Common Lessons from

Disparate Information Security Incidents

A White Paper Analysis

October, 2019

Kapil Padwal, Amy Thomas, Travis Howard, Michael Carr

Certified Information System Security Professionals

(ISC)^2 National Capital Region Chapter

Table of Contents

About the Authors

Travis Howard, CISSP, and (ISC)^2 National Capital Region chapter member is an active duty U.S. Naval officer specializing in information warfare, currently assigned to the Pentagon in Washington, D.C. He holds advanced degrees in cybersecurity policy and business administration from the University of Maryland University College, and is a frequent author in professional journals. His work in this white paper consists of his own opinions and individual expertise and are not representative of the U.S. Government.

Amy N. Thomas, CISSP, and (ISC)^2 National Capital Region chapter member, has experience in research, teaching, project management, emergency preparedness, information technology, and information security. Also a CEH(Master) and CompTIA Security+ce, she earned her Master of Science in Cybersecurity from Marymount University in 2018.

Michael Carr, CISSP, CSCS, (ISC)^2 National Capital Region chapter member and ISSA member, has worked in various IT positions for the past 20 years. He has recently held positions in security specializing in auditing, vulnerability management, security education training/awareness, encryption and phishing investigations.

Kapil Padwal, CISSP, ITIL Expert, PMP, CEH is the Director of Programs and serves on the Board of Directors of (ISC)^2's National Capital Region chapter. He holds graduate and undergraduate degrees in Computer Science and has 20 years of IT and Cybersecurity experience across the entire SDLC. His expertise is in Program Management, data governance, digital transformation, mentoring/coaching, security education/training, and continuous learning and development.

Disclaimer: *The opinions presented in this paper are not necessarily those of (ISC)^2 or the (ISC)^2 National Capital Region Chapter.*

Common Lessons from Disparate Information Security Incidents: A White Paper Analysis

Introduction

In 2019, an estimated 56% of the world's population uses the Internet - approximately 7.676 billion users (Kemp, 2019). The data flowing across disparate networks increases as the Internet continues to expand. Cisco (2019) forecasts 4.8 zettabytes (ZB) per year by 2022, which is up from just 1.5 ZB per year in 2017. Therefore, there are substantial risks associated with data theft and bad behavior when such enormous quantities of consumer data are available. Corporations are under increasing pressure to prevent this theft and protect their data - for their clients as well as their employees. Likewise, governments are feeling pressure to regulate and protect constituents from fraud and unauthorized disclosure of personal information.

This white paper examines two recent case studies of criminal attacks against critical financial infrastructure and local government information. Both attacks had direct costs for the victim organizations, and second-order effects were felt by the organizations' clients that suffered potential identity theft. This paper provides technical recommendations, including practices to mitigate future attacks, to organizational management and information security practitioners. These case studies are cautionary tales - of many in 2019 – that are informative lessons for examination by security professionals who want to improve their defenses, policies, practices and core capabilities.

First American Financial: Web Security Risk

Overview of the incident. A misconfigured web server allowed access to 885M title documents without authentication. Krebs (2019) noted that "information exposed by First American would be a virtual gold mine for phishers and scammers" (Krebs, 2019). In this case, technology was likely in place but people and processes were not to ensure confidentiality of client information. The company notified customers and issued a press release, and posted subsequent updates through web publications (First American Financial Corp, 2019).

Impacts of the incident. Several economic and social impacts can be observed from a leak of this type, including:

- Lawsuit: Gritz v. First American Financial Corp., 19-cv-01009, U.S. District Court, Central, District of California (Santa Ana) (Fisk, 2019).
- Retention of outside expertise to assess damage

- Loss of trust and confidence from clients over time (difficult to measure in real time)
- Impact to exposed client data may not be known for months or years, impossible to determine if and when leaked data may surface

Threat assessment. The primary threat of exposed information is criminal in nature; Business Email Compromise (BEC) scammers and individuals or groups using dark web marketplaces can resell leaked personally-identifiable information, which then can be used to conduct fraud or widespread identify theft. Criminals running a BEC scam can use leaked information to conduct a social engineering campaign against clients by impersonating company officers or attorneys citing privileged information only they would have access to (TrendMicro, n.d.). Krebs (2019) notes that "BEC scams are the most costly form of cybercrime today" according to FBI reporting.

Baltimore, Maryland: A City's Information Held Ransom

Overview of the incident: In May 2019, the U.S. City of Baltimore, Maryland, was attacked with the *RobbinHood* malware, a frequently used ransomware variant that encrypts files of affected systems and offers to restore the files if a ransom is paid (Chokshi, 2019). Baltimore refused to pay the ransom, which asked for 13 Bitcoins (roughly $102,000 USD) to decrypt all infected systems, and took several weeks to recover from the immediate effects by installing offline workarounds, restoring systems from backups, and completely rebuilding others. By mid-June, almost a month after the initial attack took place, over 95% of Baltimore's affected systems were restored, however the second- and third-order effects may be felt for weeks, such as scheduled billing for thousands of Baltimore residents (Chokshi, 2019).

Impacts of the incident. The city government suffered several immediate impacts of the ransomware incident, some of which continue to be felt to this day, including:

- Estimated $18.2M USD in damages - lost or delayed revenue and direct costs to restore systems (Davis, 2019).
- Loss of critical residential support processes: water billing, parking tickets, permits, real estate sales
- Erosion of citizenry's trust in local and federal government

Threat assessment: Ransomware threat actors can exploit external-facing vulnerabilities to gain privileged access to internal systems (many times a benign web server), then move laterally to other critical systems by exploiting trust relationships within the network. Additionally and more generally, malware infestations are commonly enabled by poor user behavior and non-compliance with security standards, often by falling for spear-phishing campaigns in which the user unknowingly downloads a malicious file that exploits their trusted user credentials. Since 2015, Crypto-Ransomware attacks became widespread and the dominant form of ransomware, with ransomware-as-a-service a popular platform for criminals without deep technical knowledge to launch attacks (Wright, 2016).

Prevention, detection, and response to these data attacks require a holistic approach. This paper describes management, technology, and human factors recommended for a comprehensive plan. The next section examines management role.

Management Impact

Studies have shown that management practices impact personnel actions. For example, a survey of businesses across seven countries concluded that employee compliance was enabled if management wrote, modeled, and followed a code of ethics (Withange, 2010).

Conversely, periods of information technology turmoil led to leadership turnover at the C-suite level. For example, a recent research study of companies bound by Sarbanes-Oxley rules found that IT deficiencies led to CEO and CFO turnover at a higher rate than non-IT deficiencies (Masli, Richardson, Watson, & Zmud, 2016).

Management commitment on paper and in practice should not be underestimated as a means to mitigate data breaches. Management oversight should take place in technology implementation, security planning, and employee training.

Leveraging Technology to Secure Security Posture

According to a federal inter-agency report, ransomware attacks have increased 300 percent in four years (U.S. Dept. of Justice, 2016). The National Cybersecurity Center of Excellence said recovering from ransomware and data loss required a focus on data integrity in order to restore a system to the last known good state (NCCoE & NIST, 2019). Both studies recommended preventive measures as the best defense. For this paper, researchers sought easy-to-implement, cost-efficient technical solutions for data loss prevention and data recovery.

Baseline Creation

Information technology security involves the use of checklists. These include enterprise hardware, cords and power supplies required by hardware, tokens and access cards, software packages and their keys. In the same way, it is important to establish a system baseline: a picture of the system at a point in time. The first snapshot can be compared to a second snapshot after adding software, installing patches, or running a program to see what changed. This can aid in identifying unwanted software on the system (including malware), and finding indicators of advanced persistent threats.

Free, open source tools: regshot compares the registry immediately before and after making a change (maddes, regshot, & xhmikosr, 2008). RegistryChangesView allows comparison from two different points in time or comparison with the registry shadow copy created by Windows (NirSoft, n.d.).

System Testing

A testing environment is one that mimics the main production environment. In addition to any mandatory annual tests required under policy, a copy of the system should be tested before new software, patches, or updates are applied to the production environment. Testing should take place in a simulated, non-production environment.

Free open source tools: For vulnerability scanning and penetration testing, the Open Vulnerability Assessment Scanner (OpenVAS) (Greenbone Networks GmbH, n.d.) and the open source Kali Linux Tool suite (Kali Tools, n.d.) are recommended. Both run in Linux and can scan Linux, Unix, and Windows systems.

Additionally, OWASP maintains a list of vulnerability scanning tools, the platforms on which they run, and whether they are commercial or open source (OWASP, 2019).

Website Testing

Testing of publicly accessible websites is necessary to identify leakage of private or sensitive business data. First Financial attributed data exposure to a design flaw that publicly exposed records dating back to 2003. Web application penetration testing might have revealed the design flaw, described as Insecure Direct Object Reference (IDOR) (Dellinger, 2019).

Free open source tools: There are a few Subdomain Enumerators (Trinka, 2018) to reveal website directories. Fierce (RSnake, 2007) and sublist3r (Aboul-Ela, n.d.) scan domains to show whether an internal IP address is visible outside the network.

Isolation

Private and sensitive business data should reside on a server separate from any website available to the public. Security information and event management (SIEM) tools and email attachment detection tools can detect unwanted data transmission into or out of the isolated space.

Free open source tools: Snort is a SIEM tool with new support for Microsoft Outlook email (Esler, 2019).

Most organizations will find a need to invest in a commercial SIEM tool to protect their crown jewels from data exfiltration.

Backups

This is the primary step for successful data recovery. Backups should take place on a schedule and be stored off-site with a working reader that can restore the backup. Test a full restoration from the backup at least once to confirm operability. Backup media and offsite storage incur a cost; however, the cost of data loss typically outweighs the cost of backups. The good news is many organizations include backups in their disaster recovery planning and do have backups available. The key is keeping those backups updated on a schedule and maintained in a format readable by the current system.

Free open source tools: UbuntuPIT reviewed 15 free open source backup software for Linux, some of which are compatible with Unix and Windows systems (Hasan, 2019).

Additionally, Microsoft has provided detailed backup and recovery guidance for their systems, including Active Directory (Microsoft, 2018).

Anti-Ransomware

In 2018, NCCoE, in collaboration with cybersecurity vendors, developed a solution framework to combat ransomware. The project described the need to *detect* malicious websites, malicious files that execute programs, and malware communication with an external server; to *respond* by blocking sites, blocking file execution, and notifying security; and to *recover* from backups (McBride, et al., 2018).

Free open source tools: Although free, open source anti-ransomware tools for business were not available at the time of this writing, an organization should use the NCCoE project goals as guidance for what to expect from a commercial anti-ransomware solution. An organization should also conduct third-party supply chain risk assessment prior to implementing an anti-ransomware solution.

Effective security cannot rely on tools alone. People and planning prove to be effective human measures for defense in depth, described next.

Human Factors in Information Security Incidents

First American Financial data leak was a poorly configured web server. Baltimore City in May 2019 faced a ransomware attack. Both could possibly have been prevented with better hygiene and training. Benjamin Franklin stated that “an ounce of prevention is worth a pound of cure” when he was addressing fire safety. This still holds true for IT security.

IT Security Plan

Every organization should create a system security plan to protect the IT environment. Gather information on your current security environment. Assess security in the past as well. Find out what worked well previously and what did not. Is security looking better today than before? Are your tools in good shape? Do you have enough resources? Is your employee security awareness training working well? Is your staff motivated? Gain an understanding of the risks, threats, and vulnerabilities in your environment. All of these factors are important as the first steps towards crafting an effective security plan.

Learn your environment. Using a good network monitoring tool can help find problem areas. Manage all your assets. Don’t allow for rogue devices. Periodically scan your network with Nmap for open ports, bad configurations, and unauthorized devices. Use a SIEM for data collection and analysis. Monitor your endpoint protection while looking for trends.

Document your security program. Keep a list of all of your assets. Is there a security analysis of the whole network? In the event of a major security event, do you have a plan in place? Does the security team understand their roles and expectations? Are your backups working? Have you been doing testing of all of your documented controls? IT environments are not static. Make sure that there is a good testing regimen in place so you are not caught off guard.

Create a security culture in the company. Implement mandatory security training for all staff each year. Send out periodic emails concerning worrisome trends in the workplace such as phishing emails. Post security posters throughout the office. Write security articles about issues that affect the employees on the intranet page. The goal is to continuously educate employees which should improve the security of the company.

Once you have all of the information about the network, people, risks, threats, vulnerabilities, assets, training, network monitoring, go back and reassess. Make sure nothing fell through the cracks. Security is not a set it and forget it model. It is ever-evolving.

Overview

A system security plan is as good as the people behind them. A plan could be well written but if the people are not following much of it then problems will likely occur.

If you have an IT security department, vulnerability scanning is normally a part of the many tasks that take place. Surprisingly, First American Financial may have neglected to run a scan on their website. If they had done so in the last 16 years, they would have found a common website design error called Insecure Direct Object Reference (IDOR). IDOR gives a person access to unauthorized data due to exposed reference and can lead to a loss of confidential data.

This vulnerability is an old problem. According to Colin Bastable, CEO of Lucy Security, “This is careless and incompetent complacency, and it goes back to 2003. You might have thought that there would have been a security audit in the last 16 years, or that someone would have noticed that data attracts data thieves: ‘Hey, is all this data really secure?’ Years ago, a teenager from England managed to roam around Defense Department servers, because they had no password protection. The problem is longstanding. Out of convenience or forgetfulness, and by people making assumptions, so much data is left unguarded” (Ikeda, 2019).

Security Training and Vulnerability Scanning

First American Financial should invest in their IT Security Department personnel. Not all web developers take security seriously and so investing in training is wise. Vulnerability scanning was not working very well if done at all.

A recommendation is to have all Web developers and administrators take web application security training along with new hires. After taking the course, supplemental training during the year is important. Cybrary has web application security training here based on the OWASP Top 10 https://www.cybrary.it/course/owasp/. There is other web application security training in Cybrary as well. Other vendors have training. Find the best for your needs. The best approach is to educate users and to standardize expectations.

OWASP has labeled IDOR as one of the top four vulnerabilities in web applications. Organizations should run vulnerability scans at least quarterly and or when major changes occur on websites. Use Burp Suite or BlackWidow. Both are effective at finding this vulnerability. Kali Linux is a great resource. There are many other open-source applications that are just effective. There is no need to necessarily pay a huge amount to have a great, successful vulnerability program.

With regards to the Baltimore City ransomware attack, most likely a user was successfully phished. Phishing attacks are a common way for an attacker to get into a network. The best defense is education.

Capitalizing on technology alone will not protect organizations. Human factors play a decisive role in the success of security programs. Virtually all cybersecurity incidents, 95% per a 2015 report by IBM are a result of inconsiderate work practices, ignorance, poor software patching, use of malicious software codes, unsecured network connections and poor protection of sensitive information (Nobles, 2018). Attackers go after people rather than technology. It is easier to exploit people.

Cybersecurity training and awareness are the best defenses against phishing as well as for other attacks. It is difficult to modify a user's behavior but creating a security culture through active learning is the way to go (Nobles, 2018).

Employees are often described as the weakest link in security. Arming employees with knowledge and foresight, it's possible to mitigate the risks.

Technology does have its place in organizations and can help people make the right decisions. An interesting browser plugin called Pixm analyzes in real-time, using what it calls "computer vision" websites to detect phishing attacks that impersonate a brand and its login page. It takes the guesswork that users make out of the equation and uses artificial intelligence. People can override the decision but this could really be a game-changer.

Another technology to help people improve their cybersecurity position is to implement SPF (Sender Policy Framework), DMARC and DKIM (DomainKeys Identified Mail). All three processes work together to reduce phishing.

SPF prevents email spoofing by verifying that an email message is sent from an authorized IP address. DKIM detects forged sender email addresses. DMARC ensures the integrity of email from a given domain. It requires SPF and DKIM and if either of those checks passes, then the DMARC test will pass.

If a person cannot determine if an email is phishing, then technology can step up to help. Organizations cannot depend solely on people or just on technology. A careful balance of both can make organizations stronger.

First American Financial and Baltimore City could reduce problems in their respective organizations by using annual security training, active education campaigns, appropriate technology use and vulnerability scans (at least for First American Financial). Failure to do so will help attackers win.

Best Practices & Recommendations for Protecting an Organization

The strategy for every organization should always be to improve its security posture by providing security measures at different levels, such that if one measure fails to thwart an attack, it has other measures to fall back on as additional layers of security to protect itself. This *Defense in Depth* approach, though commonly referenced in many places, is something organizations fail to implement. The following are some of the layered defenses that every organization must consider and implement to ensure resilience from different types of attacks.

Physical security. Depending on the organization and the underlying assets that it holds, physical security measures should be reviewed and implemented to adequately protect the people and the company's infrastructure. Physical data centers must be secured through perimeter security, installation of motion sensors, security cameras, and guards. Identification checks should be performed and turnstiles can be installed to prevent piggybacking.

Infrastructure security. All devices in the organization's Internet of Things (IoT) should be monitored and protected with multi-factor authentication (MFA) and Role Based Access Control (RBAC). With easy-to-crack passwords accounting for the #1 source of breaches, passwordless MFA is the way to go.You can sign-in with face recognition, fingerprint scans, with biometric sensors to verify users' identities on a specific device, authenticator apps can sign you in from a device without a password, or sign-in with a portable security key along with a fingerprint.

Underlying organizational processes. Business continuity plans should be reviewed, updated, and tested at least once a year to capture changes in business priorities and ensure compliance to Service Level Agreements (SLAs). Data governance should be in place to set priorities for managing data as a strategic asset, including establishing data policies, specifying roles and responsibilities for data privacy, security, and confidentiality protection, and monitoring compliance with standards and policies throughout the information lifecycle.

Educating workforce around cybersecurity. The most valuable and vulnerable resources an organization has is its people. Technology and processes are enablers however, if the people are not trained on the right way to use the existing platforms that help protect a business' infrastructure, the organization may not be able to realize the full power of the platform from an untrained workforce. Investing time and effort in training employees on a regular basis and raising employee awareness around cybersecurity and best practices to follow when browsing online are some things organizations must consider.

Organizations should follow Secure Software Development Lifecycle (SSDL) practices and project teams should be taught to incorporate security as core business requirements instead of adding them in the later stages of the development lifecycle as an afterthought.

Leaning on technology to improve security posture. Technology should always be looked upon as an enabler that assists in complementing the people and the underlying organizational processes.

Security Information and Event Monitoring (SIEM) software should be installed in order to identify correlated events, monitor abnormalities in incidents in real time, etc. Conducting regular periodic vulnerability assessments that highlight deficiencies are effective ways to determine areas of improvement for an organization. Efficient ways immediately to turn off accesses should be implemented when employees depart an organization so as to protect itself from disgruntled employees.

Automation and AI can significantly improve an organization's Meant-Time-to-Detect (MTTD) and Mean-Time-to-Respond (MTTR): the two critical metrics to track the maturity of a security team. AI and advanced analytics help the security team use dynamic risk analysis as well as predictive anomaly detection to support anti-malware prevention and detection.

Leaning on historical datasets as a form of automated Machine Learning can be leveraged to help train the underlying systems in understanding patterns that may make a system vulnerable to attacks. Those patterns can reveal ways to mitigate such weaknesses and assist teams to build a more robust system.

Conclusion

In this digital age where organizations and companies have a lot of Personally Identifiable Information (PII) stored in their databases with business being conducted over the Internet and where they have to exchange and share data with external organizations; protecting the company's data is of paramount importance. How an organization must protect its underlying assets and the level of security it implements depends on the type of data it holds and through a thorough analysis of the potential impacts of compromising that data. Importantly, this represents a shift in thinking for security professionals, from defending the *network* to defending the *data*, regardless of the network architecture at play.

Two very different incidents with different narratives and impacts, some not yet known publicly, yet there is a reasonably-deduced commonality: an incomplete or ineffective information security program that did not properly balance the three pillars of a successful strategy: people, processes, and technology. With First American Financial, the technology was likely there but the processes for detecting the misconfiguration was not. With Baltimore, improperly trained and aware people (users) likely led to the introduction of malware, and the technology architecture allowed it to move laterally through critical systems (a compounding problem).

Symantec (2019), in their annual Information Security Threat Report (ISTR) year-in-review for 2018, notes that one in ten URLs are malicious, and web attacks are up 56 percent (pp. 5-6); spear phishing continues to be the number one method for targeted attacks, with 65% of groups using spear phishing as the primary infection vector (p. 49). None of the three strategy pillars can be ignored, and perhaps now, more than ever, organizations should rethink how they train the entire workforce (not just the IT department) to understand the threat landscape and their duty to reduce the organization's risk.

Increased regulation and auditing requirements may be coming, at least in some sectors. The Department of Defense (DoD) is taking the initiative by developing a Cybersecurity Maturity Model Certification (CMMC) to make security requirements for the defense industrial base more rigid that would ultimately enable and empower agencies to protect their data by incorporating robust security measures and controls.

Ultimately, by incorporating continuous process improvement (CPI) in implementing robust security controls, building a competitive and skilled cyber defense workforce, and by leveraging a combination of technologies in continuous event monitoring, vulnerability management, artificial intelligence, predictive analytics, and machine learning, organizations can mature their existing security posture and help restore confidence in their consumers. Truly the attackers continue to enjoy an advantage, but as the information security profession continues to mature increasingly more powerful tools are becoming available for organizations to secure their data and protect their networks, if only they would invest in them.

References

Aboul-Ela, A. (n.d.). sublist3r package description. Retrieved from https://tools.kali.org/information-gathering/sublist3r

Chokshi, Niraj (May 22, 2019). “Hackers Are Holding Baltimore Hostage: How They Struck and What’s Next.” The New York Times. Retrieved from https://www.nytimes.com/2019/05/22/us/baltimore-ransomware.html

Cisco Systems (2019, Feb). *Cisco Visual Networking Index: Forecast and Trends, 2017-2022* [White Paper], Retrieved from https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.html#_Toc532256804

Davis, Phil (Jun 10, 2019). “Baltimore ransomware update:what city residents need to know about water bills, taxes,tickets and more.” Baltimore Sun. Retrieved from https://www.baltimoresun.com/maryland/baltimore-city/bs-md-baltimore-ransomware-update-20190610-story.html

Dellinger, A.J. (2019, May 26). Understanding the First American Financial Data Leak: How Did It Happen and What Does It Mean? Retrieved from https://www.forbes.com/sites/ajdellinger/2019/05/26/understanding-the-first-american-financial-data-leak-how-did-it-happen-and-what-does-it-mean/#171b5d1b567f

Esler, J. (2019, Aug. 2). Snort 2.9.14.1 has been released! Retrieved from https://blog.snort.org/2019/08/snort-29141-has-been-released.html

First American Financial Corp (May 28, 2019). “First American Financial Comments on its Ongoing Investigation Into Reported Information Security Incident.” Retrieved from https://www.firstam.com/incidentupdate/

Fisk, Margaret (May 28, 2019). “First American Financial Sued over Alleged Data Breach.” Bloomberg. Retrieved from https://www.bloomberg.com/news/articles/2019-05-28/first-american-financial-sued-over-alleged-client-data-breach

Greenbone Networks GmbH (n.d.). OpenVAS - Open Vulnerability Assessment Scanner. Retrieved from http://www.openvas.org/

Hasan, M. (2019). Top 15 open source backup software for Linux in 2019. Retrieved from https://www.ubuntupit.com/top-15-free-open-source-backup-software-for-linux/

Kali Tools (n.d.). Kali Linux penetration testing tools. Retrieved from https://tools.kali.org/

Krebs, Brian (May 19, 2019). “First American Financial Corp. Leaked Hundreds of Millions of Title Insurance Records.” KrebsonSecurity.com. Retrieved from https://krebsonsecurity.com/2019/05/first-american-financial-corp-leaked-hundreds-of-millions-of-title-insurance-records/

Kemp, Simon (2019, Jan 30). “Digital 2019: Global Internet Use Accelerates.” WeAreSocial.com, retrieved from https://wearesocial.com/blog/2019/01/digital-2019-global-internet-use-accelerates

McBride, T., Ekstrom, M., Lusty, L., Sexton, J., Townsend, A., & The MITRE Corp. (2018, Feb.). Data Integrity: Detecting and responding to ransomware and other destructive events project description. Retrieved from https://www.nccoe.nist.gov/library/data-integrity-detecting-and-responding-ransomware-and-other-destructive-events-project maddes, regshot, and xhmikosr (2008, Jan. 21). regshot. Retrieved from https://sourceforge.net/projects/regshot/

Masli, A., Richarson, V. J., Watson, M. W., and Zmud, R. W. (2016, Sept.). “Senior executives' IT management responsibilities: serious IT-related deficiencies and CEO/CFO turnover.” *MIS Quarterly*, 40(3): 687-708. Retrieved from https://doi.org/10.25300/MISQ/2016/40.3.08

Microsoft (2018, May 30). Backing up and restoring an Active Directory server. Retrieved from https://docs.microsoft.com/en-us/windows/win32/ad/backing-up-and-restoring-an-active-directory-server

National Cybersecurity Center of Excellence and U.S. Dept. of Commerce, National Institute of Standards and Technology (2018, April). Data integrity: Recovering from ransomware and other destructive events. Retrieved from https://www.nccoe.nist.gov/sites/default/files/library/fact-sheets/data-integrity-fact-sheet.pdf

NirSoft (n.d.). RegistryChangesView v1.21. Retrieved from https://www.nirsoft.net/utils/registry_changes_view.html

OWASP (2019, Aug. 5). Category: Vulnerability scanning tools. Retrieved from https://www.owasp.org/index.php/Category:Vulnerability_Scanning_Tools

RSnake (2007). Fierce package description. Retrieved from https://tools.kali.org/information-gathering/fierce

TrendMicro (n.d.). Business Email Compromise [definition]. Retrieved Aug 24, 2019, from https://www.trendmicro.com/vinfo/us/security/definition/business-email-compromise-(bec)

Trinka, J. (2018, April 15). Five Pentesting Tools and Techniques (That Every Sysadmin Should Know). Retrieved from https://medium.com/@jeremy.trinka/five-pentesting-tools-and-techniques-that-sysadmins-should-know-about-4ceca1488bff

U.S. Dept. of Justice (2016, June). How to protect your networks from ransomware: Interagency technical guidance document. Retrieved from https://www.justice.gov/criminal-ccips/file/872771/download

Withanage, A. J. (2010). "Motivated to be Unethical." *The International Journal of Interdisciplinary Social Sciences: Annual Review*, 5(3): 55-70. doi:10.18848/1833-1882/CGP/v05i03/51608

Wright, Bill (2016). *Symantec Government Affairs: Ransomware Threat Information Briefing*. Retrieved through NIST CSRC file repository, https://csrc.nist.gov/CSRC/media/Presentations/Ransomware-Threat-Information-Briefing/images-media/ispab-ransomware.pdf

Ikeda, S. (2019, June 11). Security Oversight at First American Causes Data Leak of 900 Million Records. Retrieved from https://www.cpomagazine.com/cyber-security/security-oversight-at-first-american-causes-data-leak-of-900-million-records/

Nobles, C. (2018, 12). Botching Human Factors in Cybersecurity in Business Organizations. *HOLISTICA – Journal of Business and Public Administration, 9*(3), 71-88. doi:10.2478/hjbpa-2018-0024

Symantec (Feb 2019). Information Security Threat Report, Vol. 24. Retrieved from https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf