The Kennesaw Journal of Undergraduate Research

Volume 6 | Issue 2 Article 4

Winter 2019

The Need for Disaster Recovery and Incident Response: Understanding Disaster Recovery for Natural Disasters Versus Cyber-Attacks

Kyle Sicard
Kennesaw State University, kylesicard.gs60@gmail.com

Recommended Citation

Sicard, Kyle (2019) "The Need for Disaster Recovery and Incident Response: Understanding Disaster Recovery for Natural Disasters Versus Cyber-Attacks," *The Kennesaw Journal of Undergraduate Research*: Vol. 6 : Iss. 2 , Article 4.
Available at: https://digitalcommons.kennesaw.edu/kjur/vol6/iss2/4

The Need for Disaster Recovery and Incident Response: Understanding Disaster Recovery for Natural Disasters Versus Cyber-Attacks

Kyle J. Sicard and Herb Mattord (Faculty Advisor)

Kennesaw State University

ABSTRACT

Disaster recovery and incident response has become a necessity in today’s technologically-driven business world. A significant amount of consumer information is put into businesses’ information systems with the expectation to protect their private and financial data. This discussion addresses the importance of why organizations need effective disaster recovery and contingency planning. A foundation of knowledge is built through the understanding of the statistical and practical implications of disaster recovery and contingency planning. The practical implications will be understood through two separate case studies. Each case study is unique in that one addresses disaster recovery when facing a natural disaster, while the other is a cyber-attack of man-made origin. This discussion will allow conclusions to be drawn on why there is a need to plan for natural disasters and cyber-attacks separately. This will be accomplished through analyzing the case studies and their statistical properties.

Keywords: disaster recovery, cyber-attacks, natural disaster recovery, incident response

Ever since the tragedy of September 11th, an important question has emerged for organizations within the business world. What do you do when your business suffers a blow that halts day-to-day operations? This very question shifted focus onto the practice of disaster recovery (DR) and contingency planning. In today’s technologically-driven world, how a DR plan and contingency plan (CP) is implemented is critical in the operations of medium-to-large sized organizations. The field of DR and CP is the solution for what actions to take if the unthinkable happens to an organization. Effective implementation of DR and CP will save an organization from the loss of customers, a damaged reputation, or bankruptcy.

To understand the criticality for implementation of DR and CP, a comparison of two separate categories of incidents will be explored to gain a foundation upon which to build. We will explore DR and CP for both natural disasters and cyber-attacks through key areas within these incidents. This comparison will be made on how DR and CP are created and implemented and the associated statistical insights for these incidents. Understanding these differences is crucial in perceiving how these two incidents can affect a business and what must happen for an organization to recover if either incident were to occur.

Once the foundation of understanding is established for the importance and need for DR and CP, we will examine practical real-world examples of two separate organizations who failed to recover effectively from an incident. This will be accomplished through a case study where we will identify the organization, incident type, what happened as the incident unfolded, and how they failed to respond to the incident. In conclusion, a solution will be drawn in how these organizations could have altered their DR and CP and prevent the failures of the organizations' ability to respond in an effective capacity.

The core function of a DR plan is to maintain functionality of business processes when and not if an incident of a disastrous proportion is to occur (Martin, 2002). For a DR plan to be effective, organizations must plan for disasters of all types. Disasters can take the shape of cyber-attacks, natural disasters, or technical/hardware disasters. Organizations need to plan for technical and hardware disasters; however, because these incidents are unique to the organization, they will be beyond the purview of this discussion. This examination will cover cyber-attacks and natural disasters in hopes of answering why it is a necessity to plan for such incidents separately.

Technology has become a vital function for organizations that exist today. When a disaster strikes, whether it be of man-made origin or from mother nature, technology disruptions can occur. When these disruptions happen, business operations can come to a halt and can cause heavy financial impact on the organization. Over 95% of large corporations report that one hour of a continuous technology disruption can result in costs that exceed $100,000 in a given year (Roguine, 2016). The financial numbers continue to grow at a staggering rate, with data center downtimes averaging a financial loss of $690,204 per incident. These unforeseen incidents occur at least once for more than 90% of data centers within a two-year period (Roguine, 2016).

These general disruptions become quite sinister when the rate of occurrence for these disruptions and the associated consequences become apparent. According to iCorps Technologies (2015), one in five businesses report a technology disruption every year. Additionally, 4 out of 5 of these businesses that experience these disruptions go out of business in less than a year and half. The statistics are profound in the amount of financial burden that is accrued from these disruptions, especially with 54% of companies experiencing an incident that was not resolved within an eight-hour period in the past five years. In an ideal environment, a business should be recovering from a disruption in the least amount of time as possible to avoid substantial damages; however, 98% of businesses are not capable of recovering from their last disruption within an hour (Guest Blogger, 2018). These are only the general figures associated with any type of disruption that results in downtime. To understand from where these figures originate, we must turn our attention to what role natural disasters and cyber-attacks play in these figures and disruptions.

To recognize how organizations create DR plans for natural disasters, we must clarify the definition of natural disasters and outline a few examples of these events. Natural disasters can be defined as "extreme, sudden events caused by environmental factors" that result in catastrophic damage or the loss of life in the affected area (Fact Monster, 2017, para. 1). There are several different types of natural disasters that are unique to a geographic area; these disasters can include hurricanes, earthquakes, wildfires, volcanos, tsunamis, and tornadoes.

There is some preliminary work in developing a DR plan for natural disasters that must be evaluated and reviewed. This preliminary work can be listed in six steps: “establish a planning team, set goals, analyze capabilities and hazards, develop action plans, create written documentation, and ensure everyone is familiar with the plan” (Post, 2018, What factors should be considered section, para. 2).

Once a DR planning team has been established, the organization can begin to set goals for what they want their DR plan to accomplish. The most common goal for a DR plan can be described as how an organization can restore operations to its information systems and application while maintaining the integrity and availability of data (Post, 2018).

Organizations can begin to draft their DR plan for natural disasters by planning for the worst-case scenario. A business owner who was affected by Hurricane Harvey in Houston, Texas stated, “many did not take the worst-case scenario seriously until it became reality” (Jefferson, 2017, para. 4). The identification of worst-case scenarios for businesses occurs by conducting an external analysis that predicts likely natural threats the organization may encounter (Jefferson, 2017). It is imperative that this external analysis is thorough in its processes to ensure an organization can identify worst-case scenarios that are likely for the geographic area. After potential risk of natural disasters are assessed, there must be a plan with sequential steps put into place to handle a scenario where the worst-case becomes reality.

Developing an action plan that responds to a natural disaster is the most crucial component in the DR plan for natural disasters. To do this effectively, certain questions need to be resolved. These questions often include: How can we ensure the safety of employees? Is my data effectively backed up to a safe location? How should communication be maintained with employees? Does the organization need to relocate its operations to a temporary location? Can my employees be equipped to work remotely? When these questions are addressed with robust answers, an organization can begin to detail the specifics of their action plan to ensure their organization’s ability to operate during a natural disaster.

Lastly, the organization needs to create written documentation, including backup protocols, plans, appointed responsibilities, and procedures. Once the plan is thoroughly documented from start to finish, the organization will need to facilitate training sessions to educate all personnel (Post, 2018). These plans must be integrated into ongoing company operations and employee training.

With a firm grasp on what is required for DR planning for natural disasters, we can now examine the differences between planning for natural disasters versus cyber-attacks. The idea is the same for both types of incidents; the goal for the DR plan is to resume normal business operations in the least amount of time to mitigate the damage and loss for when an incident occurs. Although the two have some overlap and the result is the same when not effectively responded to, a significant difference in planning for a cyber security breach versus a natural disaster is that recovery operations for security breaches are dynamic and planned from a high-level perspective. Cyber breaches can take shape in numerous ways requiring the organizations to adapt to the threat event (Todev, 2018). This difference requires organizations to be more vigilant and adaptable for cyber security breaches.

Another differentiating factor is that natural disasters only manifest as an external threat. Cyber breaches can occur both internally and externally; therefore, an organization must be prepared for either scenario. Threats from within the organization can cause an equal amount of damage as external breaches, making it imperative that organizations protect themselves from the very people they employ. Internal threats represent 80% of security incidents (Feldman, n.d.). The largest problem that cyber breaches present is that, unlike recovery from natural disasters where organizations can simply restore the systems, this approach will not be effective because the data is now corrupted. Organizations plan for data loss when mitigating infections corrupt data. The remediation of corrupted data requires data to be restored prior to the date of infection (Fearn, 2018). If an organization were to restore the infected systems from a corrupted back-up, the perfect bridge would be provided for the infectious malware to traverse into the restored or new system.

With some of the differences highlighted between the two types of incidents, we can explore DR planning for cyber-attacks. As the steps and processes are made evident, we can begin to correlate the similarities between DR planning for natural disasters and cyber-attacks. DR planning for cyber-attacks has a similar architecture as recovery plans from natural disasters. A planning team must be formed that is well-versed in cyber threats, with clear expectations set forth by the organization of what is expected of the team in the event of an incident.

The action plan begins with the implementation of layered security controls and continuous monitoring tools to trap infectious threats before the entire network becomes compromised (Todev, 2018). Following the hardening of organizational resources, there should be scanning and detection software that can alert the response team when an incident occurs. The length of time a breach goes undetected directly correlates with the financial losses an organization will sustain. Over 25% of security breaches are undetected for at least a 30-day period, and 10% of these threats remain undetected for a minimum of one year (Collins, 2017).

The goal of most organizations is to completely avoid a cyber breach, but this becomes a flawed approach when faced with a cyber-attack that cannot be stopped before it has run its course. The National Institute of Standards and Technology states, “over-reliance on prevention is just as bad as not being prepared.” Instead, organizations should be equipped for any cyber threat, corrective actions, and recovery operations (as cited in Todev, 2018, Cybersecurity Recovery Objectives section, para. 3).

After planning for the recovery phase, organizations need to begin an ongoing process of seeking constant improvement with the hardening of their systems, the ability to detect vulnerabilities and their resolution, and the speed with which they can respond to various types of incidents. Organizations cannot overlook their documented DR plans and must continually educate themselves on the current threat landscape and adjust their DR plans accordingly. (Todev, 2018).

The last part of the planning process for cyber-attacks is to continuously assess vulnerabilities within the perimeter and to harden the system against future occurrences. DR teams need to analyze and document useful and accurate data to define a base line (Todev, 2018). It is critical that organizations document standard operating procedures, designated roles, and changes within their planned processes to allow the organization the ability to improve upon their response and recovery times (Todev, 2018).

Thus far, we have established the core understanding on the need for DR and CP and analyzed the processes of DR for cyber breaches and natural disasters. Now we can turn our attention to the importance of proper implementation of DR. This will be realized through the examination of real-world case examples. The study of businesses who faced a disaster is a powerful tool that provides learning opportunities for security professionals to identify obscure vulnerabilities within their own organization. Within these case studies, the incident that occurred and its ramifications will be detailed. More importantly, how the company responded to the incident with their DR plan, or the lack thereof, will be reviewed and critiqued.

On August 29, 2005, Hurricane Katrina devastated Louisiana with damages exceeding $90 billion from the combination of Hurricane Katrina and the New Orleans flood (Bradley, 2015). This storm left Louisiana businesses in disrepair, effectively rendering their day-to-day operations inoperable. Two years after the incident occurred, over 7,900 businesses in Louisiana went out of business (Bradley, 2015). This scenario begs the question, how can a business recover in the wake of such a disaster?

Among the many businesses that were impacted by Hurricane Katrina, LifeShare Blood Centers can be identified as an organization that was irreparable when faced with a disaster of such magnitude. The nonprofit organization is based out of Shreveport, Louisiana and provides blood for 3.7 million residents. The organization has provided blood for hospitals and other facilities for over 70 years, and studies have shown that 33% of patients' lives depend on blood being readily available (Jones, 2016). The need for DR became abruptly apparent for Ric Jones, CIO of LifeShare Blood Centers: "When Hurricane Katrina's devastation struck New Orleans, several of our regional centers were closed, demand for blood product substantially increased and donors were not able to give blood due to our site closures, interrupting the flow of business" (Bradley, 2015, para. 7). In addition, the company lacked alternative data back-ups of their extensive blood database.

When companies fail to respond to or prepare for a natural disaster, there are often repercussions beyond the inability to generate revenue. In this instance, LifeShare Blood Centers found themselves unable to provide the vital service of providing blood for those in need.

This dire situation occurred due to the complete lack of a DR and CP on the organization's behalf. An effective and well thought out plan was not in place prior to this landmark storm and caught the company unprepared. This lack of planning could have led to the supply of blood running out and in effect cost lives. Ric Jones stated, "We did not have a disaster recovery plan in place when Katrina struck our office in Shreveport Louisiana and several other regional centers 10 years ago. The storm closed several locations, and as a result, kept blood donors from being able to give blood at a time of substantial demand increase. The levels of critical blood types dropped to dangerously low levels" (Jones, 2016, para. 10).

LifeShare Blood Centers managed to eventually recover from this disaster. However, it remains clear that their response to Hurricane Katrina should have been immensely dissimilar to what transpired after the storm struck. Numerous actions and controls should have ensued well in advance of the hurricane arriving ashore. What LifeShare Blood Centers lacked was a prepared response and plan that ensured the continuation of processes that would allow for the blood supply to be ready and available for those in need (Bradley, 2015). The lack of a detailed plan left LifeShare Blood Centers in a position to react rather than to respond to the incident. When an organization is reacting to an incident in an ill-prepared manner, they have already failed in their ability to respond to a disaster.

The organization would have experienced a different outcome if they were able to commence the necessary processes the moment the storm was projected to hit their base of operations. These processes would begin with threat identification and risk assessment of the associated risk. An effective risk assessment provides an organization with information on where to allocate their attention and resources to mitigate the greatest risk. LifeShare Blood Centers should have identified the threat, profiled the potential threat events, taken inventory of assets, and factored in the potential for loss of life and resources using the threat events perceived impact on operations as a baseline (FEMA, 2018). Armed with this information, they would have been capable of forming a business continuity plan (BCP) that allowed business operations to continue.

After conducting a risk assessment, the company should launch the newly formed CP. This CP would involve several moving parts. The organization needed to already have multiple data storage locations to preserve their blood supply database. This would effectively place redundancy on information that is pertinent to business operations. Most importantly, they would need to protect their physical blood supply and its availability. To ensure the availability of blood, the company would contract an independent blood supplier as a redundant failsafe (Bradley, 2015). The preservation of the blood supply within the affected area of the hurricane would need to be moved to off-site locations out of harm's way. With the blood supply now safe, coordinated efforts will need to follow to accomplish LifeShare Blood Center's priority of ensuring an accessible blood supply for those in need (Jones, 2016).

Thus far, the BCP allows for the company to continue to operate outside the impacted area. This was made possible by moving their supply of blood to alternate locations and hiring a third-party vendor to support them during a state of emergency. However, once the hurricane lands, the state of travel and infrastructure would be unknown, making it problematic to make the blood supply available to those in need who are in the affected area.

Cooperation at the local, state, and government levels will be necessary to continue to provide blood in the impacted regions. The combined efforts of these entities and government agencies will provide for the formation of a feasible plan that will get blood to those in need while keeping the company's employee's safe. Temporary storage for the blood would be strategically placed where it can be made available to those without infrastructure. State and government agencies will need to be contacted to find the best solution for transporting blood into the more devastated areas where the need for blood is vital. Equipped with the necessary DR and CP, LifeShare Blood Centers would have been able to maintain operations and the priority of safeguarding the availability and integrity of its blood supply (Jones, 2016).

Unfortunately, the BCP does not end at this point in the timeline. A worst-case disaster scenario of this magnitude would call for a long-term plan to return to normalcy. The extent of the damage inflicted by Katrina would call for the CP to be on-going for years to come. In this case example, the company would need to establish a new base of operations until the Louisiana infrastructure could be restored. Effective communication between management and the employees would have to occur to resume large scale operations. The organization's CP will detail methods of communication throughout the company during this time, as well as when and where non-essential disaster personnel can resume work. These details would have been documented and planned for prior to the incident occurring.

If the necessary steps were to have been taken, a predictively different outcome might have transpired. This organization's experience has still proven to be valuable. The CIO, Ric Jones, has come to a new understanding of the importance of DR and CP. It is no longer a component of their organization that is not considered. LifeShare Blood Centers now has extensive resources invested into DR and CP. Since Katrina, according to Ric Jones LifeShare has shifted to "a cloud-based data-recovery system that ensures data is backed up continually and protected and that the system is tested annually. Specifically, LifeShare is supported with secure cloud-based recovery by 12 servers and numerous critical applications that handle its vital blood data – donors, inventory, blood drives – as well as its financial and payroll systems" (Jones, 2016, para. 15). Jones enhanced these controls even further through mirroring the Shreveport data systems in a secondary data center that is located in another geographic area in the United States. This would ensure a natural disaster would not impact both data centers in a single event. IT personnel are now able to monitor data and statistics in real time across their 12 servers.

The tragedy and hardship Hurricane Katrina brought on to the citizens and businesses of Louisiana is indescribable. However, this storm taught businesses the value of DR and CP. Many believe the unthinkable will not occur, until it does, leaving the organization unprepared. LifeShare Blood Centers was able to recover in time, but often many do not recover when they fail to effectively respond to a natural disaster. The valuable lesson to take away from this case study is to develop and be capable of implementing a plan prior to a threat occurring (Bradley, 2015).

The examination of DR and CP and their role in responding to a natural disaster has been made apparent. We learned the importance in being prepared for such incidents. Now, we can begin to shift our focus to DR for cyber breaches. These two areas of incidence have overlap, but businesses must realize the differences in the incidents. The study of a real-world case example of how a business responded, or improperly responded, to a cyber breach will allow us to draw a conclusion on what these similarities and differences are.

On September 8th, 2014, Home Depot (HD) was forced to announce a data breach that is classified as the largest compromise of payment information in the United States (Seals, 2017). This data breach cost HD $27.25 million U.S. dollars in settlement fees. The breach that led to this massive payout was the theft of HD's customers' credit and debit card information. To understand why the attackers targeted HD's point-of-sale (POS) system, we first must understand how attackers use the stolen information.

The goal of hackers who target payment information is to profit at the expense of others. There are several ways that attackers use this stolen information to generate cash for themselves. The most common uses for a stolen card are large online purchases, cash withdraws, or illegal sales to other cyber criminals (Michael, 2017). Typically, the more sophisticated attackers will sell the card information over the dark web to other cybercriminals. Paul Michael explains how pricing for these stolen cards varies, "depending on how much information is provided. If it is simply the card number and expiration date, it will not bring much money. These cards are sold for a few bucks, because the chances of successfully making off with a chunk of money is slim. If the security number on the back is added, the price goes up. If the PIN is known, the asking price is higher" (2017, para. 8). If the seller provides more detailed information, such as purchasing behaviors and the answers to security questions, then the seller can fetch a premium price for the card.

With an understanding of why cybercriminals target payment card information, we can explore how the attackers were able to breach HD. Mitch MoosBrugger (personal communication, September 2018), the South East Regional Director of CyberArk, has stated that 85-95% of data breaches occur from the compromise of privileged credentials. Unfortunately for HD, this was how the attackers were able to gain access using a third-party vendor's login credentials. After securing the logon credentials to HD's vendor environment, the exploit of a Windows zero-day weakness provided access to the HD intranet through a hired third party's environment (Hawkins, 2015).

Once the cybercriminals penetrated HD's network, they had enough privileges to install memory scraping malware on over 7,500 self-checkout POS terminals (Smith, 2014). The installed malware stole 56 million credit and debit cards. In addition to the stolen card data, the hackers captured over 53 million e-mail addresses. The cybercriminals sold the card information on the dark web and used the stolen e-mail addresses to launch a massive phishing campaign, effectively capitalizing their efforts.

Home Depot could have avoided this breach in several ways. Preventing, detecting, and containing a cyber breach is a multi-layer process. This process is case-by-case due to the dynamic nature of cyber breaches. We will examine from the outside what HD missed in the hardening of their systems that is specific to this breach.

Starting at the point of breach, the hardening of HD's authentication factor would have prevented the attackers from gaining access through the third-party's credentials. The deployment of CyberArk's password vault software would have stopped the hackers from ever penetrating the system. Using CyberArk's product HD would have prevented the attackers from using valid authentication credentials, while ensuring that users are still capable of carrying out business operations (CyberArk, 2018). This authentication control works by updating and rotating secure credentials and Secure Shell keys at pre-determined points or as requested per organizational policies (CyberArk, 2018). If HD had this authentication factor implemented, the attackers would have been unsuccessful in their login attempts. The automatic rotation system for CyberArk's password vault would have recycled the authorized credentials as soon as the third-party vendor's login was used the first time. This would have resulted in the cybercriminals being denied access after attempting to re-use credentials.

Home Depot's software and hardware configuration presented numerous vulnerabilities. The hardening of these configurations would have prevented the breach or allowed the intrusion to be detected almost instantaneously, allowing for a swift response. A glaring vulnerability presented itself at arguably the most important piece of software: the operating system (OS). HD's POS devices were running Windows XP, a heavily outdated OS. Windows XP is known to be easily compromised, and it is shocking that HD was still allowing this OS to run on its POS machines (Hawkins, 2015). There are several newer OS's that should have been in use that are compatible with security features, such as, "P2P (point-to-point) encryption, antivirus, and many other applications that are vital to locking down your POS systems" (Hawkins, 2015, p. 8).

HD was using Symantec Endpoint Protection for anti-virus software but were lacking in some of their configuration settings. Brett Hawkins from the SANS Institute commented that HD did not utilize a vital feature known as Network Threat Protection (2015). This feature works as a host intrusion prevention system. Hawkins continues by claiming that, "Having configured POS devices with this feature activated at my own organization, I can attest to the success of this feature when doing vulnerability assessments on these systems" (Hawkins, 2015, p. 8).

With HD's systems running Windows XP and the lack of necessary hardware, they were not capable of supporting P2P encryption. This security feature would have allowed credit card information to be protected the moment it is collected and would encrypt the data as it is stored in memory (Hawkins, 2015). The attackers would have been able to still steal the payment data but would have been unsuccessful in reading the encrypted data once removed from HD's environment.

The security vulnerabilities do not stop at the software and hardware level. At the network level, HD did not have their networks segmented onto VLANs (Virtual Local Area Network). Network segmentation is defined as separating a larger network into smaller networks that isolates them. This practice allows a network to be more robust, since the isolation of the networks allows for a layered security approach that prevents breaches from rapidly spreading (Metivier, 2017). Network segmentation hardens the system by preventing intruders from navigating around within the system. In the case of HD, once the intruders penetrated the network and gained access to the vendor environment, they would have been unable to jump to the POS network if it were on a segregated network.

Vulnerabilities persisted at the organizational level; the lack of a vulnerability management system allowed the previously documented vulnerabilities to be exploited. Vulnerability management systems can be described as the process of "identifying, classifying, remediating and mitigating vulnerabilities. It is also described as the discovery, reporting, prioritization, and response to vulnerabilities in your network" (Hilaire, 2017, para. 3). The importance of this system is evident as it is required by respected risk management frameworks that are widely accepted and practiced. The SANS Institute posits on their most recent framework that vulnerability assessment must “continuously acquire, assess, and take action on new information in order to identify vulnerabilities, and to remediate and minimize the window of opportunity for attackers” (Hilaire, 2017, para. 4).

Lastly, HD took five months to detect that an intrusion had occurred. No matter how efficient an organization is at preventing intrusions, eventually a breach will occur. Therefore, detection is crucial in an organization’s security practices. HD lacked sufficient monitoring software, such as a security information and event management (SIEM) system that would detect and notify administrators of any activity within their POS system (Hawkins, 2018). Once deployed, SIEM software will scan the network and “gather security-related events from end-user devices, servers, network equipment, as well as specialized security equipment like firewalls, antivirus or intrusion prevention systems” (Rouse, 2018, para. 5). For five months, intruders were inside HD’s network collecting and stealing their customers’ data, resulting in large settlement fees of over $27 million U.S. dollars. If HD had a SIEM system, they would have been able to respond more quickly and mitigate any potential data theft that occurred.

The conclusion that can be drawn from this case study is that there is no specific way to respond to a cyber breach. It requires a dynamic effort that is accomplished through the hardening of the entire system at the external, internal, network, hardware, and software levels. By taking a layered security approach that is effective in its practice, an incident will be prevented or detected, contained, and remediated. Businesses have a choice to learn from other organizations’ mistakes. It becomes a matter of responsibility for businesses to learn from the mistakes of others and to implement what they learn into the hardening of their own systems. The knowledge and experiences are readily available for proactive businesses to apply within their own environments.

References

Bradley, T. (2015 August 28). The disaster recovery lessons we learned after Katrina. Retrieved from https://www.csoonline.com/article/2977193/disaster-recovery/the-disaster-recovery-lessons-we-learned-after-katrina.html

Collins, K. (2017 May 9). One in 10 data breaches discovered in 2016 had gone undetected for more than a year. Retrieved from https://qz.com/978601/one-in-10-data-breaches-discovered-in-2016-had-gone-undetected-for-more-than-a-year/

CyberArk. (2018). Key features. Retrieved from https://www.cyberark.com/products/privileged-account-security-solution/enterprise-password-vault/

Fact Monster. (2017). Natural disasters. Sandbox Networks, Inc. Retrieved from https://www.factmonster.com/world/natural-disasters

Fearn, N. (2018 July). Matching disaster recovery to cyber threats. Retrieved from https://www.computerweekly.com/feature/Matching-disaster-recovery-to-cyber-threats

How to Prepare for and Respond to a Cyber Attack: Have a Disaster Recovery Plan. (n.d.). Retrieved from https://www.olenderfeldman.com/how-to-prepare-for-and-respond-to-a-cyber-attack-have-a-disaster-recovery-plan/

FEMA. (2018 July 26). Hazard identification and risk assessment. Retrieved from https://www.fema.gov/hazard-identification-and-risk-assessment

Fox News. (2015 January 13). Fox facts: Hurricane Katrina damage. Retrieved from https://www.foxnews.com/story/fox-facts-hurricane-katrina-damage

Guest Blogger. (2018). 17 shocking statistics about disaster recovery and business resiliency. Retrieved from https://www.datacore.com/blog/17-shocking-statistics-about-disaster-recovery-and-business-resiliency-where-does-your-organization-stand-part-1/

Hawkins, B. (2015 January). Case study: The Home Depot breach. *SANS Institute*. Retrieved from https://www.sans.org/reading-room/whitepapers/breaches/case-study-home-depot-data-breach-36367

Hilaire, C. (2017 October 5). What is a vulnerability management program? Retrieved from https://www.coresecurity.com/blog/what-vulnerability-management-program

iCorps Technologies. (2015). Disaster recovery statistics & facts, business continuity stats. Retrieved from https://blog.icorps.com/it-disaster-recovery-facts

Jefferson, L. (2017 September 6). How businesses can prepare for natural disasters. Retrieved from https://strategiccfo.com/how-businesses-can-prepare-for-natural-disasters/

Jones, R. (2016 January 26). How resilient businesses weather hurricanes, other disasters. Retrieved from https://www.drj.com/articles/online-exclusive/how-resilient-businesses-weather-hurricanes-other-disasters.html

Martin, B. (2002). Disaster recovery plan strategies and processes. *SANS*

Institute InfoSec Reading Room. Retrieved from https://www.sans.org/reading-room/whitepapers/recovery/disaster-recovery-plan-strategies-processes-564

Metivier, B. (2017 June 6). The security benefits of network segmentation. Retrieved from https://www.sagedatasecurity.com/blog/the-security-benefits-of-network-segmentation

Michael, P. (2017 June 6). Top 5 ways thieves use your stolen credit card. Retrieved from https://www.wisebread.com/top-5-ways-thieves-use-your-stolen-credit-card

Post, J. (2018 July 31). 6 tips for creating your business's disaster plan. Retrieved from https://www.businessnewsdaily.com/7327-disaster-plan-tips.html

Roguine, S. (2016 August 16). Don't let your company become a statistic. *Disaster Recovery Journal.* Retrieved from https://www.drj.com/articles/online-exclusive/don-t-let-your-company-become-a-statistic.html

Rouse, M. (2018 January). Security information and event management (SIEM). Retrieved from https://searchsecurity.techtarget.com/definition/security-information-and-event-management-SIEM

Seals, T. (2017 March 13). Home Depot to pay $27.25m in latest data breach settlement. Retrieved from https://www.infosecurity-magazine.com/news/home-depot-to-pay-2725m/

Smith, M. (2014, November 10). Home Depot IT: Get hacked, blame Windows, switch execs to MacBooks. *Network World*. Retrieved from http://www.networkworld.com/article/2845620/microsoft-subnet/home-depot-it-gethacked-blame-windows-switch-execs-to-macbooks.html

Todev, N. (2018 January 16). Here's how to develop a cybersecurity recovery plan. Retrieved from https://www.convergetechmedia.com/heres-how-to-develop-a-cybersecurity-recovery-plan/