White Paper

Bitdefender®

Ransomware – A Growing Menace for Healthcare Providers

-Protecting sensitive medical records -

Introduction

In May 2017, a malware strain wielding both an NSA exploit and a jerry-rigged ransomware mechanism hijacked computers across 150 countries. WannaCry took copious amounts of data hostage and demanded hefty sums in exchange for the decryption keys.

The contagion, allegedly the work of North Korean hackers, spread like wildfire, infecting countless systems worldwide and dealing billions of dollars in damages. Some victims ceded to the attackers' demands, but few got their data back.

In the months that followed the WannaCry outbreak, ransomware became the most virulent form of malware to threaten digital economy – and has remained so to this day. Among the verticals affected by WannaCry and its successors, the healthcare sector was hit particularly hard, as hackers quickly developed a taste for holding medical records hostage.

This whitepaper examines:

- The growing number of data breaches targeting healthcare
- Notorious ransomware attacks targeting healthcare providers (HCPs) in 2018
- Financial and reputational costs associated with compromised medical records
- SamSam – the most prolific ransomware family used against healthcare institutions
- Key actions that HCPs can undertake to keep ransomware operators at bay

Executive summary

For the eighth year in a row, healthcare organizations have incurred higher costs than any other sector from data breaches, costing them an average of $408 per lost or stolen record. Costs associated with data breaches in healthcare are nearly three times higher than in other industries.

Reporting data breaches wasn't mandatory for every type of organizations before the General Data Protection Regulation (GDPR) came into force, but the health sector is a different animal. Healthcare is more tightly regulated than most other industries, and it's also seen a spike in data breaches in the last year – especially ransomware attacks.

Health or clinical data is also the most common type of personal data compromised. With the new regulations in place, reported incidents in healthcare are on the rise, and analysts expect this trend to march forward.

In the United States, healthcare organizations suffered a substantial increase in hacking in the second quarter of 2018. Between January and March of this year, nearly three dozen incidents targeted hospitals and clinics. Between April and June, the number of attacks almost doubled. Between 2 million and 3 million patient records were reportedly affected in the second quarter of 2018, and seven of the reported incidents specifically mentioned ransomware.

A ransomware strain christened 'SamSam' has been responsible for key attacks targeting healthcare in 2017 and 2018, with some hospitals forced to turn away their patients, while others turned to pen-and-paper. An attack on Singapore's Ministry of Health compromised 1.5 million patient records, including the patient chart belonging to the country's prime minister.

The costs associated with ransomware attacks were sky-high for some HCPs, and moderate for others. But as the ransomware menace continues to loom over the industry, and bad actors steadily hone their infiltration techniques, healthcare businesses must take quick action or risk dire consequences.

Key findings

- Data breaches targeting healthcare are on the rise
- Healthcare organizations incur the highest costs from data breaches ($408 per lost or stolen record); stolen medical information is now worth more than stolen credit information
- Ransomware can be potentially life threatening, as some hospitals are forced to suspend operations after falling victim
- Electronic health records (EHR) contain highly sensitive data, yet many clinics communicate through unsecure channels and their systems are poorly patched
- Stolen patient health information (PHI) that makes its way onto the dark web can be used for various kinds of fraud and extortion, such as banking and credit fraud, healthcare fraud, identity theft and ransom extortion
- The SamSam ransomware family is responsible for most ransomware attacks targeting healthcare in the past year; its authors have extorted millions from their victims
- Healthcare has the highest "abnormal" churn rate of all industries (6.7%), followed closely by Finance (6.1%) and Pharmaceuticals (5.5%); companies experiencing a churn rate greater than 4 percent incur an average cost of $4.9 million
- Using a security tool that operates in another tool's detriment can lead to disaster
- Employing a single-pane solution gives doctors, nurses and administrators secure, reliable access to electronic medical records (EMR)

Data breaches targeting healthcare on the rise

New research reveals that half of U.S. adults are on their toes when it comes to health data security. Surveys indicate that the average Joe is aware of the sensitive nature of medical records.

From April to June 2018, a routine number of health data breaches was reported to the U.S. Department of Health and Human Services (HHS) and the media. In most of these cases, actual details of the breach were disclosed. While some reports indicated 2 million records were compromised, other assessments pinned the figure at more than 3 million patient files. Decisively, the number of affected patient records at least doubled and as much as tripled from Q1 2018 (1.13 million compromised records reported).

But why is healthcare hacking spreading so quickly, and how do fraudsters profit from stolen medical records? Mark Beckmeyer, Director of IT Security at healthcare reputation management firm Binary Fountain, believes ransomware is the most significant threat to healthcare organizations. First, because HCPs use specialized equipment running software that sometimes can't be patched. Secondly, the data flowing through these systems can be accessed by a plethora of personnel, including physicians, nurses, clinicians, administrative, information technologists, compliance, receptionists, patients and numerous other medical and support personnel.

And, as it turns out, stolen medical information is now worth more than stolen credit information. Electronic health records (EHR) contain some of the most private information about us, yet many clinics either communicate through unsecure channels, or their systems are poorly patched (or both). For example, Missouri-based Cass Regional Medical Center was forced to shut down some operations and divert patients after ransomware infected its infrastructure and its EHR vendor.

In July 2018, Missouri-based Cass Regional Medical Center was forced to shut down some operations and divert patients after suffering a ransomware infection on its infrastructure and its EHR vendor – full report.

Patient health information (PHI) that makes its way onto the dark web following a breach is typically sold in bundles called “fullz.”

Fullz can be used for fraud and extortion, including banking and credit fraud, as well as ransom extortion. And because hackers find it relatively easy to steal PHI and sell it on underground markets, it becomes obvious why healthcare hacking has been continuously on the rise in the past year.

> **“Fullz are records of structured personal information that can later be used for various kinds of fraud and extortion such as banking and credit fraud, healthcare fraud, identity theft and ransom extortion. In some cases, fraudsters are interested in buying specific medical records […]” – Cynerio.**

Worse still, children’s PHI currently represents roughly 10% of all PHI records. HCPs often store this data in medical servers that aren’t sufficiently safeguarded.

They often transfer this data over unencrypted and unprotected channels. Even the dead now need to be protected from identity theft, as crooks literally make up Social Security numbers that match those of the deceased. “Ghosting,” as the practice is called, lets crooks rack up charges as financial institutions take months to receive, share or register death records.

Key ransomware attacks targeting healthcare in 2018

New ransomware attack forces hospitals to turn away patients
Provider of electronic health record (EHR) technology Allscripts was hit by SamSam ransomware, provoking an outage that affected thousands of physicians’ practices and healthcare providers across the United States -- hotforsecurity.bitdefender.com

‘Im Sorry’ – Second Indiana hospital hit by ransomware
“The very day that Hancock Health fell victim to a ransomware attack, another hospital in Indiana suffered a similar breach. Adams Health Network, which runs Adams Memorial Hospital, said the attack did not affect the quality and safety of patient care.” – hotforsecurity.bitdefender.com

Ransomware attack drives Indianapolis hospital back to pen and paper
“A hacker out to make a fast buck last week decided to hit an Indianapolis hospital with a ransomware attack, demanding a ransom payment to his Bitcoin wallet in exchange for de-crippling the facility’s computer network.” – hotforsecurity.bitdefender.com

Ransomware attack against California provider breaches data of 85,000 patients
“The California-based Center for Orthopaedic Specialists (COS) is notifying 85,000 of its current and former patients that a ransomware attack on its IT vendor may have breached their data.” -- healthcareitnews.com

Ransomware, malware attack breaches 45,000 patient records
“Missouri-based Blue Springs Family Care reported a breach of 44,979 patient records after hackers peppered the provider with a variety of malware, including ransomware.” – healthcareitnews.com

Missouri hospital forced to divert patients after ransomware attack
“A Harrisonville, Missouri-based hospital has been forced to shut down some operations and divert patients after a ransomware attack on its infrastructure and electronic health record (EHR) vendor.” – hotforsecurity.bitdefender.com

US clinical lab recovers within 50 minutes of getting hit by SamSam ransomware

"LabCorp, a clinical lab based in Burlington, North Carolina, fell victim to a ransomware attack last week, in the latest in a long string of hacker attacks on the healthcare sector." – hotforsecurity.bitdefender.com

Hackers breach Singapore's largest healthcare provider; steal records of 1.5 million patients, including the Prime Minister's

"A hacker attack on Singapore's largest group of healthcare institutions has compromised 1.5 million patient records, the Ministry of Health (MOH) said in a press release." – hotforsecurity.bitdefender.com

Thousands of patient records held for ransom in Ontario home care data breach, attackers claim

"The detailed medical histories and contact information of possibly tens of thousands of home-care patients in Ontario are allegedly being held for ransom by thieves who recently raided the computer systems of a health-care provider." -- cbc.ca

Missouri hospital forced to divert patients after ransomware attack

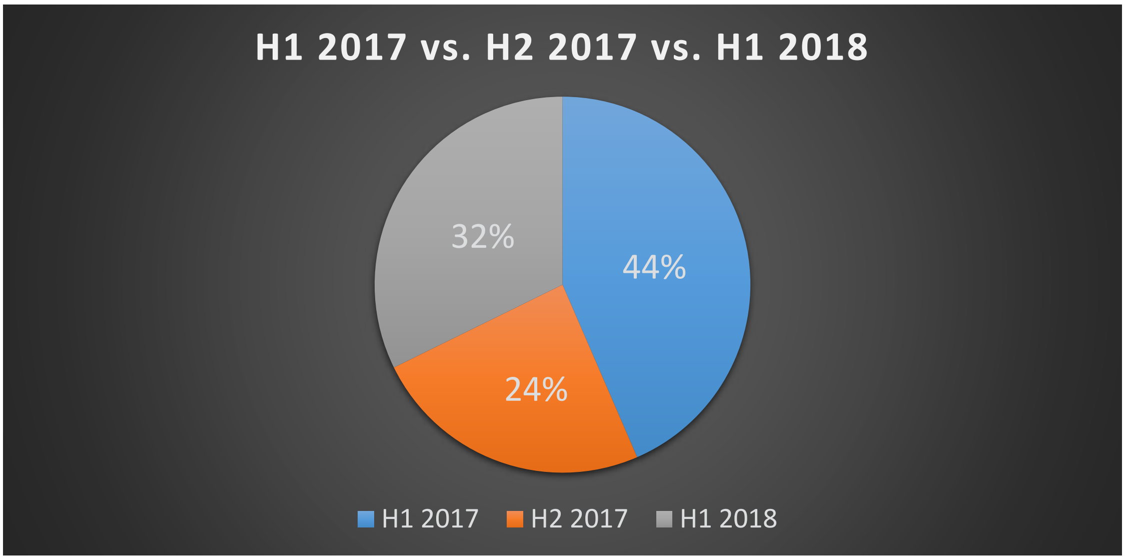
"A Harrisonville, Missouri-based hospital has been forced to shut down some operations and divert patients after a ransomware attack on its infrastructure and electronic health record (EHR) vendor." -- hotforsecurity.bitdefender.com

SamSam is 'Sorry' – the ransomware family predominantly used in healthcare attacks

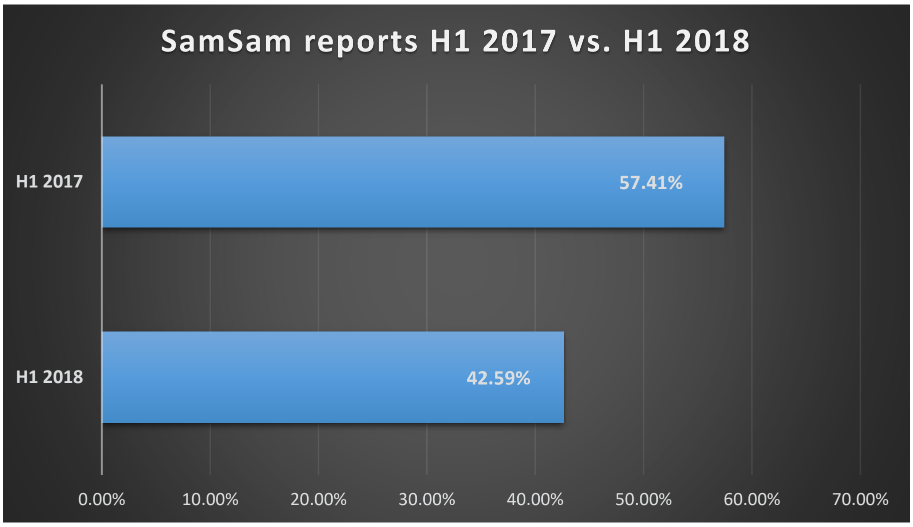
Many (if not most) ransomware operators targeting the healthcare sector in 2017 and 2018 used SamSam, which – like the infamous WannaCry – leverages a wormable component to gain a foothold on the targeted infrastructure. Since its inception, SamSam has reportedly extorted a total of $6 million from its victims.

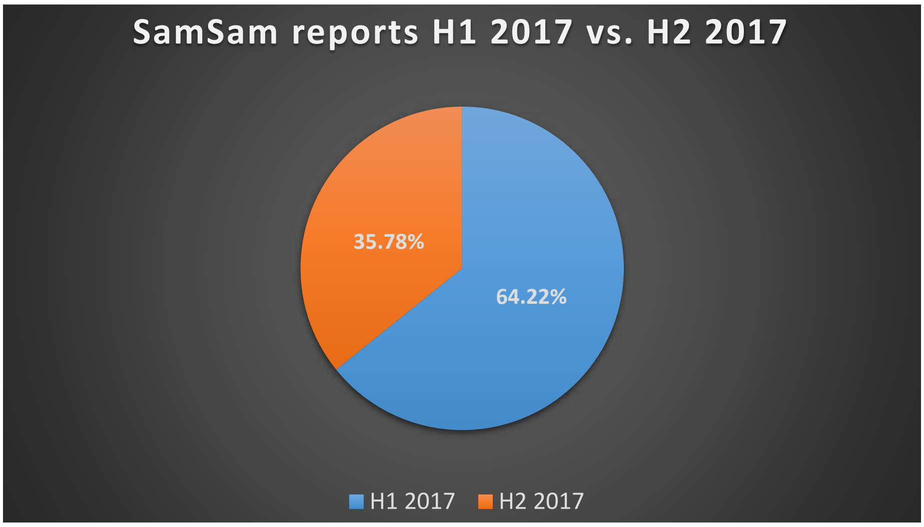
SamSam spreads through the web and Java apps, and specifically targets external-facing RDP servers. It relies on unsophisticated techniques (i.e. brute force tools) to guess weak passwords and make its way into the network. Thanks to a wormable component, once it makes its way inside, it spreads laterally to infect other vulnerable systems. The apologetic SamSam displays an ironic "I'm sorry" in its ransom notes, URLs, and/or infected files.

Over the 18-month period between January 2017 and June 2018, H1 2017 was responsible for 43.5% of the total SamSam infections. The second half of 2017 saw just 24.24% of the total SamSam reports, while H1 2018 stood slightly higher at 32.27%.

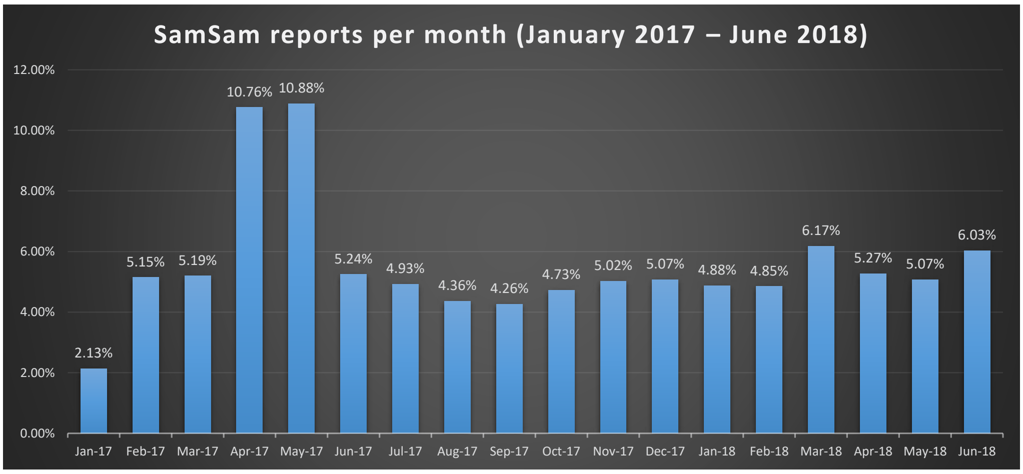


Year over year, H1 2017 recorded 57.4% of infections while H1 2018 saw 42.6% of the total SamSam reports over this 12 month period.





H1 2017 recorded 44% more SamSam reports compared to H2 2017 and 26% more than H1 2018. The numbers are somewhat surprising considering that ransomware attacks in healthcare mostly attracted media attention this year, whereas 2017 was substantially more packed with incidents – at least those involving the SamSam ransomware family. A chart showing the detection rate per month across the full, 18-month time-frame can be found below. April and May of 2017 are clear standouts as far as SamSam infections in a single month.



These numbers reflect only a portion of SamSam infections in 2017 and the first half of 2018, and just those detected by Bitdefender solutions in the given time frame. The number of actual SamSam infections (and other types of ransomware) targeting healthcare are likely much higher. For example, many ransomware families get caught in our net under completely generic names, such as 'Gen:Variant.Razy.12345'. There is a fair chance of encountering SamSam under such a name. And, although ransomware in healthcare mostly attracted media attention this year, 2017 appears much more packed with ransomware incidents – at least those involving the SamSam family.

The cost of data breaches in healthcare

As noted above, the SamSam ransomware family alone was said in July to have extorted some $6 million from its victims since researchers first started tracking it. That number may well be higher today.

A data privacy report prepared by Cornerstone Capital Group (CCG) and commissioned by the Investor Research Responsibility Center Institute (IRRCi) shows that companies reliant on collecting, processing, and managing consumer data are at a higher risk than ever. For example, the widely circulated Cambridge Analytica scandal cost social networking giant Facebook a staggering $119 billion in market valuation.

But it's not just social networks that must be careful handling precious user data. Retailers like Amazon, financial services providers like American Express, telcos like AT&T, and healthcare providers like Britain's National Health Service (NHS) or the US Health & Human Services (HHS) are in the same boat. The data these entities collect and capitalize on is a double-edged sword – if hackers grab hold of it, millions or even billions of dollars are at stake.

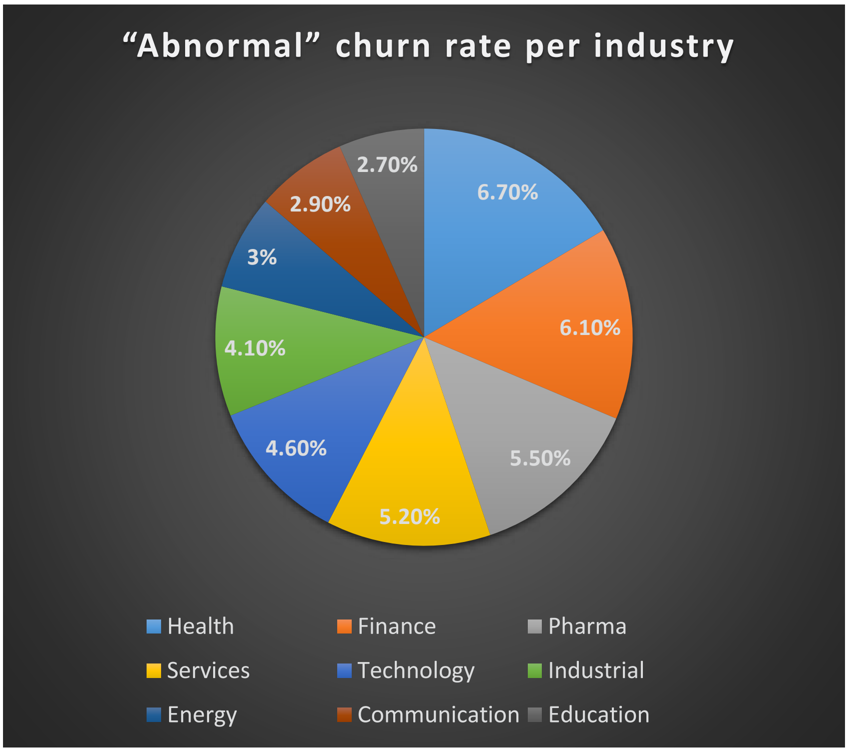
As the IRRC Institute notes, stakeholders must understand how they are exposed to uncertainties related to public acceptance of data collection and use. They must also comprehend how the magnitude of those uncertainties increases exponentially with the explosive expansion of available passive data.

"As policymakers and consumers struggle with data privacy issues, investors need frameworks to understand both the different ways companies monetize personal data and the business risks those business models face. Given the recent data scandals and the soaring level of concern around data privacy issues, investors are increasingly wary about how companies will evolve business strategies reliant on consumer data. As expectations for privacy shifts, some companies will flounder, and others will flourish." -- Jon Lukomnik, IRRCi executive director.

As Ponemon Institute shows in a recent study, certain industries are more vulnerable to churn when customers can easily take their business to another competitor. In highly regulated industries such as healthcare, customers typically have high expectations for the protection of their data.

"When these organizations have a data breach, customers' trust will decline and they will try to find a substitute. In contrast, the public sector, which has the lowest churn, has no competitor and customers have no other options," Ponemon researchers said.

In fact, healthcare has the highest "abnormal" churn rate of all industries at 6.7%, followed by finance (6.1%), pharmaceuticals (5.5%), services (5.2%), technology (4.6%), industrial (3.1%), energy (3.0%), communication (2.9%), and education (2.7%).



Furthermore, the average cost for each lost or stolen record containing sensitive and confidential information, for all industries, has increased by 4.8 percent year-over-year (YoY) and now sits at $148. For healthcare businesses, triple that figure: $408 per lost or stolen record. The costs associated with "mega breaches" (1 million records upwards) are monumental. Ponemon projects that, for 50 million records lost, the average financial damage is $350 million. Companies that experience less than a 1 percent loss of existing customers experience an average total damage of $2.7 million. However, for companies experiencing a churn rate greater than 4 percent, researchers project an average cost of $4.9 million.

Finally, healthcare organizations are among the slowest to contain a breach, at 103 days. Failure to swiftly identify the data breach leads to higher costs. In 2017, the average total cost was $2.80 million for less than 100 days to identify, and $3.83 million for more than 100 days.

Partners shoulder the responsibility of protecting data

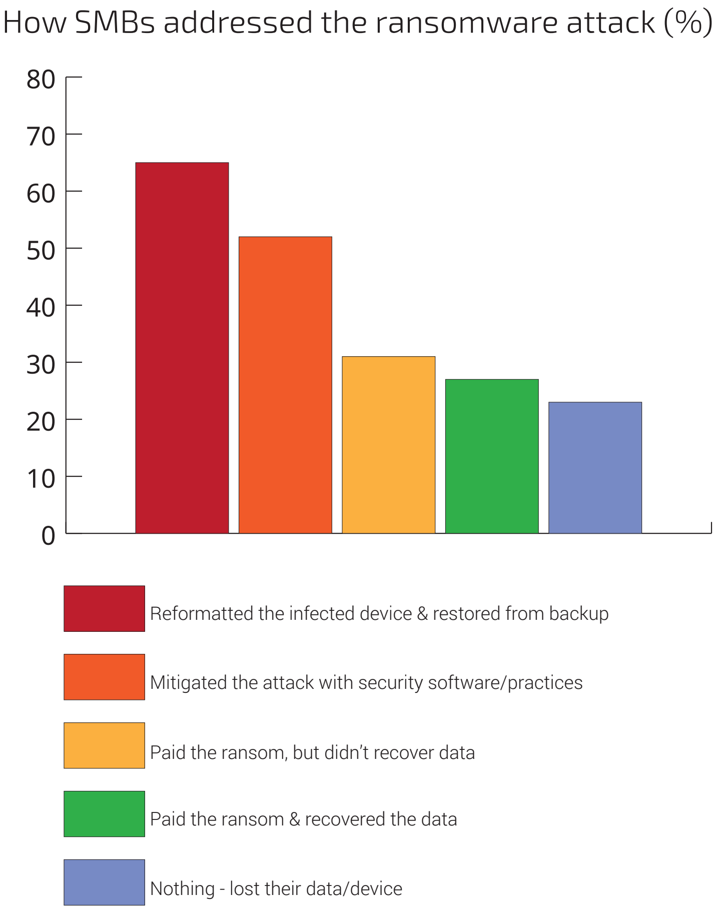
According to Taylor Lehmann, CISO of Wellforce – parent organization of a health system that includes Tufts Medical Center and Floating Hospital for Children – cyber-threats in healthcare stretch far and wide, forcing many parties to shoulder the responsibility of safeguarding patient data.

In a joint press release by leading health systems and providers announcing the Provider Third Party Risk Management Council – an effort to develop and promote a series of practices to manage information security-related risks in their supply chain and to safeguard patient safety and information – Lehmann makes the following remark:

> **"Health systems and other providers need to be more active in assessing and monitoring risks posed by third parties to protect patient information while delivering effective care. The primary challenge is organizations can engage with vendors of various sizes, maturity and complexity without really knowing whether the vendor should be engaged in the first place based on their beliefs and investment in cybersecurity."**

Lehmann underscores that third parties can have anywhere from dozens to hundreds of thousands to serve. He also warns that this challenge results in lost time and resources in attempting to comply with each organization's risk management requirements and ensure efficiency for both parties.

Many, if not most, healthcare providers operate as small-to-medium businesses (SMBs) – precisely the business segment attackers are now increasingly targeting to extort higher fees. Meeting our predictions for 2017, a Bitdefender survey showed that one in every five small and medium businesses in the US reported a ransomware attack in the past 12 months. 38% paid the ransom ($2,423 on average) but only 45% of the SMBs that paid their attackers actually got their information back. Most were able to mitigate the attack by restoring from backup or through security software/practices. A quarter of the ransomware victims couldn't find a solution to address the attack and lost their data.



'Gravitating' towards a solution

Even when an organization is protected by multiple security solutions, ransomware can creep into the infrastructure. In fact, as one healthcare provider learned the hard way, using multiple solutions from different vendors simultaneously can sometimes spell disaster.

Saint Francis Healthcare System is a 300-bed facility serving more than 713,000 people throughout Missouri, Illinois, Kentucky, Tennessee and Arkansas. With so many patients' health at stake, physicians need uninterrupted access to vital medical information, as well as reliable systems that won't compromise the patients' personal data. The hospital used an antimalware solution that worked well for the most part, but erroneously blocked critical applications (requiring doctors to call for support at all hours), created scan storms, and dragged virtual desktop sessions to a crawl. This forced IT to remove antivirus software from the virtual desktop infrastructure, leaving thousands of endpoints unprotected. To fill the gap, IT threw a separate anti-malware solution into the mix. Because policies across the two solutions conflicted, the infamous CryptoLocker ransomware eventually evaded the protective layer and infected Saint Francis Healthcare System.

To avoid falling into the same trap in the future, Saint Francis Healthcare System 'gravitated' towards Bitdefender's GravityZone business security suite, which includes security for virtualized environments as well as endpoint protection. Deployed on premises, GravityZone now protects the hospital's 2,200 Microsoft Windows-based physical PCs, 2,100 virtual desktops delivered through VMware Horizon and Citrix XenApp, and 425 Windows and Linux servers. GravityZone provides Saint Francis physicians, nurses and administrators with secure, reliable access to the provider's Epic electronic medical record (EMR) systems and legacy EMRs such as AllScripts, Mosaic and eClinicalWorks, as well as payroll, asset tracking and other business applications.

Closing statements

The public is becoming increasingly aware of the dangers of exposed personal data, and with strict new regulations (GDPR) in place threatening to close businesses that fail to protect the data, healthcare providers everywhere have no choice but to act. Using the right technologies that meet both your business needs and your clients' needs is key to staying competitive, while ensuring perpetuity. As ransomware operators continue to target the healthcare sector in an increasingly legislated landscape, HCPs now more than ever need to invest in a streamlined security strategy that lets them care not just for patients' health, but also for the security of their data, and their privacy. To learn more about Bitdefender's offering, visit our Business Security page.

Sources:

[1] https://businessinsights.bitdefender.com/when-it-comes-to-data-breaches-healthcare-businesses-stand-to-lose-most

[2] https://marketing.protenus.com/hubfs/Breach_Barometer/2018/Q2%202018/Q2%202018%20Protenus%20Breach%20Barometer.pdf

[3] http://cynerio.co/healthcare-hacking-trends-dark-web/

[4] https://www.aarp.org/money/scams-fraud/info-03-2013/protecting-the-dead-from-identity-theft.html

[5] http://newsroom.ibm.com/2018-07-11-IBM-Study-Hidden-Costs-of-Data-Breaches-Increase-Expenses-for-Businesses

[6] https://www.helpnetsecurity.com/2018/07/26/securing-healthcare-organizations/

[7] https://www.businesswire.com/news/home/20180829005255/en/Nation%E2%80%99s-Health-CISOs-Lead-Manage-Third-Party-Risk

[8] https://www.bleepingcomputer.com/news/security/samsam-ransomware-crew-made-nearly-6-million-from-ransom-payments/

[9] https://download.bitdefender.com/resources/files/News/CaseStudies/study/178/Bitdefender-Business-CaseStudy-SFrancis-crea2058-210x297-en-EN-GenericUse.pdf?adobe_mc=MCMID%3D02440733356223831711638424006370811913%7CMCORGID%3D0E920C0F53DA9E9B0A490D45%2540AdobeOrg%7CTS%3D1535630258

[10] https://www.bitdefender.ro/files/News/CaseStudies/study/237/BriefingsDirect-Transcript-How-MSPs-Leverage-Bitdefenders-Layered-Approach-to-Security-For-Comprehensive-Client-Protection.pdf

[11] https://download.bitdefender.com/resources/files/News/CaseStudies/study/153/Ransomware-SMB-survey-crea1289-A4-en-EN-web.pdf?adobe_mc=MCMID%3D75844485696167430231514170731505923126%7CMCORGID%3D0E920C0F53DA9E9B0A490D45%2540AdobeOrg%7CTS%3D1536047480

[12] http://www.itsecurityguru.org/2018/09/03/data-breach-reports-information-commissioner-increase-75/

Author: Filip Truta, Security Specialist

Bitdefender is a global security technology company that delivers solutions in more than 100 countries through a network of value-added alliances, distributors and reseller partners. Since 2001, Bitdefender has consistently produced award-winning business and consumer security technology, and is a leading security provider in virtualization and cloud technologies. Through R&D, alliances and partnership teams, Bitdefender has elevated the highest standards of security excellence in both its number-one-ranked technology and its strategic alliances with the world's leading virtualization and cloud technology providers. More information is available at http://www.bitdefender.com/.