CRYPTONITE NXT

1st Half of 2018 — Healthcare Cyber Research Report

SPECIAL REPORT | Cryptonite Labs Research Team | July 7, 2018

Contents

Notice

This publication is made available for information purposes only. At the time of publication, all information referenced in this publication is as current and accurate as we could determine. Any additional developments or research, since publication, will not be reflected in this report. Please note that this publication may be changed, improved, or updated without notice.

Cryptonite, LLC is not responsible for any errors or omissions in the content of this report or for damages arising from the use of this report under any circumstances.

Executive Summary

This Healthcare Cyber Research Report for the 1st half of 2018 overviews our analysis and review of data on cyberattacks impacting healthcare institutions across the United States. This new report builds upon our earlier research published in early 2018 within the 2017 Healthcare Cyber Research Report. Our analysis and review of government data, internet sources and the direct experience of our security operations center (SOC) provide the baseline data for our analysis. We perform our analysis based upon information reported between and including January 1, 2018 through June 30, 2018.

As in our Healthcare Cyber Research Report 2017 our data flows, in part, from major data breaches reported to the Health and Human Services Office of Civil Rights (HHS/OCR) as required by federal law. Major data breaches reported to HHS/OCR are required by section 13402(e)(4) of the HITECH Act which affect the unsecured protected health information (PHI) of 500 or more individuals.

In the case of this report we are predominantly focused on that subset of reported breaches categorized by the reporting entity as "IT/Hacking" and then supplement that information with our original research. We then correlate that data with additional independent research as possible against other internet sources.

Highlights for 1st Half 2018:

- Ransomware REVERSES COURSE in 2018 and TRENDS LOWER in the 1st half of 2018
- Ransomware attacks reported as major IT/hacking data breach events impacting over 500 patient records DROPPED from 19 major data breaches in the 1st half of 2017 (the comparison period) to 8 major data breaches in the 1st half of 2018. This is a decrease of 57%.
- Ransomware attacks reported as a percent of major IT/hacking data breach events impacting over 500 patient records DROPPED to 13.56%. This metric peaked in the 1st half of 2017 and then has declined in the two subsequent periods.
- Patient records (ePHI) breached in the 1st half of 2018 came in at 1,928,432 which is slightly higher than previous time periods.
- In context 1,674,793 ePHI records were breached in the 1st half of 2017 and 1,767,955 ePHI records were breached in the 2nd half of 2017.
- Total healthcare major data breaches for the 1st half of 2018 came in at 59 events which seems to be TRENDING lower. In context, if the 1st half of 2018 was annualized to 118 events, this would compare favorably to 2017 measured at 140 reported major IT/Hacking events.

Michael Simon
Co-Founder and Chief Executive Officer
Cryptonite, LLC

Why is Healthcare Targeted?

Healthcare accounts for almost 18% of gross domestic product (GDP) within the United States rivaled only perhaps by the U.S. Federal Government's 20% share of GDP. As healthcare sector technology grows into a very complex ecosystem, so does the sector's cybersecurity attack surface also expand and exposes new vulnerabilities.

Modern healthcare networks include hospitals, clinics and doctor's offices, connected across a wide variety of networks and application systems. Medical devices, permeate hospitals and healthcare systems and bring many points of vulnerability to these networks. Finally, ambulatory physicians and highly distributed healthcare organizations rely on information sharing across a multitude of users networks, departments, and organizations. Patients and ambulatory physicians require almost instant access to medical information systems, scheduling, and more.

Health care networks remain under sustained attack by cybercriminals who intentionally target healthcare networks for two primary reasons. Cybercriminals want to steal the medical records for sale on the dark web. Medical records are prime targets, as this data is highly prized to support identity theft and financial fraud. Medical records are an attractive commodity on the dark web where they demand high premiums from criminal purchasers. Many cyber criminals also want to extort ransom payments by locking up and jeopardizing access to these critical records.

The opportunity appears more attractive to cyberthieves due to the complexity of the healthcare networks, and the many vulnerabilities present in these networks. The number of vulnerabilities and potential exploits is far more than found within typical networks in other industries. From a broad mix of medical devices, to internet of things (IoT) device and more, healthcare networks present a broad opportunity for cyberthieves to find safe harbor from which to identify and steal patient data.

> The opportunity appears more attractive to cyberthieves due to the complexity of the healthcare networks, and the many vulnerabilities present in these networks.

Healthcare 1st Half 2018 — Ransomware Trends Down

In July of 2016 the Health and Human Services Office of Civil Rights (HHS/OCR) indicated that a healthcare organization or an associated business that has been attacked by ransomware should comply with the applicable breach notification provisions per the HIPAA regulations. The logic is clear - if a cyberattacker can encrypt your data and hold it hostage then they have access to it and can be generally assumed that they have therefore viewed and breached the data.

The risk associated with ransomware moved to the forefront in healthcare beginning in 2016 where it was identified by many as a rapidly emerging and dangerous attack. Ransomware provides more immediate rewards to cyberattackers by threatening a patient's access to medical care in exchange for the immediate disbursement of digital funds. Ransomware attacks continued to rise in 2017 with an 89% increase in the frequency of reported attacks.

Our research team has just completed a review of the 1st half 2018 cyberattack data. This includes reported events from between 1 January, 2018 thru 30 June, 2018 inclusive. Our referenced data sets include all entities that have provided notification to HHS/OCR pursuant to the HIPAA regulation.

In the first half of 2018 the successful deployment and attribution of ransomware in major healthcare data breaches, as reported, has diminished substantially. The analysis of the 2018 1st half data shows that frequency of ransomware decreased as an overall percentage of reported IT/Hacking data breaches.

Our data appears to be consistent with other sources. Kaspersky Lab recently found that the total number of ransomware events decreased by approximately 30 percent from 2016-2017 to 2017-2018. The Kaspersky report notes that ransomware attackers are searching for more profitable activities such as cryptojacking. Per Kaspersky, they have found that ransomware is "rapidly vanishing," and that cryptocurrency mining is starting to take its place.

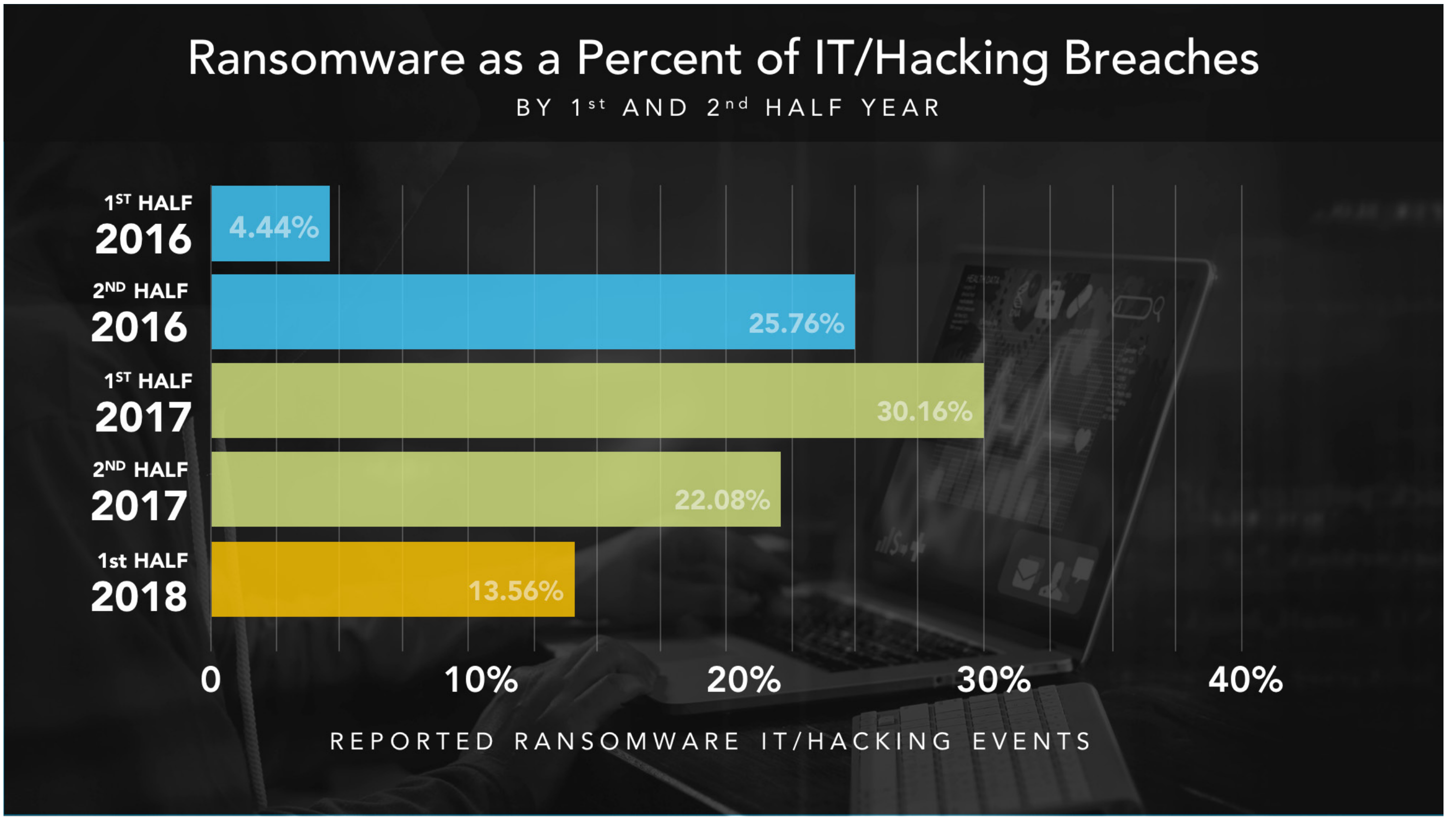
We do believe that ransomware still presents a formidable threat to healthcare and expect new variants, such as AI based malware, to present very difficult challenges to healthcare institutions later in 2018 and into 2019.

Chart 1 - Ransomware as a Percent of Reported IT/Hacking Data Breaches

YEAR	REPORTED RANSOMWARE AS A PERCENT OF IT/ HACKING EVENTS
2016 - 1st HALF YEAR	4.44%
2016 - 2nd HALF YEAR	25.76%
2017 - 1st HALF YEAR	30.16%
2017 - 2nd HALF YEAR	22.08%
2018 - 1st HALF YEAR	13.56%

This is excellent news on all fronts.

Customers have started to add micro-segmentation to networks, as well as specialized software to address ransomware threats. In general, in the largest hospitals, new Zero Trust technologies have been added to the existing mix of defense in depth technologies to expand and harden the defensive perimeters.



Healthcare 1st Half 2018 — Volume of Cyberattacks and Breached Data Records Remains Steady

Overall, IT/Hacking events drive a significant number of major breaches each year in healthcare. The first half of 2018 yielded 59 reported events as of 1 July, 2018, and seems headed towards a projected total of between 120 to 150 total events by the end of 2018.

Chart 2 - Reported Major IT/Hacking Ransomware by Year

YEAR	REPORTED MAJOR IT/HACKING EVENTS	PERCENT CHANGE FROM THE PREVIOUS YEAR
2014 - FULL YEAR	35	
2015 - FULL YEAR	57	62.86%
2016 - FULL YEAR	113	98.25%
2017 - FULL YEAR	140	23.89%
2018 - 1st HALF ONLY	59	

[Projected to 120 to 150 for the entire 2018 year]

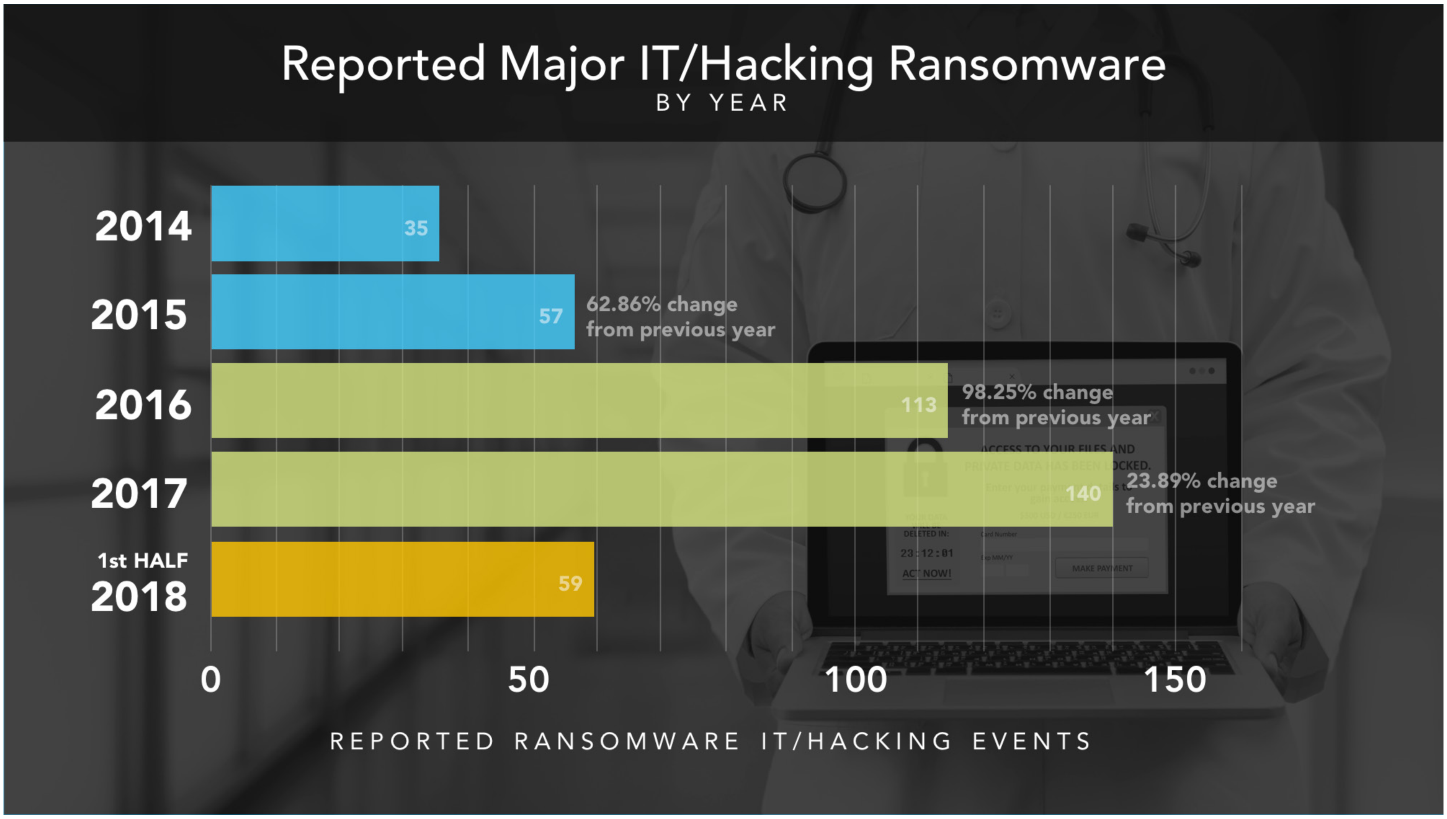
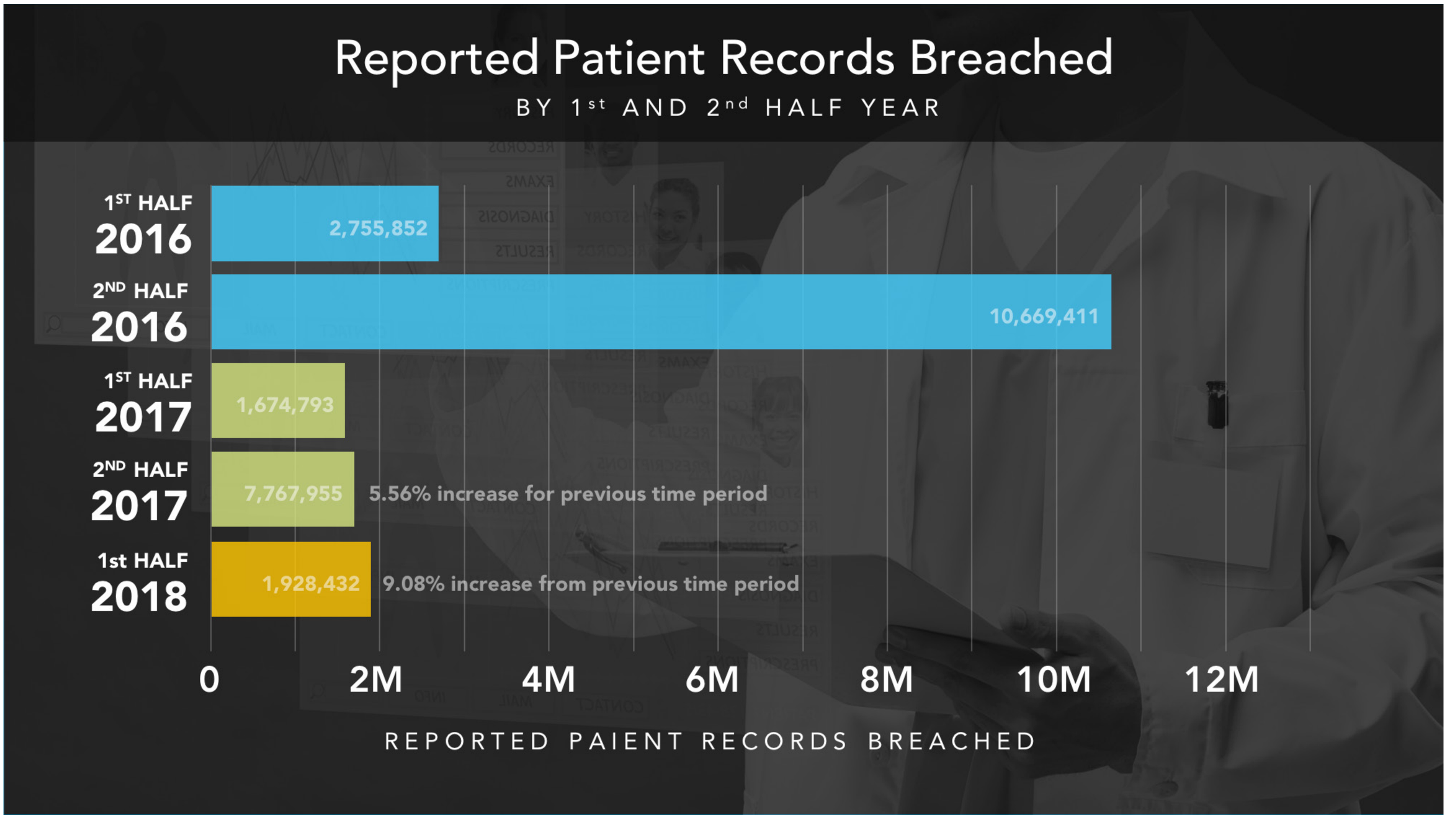


Chart 3 - Healthcare Records Compromised by Year by IT/ Hacking Data Breaches

There were 3,442,748 records reported compromised in 2017, a substantial decrease from 13,425,263 reported compromised in 2016.

YEAR	REPORTED CONFIDENTIAL PATIENT RECORDS BREACHED	PERCENT INCREASE FROM PREVIOUS TIME PERIOD
2016 - 1st HALF YEAR	2,755,852	
2016 - 2nd HALF YEAR	10,669,411	
2017 - 1st HALF YEAR	1,674,793	
2017 - 2nd HALF YEAR	1,767,955	5.56%
2018 - 1st HALF YEAR	1,928,432	9.08%



Healthcare 1st Half 2018 — All IT/Hacking Data Breaches in Healthcare

Chart 4 - All IT/Hacking Data Breaches in Healthcare - 1st Half 2018

NO.	NAME	STATE	COVERED ENTITY TYPE	INDIVIDUALS AFFECTED	BREACH SUBMISSION DATE	RANSOMWARE
1	LifeBridge Health, Inc	MD	Healthcare Provider	538,127	05/15/2018	N/A note: actual breach was in 2016
2	Oklahoma State University Center for Health Sciences	OK	Healthcare Provider	279,865	01/05/2018	N/A
3	Med Associates, Inc.	NY	Business Associate	276,057	06/14/2018	N/A
4	St. Peter's Ambulatory Surgery Center LLC - d/b/a St. Peter's Surgery & Endoscopy Center	NY	Healthcare Provider	134,512	02/28/2018	RANSOMWARE
5	Center for Orthopaedic Specialists - Providence Medical Institute (PMI)	CA	Healthcare Provider	81,550	04/18/2018	RANSOMWARE
6	The Oregon Clinic, P.C. ("The Oregon Clinic")	OR	Healthcare Provider	64,487	05/08/2018	N/A
7	Florida Agency Persons for Disabilities	FL	Health Plan	63,627	03/01/2018	N/A
8	Onco360 and CareMed Specialty Pharmacy	KY	Healthcare Provider	53,173	01/12/2018	N/A
9	Aultman Hospital	OH	Healthcare Provider	42,625	05/25/2018	N/A
10	Holland Eye Surgery and Laser Center	MI	Healthcare Provider	42,200	05/18/2018	N/A note: actual breach was in 2016
11	ATI Holdings, LLC and its subsidiaries	IL	Healthcare Provider	35,136	03/12/2018	N/A
12	Agency for Health Care Administration	FL	Health Plan	30,000	01/05/2018	N/A
13	Inogen, Inc.	CA	Healthcare Provider	29,528	04/17/2018	N/A
14	Decatur County General Hospital	TN	Healthcare Provider	24,000	01/26/2018	N/A
15	Iowa Health System d/b/a UnityPoint Health	IA	Business Associate	16,429	04/16/2018	N/A
16	HealthEquity, Inc.	UT	Business Associate	16,000	06/12/2018	N/A
17	Knoxville Heart Group, Inc.	TN	Healthcare Provider	15,995	04/27/2018	N/A
18	USACS Management Group, Ltd.	OH	Business Associate	15,552	05/08/2018	N/A
19	Esther V. Rettig, M.D., P.A.	KS	Healthcare Provider	13,500	03/01/2018	RANSOMWARE
20	Black River Medical Center	MO	Healthcare Provider	13,443	06/13/2018	N/A
21	Florida Hospital	FL	Healthcare Provider	12,724	05/03/2018	N/A
22	Athens Heart Center, P.C.	GA	Healthcare Provider	12,158	04/16/2018	N/A
23	Guardian Pharmacy of Jacksonville	FL	Healthcare Provider	11,521	03/30/2018	N/A
24	Aflac	GA	Health Plan	10,396	05/29/2018	N/A
25	Elmcroft Senior Living, Inc.	TX	Healthcare Provider	10,000	05/21/2018	N/A
26	Ron's Pharmacy Services	CA	Healthcare Provider	6,781	02/02/2018	N/A
27	Jemison Internal Medicine, PC	AL	Health Plan	6,550	02/16/2018	RANSOMWARE

28	Associates in Psychiatry and Psychology	MN	Healthcare Provider	6,546	05/18/2018	RANSOMWARE
29	CareFirst BlueCross BlueShield	MD	Health Plan	6,200	04/26/2018	N/A
30	Flexible Benefit Service Corporation	IL	Business Associate	5,123	02/16/2018	N/A
31	Michael Gruber DMD PA	NJ	Healthcare Provider	4,624	04/20/2018	N/A
32	InfuSystem, Inc.	MI	Healthcare Provider	3,882	06/22/2018	N/A
33	Texas Health Physicians Group	TX	Healthcare Provider	3,808	04/13/2018	N/A
34	RISE Wisconsin, Inc.	WI	Healthcare Provider	3,731	06/07/2018	RANSOMWARE
35	Scenic Bluffs Health Center Inc	WI	Healthcare Provider	2,889	04/24/2018	N/A
36	Gwenn S Robinson MD	NM	Healthcare Provider	2,500	06/14/2018	N/A
37	Partners HealthCare System, Inc.	MA	Healthcare Provider	2,450	02/05/2018	N/A
38	Cambridge Health Alliance	MA	Healthcare Provider	2,280	03/28/2018	N/A
39	Capitol Anesthesiology Association	TX	Healthcare Provider	2,231	06/01/2018	N/A
40	Boys Town National Research Hospital	NE		2,182	05/09/2018	N/A
41	Massac County Surgery Center dba Orthopaedic Institute Surgery Center	IL	Healthcare Provider	2,000	06/08/2018	N/A
42	University of Virginia Medical Center	VA	Healthcare Provider	1,882	02/21/2018	N/A
43	ATI Holdings, LLC and its subsidiaries	IL	Business Associate	1,776	04/13/2018	N/A
44	Capitol Administrators, Inc	CA	Business Associate	1,733	05/11/2018	N/A
45	The Trustees of Purdue University	IN	Healthcare Provider	1,711	05/25/2018	N/A
46	Worldwide Insurance Services, LLC	PA	Business Associate	1,692	04/30/2018	N/A
47	Forrest General Hospital	MS	Healthcare Provider	1,670	02/01/2018	N/A
48	Terros Incorporated	AZ	Healthcare Provider	1,618	06/05/2018	N/A
49	Robert Smith DMD, PC	TN	Healthcare Provider	1,500	01/22/2018	RANSOMWARE
50	FastHealth Corporation	AL	Business Associate	1,345	02/27/2018	N/A
51	The Pediatric Endocrinology and Diabetes Specialists	NV	Healthcare Provider	1,021	01/18/2018	N/A note: actual breach was in 2014
52	Billings Clinic	MT	Healthcare Provider	949	04/27/2018	N/A
53	Coastal Cape Fear Eye Associates, P.A.	NC	Healthcare Provider	925	02/01/2018	RANSOMWARE
54	Artesia General Hospital	NM	Healthcare Provider	864	02/27/2018	N/A
55	Diagnostic Radiology & Imaging, LLC	NC	Healthcare Provider	800	04/05/2018	N/A
56	Prestera Center for Mental Health Services, Inc.	WV	Healthcare Provider	670	03/20/2018	N/A
57	Atchison Hospital Association	KS	Healthcare Provider	667	04/11/2018	N/A
58	Kelley Imaging Systems	WA	Business Associate	627	06/13/2018	N/A
59	Care Partners Hospice and Palliative Care	OR	Healthcare Provider	600	05/25/2018	N/A
Total Individuals Affected				1,928,432		

The Legal Environment Impacting Healthcare Cybersecurity

The legal environment impacting healthcare institutions and cybersecurity in the United States is quite complex. At the heart of the regulatory environment, at the Federal government level, is the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191. This required the Department of Health and Human Services (HHS) to adopt national standards for electronic healthcare transactions and code sets, unique health identifiers, and security. Congress subsequently incorporated HIPAA provisions that mandated the adoption of Federal privacy protections for individually identifiable health information.

HHS published the final Privacy Rule in December 2000 (modified in August 2002). This Rule set required standards for the protection of individually identifiable health information. Three types of regulated entities were defined - these included: health plans, healthcare clearinghouses, and healthcare providers (entities that conduct standard healthcare transactions electronically). Compliance with the Privacy Rule was required and mandatory as of April 14, 2003 (April 14, 2004, for smaller health plan entities).

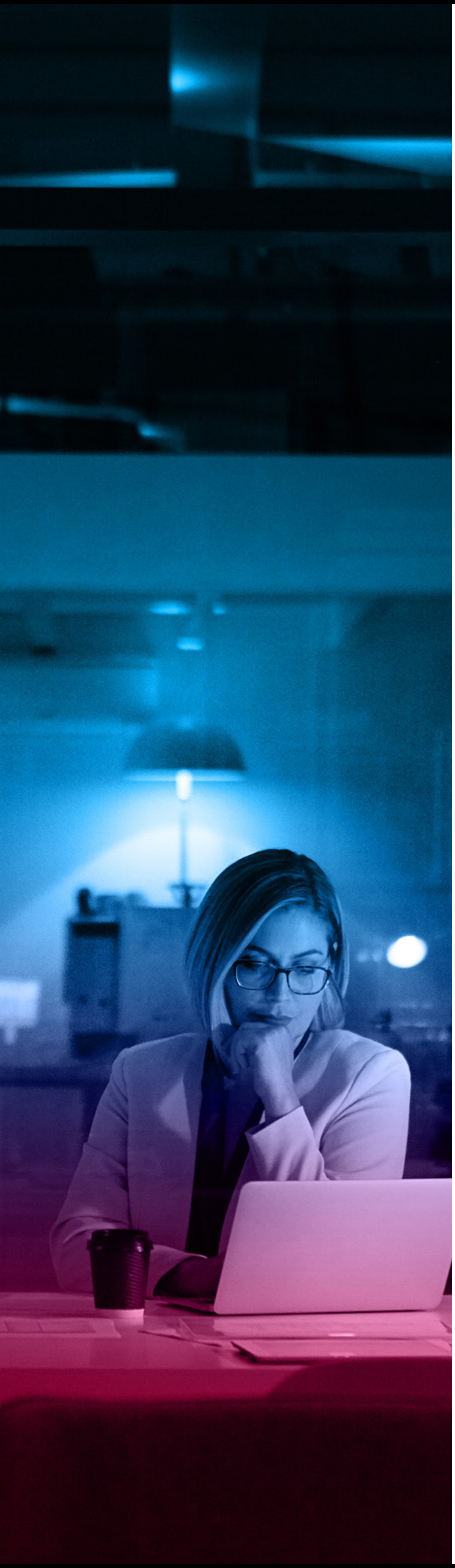
The final Security Rule was published in February 2003. This final Security Rule set national standards for protecting the confidentiality, integrity, and availability of electronic protected health information. Compliance with the Security Rule was required and mandatory as of April 20, 2005 (with an additional year for compliance by small health plans - April 20, 2006).

HHS enacted a final Omnibus rule that implements a number of provisions of the Health Information Technology for Economic and Clinical Health (HITECH) Act, to strengthen the privacy and security protections for health information established under HIPAA, finalizing the Breach Notification Rule. The HITECH act was enacted as part of the American Recovery and Reinvestment Act of 2009, was signed into law on February 17, 2009, to promote the adoption and meaningful use of health information technology. The HITECH act adds considerable strength to the enforcement and associated penalties for failure to comply with the provisions of HIPAA.

As required by section 13402(e)(4) of the HITECH Act, the Secretary must post a list of breaches of unsecured protected health information affecting 500 or more individuals. The breaches that were reported may be found online and accessible via https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

To demonstrate the complicated patchwork of state laws in addition to federal laws and regulations, members of the healthcare industry need to adhere to computer crime laws touching upon issues such as:

- New data privacy laws, such as the one just passed in the state of California;
- New forced disclosure laws, such as the Cloud Act and the Encrypt Act both working their way through the U.S. Congress;
- Unauthorized access (data breach), malware, and viruses in all 50 states. This is a summary of applicable laws by state - http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx ;
- Denial of service attack laws in 25 states, with additional states likely considering the same;
- Ransomware laws in two states, with additional states currently under consideration;
- Spyware laws in 20 states and two territories, with additional states likely under consideration; and
- Phishing laws in 23 states and one territory, with additional states likely under consideration.



Conclusions

Many types of healthcare institutions continue to fall victim to cyberattacks in 2018. The positive trend in reduction of the use of ransomware is overshadowed by the continue high volume of major attacks. Healthcare insurers, hospitals, physician practices, organizations (accountable care organizations - ACOs, independent physician organizations - IPAs, and managed care organizations - MCOs) and a broad variety of other important health entities such as surgical centers, skilled nursing facilities, urology centers, vision surgical centers, cancer treatment centers, MRI/CT-scan centers and diagnostic laboratories fall victim to these attacks every month.

Industry data suggests that approximately 90% of the office-based physicians have moved to use an electronic system (electronic health records - EHR / electronic medical records - EMR) for the storage, retrieval and management of this electronic health data. Virtually all of these systems and the critical data they contain are online and internet accessible. Many have additional online electronic interfaces to diagnostic laboratories. Many also provide online access to ambulatory physicians using mobile and tablet computing devices. All of this creates a perfect and exploit rich environment for cyberattackers and sets the stage for a continued successful breach of electronic protected healthcare information.

Finally, medical devices bring very unique and well known vulnerabilities into healthcare networks. As medical devices are FDA regulated and "closed" all hospital SOC teams cannot install 3rd party cyberdefense software and have very limited to absolutely no visibility into their operation and status. Medical device vulnerabilities can be protected with new cyberdefense using Zero Trust technologies, but healthcare institutions have been slow to implement these technologies so far.

Recommendations

New best practice technologies such as moving target cyber defense (MTD) and network micro-segmentation, can detect and defeat many of the attacks leveraged by vulnerabilities found in most healthcare networks. MTD and network level micro-segmentation technology sets can directly address the inherent weakness in TCP/IP networks. By building out a Zero Trust environment healthcare institutions can directly address the top vulnerability use cases that exist in their networks today. MTD does not allow attackers to use their standard strategies and tools.

A Zero Trust environment can be constructed by combining moving target cyber defense (MTD) and network micro-segmentation technologies. There are no alerts that require immediate action - the system infrastructure will do that automatically. Cyberattackers that seek to perform reconnaissance and enumerate the healthcare network are logged and alerted to the SIEM, and, most importantly, they are immediately shut down and stopped. Attacker or insider threat lateral movement out of policy is logged and alerted to the SIEM, and in a similar fashion they are restricted and shut down. In summary, a Zero Trust environment allows healthcare networks to stop and defeat attackers, ransomware, and insider threats.

About Cryptonite, LLC

Cryptonite is a leader in moving target cyber defense. CryptoniteNXT enables any network to actively shield itself from cyberattacks by preventing all attacker reconnaissance and lateral movement. Patent pending moving target cyber defense and micro-segmentation technologies protect enterprise networks from advanced cyberattacker, insider threats, and ransomware. The Cryptonite customer base includes Forbes Global 2000 commercial and government customers around the world. Learn more at **www.cryptonitenxt.com.**

CRYPTONITE NXT

For More Information

To learn more about Cryptonite, LLC and CryptoniteNXT,
please email **info@cryptonitenxt.com**

This document is current as of the initial date of publication and may be changed by Cryptonite at any time.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NONINFRINGEMENT.

Cryptonite products are warranted according to the terms and conditions of the agreements under which they are provided. The client is responsible for ensuring compliance with laws and regulations applicable to it. Cryptonite does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection, and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated, or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service, or security measure can be completely effective in preventing improper use or access.

CRYPTONITE DOES NOT WARRANT THAT ITS PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Cryptonite, 2275 Research Blvd. Suite 750, Rockville, Maryland 20850