comprehensive healthcare IT strategy shows considerable consequence when reviewing the findings of the Raytheon|Websense Security

Copyright © 2015 Raytheon Company.

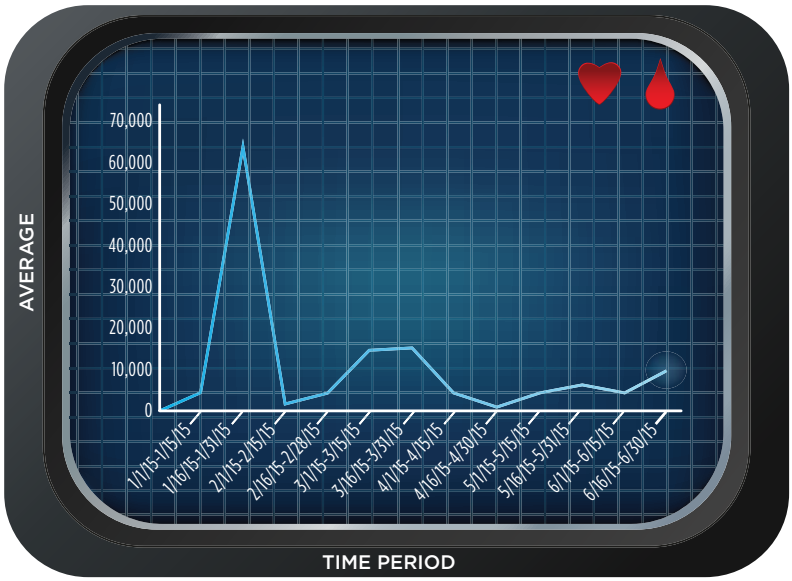
Labs. **In 2015, 83.7 percent of all Dropper incidents were encountered in healthcare (Figure 2).** Dropper files are used to deposit a vast variety of malware and to open backdoors into the systems that allow attackers to establish and maintain residency on a system in an attempt to garner the information they find valuable, either for themselves (in the case of nation-state attackers attempting to gain intelligence) or for sale on the Dark Markets frequented by cybercriminals. **As an industry, healthcare is 376 percent more likely to encounter Dropper Files than an average industry.** With a wide variety of malware being introduced, it makes it a challenge for time-pressed IT security professionals to identify and remediate compromised systems and networks.

A dearth of resources also minimizes the likelihood of effective security awareness training and employee security awareness programs. A lack of employee awareness can result in a higher number of incidents of compromise through black search engine optimization, waterhole attacks and phishing attempts. This is especially dangerous to healthcare in light of the Raytheon|Websense Security Labs findings that demonstrate that **the healthcare sector is 74 percent more likely to be impacted by phishing schemes such as FakeBank. In 2014, healthcare was more than 200 percent more likely to encounter Lures and Redirects than other industries.**

While external attacks remain one of the greatest vulnerabilities within an organization, according to results from an August 2015 KPMG survey of healthcare executives,[17] employee negligence and the insider threat are costing companies millions of dollars each year. Improperly trained employees and senior executives for whom data security is not a priority, result in security incidents caused more often by unintentional mistakes than intentional and/or malicious acts as evidenced by an independently commissioned Raytheon|Websense/Ponemon Institute report.[18]

Botnets present another challenge to strapped IT security professionals. **Raytheon|Websense Security Labs identify more than 50,000 botnet encounters and incidents affecting healthcare on an average day.** Not only is the number of encounters high, again requiring a large number of man-hours to identify, mediate and reimage infected endpoints, but spikes in activity both can increase the perniciousness of the malware and the amount of endpoints compromised. **For example, an attack wave in January 2015 saw a dramatic surge in botnet activity affecting healthcare, with more than 700,000 botnet incidents affecting healthcare in a single day (Figure 3).**

Figure 3. Botnet incidents in healthcare – first half of 2015



As far as the prevalence of specific botnets pervasive, or overrepresented in the healthcare

Copyright © 2015 Raytheon Company.

sector, **this industry sees the Andromeda botnet 14 times more than the average industry.** The Andromeda loader has both anti-VM and anti-debug capabilities, can detect virtual machines in an attempt to evade sandboxing and can stay quiet on the system for months at a time without reaching out to its command and control server. It can also create a very effective backdoor into an organization for additional data-stealing malware.

A GLOBAL CHALLENGE WITH REGIONAL ISSUES

These alarming trends are not just limited to the United States. In Australia, "healthcare provider organizations forget about the 'people and process factor', and fail to provide staff with the awareness to identify threats, or the policy to address them" stated Bryan Foster and Yvette Lejins of Australia's National E-Health Transition Authority (NEHTA) in a December 2013 presentation[19] given at the 2nd Australian eHealth Informatics and Security Conference. Plans to significantly increase use of and investment in digital platforms to provide healthcare services to its citizens, as detailed by Australia's Department of Broadband, Communications, and the Digital Economy,[20] will also likely require a considerable expenditure in security technologies as cyberattacks against hospitals surge.

Emphasizing the global nature of threats against healthcare, two infamous pieces of destructive and damaging malware are increasingly pervasive in healthcare organizations, regardless of their geography.

Raytheon|Websense Security Labs has observed that global healthcare organizations are 450 percent more likely to be impacted by Cryptowall than average the industry. When activated, the malware encrypts certain types of files stored on local and mounted network drives using RSA public-key cryptography, with the private key stored only on the malware's control servers, effectively holding these files for ransom. This ransomware is increasingly being targeted towards businesses, and healthcare in particular. According to recent research, nearly 625,000 systems were infected with CryptoWall in a six-month period last year, affecting more than 5.25 billion files. Significantly, more than 60 percent of compromises were outside of the United States. The threat against healthcare organizations is decidedly a global issue.

In addition, **Raytheon|Websense Security Labs has identified that healthcare businesses are 300 percent more likely to be impacted by Dyre**, an active banking trojan with variants that have been attributed to have targeted enterprise organizations and successfully stole more than $1M in a single campaign. In recent incidents, organizations have lost between $500,000 and $1.5 million to attackers.[21]

Copyright © 2015 Raytheon Company.

Computer users in France, Germany, the US, Australia and Romania, as well as the UK, are in the firing line of the latest run of attacks,[22] while Dyre becomes more challenging to combat as it continues to add new exploits to its capabilities, including those related to relatively fresh CVE.

The type of man-in-the-middle code injection used by Dyre can also be used to contribute to significant data loss for healthcare organizations globally; and data loss for healthcare organizations has its own significant challenges.

With Australia set to introduce mandatory data breach notification laws by the end of 2015,[23] making failure to notify of material breaches a criminal offense, healthcare organizations are increasingly in the spotlight to protect the valuable data they have.

Concurrently, results of a recent survey[24] in Canada showed eight of twelve health jurisdictions have passed legislation to force hospitals to report breaches to the relevant privacy body, while the remaining four still have no well-defined strategy in place. The latter includes Ontario – especially surprising given a February 2015 ruling[25] by the Ontario Court of Appeal granting patients the right to sue hospitals over privacy breaches – though proposed legislation[26] would make reporting privacy breaches to Ontario's Information and Privacy Commissioner and to the relevant regulatory colleges that govern healthcare professionals mandatory. Also without a well-defined strategy, according to the same survey, is Manitoba, whose auditor general claimed in a July 2015 report[27] on risks associated with end-user devices that "significant cyber security control weaknesses" including remote access to the health system networks and a lack of encryption, resulted in the Winnipeg Regional Health Authority (WRHA) being "unnecessarily vulnerable" to information breaches. Also a consequence of cyber intrusions: a loss of trust or confidence in healthcare providers and in electronic health records, patients withholding or falsifying information or being deterred from seeking testing or treatment altogether, according to Acting Information and Privacy Commissioner of Ontario, Brian Beamish.[28]

> "Time and time again we see data breaches caused by poor procedures and insufficient training. It simply isn't good enough."
>
> — Christopher Graham, ICO, Feb. 2, 2015

In the United Kingdom, the Information Commissioner's Office (ICO), an independent regulatory office that reports to Britain's Parliament, has stated that while the UK's National Health Service (NHS) holds "some of the most sensitive personal information available" it remains "one of the worst performers" with regard to data protection. As of February 2015, the ICO had levied the NHS fines totaling more than a million pounds (or approximately two million dollars) for failing to adequately manage and protect confidential data.[29]

Copyright © 2015 Raytheon Company.

CONNECTED MEDICAL DEVICES AND THE INTERNET OF THINGS

As reported by a December 2014 Gartner forecast,[30] digital and connected diagnostic and screening systems in the healthcare field will reach more than 40% global penetration by 2020. While connected medical devices have proven invaluable to medical facilities, staff and patients in advancing overall progress and care, vulnerabilities can "jeopardize a hospital's entire information system, with possible implications for patient safety as well as security of information" according to comments submitted last year[31] by the AHA to the Food and Drug Administration (FDA) on collaborative approaches for medical device and healthcare cybersecurity. With an attack surface already massive in scope (for example: The University of Pittsburgh Medical Center has a connected network of 22 hospitals, 4,000 physicians, imaging centers, labs and others using dozens of different IT systems)[32] mobile devices only further expand the given terrain for cybercriminals to negatively impact data security even further; as stated by the FDA,[33] "rather than impacting a single device or single system, multiple devices or an entire hospital network may be compromised."

Researchers have lately proven this prediction,[34] demonstrating how careless security can leak valuable information to the internet, leaving a slew of systems and equipment vulnerable to hackers and targeted attacks. In a controlled exercise, a healthcare organization's incorrectly configured internet-connected computer exposed the data of 32 pacemaker systems, 21 anesthesiology systems, 488 cardiology systems and 323 radiology systems along with telemetry systems for monitoring the movement of elderly patients to potential attack. And because the network was connected to third-party providers common to hospitals – like pharmacies and laboratories – their data was also exposed.

Yet the FDA Manufacturer and User Facility Device Experience (MAUDE) – which houses reports of suspected device-associated deaths, serious injuries and malfunctions submitted to the FDA by mandatory and voluntary reporters – only tracks malfunctions related to a catch-all category of computer failure. Currently MAUDE provides no insight into whether a computer related device failure might be the result of an injection of malware or other cybersecurity related issue, rather than just a technological malfunction.

The challenges of IoT for healthcare are myriad and driven primarily by security having been thought of only AFTER something is already online and connected. Healthcare professionals also have an increased tendency to try and get around IT security policy in order to better serve their patients; when a doctor or nurse needs access to computing resources or data because a patient's health is at risk, IT policy takes a back seat in the heat of the moment and can lead to increased risk to cyber threats or insecure access and storage of sensitive information. Compounding the problem, many

Copyright © 2015 Raytheon Company.

of the new network-connected devices in a hospital setting have machine-assisted or determined sharing of information. EKG monitors, blood pressure and intensive care assisted breathing machines automatically send patient data for monitoring at a separate location, such as the nurses station. Hospitals are hesitant to put security measures in between these devices and the network because a false positive of a threat could potentially disrupt the function of the equipment. Raytheon|Websense experts suggest that **up to 75 percent of hospital network traffic goes unmonitored** by security solutions out of fear that improperly configured security measures or alarming false positives could dramatically increase the risk to patient health or well-being.

The combination of challenges confounds security efforts and is likely to increase the prevalence of both attacks and subsequent data loss or theft. With adoption patterns mimicked closely in other industries, this might be said to be a danger for any industry adopting an Internet of Things environment if proper security measures are not established before widespread deployments.

CONCLUSION

It's clear that with the amount of personally identifiable and proprietary information available and inherent as part of the healthcare industry it will remain an attractive target to attackers and a potential weak point for untrained employees. As healthcare continues to avail itself of the technology and advantages of the Internet of Things, it's crucial that its practitioners and executives become more cognizant of how to protect their organizations and the individuals who use their services. Better, ongoing security training for employees as well as a thorough understanding of the specific and evolving cyber threats affecting their organizations and how to defend against them is the only way to counter breaches and the high cost of remediation.

METHODOLOGY

Metrics and data attributed to the Raytheon|Websense Security Labs are based on analysis of real-world security telemetry feeds from global healthcare organizations. This is part of up to 5 billion daily email and web events identified by a global threat intelligence network. Threat activity is monitored across the kill chain which helps reveal the increasingly complex, multi-stage nature of modern threats that involve advanced malware as well as exploit kits, lures, redirects and other malicious acts that comprise a complete threat.

Copyright © 2015 Raytheon Company.

SOURCES

1. United States of America. FBI. Cyber Division. "Private Industry Notification." FBI. American Hospital Association, 8 Apr. 2014. Web. http://www.aha.org/content/14/140408--fbipin-healthsyscyberintrud.pdf

2. Allen, Arthur. "Billions to Install, Now Billions to Protect." Politico. Politico.com, 1 June 2015. Web. http://www.politico.com/story/2015/06/health-care-spending-billions-to-protect-the-records-it-spent-billions-to-install-118432

3. Thompson, Cadie. "Hack Attacks on Hospitals Jump 600% This Year: CEO." CNBC. CNBC.com, 25 Sept. 2014. Web. http://www.cnbc.com/2014/09/25/hack-attacks-on-hospitals-jump-600-this-year-ceo.html

4. "2015 Industry Drill-Down Report - Financial Services." Raytheon|Websense, 23 June 2015. Web. http://www.websense.com/content/2015-finance-industry-drilldown.aspx?intcmp=hp-promo-2015-finance-drill-down-report

5. "Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information." U.S. Department of Health & Human Services - Office for Civil Rights, Web. https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

6. "HIMSS Survey Finds Two-Thirds of Healthcare Organizations Experienced a Significant Security Incident in Recent Past." HIMSS News. Healthcare Information and Management Systems Society, 30 June 2015. Web. http://www.himss.org/News/NewsDetail.aspx?ItemNumber=42944

7. KPMG, LLP. "HEALTHCARE AND CYBER SECURITY: Increasing Threats Require Increased Capabilities." p. 4. 27 Aug. 2015. Web. http://advisory.kpmg.us/content/dam/kpmg-advisory/PDFs/ManagementConsulting/2015/KPMG-2015-Cyber-Healthcare-Survey.pdf

8. "26th Annual HIMSS Leadership Survey Reveals Top Priorities for Healthcare Leaders." HIMSS News. Healthcare Information and Management Systems Society, 13 Apr. 2015. Web. http://www.himss.org/News/NewsDetail.aspx?ItemNumber=41555

9. Dixon, Pamela. "Can CIOs Keep up with pace of Change?" Insights & Publications. SSi-SEARCH, 29 Dec. 2014. Web. http://www.ssi-search.com/images/pdfs/Keeping-Pace-with-Change.pdf

10. SSi-SEARCH, "Why the CIO Is Healthcare's Million Dollar Man." Insights & Publications. SSi-SEARCH, 29 Apr. 2014. Web. http://www.ssi-search.com/images/pdfs/Million-Dollar-Man-WHITEPAPER-April-14.pdf

11. Allen, Arthur. "Billions to Install, Now Billions to Protect." Politico. Politico.com, 1 June 2015. Web. http://www.politico.com/story/2015/06/health-care-spending-billions-to-protect-the-records-it-spent-billions-to-install-118432

12. Filkins, Barbara. "New Threats Drive Improved Practices: State of Cybersecurity in Health Care Organizations." SANS InfoSec Reading Room. SANS Institute, Dec. 2014. Web. https://www.sans.org/reading-room/whitepapers/analyst/threats-drive-improved-practices-state-cybersecurity-health-care-organizations-35652

13. "2015 Most Wired." H&HN July 2015: 26-39. Hospitals & Health Networks. American Hospital Association, July 2015. Web. http://www.hhnmag.com/inc-hhn/pdfs/2015/MostWired_2015_complete.pdf

14. "2015 Travelers Business Risk Index." 2015 Travelers Business Risk Index p: 5. Travelers Business Risk Index. The Travelers Indemnity Company, May 2015. Web. https://www.travelers.com/prepare-prevent/risk-index/business/2015/business-risk-index-report.pdf

Copyright © 2015 Raytheon Company.

15. "Hospitals Implementing Security Measures." American Hospital Association, Sept. 2014. Web. http://www.aha.org/content/13/cyber-measures.pdf

16. Schweber, Arieanna. "Healthcare Security Incidents Need Not Lead to Data Breaches." InTelligence Blog. Absolute, 10 Nov. 2014. Web. http://blogs.absolute.com/blog/healthcare-security-incidents-need-lead-data-breaches/

17. KPMG, LLP. "HEALTHCARE AND CYBER SECURITY: Increasing Threats Require Increased Capabilities." p. 2. 27 Aug. 2015. Web. http://advisory.kpmg.us/content/dam/kpmg-advisory/PDFs/ManagementConsulting/2015/KPMG-2015-Cyber-Healthcare-Survey.pdf

18. Ponemon. "The Unintentional Insider Risk in United States and German Organizations." Ponemon Study: The Unintentional Insider Risk in United States and German Organizations. Raytheon|Websense, 30 July 2015. Web. http://www.raytheoncyber.com/spotlight/ponemon/index.html

19. Foster, Bryan, and Yvette Lejins. "Ehealth Security Australia: The Solution Lies with Frameworks and Standards." Edith Cowan University Research Online. Edith Cowan University, Dec. 2013. Web. http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1010&context=aeis

20. Department of Broadband, Communications and the Digital Economy. "Advancing Australia as a Digital Economy: AN UPDATE TO THE NATIONAL DIGITAL ECONOMY STRATEGY." (n.d.): n. pag. PANDORA. National Library of Australia, 2013. Web. http://pandora.nla.gov.au/pan/123103/20130910-0946/www.nbn.gov.au/files/2011/06/Advancing-Australia-as-a-Digital-Economy-BOOK-WEB.pdf

21. Kuhn, John. "The Dyre Wolf Campaign: Stealing Millions and Hungry for More." Security Intelligence. IBM, 2 Apr. 2015. Web. https://securityintelligence.com/dyre-wolf/

22. Leyden, John. "Dyre times Ahead: Zeus-style Trojan Slurps Your Banking Login Creds." Security. The Register, 8 July 2015. Web. http://www.theregister.co.uk/2015/07/08/dyre_banking_trojan_spam_surge/

23. Brandis, Hon George, and Hon Malcolm Turnbull MP. "Government Response to Committee Report on the Telecommunications (interception and Access) Amendment (data Retention) Bill 2014." Media Releases. Attorney-General for Australia, 3 Mar. 2015. Web. http://www.attorneygeneral.gov.au/Mediareleases/Pages/2015/FirstQuarter/Government-Response-To-Committee-Report-On-The-Telecommunications-Interception-And-Access-Amendment-Data-Retention-Bill.aspx

24. Carville, Olivia. "Ontario Lags Other Provinces in Updating Health Privacy Laws | Toronto Star." Thestar.com. The Star, 6 Feb. 2015. Web. http://www.thestar.com/life/health_wellness/2015/02/06/ontario-lags-other-provinces-in-updating-health-privacy-laws.html

25. Sharpe J.A., Roger J. "Hopkins v. Kay, 2015 ONCA 112." Hopkins v. Kay, 2015 ONCA 112. COURT OF APPEAL FOR ONTARIO, 18 Feb. 2015. Web. http://www.ontariocourts.ca/decisions/2015/2015ONCA0112.htm

26. Ministry of Health and Long-Term Care. "Ontario to Introduce New Measures to Protect Patient Privacy." News Release. Government of Ontario, 10 June 2015. Web. http://news.ontario.ca/mohltc/en/2015/06/ontario-to-introduce-new-measures-to-protect-patient-privacy.html

27. Office of the Auditor General, Manitoba. WRHA'S Management of Risks Associated with End-user Devices. Department of Health, Healthy Living and Seniors, July 2015. Web. http://www.oag.mb.ca/wp-content/uploads/2015/07/FINAL-Report-WRHA-Mgmt-Risks-End-user-Devices-Web-Version.pdf

28. Beamish, Commissioner (Acting), Brian. "Preventing Privacy Breaches and Building Confidence in Electronic Health Records." p.5. Resources, Presentations and Speeches. Information and Privacy Commissioner / Ontario, 9 Feb. 2015. Web. https://www.ipc.on.ca/images/Resources/2015-02-09%20-%20OHA%20-%20Cyber%20Risk%20Conf%20(Web).pdf

Copyright © 2015 Raytheon Company.

29. "ICO given New Powers to Audit NHS." News and Blogs. Information Commissioners Office, 2 Feb. 2015. Web. https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2015/02/ico-given-new-powers-to-audit-nhs/

30. "Forecast: Internet of Things, Endpoints and Associated Services, Worldwide, 2014." Gartner, Inc., 20 Oct. 2014. Web. https://www.gartner.com/doc/2880717/forecast-internet-things-endpoints-associated

31. Fishman, Linda. "American Hospital Association (AHA) Detailed Answers to Questions Posed in the Food and Drug Administration's (FDA) Collaborative Approaches for Medical Device and Healthcare Cybersecurity." (n.d.): n. pag. Aha.org. American Hospital Association, 21 Nov. 2014. Web. http://www.aha.org/advocacy-issues/letter/2014/141121-let-fishman-fda.pdf

32. "Testimony of Paul Black, Before the Senate Committee on Health Education Labor and Pensions Achieving the Promise of Health Information Technology: Information Blocking and Potential Solutions." Hearings/Achieving the Promise of Health Information Technology: Information Blocking and Potential Solutions. Senate Committee on Health Education Labor and Pensions, 23 July 2015. Web. http://www.help.senate.gov/imo/media/doc/Black%20.pdf

33. "Collaborative Approaches for Medical Device and Healthcare Cybersecurity; Public Workshop; Request for Comments." Federal Register. United States Food and Drug Administration, 23 Sept. 2014. Web. https://www.federalregister.gov/articles/2014/09/23/2014-22515/collaborative-approaches-for-medical-device-and-healthcare-cybersecurity-public-workshop-request-for

34. "Def Con 22 Just What The Doctor Ordered." Videos. Security Tube, 01 Jan. 2015. Web. http://www.securitytube.net/video/12020

Copyright © 2015 Raytheon Company.

Copyright © 2015 Raytheon Company. [DTP-PR-HEALTHCAREDRILLDOWNREPORT-22SEPT15]

Insight®

Work smarter

At Insight, we'll help you solve challenges and improve performance with intelligent technology solutions.

Learn more