Journal of Cybersecurity and Privacy

MDPI

Review

Insights into Organizational Security Readiness: Lessons Learned from Cyber-Attack Case Studies

Faisal Quader * and Vandana P. Janeja *

Department of Information Systems, College of Engineering and Information Technology, University of Maryland, Baltimore, MD 21250, USA
* Correspondence: fquader1@umbc.edu (F.Q.); vjaneja@umbc.edu (V.P.J.)

Abstract: This paper focuses on understanding the characteristics of multiple types of cyber-attacks through a comprehensive evaluation of case studies of real-world cyber-attacks. For each type of attack, we identify and link the attack type to the characteristics of that attack and the factors leading up to the attack, as observed from the review of case studies for that type of attack. We explored both the quantitative and qualitative characteristics for the types of attacks, including the type of industry, the financial intensity of the attack, non-financial intensity impacts, the number of impacted customers, and the impact on users' trust and loyalty. In addition, we investigated the key factors leading up to an attack, including the human behavioral aspects; the organizational–cultural factors at play; the security policies adapted; the technology adoption and investment by the business; the training and awareness of all stakeholders, including users, customers and employees; and the investments in cybersecurity. In our study, we also analyzed how these factors are related to each other by evaluating the co-occurrence and linkage of factors to form graphs of connected frequent rules seen across the case studies. This study aims to help organizations take a proactive approach to the study of relevant cyber threats and aims to educate organizations to become more knowledgeable through lessons learned from other organizations experiencing cyber-attacks. Our findings indicate that the human behavioral aspects leading up to attacks are the weakest link in the successful prevention of cyber threats. We focus on human factors and discuss mitigation strategies.

Keywords: types of cyber-attacks; human factors in cyber threats; case studies; advanced persistent threat (APT); Association Rule Mining (ARM); organizational security readiness; lessons learned

Citation: Quader, F.; Janeja, V.P. Insights into Organizational Security Readiness: Lessons Learned from Cyber-Attack Case Studies. *J. Cybersecur. Priv.* **2021**, *1*, 638–659. https://doi.org/10.3390/jcp1040032

Academic Editor: Nour Moustafa

Received: 5 August 2021
Accepted: 25 October 2021
Published: 11 November 2021

1. Introduction

Cyber threats are increasing for all entities, including individuals, small businesses and large corporations, leading to a varying degree of loss. In some cases, even amateur-led cyber-attacks can lead to massive disruptions. Cyber threats will become worse and more intense due to the pervasive nature of connectivity and the constant movement of data, which is not always well protected. There are well-studied areas of physical threats, such as fire and flood hazards; however, we still lack a deeper understanding of cyber-attacks. In traditional threats, prior events are studied and analyzed, and the lessons learnt are utilized for the future handling of such events. In this paper, we take this approach to study a vast array of cyber-attacks, in order to understand and inform the decision making and mitigation strategies for different types of cyber-attacks. We classify real-world cyber-attack case studies based on different types of attacks, analyze the major factors contributing to these attacks, and discuss possible mitigation strategies. Our aim is to provide knowledge which can be used to potentially prevent organizations from being victims of cyber threats by studying existing cyber-attacks.

In most cyber-attacks, human behavioral aspects and the response to malicious stimuli are the weakest link in bringing about a successful cyber-attack. Behaviors such as distraction, ignorance, curiosity, failure to comply with security policy, and a lack of awareness of

cyber threats can cause major damage or potentially lead to an attack [1]. In our survey of real-world cyber-attack case studies, we identify and categorize the human aspects of the attacks, look at the financial and any other adverse impacts from these attacks, identify the challenges, and come up with potential mitigation strategies. The connection of these cyber threats to human aspects can help educate the stakeholders—including end users, decision makers and system administrators alike—to potentially be more aware of cyber-attacks.

While the existing surveys take more of a theoretical perspective of different cyber-attacks, none of the surveys have addressed the evaluation of such a vast array of real-world cyber-attacks. For instance, Abraham gives an overview of Social Engineering attacks [2], and Wheatley talks about Sony's data beach incident [3] in general. These surveys, however, do not provide an aggregated analysis of real-world cyber-attacks. In this paper, we attempt to explore multiple cyber-attacks and derive some common lessons learned by mining the factors we collected from these case studies to find commonalities across these cases.

The contributions in this study are as follows:

- the evaluation of multiple real-world cyber-attacks to understand the types of attack;
- the categorization of the human factors leading up to the cyber threats;
- The characterization of cyber-attacks;
- the mitigation strategies; and
- the lessons learned for providing actionable knowledge to create more awareness for all stakeholders.

We evaluate over 43 cyber-attack incidents and study the process, impact, and outcomes of the threats. Specifically, we study both qualitative and quantitative characteristics, including the type of industry, financial intensity of the attack, non-financial intensity impacts, number of impacted customers, and the impact on users' trust and loyalty. In addition, we explore the factors leading up to the attacks: the human behavioral aspects; organizational cultural factors at play; security policies adapted; technology adoption and investment of the business; training and awareness of all stakeholders, including users, customers and employees; and investments in cybersecurity. We also analyze how these factors are related to each other by evaluating the co-occurrence and linkage of factors to form graphs of connected frequent rules seen across the case studies.

The rest of the paper is organized as follows: In Section 2, we talk about the motivation, explaining why it is useful to perform this evaluation of case studies of cyber-attacks. In Sections 3 and 4, we discuss the methodology of our evaluation/survey, which includes the categorization of cyber threats, the observations related to these attacks, and the key factors causing these attacks. We then summarize the mitigation strategies to avoid these attacks in Section 5. In Sections 6 and 7, we conclude our paper with relevant future work mainly on the human aspects leading to cyber-attacks, and portray the related open challenges in cyber wars.

2. Motivation

Cyber threats are not only rapidly spreading across the world; serious threats which lead to massive financial loss with credibility impact have surprisingly become prevalent at many established companies, such as Home Depot [4,5], Sony [6–8], Central Bank [9], and the Heartland Payment System [10] to name a few. Organizations, both established and new, often struggle with how to tackle these threats. As such, the prominent question is "Why do we become victims to these imminent threats?" In order to answer the question adequately, we need to perform a thorough analysis of cyber-attacks and identify the lessons learned from these attacks so that we can be proactive towards future threats. We noticed a lack of systematic study on cyber threats, unlike traditional security hazards. Moreover, human behavioral aspects play a big role in cyber-attacks; such behavioral aspects may include negligence and ignorance of cyber-attacks, as well possible deceitful acts. Human behavior often influences the progression of cyber threats; however, it is generally difficult to pinpoint the specific cause. Some factors—such as caution, security education, increased awareness, and security competence—play a significant role in avoid-

ing cyber threats. In order to address these issues and quantify them through the lens of existing cyber-attack scenarios, we study how the human behavioral aspects impact the intensity of the cyber threats. We anticipate that this survey of cyber threats will be useful to organizations—small, medium, and large—to learn from the cyber-attacks and engage in appropriate cybersecurity initiatives.

Interestingly enough, cyber threats are no different from physical security threats, as shown in Table 1; however, there is a need to study them in a similar way to physical security threats [11]. As we see below, the characteristics of physical security [12] and cybersecurity are very similar, except that we pay a lot more attention to physical security than cybersecurity. Cybersecurity threats are not as visible as the physical security threats, and yet the impacts of cybersecurity threats can be quite substantial; hence, we need to pay attention to cyber threats.

Table 1. Physical intrusion vs. cyber intrusion.

Physical Intrusion (Security Violation)	Cyber Intrusion (Security Violation)
Reason—Greed, Activism, Political, Hurt	Reason—Greed, Activism, Political, Hurt
Outcome to victims—Destruction, Financial Loss	Outcome to victims—Destruction, Financial Loss
Outcome to attacker—Gain, fulfilling a political or personal agenda	Outcome to attacker—Gain, fulfilling a political or personal agenda
Physical	Virtual
Attacker—sense of power	Attacker—sense of power, accomplishing a political agenda
Likelihood of getting caught is higher	Likelihood of getting caught is lower
Mostly Visible	Not always visible—APT (takes long time)
Visible breakage	Likely Invisible breakage
Protection is by physical security (guard, lock)	Protection is by cyber security (Firewall, password protection)

Currently, there are minimal comprehensive studies of real-world cyber-attack events. Moreover, surveys of these cyber-attacks which can help us extract lessons learned for future decision-making and mitigation strategies are also lacking. We fill this gap in this paper, in which where we study over 43 real-world cyber-attacks, along with their financial impacts, and identify and correlate the leading causes of these attacks, as well as the lessons learnt, such that we are better prepared to protect and tackle similar types of situations [13]. For instance, after the horrible cyber-attack in Estonia, which is a NATO member, NATO extracted key lessons learned from that attack and developed the ability to prevent, detect, defend against, and recover from cyber threats [14]. In this paper, we extend this idea to look at multiple cyber-attack events together and identify key characteristics from the attacks and discuss mitigation strategies. We have many papers talking about specific cyber threats without looking at other types. For instance, we have papers on security compromise at a university network [15], on the investigation of identity theft and its processes [16], on a security breach at Kaiser Permanente [17], and about a case study on security incident management [18], to highlight a few. In our paper, we touched upon the accumulation of a similar set of cybersecurity threats in the industry at one place for the reader, and what the industry should focus on to mitigate these threats.

3. Case Study Methodology

The frequency of cyber-attacks is increasing, both for individuals and for large, well-established organizations. The attackers can vary from amateurs to nation-states utilizing more sophisticated technology to infiltrate large corporations. We also become victims of these threats because of human factors and behaviors such as negligence and ignorance.

We studied over 43 real-world cyber-attacks that have occurred in the past several years. We collected these case studies by curating several news articles, papers, and other discussions on these cyber-attacks. We categorized the attacks by types, classified them into related industries, analyzed the human factors that may have been at play, scrutinized the financial and non-financial intensity of the attack, identified the number of victims,

analyzed the corporate cultural factors and whether the victims were cyber-threat-aware, and finally evaluated the threats in terms of the amount of investment made for cyber security to judge any policy implications for the organizations where these attacks took place. A lot of this discovery was achieved by reading and analyzing the material we collected. This does bring in a level of subjectivity into the analysis. However, we also used presentations made by several students in a cybersecurity class to cross-check some of the findings that we discovered in our analysis.

Through this analysis of factors, we created a dataset in the form of a matrix of parameters across all of the attacks. We then identified frequent patterns in this matrix of data we collated [19]. We identified interesting patterns which indicate relationships or linkages between certain types of attacks and parameters. Additionally, we also looked at what factors predominantly co-occur across these case studies. Our survey analysis using frequent patterns provides novel insights across a vast variety of factors and types of attacks, and can be used for better decision making in future scenarios.

We next explain each component of our study methodology, including (a) types of attacks, (b) the categorization of the human aspects, (c) a cyber-attack case study by industry, (d) financial impacts, (e) non-financial impacts, (f) the number of customers impacted, (g) cultural factors, (h) end-user trust and loyalty, (i) policy issues, (j) training and awareness, (k) technology adoption for cyber threat prevention, (l) investment, and (m) the factors leading up to the cyber-attacks.

3.1. Understanding the Types of Attacks

We consider a detailed categorization of the cyber-attacks, as shown in Figure 1, which includes Social Engineering [20], Malware, Password attacks, DOS, APT, Database/Software-based/Browser-based attacks, Mobile Ad Hoc Networks-based attacks [21] and Cyber–physical Systems attacks. There are similar taxonomies of cyber threats [22]. However, based on our comprehensive survey of different real world cyber-attacks, we have classified the attacks below into the right buckets according to the characteristics and the nature of the attacks. For instance, Eavesdropping is a kind of Social Engineering attack [23], SQL Injection is an attack that can happen to the Database layer, Flood Rushing attacks may happen to the network in a mobile platform to name a few. Cyber-attacks tend to be very complex, and we can experience threats with a combination of multiple types such as APT, which is a complex threat, sometimes comprising multiple cyber-attacks with password attacks or social engineering with malware injections once the intruder gets into the system. Therefore, it is critical to classify these reoccurring threats and attacks with a good knowledgebase to tackle for the industry.

3.2. Cyber-Attack Case Studies by the Industry

In Figure 2, we provide a categorization of real-world case studies of cyber-attacks highlighting the organizations impacted by different cyber threats. We also highlight the financial consequences for these attacks. For instance, 'high tech' Ubiquity Networks suffered a loss of $39 million from Social Engineering attacks [24–26]. Epsilon also suffered a social engineering attack that cost them $4 billion. Sony's malware attack had an impact of close to $100 million, while the Heartland Payment System hack cost them a hefty $170 million. Even high-tech security companies like RSA became the victim of APT attacks. Moreover, nuclear power plants, power grids, energy, mobile platforms, chemical industries, education, advertisements, communication, retail, and the food and agriculture sectors became the victims of these cyber threats. Cyber threats impact the spectrum of all types of industries; therefore, we analyzed them closely, identified the factors causing these cyber-attacks and evaluated them by industry.

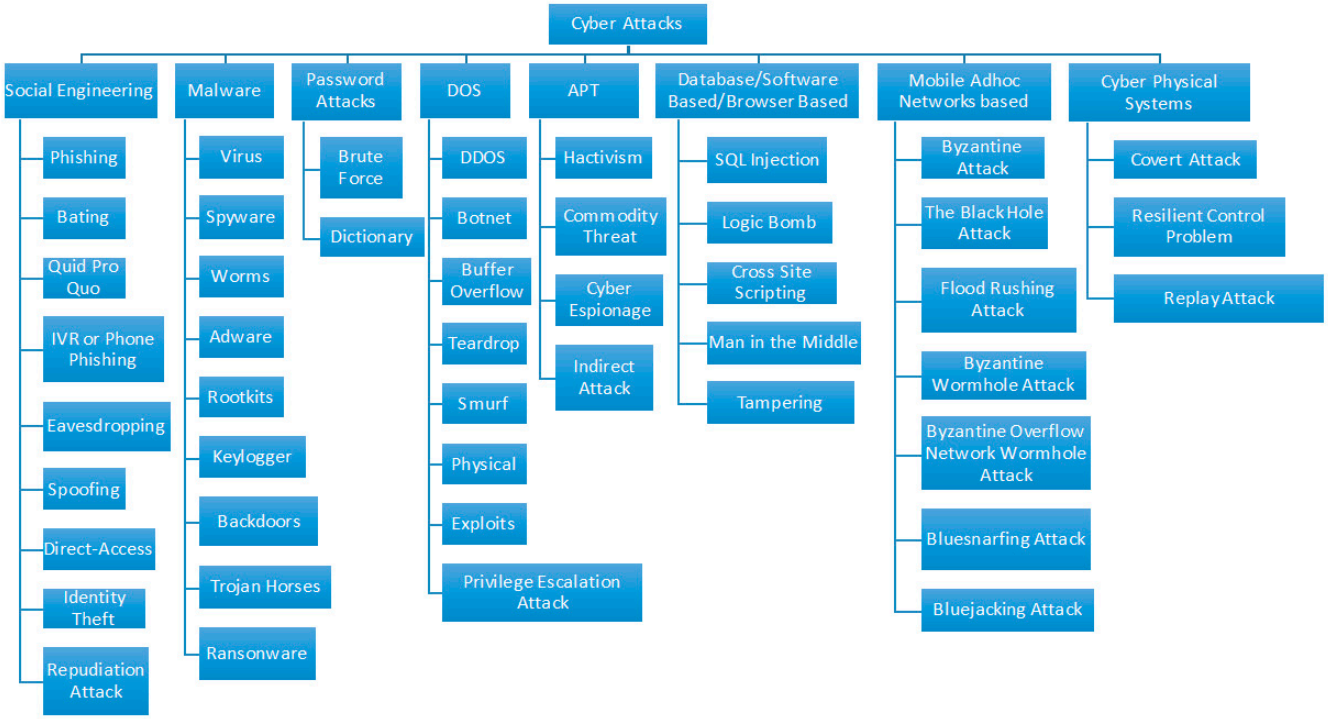


Figure 1. Types of cyber-attacks.

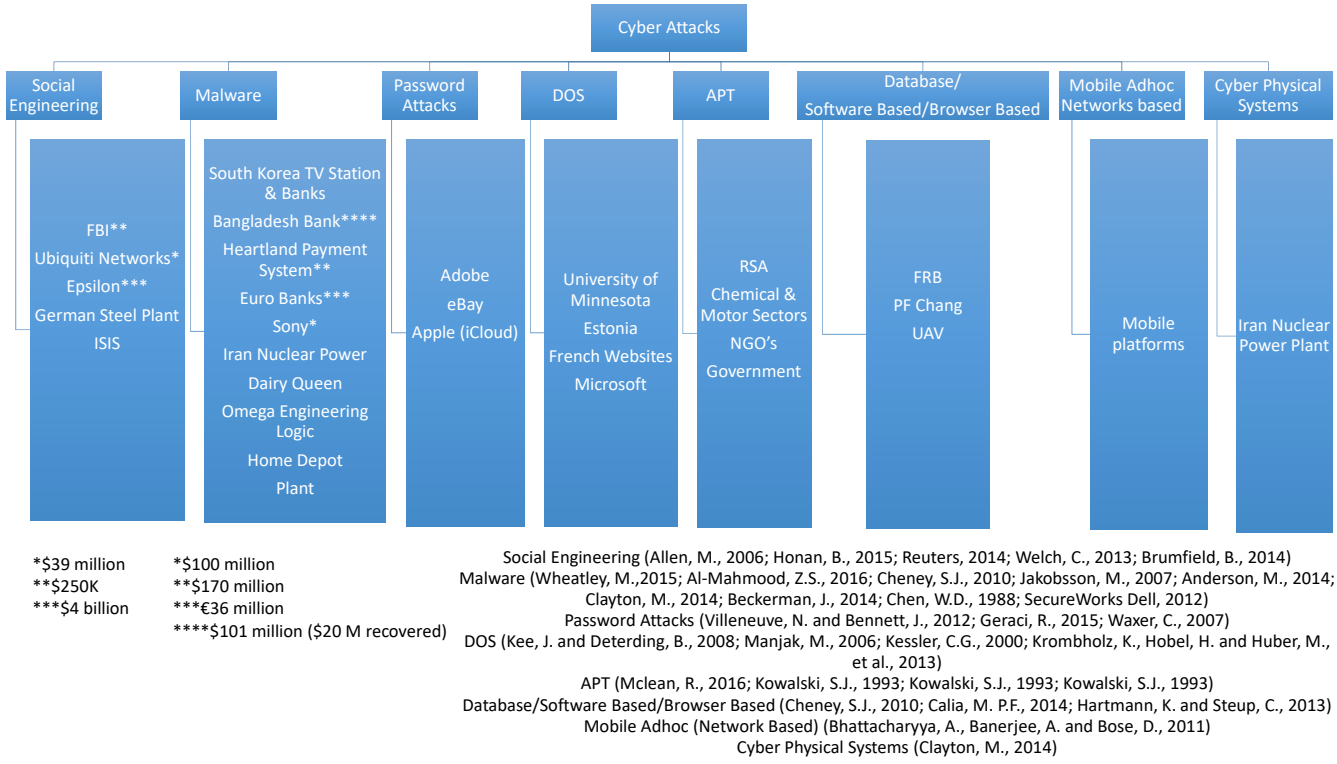


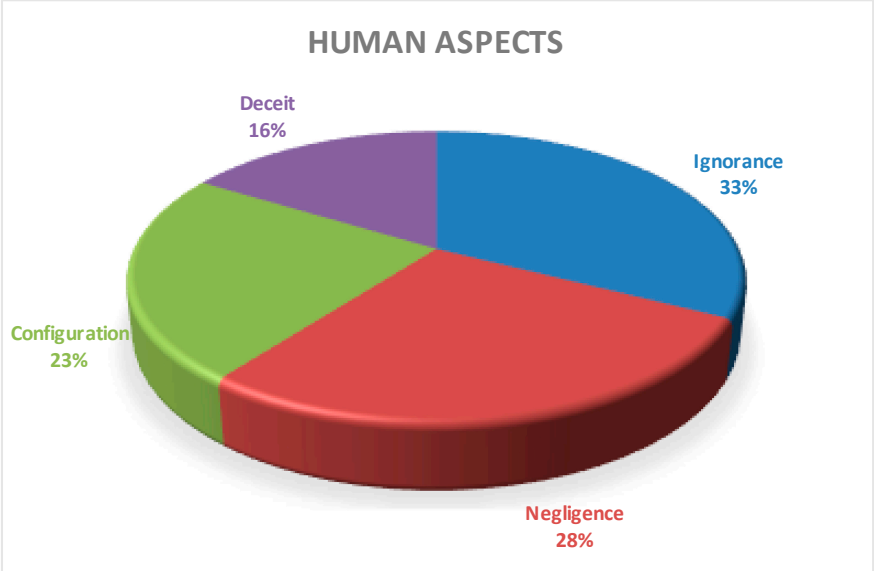
Figure 2. Cyber-attacks.

We next discuss some human behavioral aspects which may be at play in propagating some of these attacks.

3.3. Categorization of the Human Aspects

Our personalities decide how we react to situations in real life; this is our behavior in situations. Similarly, to real-life situations, when we see a stimulus in the cyber world, we tend to react based on our fundamental nature, e.g., whether to click on a link embedded in an email or not, whether to open the attachment on the email, and whether to click on a link on the website we are browsing or not [27].

It is discussed in the literature [28] that there are certain key human behavioral aspects to becoming a victim of cyber threats. From the 43 case studies of different cyber-attacks in the past 10 years, we identified four human factors at play, namely ignorance, negligence, configuration and deceit, as shown in Figure 3a.



(**a**)

Evaluating Cyber-attack case studies on set of factors and their scales

Case Studies: All the case studies on cyber attacks
Types of Attacks: Categorization of cyber attacks
Human Factors: Ignorace, Negligence, Configration, Deceit
Industry: Technology, Health, Entertainment, Advertisement, Transportation, Energy, Food & Agriculture, Communication, Nuclear, Financial, Manufacturing, Retail, Education
Financial Intensity: Low (1) = less than $100K, Less than Moderare (2) = less than $250K, Moderate (3) = less than $500K, High (4) = less than $1 Million, Huge (5) = greater than $1 Million
Non-Financial Intensity: Biometric, Health, PII, Reputation, Credebility, Maturity, Privacy
# of Customers (Victims) Impacted: Low (1) = less than 50K, Less than Moderare (2) = less than 100K, Moderate (3) = less than 250K, High (4) = less than 500K, Huge (5) = greater than 500K
Cultural Factors: Cultural coherence with cyber awareness, be acclimated with the corporate culture
End User Trust & Loyalty: Buy-in within the organization and be loyal to follow cyber policies and protect digital assets for the company
Policy Issues: Minimal/weak cybersecurity policy (Y = having policy issue or no policy, N = Having sound cybersecurity policy)
Training & Awareness: Adequate training to educate the employees on cyber threats
Technology Adoption (for Cybersecurity Prevention): Efficient technology applied to protect from cyber threats
Investment: Enough Funding (investment) on cybersecurity implementation/precautions

(**b**)

Figure 3. (**a**) Human aspects of cyber threats. (**b**) Summary of the factors in Table 2.

Table 2. Factors to evaluate in cyber-attack case studies.

Case Studies	Types of Cyber Attacks	Human Factors	Industry	Financial Intensity (1–5)	Non-Financial Intensity	# of Customers Impacted (1–5)	Cultural Factors	End User Trust & Loyalty	Policy Issues	Training & Awareness	Technology Adoption	Investment
Stuxnet Cyber Warfare	Malware (Worm)	Ignorance	Nuclear	5	Reputation	4	Y	N	Y	N	N	Y
RSA APT Attack	APT	Ignorance	Technology	3	Credibility	5	Y	Y	Y	N	N	Y
eBay Account Hack	Password Attacks	Ignorance	Technology	3	Reputation	4	N	N	Y	N	N	N
German Steel Plant Attack	Social Engineering	Ignorance	Manufacturing	3	Maturity	3	N	N	Y	N	N	N
Social Engineering Malware Attack (ISIS)	Social Engineering/Malware	Ignorance	Advertisement	2	Maturity	3	N	N	Y	N	N	N
Heartland Payment System Data Breach 2008	SQL Injection Attack	Ignorance	Financial	5	Credibility	5	Y	Y	N	N	Y	Y
Home Depot Data Access Attack	malware (Worm)	Ignorance	Retail	5	Reputation	5	N	N	Y	N	N	N
UAV (Unmanned Aerial/Air Vehicles) Feed Interception.	Cyber-Physical Attack	Ignorance	Communication	5	Maturity	5	N	N	Y	N	N	N
Trojan Attack	Malware (Worm)	Ignorance	Financial	4	Maturity	4	N	N	Y	N	N	N
South Korea Financial & TV Station cyber-attack—Summer of 2013	Social Engineering/Malware	Ignorance	Entertainment/ Financial	3	Reputation	4	N	N	Y	N	N	N
Botnet Attack	DOS	Ignorance	Technology	2	Maturity	3	N	N	Y	N	N	N
Francophoned	Social Engineering	Ignorance	Financial	3	Maturity	3	N	N	Y	N	N	N
Interactive voice response (IVR) or Phone Phishing	Social Engineering	Ignorance	Financial	3	Maturity	4	N	N	Y	N	N	N
Cross-Site Request Forgery (CSRF)	Browser Based Attack	Ignorance	Advertisement	2	Reputation	3	N	N	Y	N	N	N
Sony—the wiper malware attack in 2014	Malware (Worm)	Negligence	Entertainment	5	Reputation	5	N	N	N	Y	N	Y
P.F. Chang's Sales Machine Hacked	Malware	Negligence	Food	4	Maturity	4	N	N	Y	N	N	N
Epsilon data breach attack	Malware	Negligence	Financial	5	Reputation	5	N	N	Y	N	N	N
Omega Engineering Logic Bomb	Software Based Attack	Negligence	Technology	5	Credibility	4	N	N	Y	N	N	N

Table 2. *Cont.*

Case Studies	Types of Cyber Attacks	Human Factors	Industry	Financial Intensity (1–5)	Non-Financial Intensity	# of Customers Impacted (1–5)	Cultural Factors	End User Trust & Loyalty	Policy Issues	Training & Awareness	Technology Adoption	Investment
Living social hack and password hack 2013	Password Attacks/SQL Injection	Negligence	Communication	4	PII	5	N	N	Y	N	N	N
Stuxnet attack through USB	APT	Negligence	Communication	3	Maturity	3	N	N	Y	N	N	N
Hacktivism–Estonia	DOS	Negligence	Financial/Educat	4	Reputation	4	Y	N	Y	N	Y	N
Capture password by brute force	Password Attacks	Negligence	Retail	3	Maturity	3	N	N	Y	N	N	N
TJX Cyber attack: WEP (Wired Equivalent Privacy) attack.	Malware	Negligence	Retail	5	PII	5	N	N	Y	N	N	N
SQL Injection Attack at the Federal Reserve Bank.	Database Attack	Negligence	Financial	5	PII	4	N	N	Y	Y	N	Y
Man in the middle attack	Software/Browser Based Attack	Negligence	Retail	4	Maturity	4	N	N	Y	N	N	N
Tailgating	Social Engineering	Negligence	Retail	3	Maturity	3	N	N	Y	N	N	N
Evernote DDOS Attack	DOS	Configuration	Retail	4	Credibility	3	N	N	Y	Y	N	N
Adobe password breach 2013	Password Attacks	Configuration	Technology	4	Reputation	4	Y	N	Y	Y	Y	N
Dairy Queen International Data Breach	Malware	Configuration	Food & Agriculture	4	PII	4	N	N	Y	N	N	N
Microsoft DOS Attack	DOS	Configuration	Technology	3	Reputation	5	Y	Y	N	Y	Y	Y
Cyber espionage - Titan Rain Attack	APT	Configuration	Entertainment	4	Reputation	4	Y	N	Y	Y	N	N
Flame Malware Attack	Malware	Configuration	Energy	4	Privacy	3	N	Y	Y	N	N	N
Smurf Attack	DOS	Configuration	Education	3	Credibility	3	Y	Y	Y	Y	Y	N
Logic Bomb Attack in South Korea Banks and broadcasting organizations	Database Attack	Configuration	Financial / Entertainment	3	Reputation	3	N	N	Y	N	N	N
Kerberos Replay Attack	Password Attacks	Configuration	Communication	-	Maturity	-	N	N	Y	-	N	N

Table 2. *Cont.*

Case Studies	Types of Cyber Attacks	Human Factors	Industry	Financial Intensity (1–5)	Non-Financial Intensity	# of Customers Impacted (1–5)	Cultural Factors	End User Trust & Loyalty	Policy Issues	Training & Awareness	Technology Adoption	Investment
Cross Site Scripting (XSS)	Browser Based Attack	Configuration	Entertainment	-	Reputation	-	N	N	Y	N	N	N
iCloud Account Hack –Password Attack	Social Engineering / Password Attack	Deceit	Technology	-	Reputation	5	Y	Y	N	Y	Y	Y
DOS Attack and DDOS Attack	DOS	Deceit	Entertainment	-	Reputation	4	N	N	Y	N	N	N
DDOS–NTP	DOS	Deceit	Retail	-	Credibility	-	N	N	Y	N	N	-
Bating	Social Engineering	Deceit	Transportation	3	Privacy	2	N	N	Y	-	N	N
Pretexting	Social Engineering	Deceit	Financial	-	PII	-	N	N	Y	N	Y	Y
Quid Pro Quo	Social Engineering	Deceit	Communication	-	Privacy	-	-	-	Y	-	N	N
Sybil Attack	Mobile Ad hoc Network Based	Deceit	Retail	-	PII	4	N	N	Y	N	N	N

Among these human factors, ignorance and negligence are the two main factors where the users are either not aware of the kind of threats they fell victim to, or the users neglected the fact that they could be the victims of known cyber-attacks. For instance, the Stuxnet worm exploited Iran's nuclear program in 2009–2010, which Iranians had no knowledge of. RSA-APT attack is another example of ignorance from the victims where they experienced a zero-day attack that started with a phishing email that read "2011 Recruitment Plan" [29]. The Heartland Payment System had a data breach in 2008 through a malware attack without any prior knowledge from the victims. As Reuters reported back on 21 May 2014, 145 million eBay accounts were hacked with their passwords being compromised; therefore, a massive number of password reset requests went out to all 145 million eBay users to reset their passwords. The Home Depot data attack gained access to the payment system, installed malware, and sent payment information to the hacker's server.

On the other hand, the Sony wiper malware attack in 2014 is a good example of negligence, where Sony ignored the fact that there could be a real threat on their system until it was too late [30]. A similar issue was revealed when P.F. Chang's sales machine was hacked with customers' debit card and credit card information [31]. On 30 March 2011, Epsilon revealed a Data Breach attack on brand name companies like Citibank, Capital One, Marriott, Best Buy, and JP Morgan and Chase, in which they lost close to $4 billion [32]. In the APT–Stuxnet attack, Stuxnet entered through a USB to a computer and the network, and infected it by exploiting zero-day vulnerabilities. Users were completely unaware of the Stuxnet worm attack, which started with a USB drive [33,34].

The BBC reported on 30 October 2013 that the Adobe password breach in 2013 impacted 38 million users. It generated and revealed passwords from hints, sample userids and hashed passwords was a result of a configuration issue. The Dairy Queen International data breach is also related to a configuration issue, in which the hacker was able to inject malicious code into explorer.exe [35].

Lastly, DOS and DDOS attacks often trick and deceive the victims with floods of network spoofing; for instance, it may appear to be coming from gaming services like the League of Legends. Furthermore, baiting using a malicious USB stick may deceive the victims to reveal key information.

As we can see from Figure 3a, which shows the distribution for these aspects in the cyber-attack case studies we analyzed, 33% of the attacks were based on ignorance, and 28% had negligence as key factors. These distributions are based on a qualitative evaluation of the case studies and the categorization of human factors.

3.4. Financial Impacts

The financial impact for all cyber threats can be far reaching, as a small attack can have cascading effects. Sony [36] lost about $35 million for its data breach. With every employee's security impact within Sony, the analysts at Macquarie estimated the cost to rebuild Sony's computer systems to be close to $83 million [37,38]. The financial implication of these cyber threats leads to billions of dollars lost. On 5 February 2016, a malware attack locked access to certain computer systems and prevented electronic communication within the Hollywood Presbyterian Medical Center. The hospital authority had to pay a ransom equivalent to around $17,000 in bitcoin to obtain the decryption key and get its computer systems back up and running [39]. The Central Bank of Bangladesh suffered a massive malware attack [40], where the hackers stole $101 million on 4 February 2016, and later recovered a portion of that, $20 million from Sri Lanka. The remaining $81 million is still missing and was presumably transferred to the Philippines. The investigation is still underway.

In this financial impact analysis, we categorized the intensity according to the loss in dollar amounts. For example, if a company lost less than $100,000 from cyber threats, we call it a low (1) financial impact. On the other hand, amounts greater than a million-dollar financial loss are treated as a high (5) financial consequence. The numerical ranges from 1 to 5 help us quantify these variations.

Beyond the financial impacts, these attacks also lead to several non-financial impacts, discussed next, which can have long-lasting effect on the company.

3.5. Non-Financial Impacts

Besides the financial intensity of these cyber threats, the victims also face adverse non-financial impacts, such as biometric, health, Personally Identifiable Information (PII), reputation, credibility, maturity, and privacy impacts [41]. For instance, the SQL Injection Attack at the Federal Reserve Bank exposed PII data like the SSN (Social Security Number) and DOB (Date of Birth) of the customers. Often, attacks expose biometric information such as the fingerprints, which are very difficult to remediate. Home Depot and Sony lost their reputation when they suffered malware threats.

3.6. Number of Customers (Victims) Impacted

Cyber-attacks may cause harm to hundreds and thousands of people. We therefore categorized the impacts of cyber-attacks with different thresholds of people affected. For example, Stuxnet Cyber Warfare had an adverse effect on a large number of people, which was between 250,000 to 500,000. On the other hand, the Heartland Payment System data breach in 2008 had a tremendous impact on a very large number of people (an intensity of 5 on a scale of 1–5), where the payment information of more than 500,000 people was compromised through a malware attack.

3.7. Cultural Factors

Cultural coherence is an acclimatization with a particular trend or culture, in this case, with cybersecurity. Cyber awareness can be key cultural factor in an organization, which can help protect from cyber threats. Our findings show a strong link between cybersecurity awareness and lower vulnerability to cyber threats, and vice versa. For example, the eBay account hack was a result of password attack, with potential issues with the awareness of common best practices. We denote this with an "N" in Table 2 to indicate issues in cybersecurity culture in the organization.

3.8. End-User Trust and Loyalty

It is clear that the majority of undetected cyber-attacks come from insider threats. Therefore, it is crucial to have buy-in within the organization and loyalty to follow cyber policies and protect digital assets for the company. If employees are not loyal and trustworthy, the digital assets of the company would be susceptible to all kinds of cyber threats. The Epsilon Data Breach attack was a result of a lack of end-user trust and loyalty. We attempted to identify cyber-attack case studies where this was a factor at play so that any other signs can be deciphered, as insider threats are probably the most difficult to study. This is a typical example of an insider threat where the employees of an organization may also inadvertently expose a channel of personal information.

3.9. Policy Issues

Having robust security policies is key to having a secure environment. Here, security policy refers to the set of rules and regulations for the users of the systems to follow in order to protect the IT infrastructure from any sorts of cyber-attack. For instance, the employees and contractors protect confidential information, follow password policy, grant access to the appropriate users, and do not gain access to the systems for which they are not supposed to have access to, etc. Minimal/weak cybersecurity policy (Y = having a policy issue or no policy; N = having a sound cybersecurity policy) can make an IT environment very weak and vulnerable to multiple kinds of cyber threats [42,43]. For instance, P.F. Chang's sales machine was hacked, and exposed customers' debit and credit card information with a potentially weaker cybersecurity policy and best practices and did not implement an encryption-enabled terminal.

3.10. Training and Awareness

Adequate training to educate employees on cyber threats is an absolute necessity for the protection of a corporate network. This is a continual process to make all the employees aware of new cyber threats and how we can protect ourselves from them [44,45]. A lack of training and awareness make an internal IT environment dangerous and a haven for hackers. Interactive voice response (IVR) or Phone Phishing attacks are a clear impact from the lack of awareness and training about cybersecurity. If users do not know how to differentiate between a good email and a phishing email [46], they can easily open a back door to make the IT systems vulnerable.

3.11. Technology Adoption (for Cyber-Threat Prevention)

Organizations and individuals need to adopt the right technology and implement proper security measures to secure their IT infrastructure [47]. Not too long ago, security was the last thing in management's mind to invest in, and as a result, management focused on new features and functionalities to manage the time to market without worrying about the security aspect. Understandably, this is still the focus of all major organizations. As a result, several companies had unparalleled disasters, and lost credibility and millions of customers. Mature companies like Sony experienced the wiper malware attack in 2014 because of the lack of proper cybersecurity prevention measures and related technology adoption.

3.12. Investment

Finally, companies need to allocate enough funding and investment to cybersecurity implementation/precautions to make the IT infrastructure sound and strong, and to protect from cyber hackers [48]. The more users/organizations invest and put in the right amount of effort, the more secure they make the network environment; the less they invest, the more vulnerable the systems become. Cyber-attacks on South Korea Financial and TV Station back in summer of 2013 happened because of their having minimal or no investment in cybersecurity. The key to securing IT networks is to have the right amount of investment on cybersecurity as a first line of defense.

3.13. Factors Leading to Cyber-Attacks

As discussed above, many factors contribute to cyber-attacks. In our study, we identified these key factors and evaluated these factors for each cyber-attack, in order to connect it with a good mitigation strategy.

The factors are summarized in Figure 3b and are outlined for each case study in Table 2.

4. Results and Findings

Based on the factors we interpreted through the case study evaluation depicted in Table 2, we wanted a map to discover any frequent patterns across case studies. We utilized Association Rule Mining (ARM) to quantify our findings, as shown in Table 3 below. The rules which had a strong co-occurence are indicated with metrics of confidence and lift. We ran ARM on the case study data we gathered in Table 2 that match with the associations of cyber threats intuitively, as well. Association rules essentially help quantify frequently co-occurring patterns in the data. Our aim here was to see if there are certain factors which implied policy or human factors with a high frequency [49]. All of these association rules indicate a high confidence close to 1, denoting that the left-hand side is strongly linked to the right-hand side factors. Moreover, the high lift values greater than 1 show a high correlation between the factors.

Table 3. Association Rule Mining (ARM) on the case study.

Index	Association Rule	Confidence	Lift
1	Investment=N ==> Policy Issues=Y	1.00	1.10
2	End User Trust & Loyalty=N Investment=N ==> Policy Issues=Y	1.00	1.10
3	Technology Adoption=N Investment=N ==> Policy Issues=Y	1.00	1.10
4	End User Trust & Loyalty=N ==> Policy Issues=Y	0.97	1.07
5	Technology Adoption=N ==> Policy Issues=Y	0.97	1.07
6	Cultural Factors=N ==> End User Trust & Loyalty=N	0.97	1.16
7	Cultural Factors=N ==> Policy Issues=Y	0.97	1.07
8	Cultural Factors=N ==> Technology Adoption=N	0.97	1.16
9	End User Trust & Loyalty=N Technology Adoption=N ==> Policy Issues=Y	0.97	1.07
10	Training & Awareness=N ==> Policy Issues=Y	0.97	1.07
11	Cultural Factors=N Policy Issues=Y ==> End User Trust & Loyalty=N	0.97	1.16
12	Cultural Factors=N End User Trust & Loyalty=N ==> Policy Issues=Y	0.97	1.07
13	Cultural Factors=N Technology Adoption=N ==> End User Trust & Loyalty=N	0.97	1.16
14	Cultural Factors=N End User Trust & Loyalty=N ==> Technology Adoption=N	0.97	1.16
15	Cultural Factors=N Technology Adoption=N ==> Policy Issues=Y	0.97	1.07
16	Cultural Factors=N Policy Issues=Y ==> Technology Adoption=N	0.97	1.16
17	Cultural Factors=N Policy Issues=Y Technology Adoption=N ==> End User Trust & Loyalty=N	0.97	1.16
18	Cultural Factors=N End User Trust & Loyalty=N Technology Adoption=N ==> Policy Issues=Y	0.97	1.07
19	Cultural Factors=N End User Trust & Loyalty=N Policy Issues=Y ==> Technology Adoption=N	0.97	1.16
20	Cultural Factors=N ==> End User Trust & Loyalty=N Policy Issues=Y	0.94	1.15
21	End User Trust & Loyalty=N Technology Adoption=N ==> Cultural Factors=N	0.94	1.22
22	Cultural Factors=N ==> End User Trust & Loyalty=N Technology Adoption=N	0.94	1.22
23	Cultural Factors=N ==> Policy Issues=Y Technology Adoption=N	0.94	1.15
24	End User Trust & Loyalty=N Policy Issues=Y Technology Adoption=N ==> Cultural Factors=N	0.94	1.22
25	Cultural Factors=N Technology Adoption=N ==> End User Trust & Loyalty=N Policy Issues=Y	0.94	1.15

We next used connections between these association rules to link various factors. These were visualized and evaluated to represent the factors impacting cyber-attacks using ARM and connections between these rules. We next illustrate several example observations from this data.

A. ***Denial of Service (DOS)*** attacks [50] usually occur when an environment has a weak configuration and cybersecurity policy despite training and the related cyber awareness, as shown in Figure 4 below. Strong cybersecurity policies and strong configuration in the IT infrastructure [51] are a necessity for a secure environment because training and cyber awareness are not good enough without implementing them properly. The credibility and the reputation of the organization are impacted heavily by this kind of incident. The DOS attack [52] is related to the circular impactful attributes that imply the loss of credibility.

B. ***APT:*** In Figure 5, we notice that APT attacks are linked to the lack of technology adoption, with not much training, as well as minimal security policy. They may cause medium to high financial loss. Cyber awareness is not enough if we do not have the proper training and technology adoption for cybersecurity.

C. ***Social Engineering***: We see a lack of awareness and training with a lack of technology adoption. As a result, there is no corporate culture for security and no corporate investment for cybersecurity. The outcome from this may lead to significant financial loss. Ignorance is the main human factor for this kind of attack, as shown in Figure 6.

D. ***Malware:*** If there is no strong cybersecurity policy, not much investment in security, and limited training and awareness on Cybersecurity, organizations may become victims of a Malware attack. The financial consequence from this attack could be very high, as depicted in Figure 7.

Weak Configuration
Weak Cybersecurity
Adoption of Technology
Cyber Aware and
Policy
Trained
➔ DOS Attack ➔ Loss of Credibility

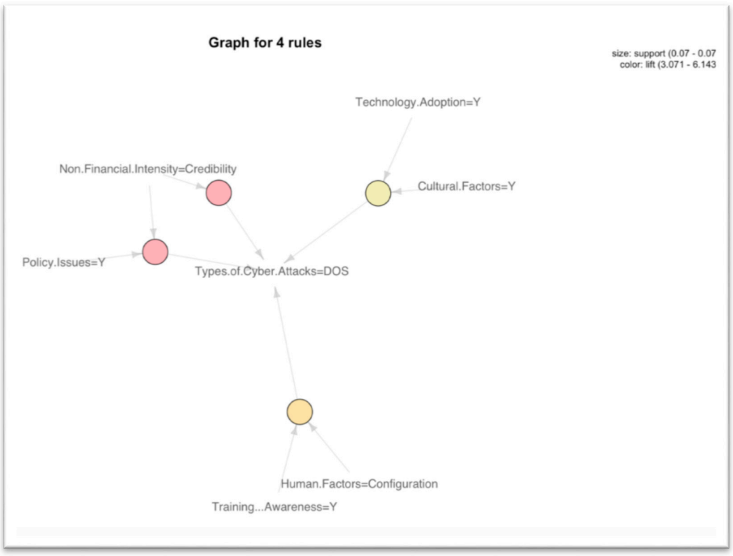


Figure 4. DOS attack factors.

Limited Training
Weak Cybersecurity Policy
Limited Technology
Cyber Aware
Adoption
➔ APT Attack ➔ Medium to High Financial Loss

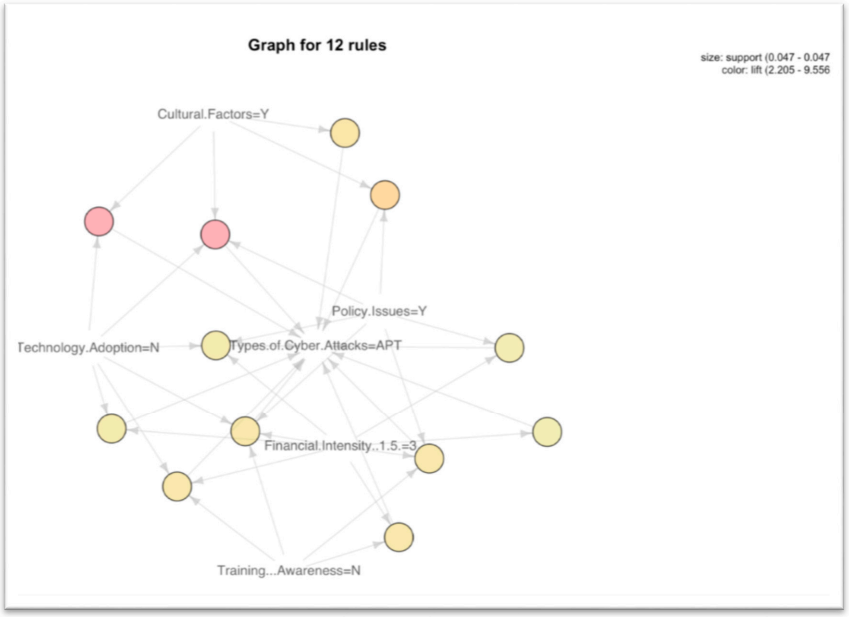


Figure 5. APT Factors.

Human Behavior -
Limited Training
Limited Cyber Awareness
Limited Technology
Loss
Limited Trust and Loyalty
Minimal Cybersecurity
Lack of Maturity

Ignorance
Adoption
Policy

➔ Social Engineering Attack ➔ Medium to High Financial

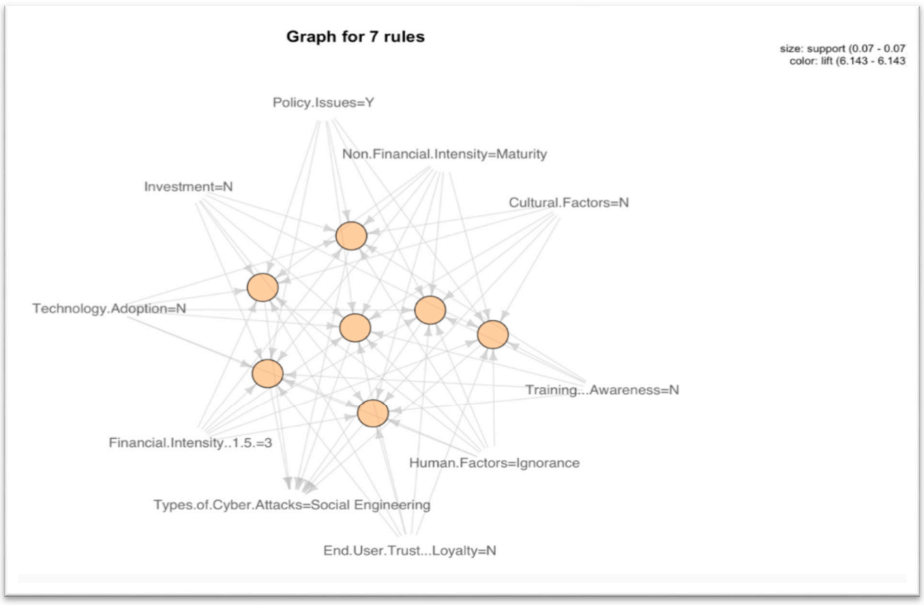


Figure 6. Social Engineering factors.

No Investment on Cybersecurity
No Cyber Awareness
No Technology Adoption
No Training on Cybersecurity
Minimal Cybersecurity Policy

Malware Attack ➔ High Financial Loss

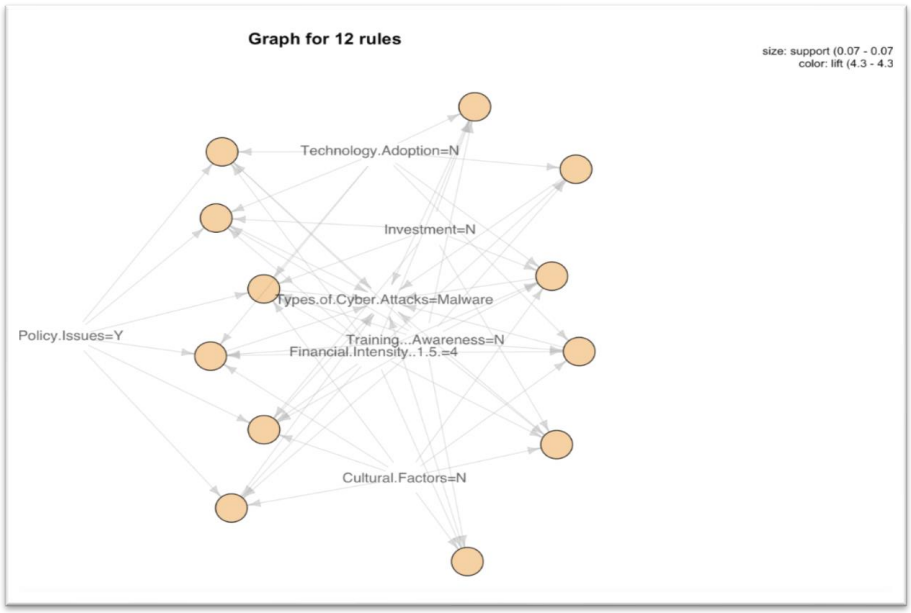


Figure 7. Malware factors.

Looking at the overall factors for cyber threats in Figure 8, technology adoption with trust and loyalty to the policies, as well as cybersecurity awareness, can make the digital environment safer. On the other hand, as is quite evident, deceitful human factors make the environment vulnerable to multiple types of cyber-attacks [53]. The cyber-attacks from deceitful behavior, along with cyber policy issues in an organization may impact huge number of customers with a high intensity of financial loss. Likewise, if an organization and its employees do not adopt the technology to make the environment secure, and are not aware of the possible cyber threats, it can make the corporate assets prone to different types of cyber threats that may cause a significant financial impact to the organization, as well a large number of the customers of that company. Figure 9 reflects how different attributes impact the major types of cyber threats.

We next highlight the relative intensity of each factor of the cyber threats, as shown in Figure 10. Investment in security, proper technology adoption, trust and loyalty in the workforce, and cybersecurity policy and procedures are the key factors for having a safe and secure IT environment. We notice a lack of cyber awareness, training, loyalty, and trust, as well as a lack of investments because of a lack of technology adoption as key factors. Similarly, if we do not have end-user trust and loyalty with a lack of cyber awareness and training, a lack of technology adoption and a lack of investment, we observe Cyber Policy issues.

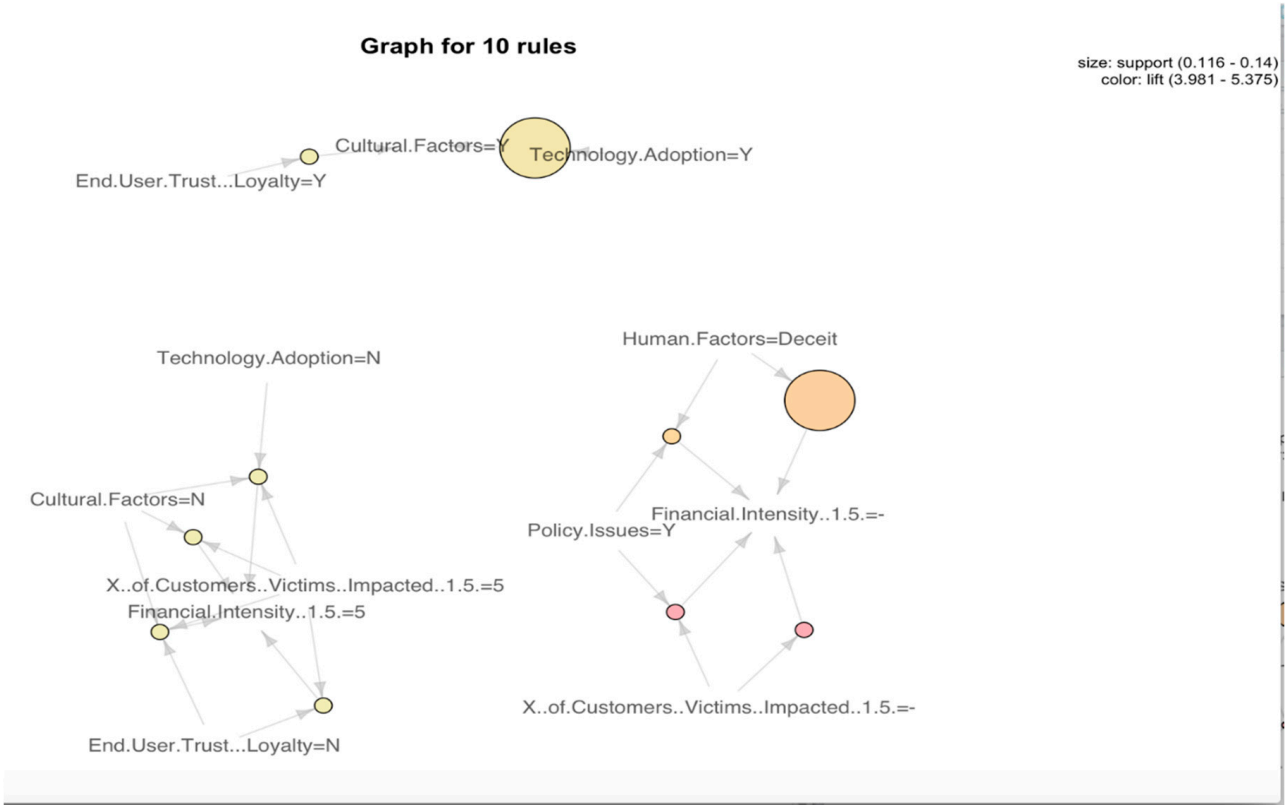


Figure 8. Overall factors for cyber-attacks.

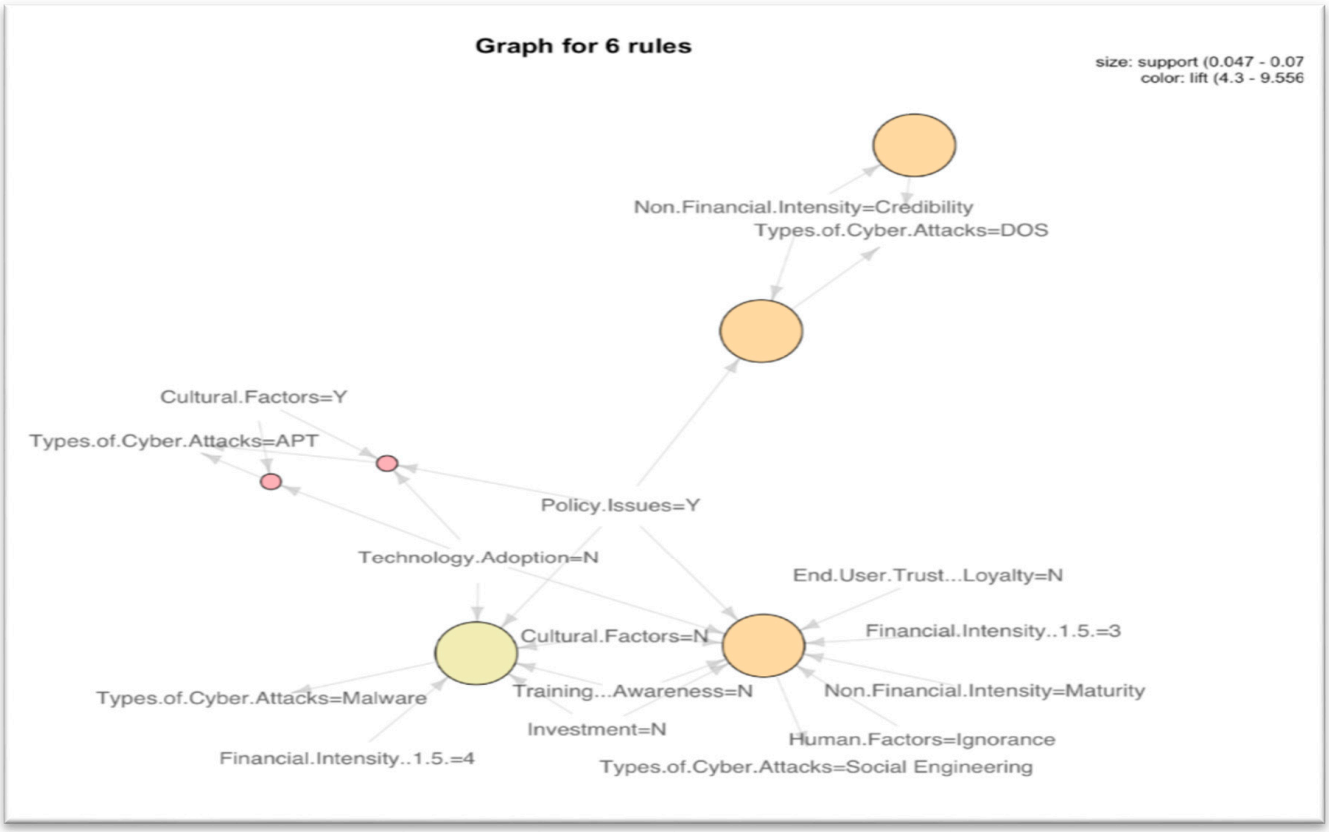


Figure 9. Associations between the types of cyber-attacks.

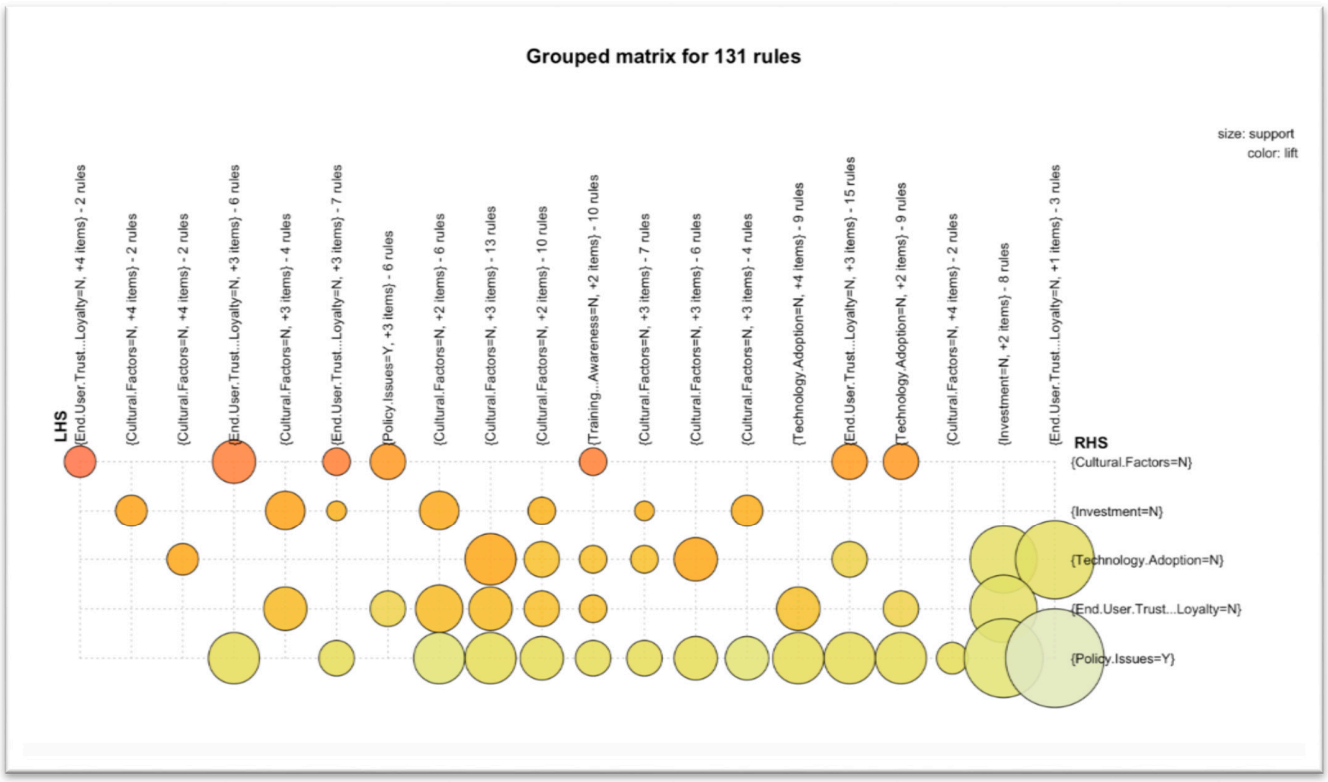


Figure 10. Cyber threat factors and their correlation.

It is apparent from the Figure 10, not surprisingly, that strong cybersecurity policy is a key contributing factor for securing the IT infrastructure. If a cyber policy is weak, it usually means that companies lack investment in protecting the digital assets, have minimal cyber awareness, a lack of cyber training, not much investment on cybersecurity, and limited secure technology adoption.

From the overall perspective in our case study, we learned an interesting correlation among the factors of cyber threats. The more investment we make in cybersecurity, the more educated we become on cybersecurity issues, and we adopt more secure technology. Lastly, simply training on cybersecurity and becoming aware of cyber threats are not enough if we do not enforce a strong cybersecurity policy. Consequently, along with good investment on cybersecurity, we need to implement effective cybersecurity policy to make the IT infrastructure secure from different kinds of cyber threats. Securing an IT environment from cyber threats is a continual process, and we need to keep adopting new technology to safeguard ourselves from innovative threats. These correlations are depicted below, and their intensity is indicated by the size of the circles.

5. Overall Observation

The following is the synopsis of the overall observation from our case study:

1. Out of the four main human factors, ignorance and negligence are the two human behaviors that appear to be linked to most of the cyber threats.
2. Financial Institutes, Retail and Entertainment industries are the main targets for hackers, in addition to Technology, Health and Energy. This is especially true when financial gains are the key factor behind an attack.
3. Biometric threats have serious consequences. When our biometrics are compromised, unfortunately, the mediation from these threats becomes very minimal, because we cannot change the configuration of our fingerprint.
4. Cyber threats usually have high customer impacts. The financial loss can be immense, and organizational credibility is at stake.
5. Insider threats are perhaps the most difficult to predict or detect. If the internal resources include an individual with bad intentions who may have significant access to the system, it becomes very difficult to protect the organizational assets.
6. Having a strong cybersecurity policy is crucial to safeguard from cyber threats. We may have the most sophisticated technology, but with a weakly articulated cyber policy and less governance, an IT environment can be vulnerable to different types of cyber threats.
7. We observed strong linkages between weak/no cyber policy and less investment on technology, no technology adoption, minimal training and education, and cyber awareness. Among these factors, technology adoption and human factors are the two dominant contributors. In other words, to make the digital assets safe, we need to invest adequately in security, train our employees, build and govern strong cybersecurity policy, and above all adopt and keep up with technology to overcome new and existing security threats. Developing and adopting a strong security policy will help increase awareness and provide opportunities for learning and establishing protocols to prevent cyber threats.

6. Mitigation Strategy

Based on our evaluation of several cyber-attacks, we identified several general mitigation strategies, including education and training, the proper configuration of the systems, building robust security infrastructure, accountability, strong security policy, and adequate investment on security, to name a few [54]. While these may seem like common-sense practices, many of these strategies were missing in the organizations at the time they were impacted by attacks, such as in the case of the German Steel Plant attack and the malware attack of the Heartland Payment System data breach in 2008. Moreover, with the new trend

of employees working from home, it has become imperative that we have strong training with the latest security infrastructure.

Organizations should also have a strong password policy, and caching should not be allowed. Users should apply Reverse Turing Tests (RTT) and utilize a strong password strategy, prevent the reuse of password history, and always use multifactor authentication. Strong encryption and authentication, Virtual Private Networks (VPN), ending a session properly, deleting cookies and changing credentials should also be part of a strong policy.

Any company is vulnerable to cyber security threats, and this is because every company has something a cyber-criminal wants—whether that be access to financial accounts or the Personally Identifiable Information of customers and employees that can be used to commit fraud. Thus, every company needs to evaluate its security processes and improve upon them. Bring Your Own Device (BYOD) and the increase in employee-owned mobile devices accessing corporate networks have created unique targets for potential attack and have necessitated new layers of cyber security [55]. Of course, it is not just employees who are using mobile devices to interact with the company. In the banking industry, especially, more customers than ever are conducting financial transactions using mobile apps. This means that those designing these apps need to be security-forward and should have protocols in place to monitor for potential malware infections.

In a world of multiple apps and multiple notifications and alerts, we tend to ignore alerts if they are too frequent. With proper security configuration (for example, reducing false-positive alerts) and being vigilant to the motives of the attacker, we can create a safe and sound cyber environment [56]. Finally, we need to be cognizant of insider threats, and make sure that we have strong security implementation within our internal IT infrastructure [57]. That said, insider threats are some of the hardest to detect.

Overall, there is a clear need for strong cyber security policy, as well as a strong cyber training program to increase awareness.

7. Conclusions and Open Challenges

In this paper, we provided an in-depth look at cyber threats and studied real-world case studies of these threats in order to identify the factors that occur across these threats. In our study, we identified ignorance and negligence as the main human factors of cyber threats [58]. Moreover, configuration issues are also linked to cyber-attacks, along with being trapped into deceitful behavior from the attackers.

We also evaluated the financial and non-financial outcomes of cyber-attacks, which helped us to evaluate the types of outcomes linked to the key factors propagating the attacks. We discovered the ground truth of the 43 case studies we evaluated, including key factors impacting the propagation of cyber-attacks, which include human aspects, education, IT security policies and procedures, social engineering, internal threats, and technology adoption [59,60]. Cybersecurity implementation happens to be a less-important factor for a technology project until a cyber-attack infiltrates the system and causes tremendous damage. We tend to focus more on the new features and functionalities of the system where security may become a lower priority for the ease of functionality. As a result, we become the victims of cyber threats and intrusion [61,62]. Consequently, we need to be proactive and invest in order to safeguard our systems from cyber threats beforehand. Being proactive to protect from cyber-attacks is not always easy, as attackers keep introducing new threats and our attack surface increases with more mobile app adoption. Therefore, we need to be ahead of the attackers to predict possible vulnerabilities and take proper precautions. With that in mind, we focused on and analyzed this comprehensive case study to identify the key factors leading to cyber-attacks, such that we are all well equipped to fight against cyber threats.

Author Contributions: Abstract, F.Q. and V.P.J.; Introduction, F.Q. and V.P.J.; Motivation, F.Q. and V.P.J.; Case Study Methodology, F.Q. and V.P.J.; Results and Findings, F.Q. and V.P.J.; Overall Observation, F.Q. and V.P.J.; Mitigation Strategy, F.Q. and V.P.J.; Conclusions and Open Challenges, F.Q. and V.P.J. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Paganinip, P. FireEye Why Humans Could Be the Weakest Link in Cyber Security Chain. *Security Affairs*, 3 October 2012. Available online: http://securityaffairs.co/wordpress/9076/social-networks/why-humans-could-be-the-weakest-link-in-cyber-security-chain.html (accessed on 23 October 2021).
2. Abraham, S.; Chengalur-Smith, I. An overview of social engineering malware: Trends, tactics, and implications. *Technol. Soc.* **2010**, *32*, 183–196. [CrossRef]
3. Wheatley, M. Hidden Costs of Sony's Data Breach Will Add up for Years, Experts Say. *Silicon Angle*, 20 February 2015. Available online: http://siliconangle.com/blog/2015/02/20/hidden-costs-of-sonys-data-breach-will-add-up-for-years-experts-say/ (accessed on 2 March 2021).
4. Smith, G. Home Depot Admits 56 million Payment Cards at Risk after Cyber Attack. *The Huffington Post*, 18 September 2014. Available online: http://www.huffingtonpost.com/2014/09/18/home-depot-hack_n_5845378.html (accessed on 23 May 2019).
5. Stevenage, S. *Human Aspects of Cybersecurity*; Super Identity Project; University of Southampton: Southampton, UK, 2010.
6. Haggard, S.; Lindsay, R.J. *North Korea and the Sony Hack: Exporting Instability Through Cyberspace*; Asia Pacific Issues, No. 117; East-West Center: Honolulu, HI, USA, 2015.
7. Love, D. Why Microsoft And Sony Couldn't Stop Lizard Squad Attack Despite Warnings. *International Business Times*, 30 December 2014. Available online: http://www.ibtimes.com/why-microsoft-sony-couldnt-stop-lizard-squad-attack-despite-warnings-1769174 (accessed on 9 January 2020).
8. Sicard, S. North Korean Cyber Attack on Sony Poses Tough Security Questions. *Natl. Def.* **2015**, *99*, 24–25.
9. Al-Mahmood, Z.S. Hackers Lurked in Bangladesh Central Bank's Servers for Weeks. 22 March 2016. The Wall Streel Journal. Economy. Available online: http://www.wsj.com/articles/hackers-in-bangladesh-bank-account-heist-part-of-larger-breach-1458582678 (accessed on 16 January 2019).
10. Cheney, S.J. *Heartland Payment Systems: Lessons Learned from a Data Breach*; Discussion Paper—Payment Cards Center; Federal Reserve Bank of Philadelphia: Philadelphia, PA, USA, 2010.
11. Cassano-Piché, A.; Vicente, K.J.; Jamieson, G.A. A Sociotechnical Systems Analysis of the Bse Epidemic in the Uk Through Case Study. *Proc. Hum. Fact. Ergon. Soc. Annu. Meet.* **2006**, *50*, 386–390. [CrossRef]
12. Zetter, K. A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever. *Security*, 8 January 2015. Available online: https://www.wired.com/2015/01/german-steel-mill-hack-destruction/ (accessed on 21 April 2018).
13. Cyber Security Crimes. Types of Cyber Attacks. Available online: www.cybersecuritycrimes.com/types-of-cyber-attacks/ (accessed on 20 February 2017).
14. Joubert, V. *Five Years after Estonia's Cyber Attacks: Lessons Learned for NATO?* Research Paper; Research Division, NATO Defense College: Rome, Italy, 2012; p. 76.
15. Nyblom, P.; Wangen, G.; Kianpour, M.; Østby, G. The Root Causes of Compromised Accounts at the University. In Proceedings of the 6th International Conference on Information Systems Security and Privacy, Valletta, Malta, 25–27 February 2020.
16. Abubakar, A.; Zadeh, P.B.; Janicke, H.; Howley, R. Root cause analysis (rca) as a preliminary tool into the investigation of identity theft. In Proceedings of the Cyber Security and Protection Of Digital Services (Cyber Security), 2016 International Conference, London, UK, 13–14 June 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 1–5.
17. Collmann, J.; Cooper, T. Breaching the security of the Kaiser permanente internet patient portal: The organizational foundations of information security. *J. Am. Med. Inf. Assoc.* **2007**, *14*, 239–243. [CrossRef] [PubMed]
18. Wen, S.F.; Kowalski, S. A Case Study: Heartbleed Vulnerability Management and Swedish Municipalities. Human Aspects of Information Security, Privacy and Trust. In Proceedings of the International Conference on Human Aspects of Information Security, Privacy, and Trust, Vancouver, BC, Canada, 9–14 July 2017; Springer: Cham, Switzerland, 2017; pp. 414–431.
19. Teradata. *Big Data Analytics in Cyber Defense*; Ponemon Institute Research Report; Ponemon Institute LLC: Traverse City, MI, USA, 2013.
20. Allen, M. *Social Engineering: A Means to Violate a Computer System*; The SANS Institute: Bethesda, MD, USA, 2006.
21. Al-Shurman, M.; Yoo, S.M.; Park, S. Black Hole Attack in Mobile Ad Hoc Networks. In Proceedings of the ACMSE'04, Huntsville, AL, USA, 2–3 April 2014.
22. Derbyshire, R.; Green, B.; Prince, D.; Mauthe, A.; Hutchison, D. An Analysis of Cyber Security Attack Taxonomies. In Proceedings of the 2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), London, UK, 23–27 April 2018; pp. 153–161. [CrossRef]
23. Kee, J.; Deterding, B. *Social Engineering: Manipulating the Source*; SANS Institute InfoSec Reading Room; The SANS Institute: Bethesda, MD, USA, 2008.

24. Honan, B. Ubiquity Networks Victim of $39 Million Social Engineering Attack. August 2015. CSO from IDG. Available online: http://www.csoonline.com/article/2961066/supply-chain-security/ubiquiti-networks-victim-of-39-million-social-engineering-attack.html (accessed on 19 February 2021).
25. Brower, J. *Which Disney Princess are YOU? 2010: (Web 2.0) Social Engineering in Social Networks*; The SANS Institute: Bethesda, MD, USA, 2010.
26. Manjak, M. *Social Engineering Your Employees to Information Security*; SANS Institute InfoSec Reading Room, The SANS Institute: Bethesda, MD, USA, 2006.
27. King, R. Cyberattackers Target 19,000 French Websites in Wake of Charlie Hebdo. *The Wall Street Journal*, 15 January 2015. Available online: http://blogs.wsj.com/cio/2015/01/15/cyberattackers-target-19000-french-websites-in-wake-of-charlie-hebdo/ (accessed on 23 October 2021).
28. Jakobsson, M. *The Human Factor in Phishing*; School of Informatics, Indiana University at Bloomington: Bloomington, IN, USA, 2007. Available online: https://www.usenix.org/legacy/event/sec07/tech/jakobsson.pdf (accessed on 21 December 2020).
29. McMillan, R. Was this the email that took down RSA? A Spear Phishing Email That Has Surfaced in a Security Database Looks Like It may Have Been the One to Hit RSA. *IDG News Service*, 26 August 2011. Available online: http://www.networkworld.com/article/2180520/malware-cybercrime/was-this-the-email-that-took-down-rsa-.html (accessed on 23 October 2021).
30. Anderson, M. How Not to Be Sony Pictures. *IEEE Spectrum*, 11 December 2014. Available online: http://spectrum.ieee.org/riskfactor/telecom/security/how-not-to-be-sony-pictures (accessed on 29 July 2018).
31. Calia, M.P.F. Chang's Says Data Breach Affected 33 Locations. *The Wall Street Journal*, 4 August 2014; Tech 1-3. Available online: http://www.wsj.com/articles/p-f-changs-says-data-breach-affected-33-locations-1407159131 (accessed on 23 October 2021).
32. Schwartz, J.M. Epsilon Fell to Spear-Phishing Attack. Information Week. 2011. Available online: http://www.darkreading.com/attacks-and-breaches/epsilon-fell-to-spear-phishing-attack/d/d-id/1097119? (accessed on 20 March 2019).
33. Clayton, M. Exclusive: New Thesis on How Stuxnet Infiltrated Iran Nuclear Facility. 25 February 2014. The Christian Science Monitor. Available online: http://www.csmonitor.com/World/Security-Watch/2014/0225/Exclusive-New-thesis-on-how-Stuxnet-infiltrated-Iran-nuclear-facility (accessed on 23 October 2021).
34. Villeneuve, N.; Bennett, J. *Detecting APT Activity with Network Traffic Analysis*; Trend Micro Incorporated. Research Paper; Trend Micro: Tokyo, Japan, 2012.
35. Beckerman, J. International Dairy Queen Confirms Data Breach. *The Wall Street Journal*, 9 October 2014; pp. 7–9. Available online: http://www.wsj.com/articles/international-dairy-queen-confirms-data-breach-1412891919 (accessed on 12 June 2019).
36. Reuters. Cyber attack could cost Sony studio as much as $100 million. *Technology News*, 10 December 2014.
37. Pfleeger, L.S.; Caputo, D.D. Leveraging Behavioral Science to Mitigate Cyber Security Risk. *Comput. Secur.* **2012**, *31*. [CrossRef]
38. Robinson, W.S. *Corporate Espionage 201*; Version 1.0; SANS Institute InfoSec Reading Room, The SANS Institute: Bethesda, MD, USA, 2007.
39. Mclean, R. Hospital Pays Bitcoin Ransom after Malware Attack. 2016. CNN Money, New York. Available online: http://money.cnn.com/2016/02/17/technology/hospital-bitcoin-ransom/ (accessed on 23 October 2021).
40. Kalige, E.; Burkey, D. A Case Study of Eurograbber: How 36 million Euros was Stolen via Malware. *Versafe* **2012**, *35*, 35–36.
41. Filkins, B. *The SANS 2013 Help Desk Security and Privacy Survey*; The SANS Institute: Bethesda, MD, USA, 2013.
42. Hartmann, K.; Steup, C. The Vulnerability of UAVs to Cyber Attacks—An Approach to the Risk Assessment. In Proceedings of the 2013 5th International Conference on Cyber Conflict, Tallinn, Estonia, 4–7 June 2013; NATO CCD COE Publications: Tallinn, Estonia, 2013.
43. Welch, C. Over 150 Million Breached Records from Adobe Hack Have Surfaced Online. *The Verge*, 7 November 2013. Available online: http://www.theverge.com/2013/11/7/5078560/over-150-million-breached-records-from-adobe-hack-surface-online (accessed on 1 February 2020).
44. Østby, G.; Berg, L.; Kianpour, M.; Katt, B.; Kowalski, S.J. A Socio-Technical Framework to Improve cyber security training: A Work in Progress. *CEUR Workshop Proceed.* **2019**, 1–3.
45. Kowalski, S.J. The SBC Model as a Conceptual Framework for Reporting IT Crimes. In Proceedings of the IFIP TC9/WG9. 6 Working Conference on Security and Control of Information Technology in Society on Board M/S Illich and Ashore, St. Petersburg, Russia, 12–17 August 1993.
46. Williams, R. Jennifer Lawrence hack: ICloud security explained. *The Telegraph*, 1 September 2014. Available online: http://www.telegraph.co.uk/technology/internet-security/11067563/Jennifer-Lawrence-hack-iCloud-security-explained.html (accessed on 17 November 2020).
47. Geraci, R. CEOs and Cyber Defense: The New Reality. *Bloomberg Business Week*, 2–5 November 2015.
48. Brumfield, B. Study: Hack Attack Aimed at ISIS' Opposition. 19 December 2014. CNN. Innovations. Available online: http://www.cnn.com/2014/12/19/world/meast/isis-opponents-malware-attack/ (accessed on 23 October 2021).
49. Colwill, C. Human factors in information security: The insider threat—Who can you trust these days? *Inf. Secur. Tech. Rep.* **2010**, *14*, 1–11. [CrossRef]
50. Kessler, C.G. Defenses Against Distributed Denial of Service Attacks. In *Computer Security Handbook*, 4th ed.; Wiley & Sons: Hoboken, NJ, USA, 2000. Available online: http://www.garykessler.net/library/ddos.html (accessed on 7 July 2018).
51. Zetter, K. Logic Bomb Set Off South Korea Cyberattack. *Cybersecurity Hacks and Cracks*, 21 March 2013. Available online: https://www.wired.com/2013/03/logic-bomb-south-korea-attack/ (accessed on 25 August 2020).

52. Marsan, D.C. 5 things Estonia did right in battling hacktivism: Being open, asking for help keys to snuffing out cyberattacks. *Network World*, 22 August 2007. Available online: http://www.networkworld.com/article/2294176/lan-wan/5-things-estonia-did-right-in-battling-hacktivism.html (accessed on 23 October 2021).
53. Kowalski, S. Do Computer Security Models Model Computer Crime: A Study of Swedish Computer Crime Cases. In Proceedings of the 5th Canadian Computer Security Symposium, Ottawa, ON, Canada, 12–14 May 1993.
54. Avecto Article. One Big Thing You Can Do to Mitigate Cyber Attacks. 2014. Available online: https://cdn2.hubspot.net/hub/333464/file-603003268-pdf/Avecto/Avecto-Article-Cyber-Security.pdf (accessed on 16 March 2020).
55. Bhattacharyya, A.; Banerjee, A.; Bose, D. *Different Types of Attacks in Mobile ADHOC Network: Prevention and Mitigation Techniques*; Department of Computer Science & Engineering, Institute of Engineering & Management; Saltlake Publisher: Salt Lake City, UT, USA, 2011.
56. Kraemer, S.; Carayon, P.; Clem, J. Human and organizational factors in computer and information security: Pathways to vulnerabilities. *Comput. Secur.* **2009**, *28*, 1–12. [CrossRef]
57. Chen, W.D. Man Charged with Sabotage of Computers. *The NY Times*, 18 February 1988; pp. 1–2. Available online: http://www.nytimes.com/1998/02/18/nyregion/man-charged-with-sabotage-of-computers.html (accessed on 23 October 2021).
58. Barrett, N. Penetration testing and social engineering: Hacking the weakest link. *Inf. Secur. Tech. Rep.* **2003**, *4*, 8.
59. Orosz, M. *Addressing Human Behavior in Cyber Security*; USC Information Sciences Institute: Arlington, VA, USA, 2010.
60. Waxer, C. The Top 5 Internal Security Threats. 2007. IT Security. Available online: http://www.itsecurity.com/features/the-top-5-internal-security-threats-041207/ (accessed on 16 March 2020).
61. SecureWorks Dell. *Advanced Threat Protection with Dell SecureWorks Security Services*; Dell SecureWorks: Atlanta, GA, USA, 2012.
62. Krombholz, K.; Hobel, H.; Huber, M.; Weippl, E. Social Engineering Attacks on the Knowledge Worker. In Proceedings of the 6th International Conference on Security of Information and Networks, Aksaray, Turkey, 26–28 November 2013.