https://doi.org/10.48009/3_iis_2019_139-150

Issues in Information Systems
Volume 20, Issue 3, pp. 139-150, 2019

CYBERSECURITY INERTIA AND SOCIAL ENGINEERING: *WHO'S WORSE, EMPLOYEES OR HACKERS?*

Debra J. Borkovich, Middle GA State University, debra.borkovich@mga.edu
Robert Joseph Skovira, Robert Morris University, skovira@rmu.edu

ABSTRACT

Subject matter experts assert that cybersecurity inertia critically contributes to successful cyberattacks that steal business confidential data and personal private information, capable of influencing major elections, crippling businesses, and causing devastating identify theft. The role cyber warfare plays in our daily lives cannot be underestimated. According to a 2018 Gallup Poll, 71% of Americans are more worried about cybercrime than violent crimes, including terrorism, murder, and sexual assault. Human error or negligent behavior is being increasingly blamed for cyberattacks, costing an organization an average of more than $15 million per year. Our research focuses on social engineering, an attack vector that relies on human interaction by manipulating people into breaking normal security protocols and best practices, permitting actors access to computer systems, networks or physical locations for fraudulent purposes. We discuss these constructs by exploring the most prevalent types of cyberattacks, the actors, and their prey, the human targets, perceived to be the weakest links within the organizational system. We close by offering recommendations to disrupt cybersecurity inertia and mitigation strategies to curb the influence of social engineering upon unsuspecting organizations.

Keywords: Cybersecurity, Cyber Inertia, Organizational Inertia, Social Engineering, Pretexting

INTRODUCTION

Subject matter experts generally agree, well-intentioned but careless employees, consultants, vendors, and other stakeholders pose as much danger to an organization's cybersecurity as faceless hackers on the outside. In fact, 90 percent of successful hack attacks or incidents are ascribed to human error or behavior (Kelly, 2017). Therefore, valuable lessons-learned, *the hard way,* are often attributed to social engineering, the use of digital, physical, and behavioral deception to manipulate individuals into divulging confidential business or personal information that may be used for fraudulent purposes. Social engineering is an attack vector that relies heavily on human interaction that involves manipulating people into breaking normal security protocols, procedures, and best practices in order to gain access to computer systems, networks or physical locations for financial or other gain.

Public and private organizations alike are often blamed for cybersecurity inertia, managements' inability or reticence to recognize, plan, and fund adequate cybersecurity measures, consistently analyze, test, scan, update, maintain, and backup networks, hardware, software, communication equipment, and storage devices, and to adequate train employees to recognize and report pretexting overtures and cyberattacks (real or perceived). But the human factor, employees or anyone with access to a keyboard, are blamed as security's weakest link due to their behavioral, social, and cultural vulnerabilities (Angwin, 2014; Garrett & Danziger, 2008).

Popularized into common parlance by Mitnick and Simon (2002), social engineering is a form of online, telephonic, or face-to-face techniques employed by social engineers designed to lure unsuspecting users into providing business confidential and personal identity information. Once the data is successfully obtained, cybercriminals then attempt to infect computer systems and networks with malware by opening links to infected sites, sending e-mail or texting scams and attachments containing computer viruses and network worms, phishing and pharming hooks, and encouraging the overall use of public networks, mobile device apps, and infected external drives, among others.

Social engineers and hackers are known to have easily exfiltrated data after gaining initial access to a network by establishing pretexts and then acquiring stolen employee or contractor credentials. A hacker with stolen administrator credentials can be especially vicious by inserting malware, establishing backdoors, escalating

privileges, and performing keylogging techniques, among others (Mitnick & Simon, 2006). Security breaches and insider threats can penetrate through any firewall, defeat expensive technology controls, expose sensitive data, cause laptops and mobile devices to go missing, grant facility access, and leak corporate or national security secrets. Employee negligence, caused by poor or no training and overall unawareness or apathy, is the single most common cause of damaging insider threats that lies at the root of many organizational digital and physical security breaches (Evans, 2019).

Traditional cybersecurity strategies are often vulnerable to insider threats due to a long-established practice of focusing on perimeter security, lacking the vital technology necessary to detect and stop attackers already within a system or network (Sobers, 2017). A social engineer primarily focuses on perimeter access via a user's behavior and not always on the data itself leaving that task to the expert hacker. An expert hacker's approach typically focuses on the data itself, not the infrastructure that permits its access. And employees and contractors already have access to this valuable organizational data, generally more access than needed, just by logging into their work computers. A hacker can infiltrate a single vulnerable user account by encrypting thousands of files without being noticed, many of which the user probably neither used nor required (Reilly, 2012). *The cybersecurity community is keenly aware that the most sophisticated and successful social engineer and expert hacker may be one in the same.*

Therefore, the purpose of this paper is to set-forth a critical 21st century literature review and exploratory narrative, albeit limited to the salient and material events of organizational cybersecurity inertia, as it relates to the construct of social engineering. We further discuss social engineering, what it is and how it began, its present underpinnings and vulnerabilities, and its future influence on the betterment of securing workplace computer systems, networks, and its valuable data. Our research concludes with recommendations to disrupt cybersecurity inertia and mitigation strategies to curb the influence of social engineering upon unsuspecting organizations.

LITERATURE REVIEW

Although computer viruses were roaming since the early 1970s when the "Creeper" was detected on ARPANET (the predecessor to the Internet), the term "cybersecurity" entered common parlance in 1988 when a computer worm was successfully released and distributed from an MIT computer eliciting mass media attention and an immediate need for security. The "Morris Worm" of 1988 had a huge impact on a nation just coming to grips with how important and vulnerable computers had become (Hospelhorn, 2018). Malware surfaced as the primary weapon of choice to carry out malicious intents in cyberspace, either by exploitation into existing human vulnerabilities or unique intrusions into the characteristics of emerging technologies. This section further examines a social engineer's discreet lingo and practices that s/he deploys to dismantle an organization's cybersecurity.

Cybersecurity

"Cybersecurity" is the practice of defending computers, servers, networks, mobile devices, electronic systems, communications, and data from malicious attacks and intrusions (Magnuson, 2017). Merely days after the Morris Worm attack, the country's first computer emergency response team (CERT) was created by the U.S. Department of Defense at Carnegie Mellon University and the construct of cybersecurity was created. As developers began creating much-needed computer intrusion detection software, the Morris Worm inspired a new generation of hackers and a wave of Internet-driven assaults that continue to plague our digital systems to this day (FBI News, 2018).

Cybersecurity Inertia and Organizational Inertia

Although most organizations face increasingly diverse, dynamic, and damaging cyber security threats, many remain hamstrung by inertia and uncertainly. By 2017, employee negligence or internal malicious acts accounted for two-thirds of cyber breaches, according to historical claim data analyzed by London-based consultancy Willis Towers Watson. Only 18% were directly driven by an external threat, and extortion accounted for a mere 2% (Kelly, 2017).

The 11th Annual CyberArk Global Advanced Threat Landscape Report 2018, a survey of 1,300 IT security decision-makers and professionals, revealed that security teams are not proactively adapting their cyber defenses to stay ahead of creative and innovative attackers. Primarily in medium to large organizations, a need exists for security teams to reset expectations where security priorities and spend should be focused. These findings support the dangers of inertia, with organizations not taking the initiative to make necessary changes immediately following an

attack or preparing for an eventual event. Additionally, budgets were identified as disproportionately focused on perimeter defenses and not on the mitigation of threats when attackers are already inside a system; further evidencing a general lack of consistent employee security education and training, and an over-reliance upon cloud providers' cyber security (Bourne, 2018).

In the 2019 Data Breach Investigations Report, Verizon stated that cyber espionage, errors by insiders and privilege misuse, accounted for 72 percent of data breaches in the public sector. Verizon analyzed over 41K security incidents and more than 2K data breaches from 86 countries and found that 16 percent of breaches occurred in the public sector. The report showed that 75 percent of breaches were associated with external threat actors and 79 percent of those external-related attacks were state-affiliated. Thirty percent of those breaches involved an insider and espionage was the top motive of threat actors, representing 66 percent of all breaches (Edwardson, 2019).

Statista (2019, January) reported the recorded number of data breaches and records exposed in the United States between 2005 and 2018, amounted to 1,244 with over 446.5 million records exposed. This report confirmed that the common theme of human vulnerability was responsible, *at least in part*, for successful social engineering tactics.

"Organizational inertia," originally relating to constraints of structural change, entered our vocabulary shortly after the appearance of the "Creeper" virus (Hannan & Freeman, 1977). Today organizational inertia has a much broader definition, describing the tendency of a mature organization to continue on its current trajectory, resisting impulses to course-correct, thereby not meeting current challenges and imminent threats for survival (Gilbert, 2005). For many organizations, cybersecurity inertia set-in with a paralyzing fear of the unknown and a lack of technical deterrence countermeasures (Kirda, et al, 2006). As digital technology matured and was ubiquitously acquired, organizations became sophisticated in their technology but over-confident in their security, setting the stage for the entrance of social engineering.

Social Engineering and How It Works

"Social engineering" is a method of gaining access to systems, data, personal information, or buildings through the exploitation of human psychology (Reynolds, 2015). Within the context of information security, social engineering is the use of digital, physical, and behavioral deception to manipulate individuals into divulging business confidential or personal information, often used for fraudulent purposes. Techniques employed by cybercriminals are designed to lure unsuspecting users into telling or sending them confidential data, then infecting their computers with malware, or opening links to infected sites (Pankov, 2019). A social engineer uses persuasion and influence to deceive people by convincing them s/he is harmless, friendly, and trustworthy (Mitnick & Simon, 2002).

From the biblical perspective, social engineering can be traced back to the Book of Genesis where it is written that the Devil, in the form of a snake, played to Eve's greed by luring her with an apple from the Tree of Life. Another preferred parallel is the Iliad, a Greek telling of the Trojan Horse ploy at the Siege of Troy. Regardless, social engineering has existed since humans learned the tactics of manipulation and coercion and almost every type of cyberattack contains some form. This section describes several basic social engineering techniques.

The classic "phishing" email and virus scams are laden with social and cultural overtones. "Phishing" emails attempt to convince users they are in fact from legitimate sources, in the hopes of procuring even a small bit of personal or company data. Emails that contain virus-filled attachments, meanwhile, often purport to be from trusted contacts or offer media content that appears innocuous (Hadnagy & Fincher, 2015). "Pharming" emails direct users to bogus web sites that appear legitimate by preying upon human curiosity and inherent trust (Reynolds, 2015).

"Shoulder surfing" and "dumpster diving" (Mitnick & Simon, 2002) are simplistic methods of social engineering to gain network or computer access. A hacker might frequent the public food court of a large office building and shoulder surf users working on their tablets or laptops resulting in a large number of passwords and usernames, all without sending an email or writing a line of virus code. Dumpster diving involves going through a company's trash, generally outside the facility but equally possible inside, by the cleaning crew, janitorial staff, disgruntled employee, or visitor. Most people don't realize that with only a few pieces of information, such as name, date of birth, address, or phone number, hackers can gain access to networks by masquerading as legitimate users to IT support personnel. From there, it's a simple matter to reset passwords and gain almost unlimited access (Zviran & Haga, 1999).

"Pretexting" is a form of social engineering in which an individual lies to obtain privileged data. A pretext is a false motive generally perpetrated via a face-to-face conversation, phone, text, or email. "Pretexting" often involves a scam or con where the liar develops a character or role, establishes trust with the victim, and pretends to need information or access to a facility or specific employee (Hadnagy, 2011). A victim may also be "baited" or lured to cooperate by disclosing information for free products or services. Similarly, a "quid pro quo" (something for something) attack promises a benefit in exchange for information, too, such as compensation for an employee phone list or log-in credentials (Hadnagy & Ekman, 2014).

"Reverse social engineering" is a con when the victim asks the attacker for help (Mitnick & Simon, 2002). A social engineer elicits sympathy or fear from an employee under a pretext to solicit verbal codes, access numbers, or passwords in order to quickly fix or protect a computer system or network vulnerability. The employee does not know how to resolve the technical problem, so s/he asks the social engineer for assistance. These attacks rely on actual communication between attackers and victims by pressuring the user into granting network access under the guise of a serious problem that needs immediate attention (Huws, 2003).

Technical Prowess & Significant Breaches

Chief Executive (Kelly, 2017) reported that 90% of cyberattacks were caused by human error or negligent behavior, estimated to cost an average American company more than $15 million per year. Over the past decade, some of the more notable breaches performed by hackers in concert with social engineering techniques are listed in Table 1. Note this list is not comprehensive, but merely states those publicly reported.

Table 1. Notable Cybersecurity Breaches Publicly Reported

American Business Hack	2005 - 2012	160 Million records breached; Hackers scraped data retrieving credit and debit card numbers. This breach cost companies & individuals at least $300 M.
T-Mobile	2009	500,000 Records breached; Employees stole proprietary and customer info.
Netflix	2010	480,000 Records breached; Contest participants received subscriber data.
Sony PSN	2011	1.6 Million records breached; Hackers stole credit card numbers, addresses, birthdays, passwords, & answers to security questions.
LinkedIn	2012	167 Million records breached; Hackers stole email addresses & passwords.
Yahoo!	2013 & 2014	3 Billion records breached; Occurred in 2013; Announced in 2016. Hackers retrieved email addresses, birthdays, answers to security questions.
Sony Pictures Entertainment	2014	47,000 Records breached; Affecting finances & reputation; Hackers retrieved internal emails, unreleased films, & celebrities' salary and contact info.
Ashley Madison	2015	37 Million records breached; Hackers stole customer online searches for extramarital affair partners, credit card numbers, addresses, & phone numbers.
US Gov't. OPM	2015	21.5 Million records breached; Hackers stole background investigation reports, user IDs, passwords, SSNs, and fingerprints.
Cambridge Analytica	2015 - 2017	87 Million records breached; Facebook profiles and users' identifying data, preferences, & relationship status.
Democratic Nat'l. Committee	2016	Hackers stole information about Democratic party candidates, including Hillary Clinton and opposition research on Donald Trump.
Equifax	2017	143 Million records breached; Hackers stole SSNs, credit card info, addresses.
Marriott Hotels	2014 - 2018	500 Million records breached; Guest personal & credit card info stolen.
Google	2015 - 2018	52.2 Million records breached; Hackers stole profiles, employer info, email addresses, birth dates, job titles, relationship status, etc.
Facebook	2017 - 2018	29 Million records breached; Hackers stole highly sensitive data, including locations, contacts, relationship status, log-in devices.
British Airways	2018	380,000 records breached; Affected booking info made on website & app.
T-Mobile	2018	2.3 Million records breached; Hackers stole billing & account info, encrypted passwords, and personal data.
Sources: Mason, J. (2019); and Nathaniel, S. (2018). ***Refer to References List.***		

Antagonists: Hackers (White, Gray, Black) vs. Protagonists: (Employees, Users)
The exponential growth of the Internet has led to a significant growth of cyber incidents. Adversaries are also switching their battle ground from desktop PCs to other platforms including smart phones, tablets, and VoIP to avoid detection. Mobile malware has risen sharply in the last few years, growing in users and sophisticated applications, resulting in clever social engineering scams. Popular social networking sites like Facebook, Twitter, Instagram, LinkedIn and others have been increasingly used as delivery mechanisms to solicit unsuspecting users to install or spread malware (Boyles, Smith, & Madden, 2012). Furthermore, organized attacks through the use of botnets have inflicted greater damage necessitating a growing concern to thwart these efforts. Recent statistics also show there is an increasing number of cyberattacks tailored to a specific system or facility using insider knowledge and the careful cultivation of explicitly identified personnel for an ad hoc purpose (Mason, 2019).

Although the word hacker tends to evoke negative connotations, it is important to remember that all hackers are not created equal. Figure 1 depicts the visual salient and material differences which are not obvious to the unsuspecting employee when approached by a social engineer.

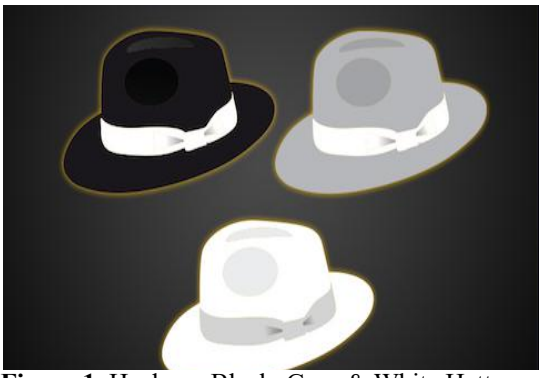

Figure 1. Hackers: Black, Gray & White Hatters

White Hat Hackers. "White hat hackers" choose to use their powers for good rather than evil. Also known as ethical hackers, white hatters are sometimes paid employees or contractors working for companies as security specialists hired to find security holes via social engineering techniques and hacking. White hatters employ the same methods as black hats; however, they have the system owner's permission to intrude, which makes the process legal. White hatters also perform penetration testing of security systems, vulnerability assessments, and compliance audits. Courses, conferences and certifications also exist for ethical hackers (Evans, Martin, & Poatsy, 2016).

Gray Hat Hackers. As in life, there are gray areas that are neither black nor white. "Gray hat hackers" are a blend of both white and black hat activities. Often, gray hatters will look for vulnerabilities in a system without the owner's permission or knowledge. If issues are found, they will report them to the owner, generally seeking recognition or a fee to fix the issue. If the owner does not respond or comply, then sometimes the hackers will post the newly found exploit online for the world to see. Generally, gray hatters are not inherently malicious and will not exploit the found vulnerabilities. However, this type of hacking is still considered illegal because the hacker did not receive permission from the owner prior to attempting to intrude the system (Evans, Martin, & Poatsy, 2016).

Black Hat Hackers. "Black hat hackers" have extensive knowledge about breaking into computer networks and bypassing security protocols, also without owner permission. Black hatters are clever at writing malware and well-versed in social engineering techniques. Their primary motivation is usually for personal or financial gain, but they can also be involved in cyber espionage or cyber warfare with intent to steal data, specifically financial information, personal private information, login credentials, security codes, and/or classified information (Evans, Martin, & Poatsy, 2016). Felonious acts may also be to modify or destroy data, dependent upon the client contract or any particular psychological mental or emotional state that affects the mind (Eastin, Glynn, & Griffiths, 2007).

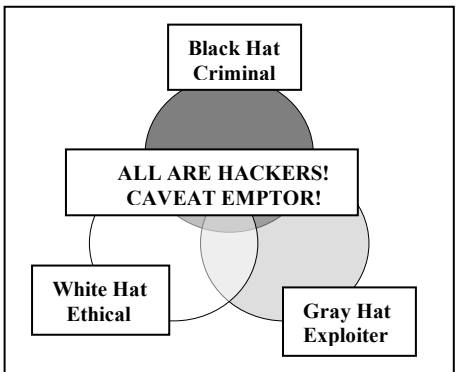

Figure 2. Beware ALL Hackers**!**

The White, Gray, and Black Hat Hackers depicted in Figure 2, are well-aligned with social engineers, have overlapping motivations and are even more confounding to the naïve and trusting employee or user.

Protagonists. The "protagonists" are the unsuspecting employees and users who are often duped by the technical prowess and the social engineering skills of the White, Gray, and Black Hat Hackers. Hatters employ persuasion with the same tactics we all use every day; albeit

with more savvy, confidence, and preparation (Sagarin, 2002). The absence of senior management buy-in to recognize the causes and mitigate the risks of organizational cybersecurity inertia are often to blame for employee naïveté, blind trust, ennui, apathy, fear, and an elephantine lack of cyber and human nature skepticism (Wilczek, 2018; Wolf, 2012).

Therefore, this research explored the theory that the first line of cyber defense must be employee awareness and proper social engineering training, in concert with a healthy dose of skepticism, *the critical humanware armor*.

RESEARCH METHODOLOGY

Our research focused on the overarching topic of organizational cybersecurity inertia as it directly related to the consequences of social engineering, by posing two specific questions: Why is social engineering considered to be information security's weakest link? – and – How does organizational cybersecurity inertia contribute to this human failure? Following extensive research, we selected the qualitative methodology of literature review (Creswell, 2016) in the narrative form of historical academic and subject matter expert research (Lundy, 2008; Berg & Lune, 2012; Tan, 2015) to pursue answers to our questions. We then evaluated and analyzed our findings, including after-action surveys and technical reports, to develop mitigation strategies, recommendations, and conclusions.

Historical literature research is a methodology for studying past events, phenomena, or occurrences that provides investigators with possible, instead of probable, understandings and influences that shape the present and may lead to future outcomes (Monaghan & Hartman, 2000). Also viewed as an advantage due to the unobtrusive nature of historical research, this method itself cannot directly affect its subject matter (Deflem & Dove, 2013). Although explicit documented historical research can be validated, it may be impossible to triangulate every finding because the contemporary witnesses to the research may no longer be living. Nevertheless, due to the limitation that some historical witnesses cannot be obtained for corroboration, this qualitative method of historical narrative comprising analyses of crucial scientific, social, and cultural events was deemed appropriate for our research approach.

DISCUSSION OF CYBER VULNERABILITIES AND INERTIA

Vulnerable humans are not only the back-door to cyber mischief, they represent the obvious front-door to intrusions, as well. The human factor in every organization is often ignored, yet it is a critical element in building a strong cyber defense as the Deloitte example illustrates below.

"Computers don't create crimes. It is the people who are using the computers that commit the crimes. And people in the organizations can be—and often are—complicit" (Viljoen, 2018, para. 10). Prior to its own 2017 email platform breach, Deloitte published this quote in a web report. A hacker compromised the firm's global email server through a stolen administrator account that provided privileged, unrestricted access to all areas. The account, stored in a Microsoft Azure cloud service platform required only a single password and did not have two-step authentification (The Guardian, 2017). The intent of this example is not to specifically denigrate Deloitte, but to merely show that any and all organizations are vulnerable to social engineering hackers, even those that purport to be cybersecurity experts. Despite its embarrassment, Deloitte ultimately followed its own cyber advice, and a year later was ranked as a cybersecurity global leader in the The ALM Best Cybersecurity Consulting Report (Becker, 2018).

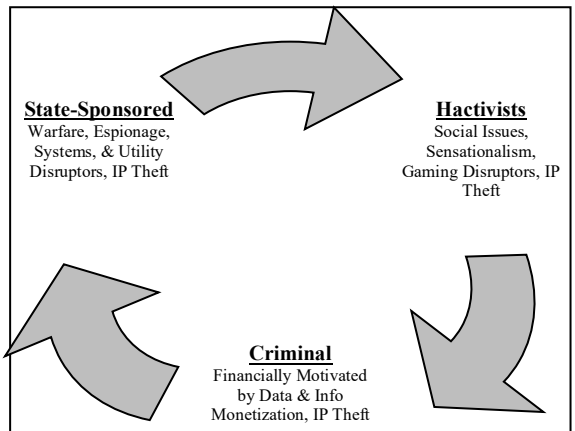

Figure 3. Actors behind cyber security threats

Our research discovered that the motivations behind cyber-crime are varied and overlapping but often fall into one of three broad categories: State-Sponsored, Hactivists, and Criminal Actors; depicted and defined in Figure 3 by those responsible for the threat. These types of cybercrime are a

growing source of major risk for organizations and all are vulnerable to social engineering tactics.

1. State-Sponsored espionage is a common strategy for nations seeking to stay a step ahead of competitors, with numerous recent public disclosures about the extent of governmental intervention, characterized by extremely advanced technologies and methods; 2. Hacktivists are organized groups of politically motivated individuals generally seeking publicity, who voice their cause publicly by targeting the reputation and brand of organizations that do not yield to their demands; and 3. Cyber Criminals plan to monetize elements that organizations or individuals value, using sophisticated methods and tools to tailor attacks to specific organizations (Tadjdeh, 2018).
As the frequency and severity of cyber security incidents increase, statistics continue to report that threat response and mitigation are not keeping pace with unabated risks. According to the CyberArk Report (Bourne, 2018), global security professionals report that some of the top cyber security threats faced are: targeted phishing attacks (56%); insider threats (51%); ransomware/malware (48%); unsecured privileged accounts (42%); and unsecured data stored in the cloud (41%). Even though the nature of the perceived threats has not significantly changed in recent years, many organizations are not proactively adapting their cyber defenses to stay ahead of attackers and protect their sensitive information and systems. Almost half (46%) state their security strategy rarely change substantially after cyberattacks and despite known risks, many organizations do not adequately manage or secure their privileged user accounts. Unmanaged, unsecured third-party and remote consultant and vendor access remains a significant security risk, too, as 51% of all CyberArk Survey respondents reported they give third-parties remote access to their internal networks but rarely monitor their activity. *Credentials for these accounts are a golden ticket to cyber threat actors.*

High profile breaches like Yahoo! (2016) were caused by poor security associated with unsecured privileged credentials, easily compromised at endpoints and on-premise systems, cloud services, hybrid environments and development operations. Upon further examination of the CyberArk Survey, we discovered that 89% of IT security professionals surveyed agreed that IT infrastructure and critical data are not fully protected unless privileged accounts and credentials are secured. Unfortunately, 1/3 of those surveyed admitted their organization had not implemented a security solution to store and manage privileged and/or administrative passwords (Natase, 2018).

Other pernicious attacks entered through endpoints, such as spear phishing and ransomware/malware and were ably demonstrated by WannaCry (2017) and NotPetya (2016) exploits, which quickly spread across more than 150 countries (Mason, 2019). These ransomware attacks exploited Windows computers and could have been largely avoided through patching and enforcement of privileges. Measures to stem credential theft include a combination of basic processes like patching, technologies such as multi-factor authentication, and principles like least privilege access, up-to-date antivirus software, and whitelist application controls.

While cloud adoption has increased dramatically in recent years, there is still a limited understanding of the challenges of securing cloud workloads in certain environments while managing thousands of machines and configurations. Major gaps exist regarding who is responsible for security in the cloud, even though the public cloud vendors are very clear that the enterprise is responsible for securing cloud workloads. Cloud adoption is increasing at a rapid pace driven by factors such as improved efficiency and reliability, access to on-demand computing, flexible pricing, as well as an increasing array of services being offered. Additionally, deploying Internet of Things Devices in concert with Global Positioning Systems without security checks is another vulnerability for organizations, their customers, and other stakeholders (Garamendi, 2017). All of these unabated cyber opportunities are great temptations to expert social engineers whom are well-aware that the human contact is still the weakest link.

RECOMMENDATIONS FOR SOCIAL ENGINEERING MITIGATION

Clearly, there is a pressing need for improved privacy practices globally and domestically. More definitive and enforceable regulations will drive better security protocols, and more rigorous compliance requirements are beginning to force more effective privacy practices (Keizer, 2012). Per the CyberArk Report (Bourne, 2018), 83% of IT security professionals say new privacy requirements and security recommendations such as the EU General Data Protection Regulation (GDPR) implemented in 2018 and the US National Institute of Standards and Technology (NIST) Cybersecurity Framework released in 2019 (promulgated in the U.S. Cybersecurity Enhancement Act of 2014) are enhancing our overall security and privacy posture.

Reforming the organizational security culture remains a top priority but is often overlooked or neglected, misperceived as a cost factor or necessary evil rather than a differentiating factor or competitive advantage. Consequently, banishing cybersecurity inertia will involve making it key to organizational strategy and behavior, which suggests that without C-Suite visible support and adequate funding dedicated to a formalized security program, one can presume that results will not improve exponentially (Bateman, et al., 2019; Wilczek, 2018). Despite the CyberArk Survey's (Bourne, 2018) bleak outlook, some organizations are improving their security strategies to meet the current challenges. But more work needs to be done. Rather than viewing security simply as a cost, digital business champions should recognize it as a key aspect of every project and activity, then use it to differentiate themselves from their less-secure competitors (Wilczek, 2018).

The human side of cybersecurity reveals a great deal of uncertainty and fear of the unknown amongst the individuals on security teams. Security professionals rarely admit they lack knowledge of their organization's security policies and are unsure of their specific role in incident response. An environment full of threats has also taken its toll as security decision-makers worry that they might personally introduce a cybersecurity incident into their organization. To counter this uncertainty, we believe organizations should elevate cybersecurity to a higher-level issue that is shared and communicated across the organization. As with all company culture-setting agendas, the case for cyber security should cascade top-down from the executive team, from the CIO to all employees (Ipsara, 2018).

Mitigating social engineering attacks requires a series of coordinated efforts supported and championed by senior management. The use of Red Team exercises, in which ethical hackers simulate the techniques and behaviors of likely attackers, are useful devices (Dobriansky, 2016). These exercises help organizations uncover critical vulnerabilities, identify effective responses, and understand the motives and techniques of adversaries. Table 2 illustrates our recommended Social Engineering Risk Mitigation Plan for implementation enterprise-wide, as cybersecurity inertia can only be eradicated if every company stakeholder participates in its amelioration.

Table 2. Social Engineering Risk Mitigation Plan - Strategies to Eliminate Cybersecurity Inertia

• Develop and enforce clear and concise cyber and facility security protocols, policies, and procedures
• Incorporate cybersecurity / social engineering missions in the Employee Code of Conduct & Ethics Policies
• Develop and deploy security awareness training for all employees with routine refresher training; Require all employees to complete and confirm each training with a signed acknowledgement certificate
• Develop a data and information classification policy; Communicate simple definitions for sensitive, confidential, proprietary, classified, etc., data
• Develop rules for verification of any requester's identity and confirmation of rationales for "need to know" with supervisors or management
• Develop employee training program designed to identify and resist social engineering attacks
• Routinely test employees' resistance to social engineering overtures by role-playing mock events with anonymous attackers; Remind employees that punishment or job loss will not result from mock trial failure
• Perform semi-annual Cybersecurity & Social Engineering Compliance Audits and Red Team Exercises; Communicate results of audits & tests to all employees
• Coordinate routine meetings, reviews, & audits with Cloud Storage providers, facilities, & other vendors
• Modify the corporate security culture with heightened awareness, sensitivity, and healthy skepticism
• Incentivize employees for embracing and practicing the security policies with Awards, Gift Cards, Plaques, Certificates, Spot Bonuses, Team Contests; Provide Lunches &/or Snacks
• Incorporate social engineering & cybersecurity awareness achievements as evaluation criteria on Annual Performance Reviews
• Publicize security policies with posters, screen savers, email announcements, videos, & newsletters
• Invite security & behavioral subject matter experts as guest speakers at "All Hands" meetings
• Secure senior management support and funding; Appoint a Social Engineering "Champion."

To successfully enforce the social engineering stopgaps, we recommend that employees are consistently motivated with innovative training programs, communication media, and incentives. Furthermore, organizations may opt to

develop and perform a Cybersecurity Knowledge Management Program, starting with an audit to learn both the explicit and tacit information already established. It is imperative to learn what is known and not known, prior to commencing the developing of an important new enterprise-wide initiative.

CONCLUSION

By addressing our research questions through a substantive and material literature review of subject matter experts, we confirmed that *social engineering is considered to be information security's weakest link*; and *organizational cyber inertia is indeed a major factor in successful social engineering and hack attacks that directly contribute to this human failure*. From our study we learned that moving from inertia to action is not an easy process, regardless of the type or size of the organization. We further grasped that building awareness is just the first step to develop a modern cyber defense in the workplace. Organizations must turn knowledge into action to defend against multiple threats by mitigating risk. This initiative demands support, buy-in, and funding from the most senior levels of the organization and must be extended to all stakeholders. Inertia in the face of a dynamic threat is no excuse for not building cyber warfare resilience into organizations and human resistance against social engineering attacks.

Protection against social engineering starts with robust ethics training and security education programs. Users must be trained to never click on suspicious links and always guard their log-in credentials, regardless of the workplace location. In the event that cyber intrusions are successful, it's critical to employ a high-quality cybersecurity solution that can both eliminate infections and track their source (Pankov, 2019). Protecting the organization from being victimized by hackers using social engineering tactics must be the responsibility of each and every employee. Anyone can be exploited from executive and line management, through professionals, technicians, vendors and consultants, to receptionists, security guards, cleaning crews and garage attendants. *This includes even those folks whom do not use computers in their daily work.* We argue that the challenge to defend against human-based cyber and social engineering vulnerabilities is substantial and can no longer be ignored. CAVEAT EMPTOR!

REFERENCES

Angwin, J. (2014). *Dragnet nation: A quest for privacy, security, and freedom in a world of relentless surveillance*. New York: Times Books.

Bateman, T., Snell, S., & Konopaske, R. (2019). *Management: Leading & collaborating in a competitive world* (13th ed.). New York: McGraw-Hill Education.

Becker, L. (2018). Best Cybersecurity Consulting Report for 2018. *The ALM Vanguard*. Retrieved from*:* www.alm.com/intelligence/consulting-industry

Berg, B., & Lune, H. (2012). *Qualitative research methods for the social sciences*. Upper Saddle River, NJ: Pearson.

Bourne, V. (2018). CyberArk Global Advanced Threat Landscape Report 2018. Retrieved from: https://www.cyberark.com/resource/cyberark-global-advanced-threat-landscape-report-2018-security/

Boyles, J., Smith, A., & Madden, M. (2012). Privacy and Data Management on Mobile Devices. *Pew ResearchReport - Internet & Technology.* Retrieved from: https://www.pewinternet.org/2012/09/05/privacy-and-data-management-on-mobile-devices/

Creswell, J. W. (2013). *Review of the Literature: Research Design, Qualitative, Quantitative, & Mixed Methods Approaches* (4th ed.). Thousand Oaks, CA: SAGE Publications.

Deflem, M., & Dove, A. L. (2013). Historical Research and Social Movements. In D. Snow, D. Porta, B. Klandermans, & D. McAdam (Eds.), *The Wiley-Blackwell Encyclopedia of Social and Political Movements* (pp. 560-563). Malden, MA: Wiley-Blackwell.

Dobriansky, J. (2016). Cybersecurity and acquisition: The matrix redefined. *Contract Management, 56*(2), 22-28.

Eastin, M. S., Glynn, C. J., & Griffiths, R. P. (2007). Psychology of communication technology use in the workplace. *Cyberpsychology & Behavior, 10*(3), 436-443.

Edwardson, J. (2019, May 9). Verizon: Cyber Espionage, Privilege Misuse, Miscellaneous Errors. *ExecutiveBIZ*

Online. Retrieved from: https://blog.executivebiz.com/2019/05/verizon-cyber-espionage-privilege-misuse-miscellaneous-errors-as-top-3-breach-patterns-in-public-sector/

Evans, L. (2019). Cybersecurity: *What you need to know about computer and cybersecurity, social engineering, and The Internet of Things.* No city, state: Self-published by Lester Evans.

Evans, A., Martin, K., & Poatsy, M. A. (2016). *Technology in Action Complete* (13th ed.). Saddle River, NJ: Pearson Education, Inc. publishing as Prentice Hall.

FBI News Online. (2018, Nov. 2). The Morris Worm: 30 Years since the first major attack on the Internet. Retrieved from: https://www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218

Garamendi, J. (2017). GPS vulnerable, but there is a solution. *National Defense of NDIA, CI*(758), 15-16.

Garrett, R. K., & Danziger, J. N. (2008). On cyberslacking: Workplace status and personal Internet use at work. *Cyberpsychology & Behavior, 11*(3), 287-292.

Gilbert, C. (2005). Unbundling the structure of inertia: Resource versus routine rigidity. *Academy of Management Journal, 48*(5), 741-763.

Hadnagy, C. (2011). *Social engineering: The art of human hacking.* Indianapolis, IN: Wiley & Sons, Inc.

Hadnagy, C., & Ekman, P. (2014). *Unmasking the social engineer: The human element of security.* Indianapolis, IN: Wiley & Sons, Inc.

Hadnagy, C., & Fincher, M. (2015). *Phishing dark waters: The offensive and defensive sides of malicious e-mails.* Indianapolis, IN: Wiley & Sons, Inc.

Hannan, M., & Freeman, J. (1977). The population ecology of organizations. *Journal of Sociology, 82*, 929-964.

Hospelhorn, S. (2018). 8 Events that changed cybersecurity forever. *Inside Out Security Blog*. Retrieved from: https://www.varonis.com/blog/events-that-changed-cybersecurity/

Huws, U. (2003). *The making of a cybertariat: Virtual work in a real world*. New York: Monthly Review Press.

Ipsaro, M. (2018). Building a 21st century digital government "byte" at a time. *Contract Management, 58*(8), 20-27.

Kang, J. (1998). Information privacy in cyberspace transactions. *Stanford Law Review, 50*(4), 1193-1294.

Keizer, G. (2012). *Privacy.* New York: Picador USA.

Kelly, R. (2017, March). 90% Cyberattacks are caused by human error or behavior. *Chief Executive Online*. Retrieved from: https://chiefexecutive.net/almost-90-cyber-attacks-caused-human-error-behavior/

Kirda, E., Kruegel, C., Banks, G., Vigna, G., & Kemmerer, R. (2006). Behavior-based spyware detection. *15th USENIX Security Symposium Proceedings,* 273-288.

Lundy, K. S. (2008). Historical Research. In L. M. Given (Ed.), *The SAGE Encyclopedia of Qualitative Research Methods: Volumes 1 & 2* (pp. 395-399). Thousand Oaks, CA: SAGE Publications.

Magnuson, S. (2017). Defending networks emerge as top battlefield priority. *National Defense, CI*(758), 35-36.

Markoff, J. (1997, December 18). Guidelines don't end debate on internet privacy. *The New York Times.* Retrieved from: http://www.nytimes.com/1997/12/18/us/guidelines-don-t-end-debate-on-internet-privacy.html

Mason, J. (2019, April). 14 Most alarming cyber security statistics in 2019. Thebestvpn. Retrieved from: https://thebestvpn.com/cyber-security-statistics-2019/

Mitnick, K., & Simon, W. (2002). *The art of deception: Controlling the human element of security.* Indianapolis, IN: Wiley Publishing, Inc.

Mitnick, K., & Simon, W. (2006). *The art of intrusion: The real stories behind the exploits of hackers, intruders & deceivers.* Indianapolis, IN: Wiley Publishing, Inc.

Monaghan, E., & Hartman, D. (2000). Undertaking Historical Research in Literacy. In M. Kamil, & P. Mosenthal, (Eds.), *Handbook of Reading Research: Vol. III* (pp. 109-122). New Jersey: Lawrence Erlbaum Associates.

Natase, R. (2018). *Hacking with Kali Linux: A step by step guide for you to learn the basics of cybersecurity and hacking.* Amazon Digital Services, LLC. ISBN: 1728899907.

Nathaniel, S. (2018). History & evolution of social engineering attacks. Retrieved from: https://commissum.com/blog-articles/the-history-and-evolution-of-social-engineering-attacks

Pankov, N. (2019, May). Solo: A Cybersecurity Story. Retrieved from: https://usa.kaspersky.com/blog/solo-starwars-cybersecurity/17651/

Reilly, R. (2014, June). 95% Successful security attacks are the result of human error. Retrieved from: https://venturebeat.com/2014/06/19/95-of-successful-security-attacks-are-the-result-of-human-error/

Reynolds, V. (2015). Social engineering: *The art of psychological warfare, human hacking, persuasion & deception.* No city, state: Self-published by Vince Reynolds.

Sagarin, B., Cialdini, R., Rice, W., & Serna, S. (2002). Dispelling the illusion of invulnerability: The motivations and mechanisms of resistance to persuasion. *Journal of Personality and Social Psychology, 83*(3), 526-541.

Sobers, R. (2017). Why the OPM breach report is a call to action to embrace data centric security. *Contract Management, 57*(2), 28-33.

Statista. (2019, January). Annual number of U.S. data breaches & exposed records from 2005 to 2018.

Retrieved from: https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-numberof-breaches-and-records-exposed/

Tadjdeh, Y. (2018). Cyber talent wanted: Military intelligence community strive to retain cyber workforce. *National Defense of NDIA, CII*(772), 26-29.

Tan, J. (2015). Historical research: A qualitative research method. *Academia (21 April 2015).* Retrieved from: file:///C:/Users/Downloads/HISTORICAL_RESEARCH_A_QUALITATIVE_RESEAR.pdf

The Guardian. (2017, September 25). Deloitte hit by cyberattack revealing clients' emails. Retrieved from: https://www.theguardian.com/business/2017/sep/25/deloitte-hit-by-cyber-attack-revealing-clients-emails

United States Public Law No. 113-274. *Cybersecurity Enhancement Act of 2014.* Retrieved from: https://www.congress.gov/bill/113th-congress/senate-bill/1353

Viljoen, T. (2018). Cybercrime is not just a tech problem. Deloitte Online. Retrieved from: https://www2.deloitte.com/au/en/pages/risk/articles/cybercrime-tech-problem.html

Wilczek, M. (2018). Despite risks, nearly half of IT execs don't rethink security after an attack. Retrieved from: https://www.darkreading.com/vulnerabilities---threats/despite-risks-nearly-half-of-it-execs-dont-rethink-cybersecurity-after-an-attack/a/d-id/1331627

Wolf, F. (2012). Cyber naïveté. *The International Economy*, Fall 2012, pp. 10-12. Retrieved from: http://www.international-economy.com/TIE_F12_Wolf.pdf

Zviran, M., & Haga, W. (1999). Password security: An empirical study. *Journal of Management Information Systems, 15*(4), 161-185.