Computer and Information Science; Vol. 14, No. 2; 2021
ISSN 1913-8989 E-ISSN 1913-8997
Published by Canadian Center of Science and Education

Cyber Security amid COVID-19

Hussin J. Hejase[1], Hasan F. Fayyad-Kazan[2], Ale J. Hejase[3], & Imad A. Moukadem[4]

[1] IEEE Senior Member, Senior Researcher, Prof. Business Administration, Beirut, Lebanon

[2] Department of Management of Information Technology, Al Maaref University, Beirut, Lebanon

[3] AKSOB, Lebanese American University, Beirut, Lebanon

[4] Department of Computer Science, Al Maaref University, Beirut, Lebanon

Correspondence: Hussin J. Hejase, IEEE Senior Member, Senior Researcher, Prof. Business Administration, Beirut, Lebanon.

Received: January 6, 2021 Accepted: February 15, 2021 Online Published: March 10, 2021

doi:10.5539/cis.v14n2p10 URL: https://doi.org/10.5539/cis.v14n2p10

Abstract

COVID-19 pandemic obliged thousands of companies pertaining to all economic sectors to undergo the transformation from on-board work to working from home. Along such rush, the probability for companies being hacked incremented many folds. According to VMware cybersecurity strategist Tom Kellermann, quoted in Menn (2020), "There is a digitally historic event occurring in the background of this pandemic, and that is there is a cybercrime pandemic that is occurring" (para 5). In fact, Software and security company VMware Carbon Black declared during April, "that ransomware attacks it monitored jumped 148% in March from the previous month, as governments worldwide curbed movement to slow the spread of the novel corona virus" (Para 4). On the other hand, Anft (2020) reported that "more than 500 educational institutions, including colleges and K-12 schools, faced ransom attacks in 2019" (para 2). This paper uses a descriptive qualitative approach to shed light on the aforementioned subject depending on reported secondary literature about the topic, and offers an analysis to pinpoint weaknesses and barriers, as well as best practices to counterattack the breaches to cybersecurity in organizations. The outcomes serve as an eye opener for security officers in charge of the safety of organizational intellectual properties and stimulates organizations to adopt protection systems and safety practices.

Keywords: cybersecurity, APT, ransomware, pandemic, hacking, deterrence

1. Introduction

Cybersecurity has undoubtedly gained importance and has become a priority matter of both private and public concerns. The year 2020 witnessed an increase in cyberattacks and an increment of ransomware incidents that Marr (2020, para 1) asserts the critical role that cybersecurity plays in protecting the individual's privacy, rights, freedoms, and practices up to and including his/her physical safety. Moreover, with the advent of COVID-19 pandemic, there is an increase movement of global transformation of physical and vital infrastructure to online. The transformation to online is therefore more vulnerable and open to digital attacks, to data breaches (leak of personal information and ransomware) and up to cyberwar between countries and terrorism. The attacks are more persistent and the impact is bigger, and "there's an increasing awareness of political interference and state-sanctioned cyberattacks" (Marr, 2020, para 1). Furthermore, Menn (2020), quoting Tonya Ugoretz, a senior cyber official with the US Federal Bureau of Investigation (FBI), "that incoming reports about hacking had multiplied three- or four-fold during the outbreak" (para 7). Moreover, Rob Lefferts, a cybersecurity executive with Microsoft, said "the company was seeing an upswing in the volume of digital breaches in the same places the disease was spreading the most quickly" (ibid, para 7).

The situation is actually very serious as Milkovich (2020) reports that since COVID-19 emergence, the "FBI reported a 300% increase in reported cybercrimes" (para 6) and consequently "approximately $6 trillion is expected to be spent globally on cybersecurity by 2021" (para 9), especially knowing that the "connected Internet of Things (IoT) devices will reach 75 billion by 2025" (para 10). Forsdick & Lawrence (2020) agree to the aforementioned and add that "the mass switch to remote working, a hike in opportunistic cyber-attacks and tighter budgets have all contributed to the challenges of today's IT security chiefs. Chief information security officers (CISOs) have faced more disruption than most as a result of the Covid-19 crisis" (Para 1-2). On the other hand, the opportunity of working from home has become popular by many. In fact, Choudhury's (2020)

research added insight by answering the question "Do we really need to be together, in an office, to do our work? (p. 1)." During the pandemic lockdowns, according to Choudhury, "We learned that a great many of us don't in fact need to be co-located with colleagues on-site to do our jobs" (p.1). However, such move brought forward multiple security challenges. According to Forsdick & Lawrence (2020), "It's no longer a case of protecting the office network; now every employee's home offers a new entry route for potential cyber-attacks" (para 2). As a consequence, cyber-criminals jumped into the opportunity. In fact, the "IT security service company Barracuda Networks recorded a 600% spike in opportunistic phishing attacks during the first few months of the pandemic" (ibid, Para 3). Hence, as long as the pandemic continues around the globe, cybersecurity problems will build-up to cause continuous economic problems at thousands of companies, which have led and will continue to lead to reduced budgets and the need to preserve cash.

The objective of this paper is threefold:

1. Shed light on the status-quo of cybersecurity.
2. Expose best practices to build resilience against cyberattacks.
3. Explore the implications to stakeholders.

This paper consists of five sections. The first section introduces the background and objectives of the paper. A review of theoretical models is presented in the second section of the article. What was done in this part was a comprehensive study of related theoretical models based on which one may examine and support the main variables from different perspectives including behavioral (trust), attitudinal (organizational motivation, technology acceptance), governance (agency theory), and technical (advanced persistent threats). In the third section, the methodology of the paper is covered. The fourth section is pursuing the main goal of the paper: assessing the status quo of cybersecurity based on statistical facts reported from many well- known sources about ICT progress and the recurring security issues which accompany such progress. The statistical evidence is validated by extracting the facts from original sources. In the last section, conclusion and recommendation are offered as a base that may support interested policy making parties.

2. Theoretical Foundations

Information and Communications Technology (ICT) pervades billions of lives across the globe. Tables 1 and 2 depict the latest statistics on internet users and social media players worldwide. Such data is necessary to stress both the importance of ICT and the human element in the role of creating awareness for cybersecurity and in the planning of security policies to deter hackers and other malicious players around the globe. Furthermore, the aforementioned are fundamental to justify relying on theoretical foundations to deal with cybersecurity issues. In fact, Geers (2011) stresses the fact that "a reliable connection to the Internet is more important than the power of one's computer and provides infinitely greater utility to the user" (p. 20).

Table 1. Internet Users Globally

• There are 4.66 billion internet users in the world today. • The global number of internet users grew by 321 million in the period 2019-2020, that is, at an annual rate of 7% or more than 875 000 new users each day. However, such growth is higher in many developed countries. • The average worldwide internet user spends about 7 hours online daily. • Overall, the global internet users, in the year 2020, will spend more than 1.3 billion years of human time online.

Source: Datareportal, 2020 (October).

Table 2. Social Media Users Globally

• There are 4.14 billion global social media users today – a 60% of globe's population (Kemp, 2020). • The number of global social media users grew by 453 million in the period of 2019-2020. • The global growth of social media users is at a rate of about 12 percent per year. • A social media user has, on the average, an account on 8.3 different social platforms. • Kemp (2020) citing GlobalWebIndex, reports that the average global user spends 2 hours and 24 minutes on social media each day, which adds up to more than 10 billion hours every day.

Source: Datareportal, 2020 (October).

Furthermore, Geers (2011) stresses the strategic outlook of the connected world emphasizing "Together, computers and computer networks offer individuals, organizations, and governments the ability to acquire and exploit information with unprecedented speed. In business, diplomacy, and military might, this translates into a competitive advantage, suggesting that brains will beat brawn with increasing frequency over time and that computer resources will continue to play a central role in future human conflict" (p. 20). However, over time, the criminalization of ICT systems' use has led to a serious threat of the security of data. In addition, Baronienė & Žirgutis (2017) warn that "Globally growing trend of cyber security incidents, increasing cyber-attacks statistic data shows growing level of concern at the international and at the national level" (p. 454).

Next, an exposition of theories related to curbing malicious behavior and instigating the good use of ICT is presented.

2.1 Trust Management

Organizations pertaining to all economic sectors are enabled by ICT systems. In addition, as organizations find themselves within certain business ecosystems, the complexity of relations increases, as well as the need to trust the security of the transactions that occur and which leads to closures of business deals or simply taking decisions about the innovation, evolution and continuity of the organizations themselves. According to Moore (2006), business ecosystems act as a booster to organizational inter-relations in the markets whereby managers capitalize on business ecosystems to "coordinate innovation across complementary contributions arising within multiple markets and hierarchies within an agenda for co-evolution" (Moore, 2006, p. 2). Furthermore, Moore contends that the aforementioned "complementary advances often must co-evolve across company lines because no one firm has all of the required specialized knowledge and managerial resources necessary for the whole system" (p. 2). The scenario described above necessitates consistent and a high conservation of trust and security among the different ecosystem partners. On this matter, Waidner (2005), Head of the IBM Privacy Research Institute at the Zurich Research Lab, relates the world of business to the world of computer science. According to him, the business perspective of security is related to risk management. Consequently, an ICT system provides the adequate security if it keeps the risk for the business at an acceptable and handled level. Business risk is concerned about the "potential losses due to malicious acts by disgruntled employees, criminal hackers or terrorists" (p.3). Though, accepting a risk and its level or not is a matter of a business decision. As for computer science role, is in its potential and mitigation efforts of the challenges presented on "How to describe the risk level and how to demonstrate that an ICT system meets that level" (p. 3).

Based on the concept of ecosystems, the dependencies between enterprises are rapidly growing. And, an increasing number of enterprises with different specializations, need to cooperate to provide a specific service. Consequently, making ICT systems more secure and actually more challenging and difficult than ever, especially that dependencies between enterprises is more complex and more dynamic in time. As a result, Waidner (2005, p. 2) asserts that the security boundaries between enterprises are further less strict. "Back-end servers that were carefully protected earlier through multiple protection layers are now directly exposed to the outside, as these servers offer services to many different enterprises" (p.2). Moreover, according to Waidner, "applications that used to run on dedicated servers now run on a virtual, shared infrastructure, using physical resources that might be spread worldwide" (p. 2).

Trust management, according to Blaze et al. (2009, p.44), is a fundamental requirement for business communication policy among system elements, being within one company or multiple companies' ecosystem, and demands careful checking and validation against specified policies of all credentials for access to all virtual private service resources.

Moreover, Blaze et al. (2009), believe that the Global Information Grid (GIG), [a joint ongoing effort by the US Department of Defense and Intelligence Community] architecture is a platform that encourages the studying of trust in "large-scale computing in general, not just in the military and government" (p. 44). However, Blaze et al. show their concern for the fact that "there is no unified policy-based mechanism through which to scalably handle access control, intrusion detection, and other recovery mechanisms consistently across a large distributed system" (p. 49). Consequently, Zhang and Joshi (2009, p. 422), based on their concern to have secure interoperation among different independent systems, recommend the creation of multidomain security policy which will mitigate the conflicts in policy specification and integration, policy analysis as per validation and correctness among individual as well as integrated policies, and conflict resolution.

2.2 Protection Motivation Theory (PMT)

According to Rogers (1975, 1983), PMT encourages and motivates individuals to react in a protective way towards a perceived threat. PMY was developed for the health promotion and disease prevention sector. PMY

consists of four pillars: (1) "threat appraisal", (2) "coping appraisal", (3) "response efficacy" –and (4) "self-efficacy." The first estimates the threat scale, the second appraises and understands the threat, the third identifies process to mitigate the threat, and the fourth motivates individual's own ability to implement the required actions to mitigate the threat. Maddux and Rogers (1983) found self-efficacy to be "the most powerful predictor of behavioral intentions" (p. 476) that precede actual behavior. And PMT can be applied to "any threat for which there is an effective recommended response that can be carried out by the individual" (Floyd, Prentice-Dunn & Rogers, 2000, p. 409). Furthermore, Bavel et al. (2019) and Briggs et al. (2019) assert that PMT can be used in the design of directed motives to improve an individual's behavior when dealing with online security. According to Bavel et al. (2019), PMT posits that two appraisal processes are carried out when people are facing a threatening event. the first is focused on the threat itself (appraisal) and the second is directed toward the ability to act against that threat (coping). The aforementioned "affects their intention to take precautionary action and results in adaptive or maladaptive behaviors vis-à-vis the threat" (p. 30). Moreover, Sommestad, Karlzén & Hallberg (2015) researched how to apply PMT to assess how its efficacy is influenced by the information security behavior it is applied to. Indeed, it explains information security behavior better if three conditions exist: the first is when: the individual's behavior is voluntary, the second is to what extent the "threat and coping" method is concrete or specific, and the third is when information security threat is directed to the individual him/herself. However, Westcott, Ronan, Bambrick & Taylor (2017, p. 3) believe that a robust self-efficacy is more likely to motivate protective action timeliness, to influence the magnitude of responsiveness to information, and to promote the plausibility of taking effective remedial action.

2.3 Technology Acceptance Model (TAM)

Davis, Bagozzi & Warshaw (1989) contend that TAM has been adapted from the Theory of Reasoned Action (TRA) regarding beliefs, attitude, intention and behavior for modeling user acceptance of information systems. Worth noting that TRA is a social psychology model that examines the key determinants of intended behaviors. According to TAM, an individual's performance of a particular behavior is determined by his/her behavioral intention to perform the behavior and behavioral intention is determined by multiple factors including a person's attitude and subjective norms (Davis et al., 1989).

Jones et al. (2010) suggest that the "basic premise of the Technology Acceptance Model is that the more accepting users are of new systems, the more they are willing to make changes in their practices and use their time and effort to actually start using the system" (p. 10). Davis (1989) posited that the perceptions of ease of use and usefulness were key indicators of consumer's intention to adopt a new technology. Along this premise, Jones et al. (2010) found in their research that top management commitment and training the end-users will promote employee adoption, use and compliance with the corporate information systems security measures and to encourage positive attitudes toward these measures (p. 14). On the other hand, Seuwou et al. (2016) assert that "on several instances, users are not willing to use information systems which if used will produce remarkable performance gains" (p. 2). Therefore, user acceptance is essential and a critical success factor in achieving either failure or success of any IT project including IT security practices. In fact, according to Shim (2015), "The security of information systems is compromised if a firm's employees are poorly motivated and do not properly act to keep up with new security patches and updates in the erroneous believe that they are already well-protected through the deployment of technical security solutions. In this case, even if firms employ various technical security controls, strong information security cannot be achieved without addressing a moral hazard problem" (p. 11).

2.4 Agency Theory

Agency theory, according to Eisenhardt (1989), is concerned with the universal and pervasive "agency relationship" in which a person of authority (i.e., the principal: the board, a manager, or a supervisor among others) assigns tasks to another person or persons (i.e., the agent: a manager, a supervisor, an employee among others). Actually, what triggers the agency problem is the conflict of interest between the principal (i.e., the Board) and the agent (i.e., Management) in terms of delegated tasks or work from the principal to the agent. This occurs because the aforementioned parties (the principal and the agent) may have differing levels of risk acceptance. For example, Posthumus & von Solms (2008) explain the case in terms of IT-related decisions, that is when the board (principle) questions and may not be able to verify the management (the agent) decisions and actions to effectively portray the best interests of the organization. The authors believe that the aforementioned "may be due to moral hazard and adverse selection, explained through agency theory. Moral hazard may occur because the board may not necessarily be involved in ensuring that IT delivers its said value. Additionally, adverse selection may occur because the board may not know the full degree of the organization's reliance on IT" (ibid, p. 689). Even more, according to Shim (2015), based on the Agency theory (or principal-agent (P-A)

theory), "the low effectiveness of security measures might be the outcome of moral hazard, which results in suboptimal efforts of users to maintain IT systems appropriately" (p. 1). Therefore, the observed ineffectiveness is detected by the Agency theory identifying conflicting issues of cooperating parties and having conflicting goals. For example, Herath & Rao (2009) explained inadequate cyber-security from a P-A perspective and argued that security measures are ineffective due to misaligned incentives and moral hazard of employees.

The conflict between board and management, if continuous, hinders the outcomes of the Internet-based applications and services, which have greatly helped accelerate technological and organizational innovation, and become a main source of vulnerability (Shim, 2015). In addition, bringing the conflict down the hierarchies of command will lead that potential gains from Internet-based technological innovation to be partially offset by significant losses from cyber-security incidents (Hovav and Han, 2013).

2.5 Advanced Persistent Threats (APT)

Rouse (2020), Khan and Khan (2019) and Gonzalez (2014) define an advanced persistent threat (APT) as a long term and directed cyberattack in which an intruder (unauthorized person) succeeds to penetrate a network whereby he/she remains there undiscovered for a long period of time.

Hejase, Fayyad-Kazan and Moukadem (2020) warn that the field is open to advanced persistent threats (APTs) whereby the outcomes may become very costly to all institutions and governments across the globe. In fact, Positive Technology Security (2019) reports that "Gartner estimates that worldwide expenditures on digital security will exceed $124 billion this year (2019). But attackers rarely give up on a target even if their first attempts are unsuccessful" (para 1). Moreover, FireEye statistics (2019), report that "64% of companies attacked in 2018 were attacked again in the following 19 months" (p. 10).

Accordingly, APTs are complex cyberattacks that use multi-stage techniques to target and compromise systems that often go undetected for months (Hejase et al., 2020, p. 1, citing Rouse, 2020 and Gonzalez, 2014). Therefore, it is a highly challenging task to exactly estimate APT cyberattack costs. in fact, Positive Technology Security (2019), contends that "One reason is the difficulty of putting a value on the unique software used by criminal groups" (para 5). However, Table 3 herein provides an example of APT costing.

Table 3. Cost of an APT Attack

• 90% of the APT groups use "Spear Phishing" as an effective way to penetrate a company's internal network. The cost of tools used in the creation of malicious attachments (not including the cost of exploits for "zero-day vulnerabilities"), cost about two thousand US dollars. • A cost ranging from USD8000 to USD40 000 is incurred after penetrating the internal network. 50% of APT groups use legitimate administration tools and commercial penetration testing software. • Starting at an estimate of USD55 000 is the cost of the tools needed for a banking attack. • Much more expensive campaigns like cyberespionage would cost at least USD500 000 to start.

Source: Positive Technology Security (2019, Para 5).

Security Magazine (2017) citing Michel Cukier, Clark School assistant professor and an affiliate of the Clark School's Center for Risk and Reliability and Institute for Systems Research, asserts that "Often intruders set up 'back doors'—undetected entrances into the computer that they control—so they can create 'botnets' for profit or disreputable purposes" (para 9). According to a study by Michel Cukier, "A botnet is a collection of compromised computers that are controlled by autonomous software robots answering to a hacker who manipulates the computers remotely. Botnets perpetrate fraud or identity theft, disrupt other networks, and damage computer files, among other things" (University of Maryland, 2021, para 9). Indeed, Jeun, Lee and Won (2012), confirm that APT cyberattacks are sophisticated and advanced, that even organizations equipped with most advanced cyber defenses are unguarded and at risk. For example, well-known corporations like Google, Adobe Systems, Juniper Networks and Symantec were all victims of an APT attack called Operation Aurora (Fortinet, 2013; Radzikowski, 2015; Khan and Khan, 2019; Matthews, 2019). On the other hand, Hutchins, Cloppert and Amin (2011) contend that defenders against APTs can generate metrics to build systems' resiliency by measuring the performance and effectiveness of defensive actions against the cyberattacks and intruders.

3. Methodology

This paper uses a qualitative descriptive research approach based on secondary data. Due to the sensitivity of the topic and the abundant sources of specialized reports online and the continuous generation of research on

cybersecurity. The authors had to first review the reports and blogs and from there seek the original sources of the primary data exposed. This way, the authors accessed the original statistics as well as the newer information provided whereby analytical arguments are presented. Furthermore, reported primary data from interviews with experts on cybersecurity were also used to validate the facts being discussed. Therefore, data were collected for this research from books, journals, magazines and Internet websites. According to Ghauri & Gronhaug (2005), "research design correlates with the choice of strategy to be implanted in collecting the data needed to answer the stated research objective" (p. 31). Furthermore, Hejase & Hejase (2013) contend that using descriptive research is highly suitable for structured problems, that is well understood and documented. An inductive analysis is performed on the secondary data collected to build up a status-quo platform based on theoretical models as foundation and then based on the content supported with latest statistical facts, mitigation scenarios are presented and best practices are brought forward.

4. Statistical Facts and Discussion

This section includes reported statistics that support the objective of this paper and provide a clear view of the cybersecurity field (as a whole) along with the overall impact of cyberattacks. For this purpose, based on Sobers' (2020) report and adding to it the specific references, this section presents a compilation of facts reported from a number of valid and scientifically supported sources. Reported statistics are organized in a set of Tables 4-8 and Figures 1-3 for the sake of clarity and organization.

Table 4. Cyberattacks and Cybersecurity

- Kim et al. (2018) from Gartner Research report that the forecasted worldwide information security market is to reach $170.4 billion in 2022.
- Cybint Solutions found that 64% of companies have experienced web-based attacks. 62% experienced phishing & social engineering attacks. 59% of companies experienced malicious code and botnets and 51% experienced denial of service attacks in 2018 (Milkovich, 2020).
- According to Bissell et al. (2019) quoting Accenture: 68% of business leaders assert an increase in their cybersecurity risks, a 67% increase of security breaches (2014-2019) and a 72% increase in cybercrime in the same period.
- There is an increase in the average annual cost of cybercrime (see Figure 1) (Bissell et al., 2019).
- There is an increase in the average annual cost of cybercrime by country (see Figure 1) (Bissell et al., 2019).
- There is an increase in the average annual cost of cybercrime by type (see Figure 2) (Bissell et al., 2019).
- RiskBased Security reports that Data breaches exposed 4.1 billion records in the first half of 2019 (Cyber Risk Analytics, 2020).
  - The number of records exposed in the first quarter of 2020 skyrocketed to 8.4 billion - a 273% increase compared to the same period in 2019 and the most records exposed in any first quarter period since the company began tracking data breaches in 2005.
  - Based on the above, about 70% of reported breaches were due to unauthorized access to systems or services, while about 90% of the records exposed were attributable to exposing/publishing data online.

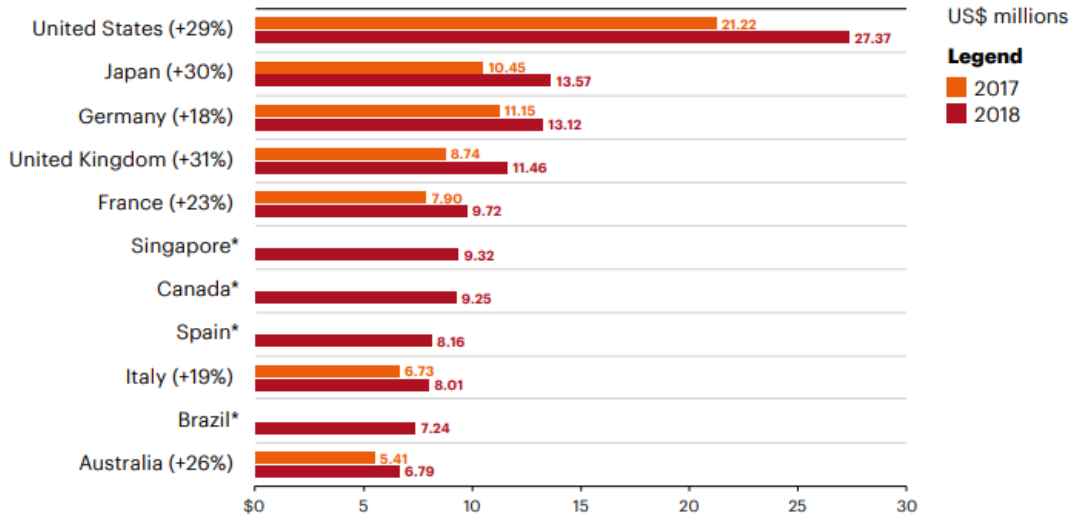

Figure 1. The average annual cost of cybercrime by country (% increase)

(Source: Bissell et al., 2019, p. 13)

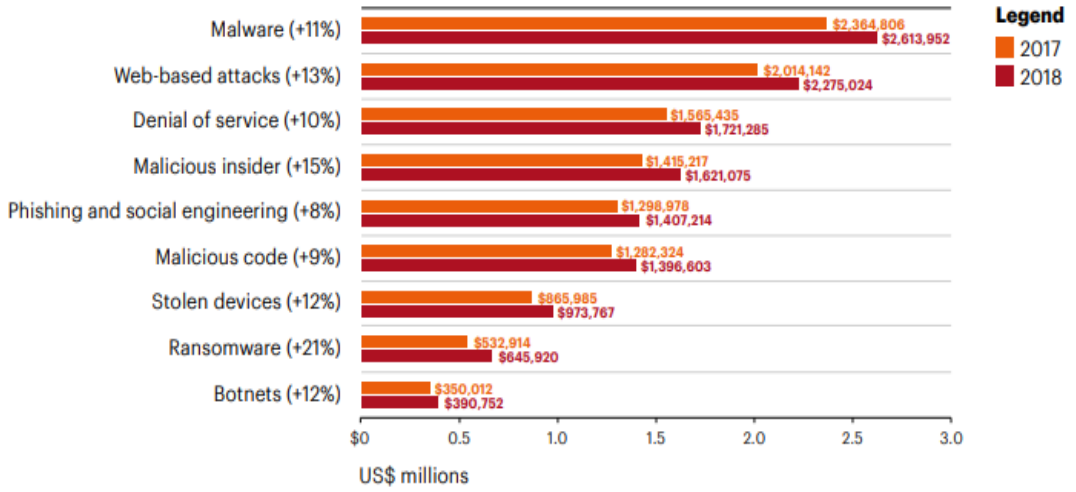

Figure 2. Average annual cost of cybercrime by type of attack (2018, total = USD13.0 million)

(Source: Bissell et al., 2019, p. 17)

Table 5. Cyberattacks and Cybersecurity

• Verizon (2020) reports that breaches were classified as follows; Financially motivated (86%), 43% web applications (43%), stolen or used credentials (37%), malware/ransomware (27%), phishing (22%), and 25% were motivated by espionage. Furthermore, Verizon reports: - Hacking is featured in 45% of breaches, while malware accounted for 17% and phishing or social engineering amounted to 22%, respectively. - Breaches related to the cryptocurrency mining malware are accounted for as follows: 2.5% of malware among breaches and only 1.5% of malware for incidents. About 10% of the organizations received cryptocurrency mining malware however, these were blocked at some point throughout the course of the year. • Kaplan (2020) quoting Semantec, the top malicious email attachment types are: .doc and .dot (both make up 37%) and .exe (19.5%, as next highest).

- According to Bluerock (2020), a Cyber Defense consultancy in Scotland, 46% of businesses and 26% of charities report having cybersecurity breaches or attacks in the year extending from August 2019 to August 2020. Moreover, 1 in 5 businesses lose money or data due to a breach or attack.
- John et al. (2020) confirm that there has been a change in the nature of cyberattacks since 2017. Over this year, phishing attacks increased from 72% to 86%, viruses or other malware decreased from 33% to 16% (see Figure 3).

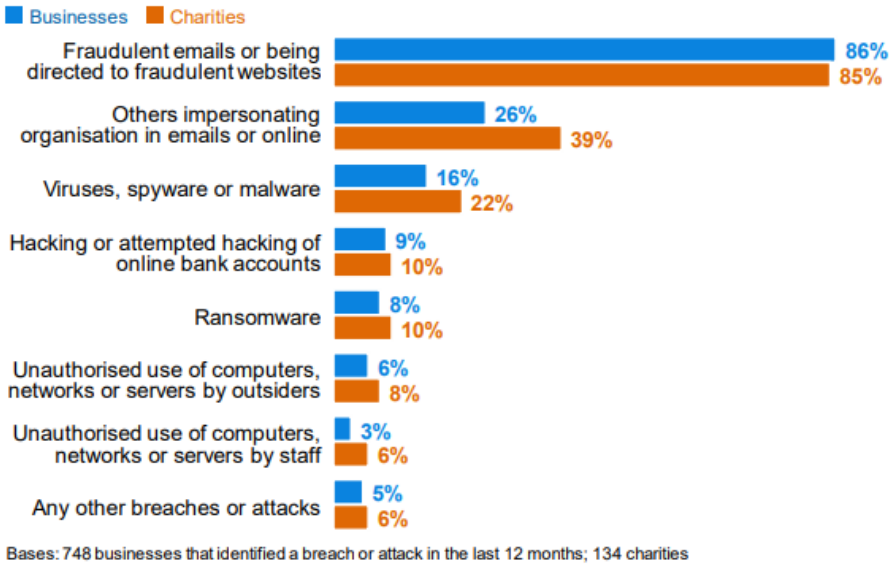

Figure 3. Percentage of identified types of breaches or attacks in the last 12 months (2019-2020)

(Source: Johns et al., 2020, p. 36)

Table 6. Cyberattacks and Cybersecurity: IT Professionals Voice

- 92% of IT professionals give a vote of no trust to their organizations as for their preparation to offer public cloud services security. Also, 75% of IT professionals view the public cloud as more secure than their own data centers.
- About 80% of IT professionals say that recent data breaches experienced by other businesses have motivated and increased their organization's focus on securing data moving forward.
- 78% of organizations use more than 50 discrete cybersecurity products to address security issues and 37% use more than 100 cybersecurity products.
- Organizations which discovered misconfigured cloud services experienced 10 or more data loss incidents in the last year.
- 59% of organizations shared that employees with privileged cloud accounts have had those credentials compromised by a spear phishing attack.

Source: Security Magazine, 2020.

Table 7. Cyberattacks and Cybersecurity: Employees Behavior

- According to Securonix, roughly 80% of dissatisfied employees (and therefore leaving the organization) will try to take proprietary data with them.
- 43.75% of employees or other internal entities forwarded content to personal emails.
- 16% abused collaboration privileges (including cloud).
- 10% performed downloads of aggregated data (including data on analyzed attacks).
- Unauthorized removable storage devices (USB, external hard disk, …) are also used to swipe data.

Source: Osborne, 2020.

Table 8. Cyberattacks and Cybersecurity: End Users Practices

- A Google (2019) survey found that at least 65% of people reuse passwords across multiple sites.
- Based on LastPass (2019) survey, 91% of respondents claim to understand the risks of reusing passwords across multiple accounts, but 59% admitted to practicing it anyway.
- Microsoft (2020) announced that 44 million accounts were subject to takeover due to compromised or stolen passwords.
- LastPass (2019) report finds that an employee reuses, on the average, each password as many as 13 times. Also, Jacobson (2020) reports 14 times.
- According to Jacobson (2020), 72% of persons reuse passwords in their personal life while about 50% of employees perform very simple change to their company passwords (change or add a digit or character) when updating every 90 days. A fact that keeps the threat.
    - 73% of end users utilize same passwords in both their work and personal accounts.
    - Unauthorized removable storage devices are commonly used to swipe data
    - 81% of hacking is related to weak passwords.
- Security Magazine (2019) found that 76% of millennials recycle their passwords.

4.1 Facets of Cybersecurity

There are many important facets to cybersecurity, which are covered in Table 9.

Table 9. Facets to cybersecurity

No. of Facets	The Facets	Reference
5	**Cyber targeting** "Kill Chain" (1) Positive identification of targets, (2) Location of targets, (3) Attribution of attack, (4) Capability/target pairing, and (5) Assessment of potential collateral damage"	Smart (2011)
3	**Systems security** 1. Confidentiality 2. Integrity 3.Availability	Zissis & Lekkas (2012); Baronienė & Žirgutis (2017); Geers (2011)
3	**System Security** 1. Physical security 2. Cybersecurity 3. Security awareness	Coleman Technologies (2020)
3	**Systems security** 1.Education & Governance 2.Security Monitoring & Response 3.Data Management & Backup	Bluerock (2020)
5	**Data Security** 1. Malicious attacks 2. Unauthorized access 3. Unusual extraction 4. Unintended use 5. Unexpected dissemination	de Montcheuil, Yves (2015)
9	**Human Factor** 1. Security procedures 2. Information sharing 3. Security culture 4. Physical environments 5. Work loads 6. Passwords 7. Threat awareness 8. Personality 9. Incident management analysis	Ritchie (2019); Radzikowski (2015); Coleman Technologies (2020); Osborne (2020); Jacobson (2020)

Table 9 shows a sample of facets to cybersecurity, which represent the many different schemes adopted to face cyberattacks since these were detected. Different researchers concentrate on different aspects of the value-chain characterizing cyber security. According to Smart (2011), an updated United States Department of Defense Joint

Staff methodology 'JP 3-60' [Kill Chain] should "introduce the concepts of an adversary's cyber center of gravity and a cyberspace joint operations area. An adversary's cyber presence consists of computers, information systems, hardware, online personas and so forth, which may be geographically separated from his physical center of gravity. Once planners identify the cyber center of gravity (a critical point—a source of power for the adversary's cyber operations), they can target it" (p. 72).

Coleman Technologies (2020) used a three-phase approach as depicted in Table 9. The purpose is to mitigate and stop intrusions, continuously innovate upgrades and updates and patches that serve to take care of security issues intrinsic in the software solutions, using virtual private networks (VPNs), and perform a thorough and full security audit. Nevertheless, human capital awareness is a must with special emphasis Coleman Technologies, 2020) on: "password hygiene; data security practices; secure processes; access control standards; social media Use; and conformity to policies" (para 6). While if the concern is data security, then de Montcheuil (2015) proposed five concerns (also refer to Table 9) and recommended that system administrators must consider first the security breaches by the human factor, that is, keeping out persons with malicious intentions to gain access to data. Therefore, system administrators need to "deploy 'perimeter protection technologies', the proper management of user accounts and permissions [data access, extraction, use and dissemination] and a wide range of intrusion detection that detect attacks and shut down accesses when needed" (para 2).

As many researchers agree, the human factor within organizations must be the primary target for awareness and compliance (Ritchie, 2019; Radzikowski (2015); Coleman Technologies (2020); Osborne, 2020; and Jacobson, 2020). In fact, Human factors consultant Amanda Widdowson (quoted by Richie, 2019) contends that "In terms of cybersecurity, what is harder to control is the human element. You can control the technical aspect a bit more. Machines are a bit more predictable: you know what they are going to do. People — less so" (Para 2).

Capitalizing on the aforementioned facts and based on her experience helped her to develop an approach centered on human knowledge, she explains. "For part of my career I was involved in rail incident investigations for London Underground. I've essentially applied a knowledge of human error, how people's actions contribute to incidents — and how you can mitigate that — to cybersecurity" (Para 2). Consequently, from that perspective, "Widdowson defines a checklist of nine elements of human behavior that all tech leaders need to keep in mind. Crucially, these all relate to unintended harm caused by employees rather than deliberately malevolent acts but are no less important" (Para 5). Worth noting that when "organizations analyze security threats or breaches, they often do so from a technology perspective. However, a human factors approach should also be part of the toolbox. Moreover, even if such an expert is not available, individuals should always ensure they include a human factors checklist within their analytical framework" (Para 25-26). The aforementioned fits John et al.'s (2020) survey results about organizational response to disruptive breaches or cyberattacks in the UK. Figure 4 shows that the first step towards cybersecurity was providing additional staff training and communications.

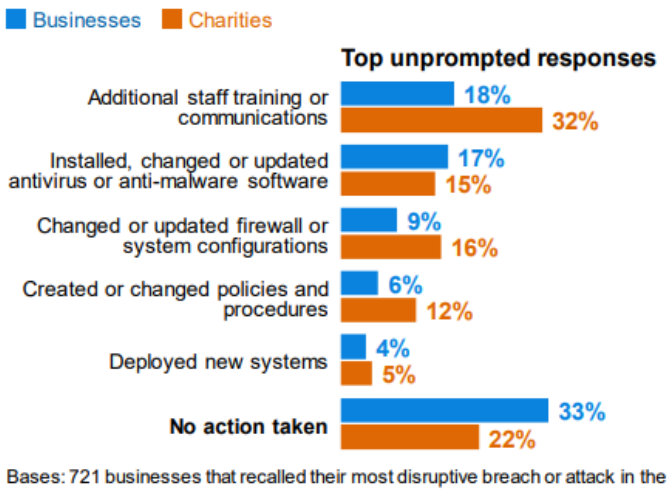

Figure 4. Percentage of organizations that have done proactive actions since their most disruptive breach or attack during the year of 2019-2020

(Source: Johns et al., 2020, p. 51)

5. Conclusion and Recommendation

Today's organizations will continue to monitor, detect and eliminate cyberattacks and intruders' threats provided proactive planning is practiced. Nevertheless, Radzikowski (2015) stresses the fact that as means and methods are available to within the hacker community, an increasing number of organizations will be victimized to targeted cyberattacks and suffer potentially irrecoverable losses.

Lymer (2013) warns since 2013 that the threat landscape has progressed from simple "script kiddies" to hackers to insiders to today's state-sponsored attacks, where organizations of all sorts are attacked because of "who they are, what they do and the value of their intellectual property (IP)" (para 2). On the other hand, James Holley, leader for Ernst & Young LLP's Information Security Incident Response services and co-author of the book "Responding to Targeted Cyberattacks" (ISACA, 2013), asserts that "There are no universal solutions to prevent being infiltrated," (Lymer, 2013, para 3). Furthermore, Holley contends that "In this rapidly evolving threat landscape, information security professionals need to adopt the mindset that their network is already compromised or soon will be" (para 3).

ISACA (2013) recommends five tactics every organization should know: (1) Supporting and developing the organizational human capital. Indeed, Microsoft (2020) stresses the fact that human resources are considered critical success factor, among others, in the risk management program of an institution.

2. Broader organizational attention. Cyberattacks are three-pronged problem: a business, a people, and a technology problem. Microsoft (2020) adds the "legal dimension" (p. 69).
3. Organizational success depends on increasing the end-user's awareness and education. the user education and awareness are critical to organizational success.
4. Organizational past prevention strategies are not enough for today's issues. Now-a-day's strategy needs to be: "Complicate – Detect – Respond – Educate – Govern."
5. The new strategy to face cyberattacks includes four emerging capabilities:

"a. Centralized log aggregation and correlation,

b. Ability to conduct forensic analysis across the enterprise,

c. Ability to sweep the enterprise for indicators of compromise,

d. Ability to inspect memory to detect malicious code" (para 4).

Organizations that perform "advanced incident response planning" can significantly improve their chances of early threat detection and assure more effective security solutions. The key to effective APT protection, detection, and response is robust implementation of security 'best practices' and offering continuous education to the organization's most liable users to breaches. However, it is critical that an organization have a strong awareness culture and having top management who are literate in technology as well as in information. Capitalizing on the aforementioned, the organization will be able to proactively mitigate threats against the organizational cybersecurity (Hejase et al, 2020). In fact, "administrators must learn how to use emerging technology effectively so that it actually provides additional protection" (Cobb, 2013, para 14). In addition, Hejase and Hejase (2015) stress the fact that a joint effort by the government, businesses and educational institutions should collaborate to at least start an awareness campaign that may "reach all ears in order to get the terms cyberwarfare, cyber-attacks, cybersecurity and cyber-weapons into the dictionary of everyday words, simply because the threat of a cyber-attack is ever present and will not go away" (p. 87).

Moreover, Howard and Olson (2020) recommend the implementation of an adversary playbook "to share threat intelligence with trusted partners in a meaningful and efficient way" (p. 68). In fact, and according to Howard and Olson, such adversary playbook "collates all known intelligence on the hacker groups' attack sequence: tactics, techniques, indicators of Compromise, attack time frame, and context about motivation as well as attribution" (p. 60). The aforementioned is to enforce the implementation of intrusion kill chain strategies. Finally, by adopting the adversary playbook construct, cyber intelligence practitioners can leverage actionable intelligence in a machine-readable format designed for the activities that are demonstrated in Table 10 herein.

Table 10. Actionable Intelligence Activities

• Intelligence collection and capture using an industry-accepted format. • Intelligence distribution by swapping information on adversary attack sequences in real time with trusted partners. • Intelligence consumption sharing with partners in a format and language that facilitates automatic processing. • DevSecOps security control deployment whereby network defenders understand the value of the DevSecOps infrastructure-as-code philosophy. • Defensive campaign design and deployment capitalizing on sharing, communication and action using the adopted adversary playbook concept.

Source: Howard and Olson, 2020, pp. 69-70.

References

Anft, M. (2020). An Emerging Threat: Ransomware. *The Chronicle of Higher Education*. Retrieved December 1, 2020, from https://connect.chronicle.com/CHE-CI-WC-2020-EmergingCyber-TrendsSnapshot-PaloAlto_LP-CHE.html

Baronienė, L., & Žirgutis, V. (2017). Cybersecurity Facets: Counterfactual Impact Evaluation of Measure "Procesas LT" in Enterprises of the IT Sector. *Journal of Security and Sustainability Issues, 6*(3), 445-456. https://doi.org/10.9770/jssi.2017.6.3(10)

Bavel, R., Rodr ́guez-Priegoad, N., Vilab, J., & Briggsc, P. (2019, March). Using Protection Motivation Theory in The Design of Nudges to Improve Online Security Behavior. *International Journal of Human-Computer Studies, 123*, 29-39. https://doi.org/10.1016/j.ijhcs.2018.11.003

Bissell, K., LaSalle, R., & Dal Cin, P. (2019). The cost of cybercrime. *Accenture.* Retrieved November 27, 2020, from https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50

Blaze, M., Kannan, S., Lee, I., Sokolsky, O., Smith, J. M., Keromytis, A. D., & Lee, W. (2009). Dynamic Trust Management. *Computer, 42*(2), 44-52. https://doi.org/10.1109/MC.2009.51

Bluerock. (2020, August 31). *Why multi-faceted cyber-attacks need a multi-faceted approach to cybersecurity*. Retrieved November 27, 2020, from https://bluerockcd.co.uk/latest-news/multi-faceted-approach-to-cyber-security/

Briggs, P., Jeske, D., & Coventry, L. (2017). Behavior change interventions for cybersecurity. In: Linda Little, Elizabeth Sillence and Adam Joinson (Eds.). *Behavior change research and theory: Psychological and technological perspectives*, 115-136. Academic Press: Elsevier Inc. https://doi.org/10.1016/B978-0-12-802690-8.00004-9

Choudhury, P. (2020). Our Work-from-Anywhere Future Best practices for all-remote organizations. *Harvard Business Review*, (November-December, 1-11. Boston, Massachusetts: Harvard Business Publishing.

Cobb, M. (2013, May). The evolution of threat detection and management. *Search Security*. Retrieved December 5, 2020, from https://searchsecurity.techtarget.com/tip/The-evolution-of-threat-detection-and-management

Coleman Technologies. (2020, May). *Three facets of security to focus on*. [Blog]. Retrieved November 25, 2020, from https://www.colemantechnologies.com/blog/three-facets-of-security-to-focus-on

Cyber Risk Analytics. (2020). 2020 Q1 Report data breach quick view. *Risk Based Security*. Retrieved November 28, 2020, from https://pages.riskbasedsecurity.com/en/2020-q1-data-breach-quickview-report

DatarePortal. (2020, October). *Digital around the world*. Retrieved December 1, 2020, from https://datareportal.com/global-digital-overview#:~:text=Roughly%204.66%20billion%20people%20ar

ound,twelve%20months%20to%20October%202020

Davis, F. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly, 13*(3), 319-340. https://doi.org/10.2307/249008

Davis, F., Bagozzi, R., & Warshaw, P. (1989). User Acceptance of Computer Technology: A Comparison of Two Theoretical Models. *Management Science, 35*(8), 982-1003. https://doi.org/10.1287/mnsc.35.8.982

de Montcheuil, Y. (2015, September 8). 5 facets of data security. *InfoWorld*. Retrieved November 25, 2020, from https://www.infoworld.com/article/2980728/5-facets-of-data-security.html

Eisenhardt, K. M. (1989). Agency Theory: An Assessment and Review. *Academy of Management Review, 14*(1), 57-74. https://doi.org/10.5465/amr.1989.4279003

FireEye. (2019). *M-trends 2019*. Retrieved February 8, 2021, from https://content.fireeye.com/m-trends/rpt-m-trends-2019

Floyd, D.L., Prentice-Dunn, S., & Rogers, R. W. (2000). A Meta-analysis of Research on Protection Motivation Theory. *J Appl Soc Psychol., 30*(2), 407-29. https://doi.org/10.1111/j.1559-1816.2000.tb02323.x

Forsdick, S., & Lawrence, J. (2020, October). Security's new normal: How CISOs are coping with pandemic challenges. *I–Global Intelligence for Digital Leaders program, Fujitsu*. Retrieved November 25, 2020, from https://www.i-cio.com/management/best-practice/item/adapting-to-a-new-security-environment-how-cisos-are-coping-with-the-challenges-of-covid-19

Fortinet. (2013). Threats on the horizon: The rise of the advanced persistent threat. *IT World Canada*. Retrieved December 2, 2020, from https://s3-us-west-2.amazonaws.com/itworldcanada/archive/Documents/whitepaper/ITW274A_Persistent_Threats.pdf

Geers, K. (2011). Strategic cyber security. *2011 NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)*. Retrieved December 1, 2020, from https://www.law.upenn.edu/institutes/cerl/conferences/cyberwar/papers/reading/Geers.pdf

Ghauri, P., & Gronhaug, K. (2005). *Research Methods in Business Studies, A practical Guide* (3rd ed.). Harlow, England: Pearson Education Limited.

Gonzalez, D. (2014). Internal and external risks. In: *Managing online risk: Apps, mobile, and social media security*, Pages 25-52. Butterworth-Heinemann. https://doi.org/10.1016/B978-0-12-420055-5.00002-5

Google. (2019, February). *Online security survey Google / Harris poll*. Retrieved February 10, 2021, from https://services.google.com/fh/files/blogs/google_security_infographic.pdf

Hejase, A. J., & Hejase, H. J. (2013). *Research methods, A practical approach for business students* (2nd ed.). Philadelphia, PA, USA: Masadir Inc.

Hejase, A. J., Hejase, H. J., & Hejase, J. A. (2015). Cyber Warfare Awareness in Lebanon: Exploratory Research. *International Journal of Cyber-Security and Digital Forensics (IJCSDF), 4*(4), 482-497. https://doi.org/10.17781/P001892

Hejase, H. J., Fayyad-Kazan, H. F., & Moukadem, I. (2020). Advanced Persistent Threats (APT): An Awareness Review. *Journal of Economics and Economic Education Research (JEEER), 21*(6), 1-8. Retrieved February 8, 2021, from https://www.abacademies.org/articles/Advanced-persistent-threats-apt-an-awareness-review-1533-3604-21-6-202.pdf

Herath, T., & Rao, R. (2009). Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness. *Decision Support Systems, 47*(2), 154-165. https://doi.org/10.1016/j.dss.2009.02.005

Hovav, A., & Han, J. (2013). The Impact of Security Breach Announcements on the Stock Value of Companies in South Korea. *Korean Internet e-Commerce Association, 13*(3), 43-67.

Howard, R., & Olson, R. (2020, Fall). Implementing intrusion Kill Chain Strategies: Creating Defensive Campaign Adversary Playbooks. *The Cyber Defense Review, 5*(3), 59-74.

Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011, January). Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. *Lockheed Martin Corporation*.

Retrieved December 4, 2020, from https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf

ISACA. (2013). *Responding to targeted cyberattacks*. ERNST & Young and ISACA. Rolling Meadows, IL, USA: ISACA.

Jacobson, K. (2020, on April 30). Scary statistics about the password reuse problem [Blog]. *Security Boulevard*. Retrieved December 2, 2020, from https://securityboulevard.com/2020/04/8-scary-statistics-about-the-password-reuse-problem/

Jeun, I., Lee, Y., & Won, D. (2012). *A practical study on advanced persistent threats. Computer applications for security, control and system engineering*. Berlin, Heidelberg: Springer, pp. 144-152. https://doi.org/10.1007/978-3-642-35264-5_21

Johns, E., Williams, H., Clark, L., Leggett, O., & Shah, J. N. (2020). Cyber security breaches survey 2020: Statistical release. *UK Department for Digital, Culture, Media and Sport and Ipsos MORI*. https://doi.org/10.1016/S1361-3723(20)30037-3

Jones, C. M., McCarthy, R. V., Halawi, L., & Mujtaba, B. (2010). Utilizing the Technology Acceptance Model to Assess the Employee Adoption of Information Systems Security Measures. *Issues in Information Systems, 11*(1), 9-16. https://commons.erau.edu/publication/310

Kaplan, Y. (2020, November 13). How to prevent your email from getting hacked. *Dunham Connect*. Retrieved December 3, 2020, from https://dunhamconnect.com/blog/how-to-prevent-your-email-from-getting-hacked

Kemp, S. (2020, January 30). *Digital 2020: 3.8 billion people use social media*. Retrieved February 7, 2021, from https://wearesocial.com/blog/2020/01/digital-2020-3-8-billion-people-use-social-media

Khan, W. Z., & Khan, K. M. (2019, September). Advanced persistent threats through industrial IoT on oil and gas industry. *Global Foundation for Cyber Studies and Research (GFCyber)*. Retrieved December 1, 2020, from https://www.researchgate.net/publication/335611873_Advanced_Persistent_Threats_Through_Industrial_IoT_On_Oil_And_Gas_Industry

Kim, E., Gardner, D., Deshpande, S., Contu, R., Kish, D., & Canales, C. (2018, September 14). Forecast analysis: Information security, worldwide, 2Q18 update. *Gartner Research*. Retrieved November 27, 2020, from https://www.gartner.com/en/documents/3889055

LastPass. (2019). *Global password use report, 3rd annual report*. Retrieved February 10, 2021, from https://www.lastpass.com/state-of-the-password/global-password-security-report-2019

Lymer, A. (2013, May 15). Five things every organization should know about detecting and responding to targeted cyberattacks. *Accounting Education*. Retrieved December 5, 2020, from http://www.accountingeducation.com/index.cfm?page=newsdetails&id=152472

Maddux, J. E., & Rogers, R. W. (1983). Protection Motivation and Self-Efficacy: A Revised Theory of Fear Appeals and Attitude Change. *J Exp Social Psychol, 19*(5), 469-79. https://doi.org/10.1016/0022-1031(83)90023-9

Marr, B. (2020, January 10). The 5 biggest cybersecurity trends in 2020 everyone should know about. *Forbes*. Retrieved November 27, 2020, from https://www.forbes.com/sites/bernardmarr/2020/01/10/the-5-biggest-cybersecurity-trends-in-2020-everyone-should-know-about/?sh=679eb0647ecc

Matthews, T. (2019, January 8). Operation aurora – 2010's major breach by Chinese hackers. *Exabeam*. Retrieved December 3, 2020, from https://www.exabeam.com/information-security/operation-aurora/

Menn, J. (2020, April 17). Hacking against corporations surges as workers take computers home. *Reuters: Technology News*. Retrieved December 1, 2020, from https://www.reuters.com/article/us-health-coronavirus-cyber-corporations/hacking-against-corporations-surges-as-workers-take-computers-home-idUKKBN21Z0Y6

Microsoft. (2020). *Microsoft digital defense report 2019*. https://doi.org/10.1016/S1353-4858(20)30114-8

Milkovich, D. (2020, June 20). *15 Alarming cyber security facts and stats*. Retrieved November 27, 2020, from https://www.cybintsolutions.com/cyber-security-facts-stats/

Moore, J. F. (2006, March). Business Ecosystems and The View of The Firm. *The Antitrust Bulletin, 51*(1), 1-58. https://doi.org/10.1177/0003603X0605100103

Osborne, C. (2020, May 20). 'Flight risk' employees involved in 60% of insider cybersecurity incidents. *Zero Day*. Retrieved December 3, 2020, from https://www.zdnet.com/article/flight-risk-employees-involved-in-60-of-insider-cybersecurity-incidents/

Positive Technologies Security. (2019, August 14). *Hack at all cost: putting a price on APT attacks*. Retrieved December 6, 2020, from https://www.ptsecurity.com/ww-en/analytics/advanced-persistent-threat-apt-attack-cost-report/

Posthumus, S., & von Solms, R. (2008). Agency theory: Can it be used to strengthen IT governance? In: IFIP international federation for information processing, volume 278; (Eds.) Sushil Jajodia, Pierangela Samarati, Stelvio Cimato. *Proceedings of the IFIP TC 11 23rd International Information Security Conference*, pp. 687-691. (Boston: Springer). https://doi.org/10.1007/978-0-387-09699-5_46

Radzikowski, S. (2015, October 8). *Cybersecurity: Origins of the advanced persistent threat (APT)*. Retrieved December 2, 2020, from http://drshem.com/2015/10/08/cybersecurity-origins-of-the-advanced-persistent-threat-apt/

Ritchie, R. (2019, September 2019). Human factors in cyber-security: nine facets of insider threat. *I–Global Intelligence for Digital Leaders program, Fujitsu*. Retrieved November 25, 2020, from https://www.i-cio.com/management/insight/item/human-factors-in-cyber-security-nine-aspects-of-insider-threat

Rogers, R. W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change. *J. Psychol, 91*, 93-114. https://doi.org/10.1080/00223980.1975.9915803

Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: a revised theory of protection motivation. J. Cacioppo, R. Petty (Eds.), *Social Psychophysiology*, New York: Guilford Press.

Rouse, M. (2020, August). Advanced persistent threat (APT). *Tech Target*. Retrieved November 28, 2020, from https://searchsecurity.techtarget.com/definition/advanced-persistent-threat-APT

Security Magazine. (2017, February 10). *Hackers attack every 19 seconds*. Retrieved December 1, 2020, from https://www.securitymagazine.com/articles/87787-hackers-attack-every-39-seconds

Security Magazine. (2019). *Majority of Americans recycle passwords up to four times*. Retrieved February 8, 2021, from https://www.securitymagazine.com/articles/90550-majority-of-americans-recycle-passwords-up-to-four-times

Security Magazine. (2020). *78% of organizations use more than 50 cybersecurity products to address security issues*. Retrieved December 2, 2020, from https://www.securitymagazine.com/articles/92395-of-organizations-use-more-than-50-cybersecurity-products-to-address-security-issues

Seuwou, P., E. B., & Ubakanma, G. (2016, January). User acceptance of information technology: A critical review of technology acceptance models and the decision to invest in information security. *Proceedings of the International Conference on Global Security, Safety, and Sustainability*. https://doi.org/10.1007/978-3-319-51064-4_19

Shim, W. (2015). Agency Problems in Information Security: Theory and Application to Korean Business. *The Journal of Internet Electronic Commerce Research, 15*(5), 1-15.

Smart, S. J. (2011). Joint Targeting in Cyberspace. *Air & Space Power Journal*, (Winter), 65-75. USAF. Retrieved December 2, 2020, from https://apps.dtic.mil/dtic/tr/fulltext/u2/a555785.pdf

Sobers, R. (2020, October 26). 110 Must-know cybersecurity statistics for 2020. *VARONIS*. Retrieved November 27, 2020, from https://www.varonis.com/blog/cybersecurity-statistics/

Sommestad, T., Karlzén, H., & Hallberg, J. (2015, January). A Meta-Analysis of Studies on Protection Motivation Theory and Information Security Behaviour. *International Journal of Information Security and Privacy, 9*(1), 26-46. https://doi.org/10.4018/IJISP.2015010102

University of Maryland. (2021). Hackers attack every 39 seconds. Retrieved February 8, 2021, from https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds

Verizon. (2020). *Data breach investigations report (DBIR) 2020*. https://doi.org/10.1016/S1361-3723(20)30059-2

Waidner, M. (2005, October). Security and trust management. *European Research Consortium for Informatics and Mathematics (ERCIM), number 63*. Retrieved December 1, 2020, from https://www.ercim.eu/publication/Ercim_News/enw63/EN63.pdf

Westcott, R., Ronan, K., Bambrick, H., & Taylor, M. (2017). Expanding Protection Motivation Theory: Investigating an Application to Animal Owners and Emergency Responders in Bushfire Emergencies. *BMC Psychol, 5*, 2-14. https://doi.org/10.1186/s40359-017-0182-3

Zhang, Y., & Joshi, J. (2009). Access Control and Trust Management for Emerging Multi-domain Environments. *Annals of Emerging Research in Information Assurance, Security and Privacy Services.* S. Upadhyaya and R.O. Rao, eds., Emerald Group Publishing, 2009, pp. 421-452.

Zissis, D., & Lekkas, D. (2012, March 3). Addressing Cloud Computing Security Issues. *Future Generation Computer Systems, 28*(3), 583-592. https://doi.org/10.1016/j.future.2010.12.006