BITSIGHT®
The Standard in SECURITY RATINGS

BITSIGHT INSIGHTS REPORT

THE RISING FACE OF CYBER CRIME: RANSOMWARE

For more information
contact us at:

BitSight Technologies
125 CambridgePark Drive
Suite 204
Cambridge, MA 02140

www.bitsighttech.com | sales@bitsighttech.com

INTRODUCTION

1989: AIDS Trojan

In 1989, long before the widespread adoption of the Internet, cyber criminals were using floppy disks to spread ransomware across computers. This AIDS Trojan, also known as the "PC Cyborg Trojan," was the first strain of ransomware ever documented.[1] More than 27 years later, ransomware is now a lucrative business for cyber criminals, with some experts estimating that hackers earn over $90,000 per year through these attacks.[2]

Today's cyber criminals have evolved their approach using advanced strains of ransomware that encrypt data on an organization's network or lock users out of their devices. These hackers then demand a ransom, typically in the form of Bitcoin, before restoring the data back to normal. They even use "ransomware-as-a-service," which offers malware-construction kits designed to be easily deployed with minimal hacking experience.[3]

Ransomware is a legitimate threat, with estimates from the U.S. Justice Department showing that over 4,000 of these attacks have occurred every day since the beginning of the year.[4] In this BitSight Insights Report, researchers analyzed the growing trend of ransomware across nearly 20,000 companies to identify common forms of ransomware, and identify which industries are most susceptible to these types of attacks. The findings show that the rate of new ransomware strains, such as Locky and Cryptowall, has spiked over the last couple of years, and numerous industries are beginning to fall victim to these ransomware attacks.

2005: Gpcoder Trojan

2006: Archievus Trojan

2009: Ransomlock Trojan

2012: Reveton Trojan, Winlock Trojan, Matsnu Trojan

2013: Cryptolocker, Dircrypt

2014: Cryptodefense, CTB-Locker, SimplLocker, Sypeng, Sypeng, Nymaim, Cryptowall

2015: LockerPin, TeslaCrypt, LowLevel04, Chimera

2016: Ransom32, 7ev3n, Locky, SamSam, KeRanger, Petya, Maktub, Jigsaw, CryptXXX, ZCryptor, Zepto, KimcilWare

KEY FINDINGS

As part of this BitSight Insights Report, data scientists examined the cybersecurity performance of nearly 20,000 companies. The findings highlight the security posture of different industries over the last 12 months and the growth of ransomware during that time.

1

Ransomware Gaining Traction

The rate of ransomware has significantly increased for every industry examined over the last 12 months. Cyber criminals seem to be finding a lucrative business through ransomware attacks.

2

Education Has Highest Rate of Ransomware

Education has the highest rate of ransomware of all industries examined in this report. In fact, these institutions have over three times the rate of ransomware found in Healthcare and more than ten times the rate found in Finance.

3

Government's Ransomware Dilemma

Of the six industries examined, Government had the second-lowest security rating and the second-highest rate of ransomware. In fact, ransomware in this sector more than tripled over the last 12 months.

4

Ransomware Continues to Rapidly Evolve

One in ten organizations in Education has been impacted by Nymaim, while 34 different Government groups have been hit with Locky, which was discovered only eight months ago.

5

The Ransomware Threat to Finance

Although ransomware is not typically associated with the Finance industry, researchers discovered that more than 115 different Financial Services organizations have some form of ransomware on their corporate networks.

INDUSTRY RATINGS

A Breakdown of Security Performance by Industry

Before examining ransomware, BitSight researchers explored the cybersecurity posture of six major industries: Government, Healthcare, Finance, Retail, Education, and Energy/Utilities. Findings revealed that certain industries have seen a steady increase in their ratings, while others have worsened (Figure 1).

15 points

Over this past year, the average security rating of Education dropped by almost 15 points.

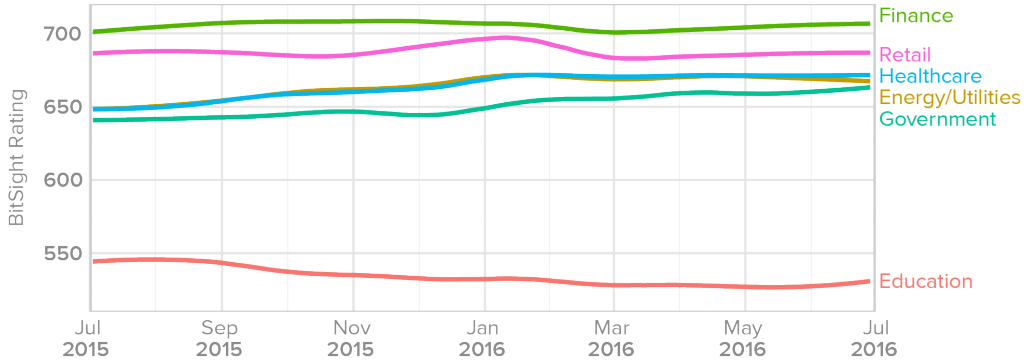

Figure 1. Average security ratings over the last 12 months by industry.

Financial Services companies continue to exhibit excellent security effectiveness, and the results are not surprising considering their continued adoption of security frameworks, such as the NIST Cybersecurity Framework (CSF),[5] along with increased scrutiny around their cybersecurity performance. A sign of this scrutiny has already been seen this year, as the Office of the Inspector General began auditing the Federal Reserve's effectiveness to ensure that banks have strong information security policies.[6]

In contrast, academic institutions show low security ratings possibly due to smaller IT teams, budgetary constraints, and a high rate of file sharing activity on their networks. Earlier this year, BitSight found that roughly 58 percent of organizations in the Education sector have some type of file sharing on their network.[7] With access to social security numbers, medical records, intellectual property, research, and financial data of faculty, staff, and students, these institutions are a prime target for cyber attacks. In fact, research by Coalfire Systems shows that 17 percent of all data breaches occur in higher education institutions.[8]

Over the past year, cyber attacks have changed the threat landscape for many of the sectors in this report. Healthcare organizations have been hit with ransomware attacks,[9] critical infrastructure has been threatened by cyber hackers from nation states, [10] millions of people have had their personal information compromised by data breaches on Financial Services organizations,[11] and thousands of taxpayer information has been accessed by cyber criminals.[12] Although some industries improved their cybersecurity performance over time, incidents throughout the year depict the widespread effect of data breaches. This threat underscores the importance of good network hygiene and the value of continuously monitoring for the existence of malware, and increasingly ransomware.

RANSOMWARE RISING

Analysis of Ransomware Across Different Industries

Over a decade ago, one of the first forms of advanced ransomware, "Gpcoder," encoded files on a network and made them unreadable.[13] Today, there is an entirely new arsenal of ransomware used by cyber thieves to extort money from organizations. Most ransomware attacks share a common trait: they begin with one seemingly benign email attachment opened by an employee. This action introduces malicious code into the network that encrypts or locks critical data (e.g. patient records, financial information, or business documents).

Hospitals, in particular, may pay the ransom because their patient data is critical in life-or-death situations. This was the case with Hollywood Presbyterian Medical Center earlier this year, which chose to pay a $17,000 ransom to hackers who had locked some of the hospital's critical data.[14] MedStar Health, another medical center, reported earlier this year that malware had caused a shutdown of some systems at its hospitals in Baltimore.[15] Methodist Hospital in Henderson, Kentucky even declared an internal state of emergency after its systems were attacked by a strain of ransomware known as Locky.[16]

Although patient data makes Healthcare organizations a prime target for ransomware attacks, other industries are well on a cyber criminal's radar. Intellectual property, classified government documents, and private financial data are just some of the types of records that cyber criminals may pursue within other industries. For example, the University of Calgary paid a $20,000 ransom earlier this year after malware encrypted the university's email server.[17] In a separate incident involving law enforcement, a police detective's laptop in Melrose, Massachusetts was infected with an email virus that forced the department to pay a Bitcoin ransom to regain control of its network.[18] Some experts predict that ransomware will become more targeted and destructive, with ransoms that vary based on the value of the data being held hostage.[19]

Education and Government exhibited the highest rates of ransomware out of the six industries examined.

BitSight researchers found that organizations in Education had the highest rate of ransomware, with at least one in ten experiencing ransomware on their network (Figure 2). Researchers also found that 133 Healthcare organizations, over 115 companies in Finance, and 67 different Government organizations (e.g. law enforcement groups, federal agencies, etc.) had ransomware on their corporate networks over the past 12 months. These numbers show that ransomware is a growing problem across multiple industries.

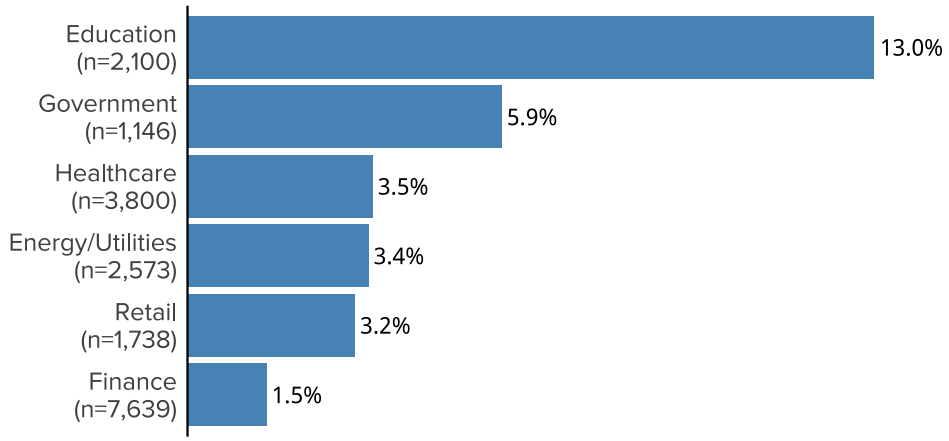

Figure 2. Percentage of companies in each industry with ransomware.

Types of Ransomware

The rate of ransomware has **tripled, or even increased tenfold**, for many industries over the last 12 months.

CryptoLocker was one of the most well-known forms of ransomware, stealing millions from businesses around the world until it was shut down in 2014.[20] More advanced forms of ransomware have taken its place, such as CryptoWall, DirCrypt, and more recently, Locky.[21] BitSight found that the overall rate of ransomware has more than tripled, and in some cases increased tenfold, for many industries over the last 12 months (Figure 3). Although the media typically considers ransomware primarily a Healthcare problem, it is evident that schools and universities, retailers, government agencies, and energy/utilities companies should also be on the lookout. According to the FBI, a number of ransomware variants have spread across different regions and industries, causing more than $200 million in damages within the first three months of the year.[22]

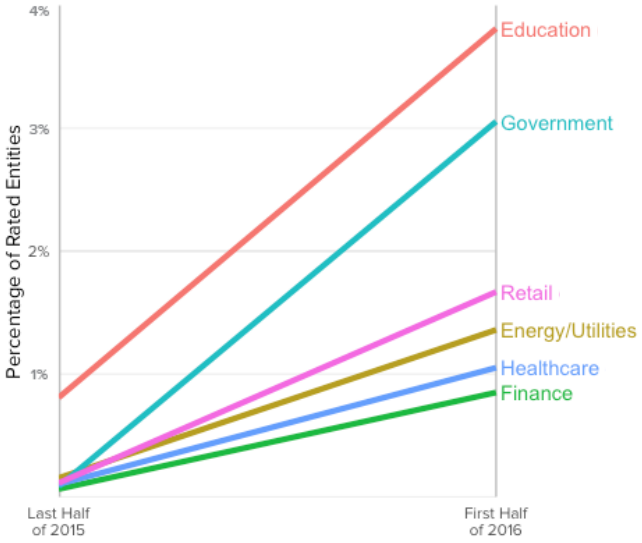

Figure 3. Percentage of ransomware observed over the past year, excluding Nymaim and Matsnu strains.

BitSight analyzed the prevalence of different strains of ransomware across industries (Figure 4). The findings show that more than 11 percent of the Education industry had the Nymaim Trojan on its networks, and almost four percent had Locky, a strain of ransomware discovered earlier this year. BitSight also found that roughly four percent of Government agencies were exposed to Nymaim, and more than three percent had Locky. This new strain also appears to be impacting the Retail industry, which exhibited the third-highest rate of Locky compared to the other industries examined in this report. It's important to note that Locky was discovered less than 8 months ago, and it is already the second-most common type of ransomware found across the six industries examined.

Another important fact to note is that Nymaim, although typically associated with ransomware, is actually a Trojan that can be used to install a variety of malware.[23] Similarly, Matsnu is another type of Trojan malware that can remotely download and execute files. One unique capability of Matsnu, however, is its ability to lock or unlock computers for ransom.[24]

Figure 4. Percentage of different ransomware strains across industries.

RECOMMENDATIONS

Despite the complexity of today's cyber threats, organizations can take steps to elevate their approach to cybersecurity and protect themselves against ransomware and other malware. Below are successful approaches to some of the most common data security challenges.

Establish Email Security Protocols

Ransomware has become a popular weapon for cyber criminals, and these attacks typically begin with one seemingly benign email attachment opened by an employee. According to Verizon, only three percent of individuals targeted with phishing emails actually alert management.[25] Organizations must train their employees on ways to stay safe on a corporate network and encourage them to report suspicious activity. To reduce spoofing and authenticate the origin of their email communications, IT security teams should also implement email security protocols such as DKIM, SPF, and DMARC.

Monitor Key Third Parties

While organizations may have excellent security controls in place, they may not know the controls of their third parties. Questionnaires only provide a moment-in-time assessment of vendor security and include information that can often be difficult to verify. Penetration tests are also point-in-time, and can be expensive and time-consuming. What happens if your organization shares critical data with third parties who are attacked with ransomware and the data becomes inaccessible? Companies that are victims of ransomware may also be exposed to other vulnerabilities. Vendor Risk Management teams should identify their key third parties and then continuously monitor them for ransomware infections.

Track Security Ratings

After performing significant system updates, IT security teams should continuously monitor their security ratings and ensure that systems are not vulnerable to exploits on systems containing sensitive information. They should monitor their networks and identify potential signs of ransomware infections and machine or asset compromises (also referred to as "botnets"). Security ratings help illustrate an organization's cybersecurity performance. A joint study between BitSight and Advisen revealed that companies with a rating of 400 or lower are over five times more likely to experience a publicly disclosed breach than companies with a 700 or higher.[26]

Avoid Peer-to-Peer File Sharing on Networks

According to Symantec, ransomware such as Ransomlock Trojan is prevalent on peer-to-peer file sharing websites and is often packaged with pirated or illegally acquired software.[27] To help prevent ransomware attacks, IT teams should monitor their network for peer-to-peer file sharing activity and ensure that employees do not illegally download software. For more insight into file sharing, refer to BitSight's report from earlier in the year, *Peer-to-Peer Peril: How Peer-to-Peer File Sharing Impacts Vendor Risk and Security Benchmarking*.

CONCLUSIONS

"Paying a ransom not only emboldens current cyber criminals to target more organizations, it also offers an incentive for other criminals to get involved in this type of illegal activity."

James Trainor
Assistant Director, FBI Cyber Division

BitSight researchers have found that over the past year, several industries have been victims of ransomware attacks. Education is the most impacted group, with findings showing that more than 10 percent of these companies have some form of ransomware on their networks. Over 67 Government organizations and 133 different Healthcare companies have been impacted by ransomware over the last 12 months.

The overall rate of ransomware has more than tripled, and in some cases increased tenfold, for many industries over the last 12 months. BitSight found that Nymaim and Locky were the two most common strains of ransomware across all industries observed. Our data support the FBI's findings that a number of ransomware variants have spread across different regions and industries this year. The regulatory landscape is trying to keep up with the threats, marked by the HHS Office for Civil Rights releasing new HIPAA guidance on ransomware earlier this year.[28]

In the meantime, paying or not paying ransoms has become a controversial topic. Organizations need to understand the risks associated with ransomware and weigh their options accordingly to determine which approach is the best one to take. However, experts suggest that paying the ransom in these attacks does not help. According to James Trainor, FBI Cyber Division Assistant Director, "paying a ransom not only emboldens current cyber criminals to target more organizations, it also offers an incentive for other criminals to get involved in this type of illegal activity."[29] While the FBI does not support paying a ransom, it does recognize that executives, when faced with inoperability issues, will evaluate all options to protect their shareholders, employees, and customers. A recent public service announcement by the FBI advises businesses to report ransomware infections to federal law enforcement.[30] Time will tell whether businesses heed this advice and report ransomware infections.

METHODOLOGY

With BitSight's patented network mapping process, researchers were able to include 18,996 organizations across six industries in this report.

BitSight collects and processes vast amounts of data in order to provide the industry standard in Security Ratings. The foundation of this research is built on our ability to accurately identify security events and attribute them to companies, which in turn, enables aggregation across industries. We determine this attribution by identifying the CIDR (Classless Inter-Domain Routing) blocks, domains, and AS (Autonomous System) numbers that organizations own, and then observing the outbound connections from ransomware originating from those organizations' assets. Customer research shows that our team constructs maps with greater than 95% accuracy, even for companies with hundreds of thousands of IP addresses.

Using a patented network mapping process,[31] BitSight has mapped more than 54,000 companies. For this study, we focused on six industries, analyzing 18,996 organizations across Finance, Healthcare, Education, Energy/Utilities, Retail, and Government. We measured ransomware infections using data collected and aggregated from several sources. We monitored ransomware infections emanating from these industries using data collected over the last 12 months from organizations that BitSight has mapped and curated. It is important to note that although we can confirm the existence of ransomware infections, we cannot confirm if files within an organization were encrypted or whether or not a ransom was paid.

ABOUT BITSIGHT

BitSight Technologies is transforming how companies manage information security risk with objective, verifiable and actionable Security Ratings. Founded in 2011, the company built its Security Rating Platform to continuously analyze vast amounts of external data on security issues and behaviors in order to help organizations manage third party risk, underwrite cyber insurance policies, benchmark performance, conduct M&A due diligence and assess aggregate risk. Seven of the top 10 cyber insurers, 56 Fortune 500 companies, and 3 of the top 5 investment banks rely on BitSight to manage cyber risks. For more information, please visit www.bitsighttech.com, read our blog, or follow @BitSight on Twitter.

REFERENCES

1. "AIDS Trojan or PC Cyborg Ransomware," Ransomware Knowledgebase, KnowBe4. Retrieved on September 13, 2016 from https://www.knowbe4.com/aids-trojan
2. "Hackers can make $90,000 per year with ransomware," Paul Szoldra, Tech Insider, June 2, 2016. Retrieved on September 10, 2016 from http://www.techinsider.io/flashpoint-report-ransomware-2016-6
3. "Meet 'Tox': Ransomware for the Rest of Us." McAfee Labs, May 23, 2015. Retrieved on August 9, 2016 from https://blogs.mcafee.com/mcafee-labs/meet-tox-ransomware-for-the-rest-of-us/
4. "How to Protect Your Networks from Ransomware" U.S. Justice Department. Retrieved on August 14, 2016 from https://www.justice.gov/criminal-ccips/file/872771/download
5. "NIST Cybersecurity Framework Adoption on the Rise" Nicole Cieslak, Tenable Network Security, March 29, 2016. Retrieved on September 1, 2016 from https://www.tenable.com/blog/nist-cybersecurity-framework-adoption-on-the-rise
6. "The Board Should Strengthen Controls to Safeguard Embargoed Sensitive Economic Information Provided to News Organizations" Office of Inspector General, April 15, 2016. Retrieved on September 10, 2016 from http://oig.federalreserve.gov/reports/board-controls-sensitive-economic-information-apr2016.htm
7. *Peer-to-Peer Peril: How Peer-to-Peer File Sharing Impacts Vendor Risk and Security Benchmarking*, BitSight Technologies, October, 2016.
8. "Universities Increasingly Falling Victim to Cyberattacks" Amir Nasr, Morning Consult, July 11, 2015. Retrieved on September 10, 2016 from https://morningconsult.com/2015/07/11/universities-increasingly-falling-victim-to-cyberattacks/
9. "Two more healthcare networks caught up in outbreak of hospital ransomware," Sean Gallagher, Ars Technica, March 29, 2016. Retrieved on September 10, 2016 from http://arstechnica.com/security/2016/03/two-more-healthcare-networks-caught-up-in-outbreak-of-hospital-ransomware/
10. "Iranian Cyber Attack on New York Dam Shows Future of War," Mark Thompson, Time, March 24, 2016. Retrieved on July 18, 2016 from http://time.com/4270728/iran-cyber-attack-dam-fi/
11. "15m T-Mobile consumers Hacked: SSN and More Taken," Chris Davies, SlashGear, October 1, 2015. Retrieved on July 19th, 2016 from http://www.slashgear.com/15m-t-mobile-customers-hacked-ssn-and-more-taken-01407526/
12. "Cyber hack got access to over 700,000 IRS accounts," Kevin McCoy, USA Today, February 26, 2016. Retrieved on July 19, 2016 from http://www.usatoday.com/story/money/2016/02/26/cyber-hack-gained-access-more-than-700000-irs-accounts/80992822/
13. "Trojan.Gpcoder", Jeong Mun, Symantec, May 22, 2005. Retrieved on September 10, 2016 from https://www.symantec.com/security_response/writeup.jsp?docid=2005-052215-5723-99
14. "Hollywood hospital pays $17,000 in bitcoin to hackers; FBI investigating." Richard Winton, Los Angeles Times, February 18, 2016. Retrieved on September 10, 2016 from http://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html
15. "Hackers offering bulk discount to unlock encrypted MedStar data," Ian Duncan, Andrea K. McDaniels, and Colin Campbell, *The Baltimore Sun*, March 30, 2016. Retrieved on Septemnber 13, 2016 from http://www.baltimoresun.com/health/bs-md-medstar-ransom-hack-20160330-story.html
16. "Hospital Declares 'Internal State of Emergency' After Ransomware Infection," KrebsonSecurity, March 22, 2016. Retrieved on September 13, 2016 from http://krebsonsecurity.com/2016/03/hospital-declares-internet-state-of-emergency-after-ransomware-infection/
17. "University of Calgary paid $20K in ransomware attack," CBC News, June 7, 2016. Retrieved on September 10, 2016 from http://www.cbc.ca/news/canada/calgary/university-calgary-ransomware-cyberattack-1.3620979
18. "UPDATE: Melrose Police pay hackers in Bitcoin to recover encryption key," Aaron Leibowitz, Wicked Local, February 29, 2016. Retrieved on September 13, 2016 from http://melrose.wickedlocal.com/news/20160229/update-melrose-police-pay-hackers-in-bitcoin-to-recover-encryption-key
19. "Ransomware Getting More Targeted, Expensive," KrebsOnSecurity, September 15, 2016. Retrieved on September 16, 2016 from http://krebsonsecurity.com/2016/09/ransomware-getting-more-targeted-expensive/
20. "U.S. Leads Multi-National Action Against GameOver Zeus Botnet and Cryptolocker Ransomware, Charges Botnet Administrator," U.S. Department of Justice, June 2, 2014. Retrieved on September 10, 2016 from https://www.fbi.gov/news/pressrel/press-releases/u.s.-leads-multi-national-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware-charges-botnet-administrator
21. "Ransom.Locky", Jeet Morparia, Symantec, February 16, 2016. Retrieved on September 13, 2016 from https://www.symantec.com/security_response/writeup.jsp?docid=2016-021706-1402-99

22. "Cyber-extortion losses skyrocket, says FBI," David Fitzpatrick and Drew Griffin, CNN, April 15, 2016. Retrieved on September 10, 2016 from http://money.cnn.com/2016/04/15/technology/ransomware-cyber-security/

23. "Nymaim Moves Past Its Ransomware Roots - What Is Old Is New Again," Proofpoint, Inc., February 26, 2016. Retrieved on September 13, 2016 from https://www.proofpoint.com/us/what-old-new-again-nymaim-moves-past-its-ransomware-roots-0

24. "Matsnu", TrendMicro, July 24, 2014. Retrieved on September 13, 2016 from http://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/matsnu

25. 2016 Verizon Data Breach Investigations Report, Verizon

26. "From the Server Room to the Board: Actionable Security Metrics," Ben Fagan, BitSight Technologies, November 4, 2015. Retrieved on September 13, 2016 from https://www.bitsighttech.com/blog/from-the-server-room-to-board-room-actionable-security-metrics?utm_content=23800774&utm_medium=social&utm_source=facebook

27. "Trojan.Ransomlock", John-Paul Power, Symantec, April 15, 2009. Retrieved on September 13, 2016 from https://www.symantec.com/security_response/writeup.jsp?docid=2009-041513-1400-99

28. "Your Money or Your PHI: New Guidance on Ransomware," Jocelyn Samuels, HHS Office for Civil Rights, July 11, 2016. Retrieved on September 10, 2016 from https://www.hhs.gov/blog/2016/07/11/your-money-or-your-phi.html

29. "Incidents of Ransomware on the Rise," US Federal Bureau of Investigations (FBI), April 29, 2016. Retrieved on September 10, 2016 from https://www.fbi.gov/news/stories/incidents-of-ransomware-on-the-rise

30. "I-091516-PSA: Ransomware Victims Urged to Report Infections to Federal Law Enforcement," US Federal Bureau of Investigations (FBI), September 15, 2016. Retrieved on September 16, 2016 from https://www.ic3.gov/media/2016/160915.aspx

31. "Security risk management," US Patent & Trademark Office, Patent Full Text and Image Database, September 6, 2016. Retrieved on September 13, 2016 from http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&p=1&u=%2Fnetahtml%2FPTO%2Fsearch-bool.html&r=1&f=G&l=50&co1=AND&d=PTXT&s1=9438615&OS=9438615&RS=9438615