PLANNING FOR CYBER SECURITY IN SCHOOLS: THE HUMAN FACTOR

MICHAEL D. RICHARDSON
Columbus State University, U.S.A.

PAMELA A. LEMOINE
Troy University, U.S.A.

WALTER E. STEPHENS
Houston County Schools, Georgia, U.S.A.

ROBERT E. WALLER
Columbus State University, U.S.A.

ABSTRACT

Cybersecurity has emerged as one of the most critical issues confronting schools in the 21st century. Computer security is an essential instrument for protecting children, but K-12 schools are considered one of the most attractive targets for data privacy crimes often due to the less-than-effective cybersecurity practices in schools. The human factor is the underlying reason why many attacks on school computers and systems are successful because the uneducated computer user is the weakest link targeted by cyber criminals using social engineering. Formal cyber security awareness is required to mitigate the exploitation of human vulnerabilities by computer hackers and attackers.

INTRODUCTION

Much of the world is now in cyber space and cyber security has become a massive issue with many facets of schools (Arlitsch & Edelman, 2014). Cybersecurity has brought about research, discussion, papers, tools for monitoring, tools for management, etc., with much of the focus from the schools' side concerning the protection of their data and information (Seemma, Nandhini, & Sowmiya, 2018). As a result of increased dependence on the Internet, cybersecurity has emerged as one of the critical issues confronting schools in the 21st century (Gioe, Goodman, & Wanless, 2019). The reliance on a complex technology infrastructure has come with a price: by accepting the Internet so widely, schools have exposed themselves to a range of nefarious cyber activities by a spectrum of offenders looking for school data and information (Shen, Chen, & Su, 2017).

Governments, businesses and schools have been victims of cyber thefts, cyber-crime, and cyber disruption. Despite recent heightened attention and increased levels of security investments in cybersecurity, the number of cyber incidents, their associated costs, and their impact on people's lives continues to rise (Abomhara & Koien, 2015). As computing and communications technologies become more entrenched in the global economy and as society enters the era of the "Internet of Everything" (IoE), security compromise of these systems will rise as well (Bailaszewski, 2015).

For the early years of technology use human factors remained unexplored and unquestioned. However, the increasing cyber-attacks, data breaches, and ransomware attacks are often a result of human-enabled errors; in fact, researchers indicate that as much as 95% of all cyber incidents are human-enabled (Nobles, 2018). Cybersecurity is fundamentally a case of human and automation teaming so both the machine and human are potentially vulnerable. The research results show that

the greatest security vulnerability is the lack of the awareness of employees (Safa, Sookhak, Von Solms, Furnell, Ghani, & Herawan, 2015). While tools and technology are important, people are the most important element of a cybersecurity strategy.

WHAT IS CYBERSECURITY?

Cyber security is defined as measures taken to protect a computer or network against unauthorized access to maintain the safety and integrity of the information stored within (Aloul, 2012). Cybersecurity involves the technical interventions that protect data, identity information, and hardware from unauthorized access or harm including security of assets in cyberspace. More formally put, cyber security is defined by Craigen, Diakun-Thibault and Purse (2014) as: "the organization and collection of resources, processes, and structures used to protect specific assets in cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights" (p. 13). Further, Seemma, Nandhini, and Sowmiya (2018) reported that "cyber security are techniques generally set forth in published materials that attempt to safeguard the cyber environment of a user or organization. It manages the set of techniques used to save the integrity of networks, programs and data from unauthorized access" (p. 25).

WHY IS CYBERSECURTIY IMPORTANT TO SCHOOLS?

Increasingly schools are repositories of large data sets that contain information valuable in a cyber marketplace. Additionally, schools have not typically expended the resources to handle cybersecurity in the same manner as government and big business (Goldsborough, 2016). Consequently, schools are a frequent target for cyberattacks because of the sensitive data their IT systems often house combined with the vulnerabilities that come with an open-access culture (Goel & Jain, 2018). Successful school cybersecurity requires communication between the IT department and institutional leaders, to be more effective in preventing attacks and bouncing back after an incident occurs. The primary data contained in school files are largely personal data which is valuable to hackers and other cyber criminals (Davis, 2018). The following is a sample list of school data stored electronically and which could be susceptible to cyber-attack.

A Partial List of Unique, Voluminous, and Valuable Data Stored by Schools

- Student ID
- Social security numbers for students, faculty and staff
- Credit card numbers for faculty, staff and school
- Immunization history and/or medical records
- Enrollment and attendance
- Special education documentation
- Names of students, faculty and staff
- Addresses
- Date of birth
- City, state and country of residence
- Bus routes
- Telephone numbers
- Email addresses
- Gender
- Race
- Criminal record
- Test scores

- Grades
- Achievements
- Free lunch applications
- Participation in school activities (dates and times)
- Family members
- Prior students at the school and their data
- Community and business involvement in school (McGettrick, 2013; Rios, 2017)

WHAT ARE THE ISSUES WITH CYBERSECURITY AND SCHOOLS?

Cyberspace has distinct advantages and disadvantages; it permits persons to work faster, more efficiently, and more effectively, but the downside of threats in cyberspace can damage the school, its reputation, and cause legal liability and financial loss (Schuesster, 2013). If there is not awareness of the potential cyber dangers, persons, product and performance could be jeopardized. Only by using a realistic and reliable cyber system can schools deal with both the opportunities and risks of cybersecurity (Whitman & Mattford, 2016). Computer security is not well regulated, and threats and vulnerabilities need real solutions, not a quick fix or a "patch and pray" effort. National leaders and computer experts warn that it is not a matter of *if*, but *when* a major cyberattack occurs (Rainie, Anderson, & Connolly 2014).

Due to the increased dependence on the Internet, cybersecurity has emerged as one of the most critical issues facing schools in the 21st century. Schools have been victims of cyber thefts, cybercrime, and cyber disruption despite recent heightened attention and increased levels of security investments in cybersecurity (Alavi, Islam, & Mouratidis, 2016). Cybersecurity threats continue to evolve and reinvent themselves, making cyber-attacks a concern for anyone utilizing technology, particularly schools (Akhtar, Azeem, & Mir, 2014). Schools have become an increasingly popular target for cyber-attacks for several reasons. Specifically, many schools lack a robust cybersecurity infrastructure capable of keeping up with the most pervasive cybersecurity threats. Furthermore, hackers perceive schools as gateways to larger opportunities given the number of persons involved at a school and the increased potential to exploit multiple venues (Katzan, 2016). The typical response from schools is to identify assets and risks, protect perilous assets, detect intrusions, respond to intrusions and recover from incidents (Chen & Shen, 2016).

For schools the currently available technology clearly provides the means for acquiring greater amounts of information with more efficiency than ever before. Data and information are more readily available and more quickly accessible today (Chen, 2014). However, the transition from an era of information scarcity to information abundance requires a re-focusing on human sense-making processes to identify threats and protect assets and people (Kyriazis, 2018).

For schools the increase of computer networks, coupled with the enlarged number of persons with access to school technology, meant a growth of digital information, which is much more difficult to protect than hard copy files and folders (Aleroud & Zhou, 2017). This makes cyber security difficult for schools because there always has to be a compromise between robustness of the security system and simplicity of the system for human use (Lestch, 2015). Additionally, the current trend is to share information, not protect it. School personnel will share their data and information on social media, visit questionable websites, and download files from the Internet that probably contain malware (Stewart & Jurjens, 2017). This increased use of and dependence on new cyberspace technologies has created new risks, particularly human factor risk. Consequently, some schools have implemented cyber-awareness programs designed to reduce the human factor risk and help secure schools (Caballero, 2017).

CYBERSECURITY RISK IN SCHOOLS

The threat of cybercrime and intrusion is dynamic and complex, and hackers now act with impunity in carrying out attacks against school targets. Cyber criminals are gaining access to schools through sophisticated spear phishing attacks, preying on the human and technical vulnerabilities in the school cybersecurity system (Arachchilage, Love, & Beznosov, 2016). Managing the risks from cyberattacks usually involves (1) removing the threat source; (2) addressing vulnerabilities in the system; and (3) lessening impacts by mitigating damage and restoring functions. However, these operations are time and labor intensive and often happen after an intrusion has happened (Sen & Borle, 2015). What is needed is a more secure system before the attacks happen.

Types of Cyber Events That Impact Schools:

- data breaches (unauthorized disclosure of personal information),
- security incidents (malicious attacks directed at a school),
- privacy violations (alleged violation of consumer privacy),
- phishing/skimming incidents (individual financial crimes),
- technology-focused threats (hacking, malware and spyware),
- content-related risks (exposure to illicit or inappropriate content),
- harassment-related threats (cyber-bullying, cyber-stalking and other forms of unwanted contact), and risk of exposing information (children exposing their personal information through phishing or sharing information on social networking platforms) (Atkinson, Furnell, & Phippen, 2009).

CYBERSECURITY ASSESSMENT

The Internet, or cyberspace, has become so attractive that its use is second nature to most persons. However, it has also made all users, including schools, more exposed and vulnerable to cyber criminals (Gupta, Tewari, Jain, & Agrawal, 2017). The risk of losing personal data or the theft of an important personal and/or organizational data makes cyber security the prime challenge faced by organizations, especially schools. Therefore, schools should be proactive in assessing potential weakness in their cybersecurity systems and developing alternatives to mitigate as much risk as possible (Kaur, 2016).

WHAT MAKES EDUCATION A PRIME TARGET FOR CYBER-CRIMINALS?

"A little over half of all digital data breaches were caused by members of the affected school community (staff, students) and 23 percent were caused by school vendors or partners. The remaining 23 percent were carried out by unknown actors. Furthermore, student data was included in more than 60 percent of the 2018 data breaches" (p. 1). Such were the conclusions reported in the "The State of K-12 Cybersecurity: 2018 Year in Review," released by the K-12 Cybersecurity Resource Center (Rock, 2019).

Personal information and social security numbers are prime targets for data breaches (Kleinberg, Reinicke, & Cummings, 2015). Many persons perceive that there is little data in schools that would be of benefit to cyber criminals, but in reality, schools have a vast store of information that is valuable on the cyber black market, including personal data. Schools have information on students and their parents that can include social security numbers, e-mail addresses, credit card numbers, financial data, and other personally identifiable information that could be stolen and sold on the black market (Coleman & Reeder, 2018). Additionally, schools have business offices that manage accounts payable that provide access to organizational financial data (Chen & Shen, 2019).

Wide Variety of Valuable Data

Schools have sensitive data about students, parents, alumni, faculty, and staff. Records are routinely retained decades after students have left an institution. Moreover, the sheer volume of potentially valuable data housed at most schools tends to make them highly attractive targets (Lestch, 2015; Rock, 2019) (see above for a listing of potentially valuable data).

Lack of Centralized Structure for Cybersecurity

Schools may house their data in many different locations rather than one centralized location. Student data may be kept separately at each school and may be aggregated centrally at a district office. Student data and financial data may be housed separately. This decentralized structure can give cybercriminals a greater opportunity to exploit vulnerabilities in the disparate systems housing sensitive data (Javidi & Sheybani, 2018).

Organizational Vulnerabilities

The decentralized nature of data storage in schools is often paralleled by similar administrative and operational problems. The responsibility for implementing and operating security measures and determining processes may reside with a number of different individuals within a variety of departments, often with a different reporting structure. Schools generally lack a top-down command structure that makes new safeguards easy to implement and improve security (Coleman & Reeder, 2018).

Prevalent Use of Personal Devices

Administrators, faculty, and staff are often unaware of the extent to which they may be exposing their institution to cyber risks when they download sensitive data to less well-protected personal devices (Ki-Aries & Failey, 2017). Approximately 90 percent of faculty own a smartphone, while just 27 percent received mandatory information security training (Hipsky & Younes, 2015). Additionally, many elementary students, and most high school students, have a cell phone, most of whom have never received security training. As a result, even if the school has robust security measures in place, any number of individuals at the institution may, through carelessness, or unintentionally through lack of awareness, expose sensitive data (Hope, 2018).

THREAT APPRAISAL: THE HUMAN ELEMENT

Threat refers to the possibility of danger and the probability of losing something of value. Threat relates to intentional interaction with uncertainty and is the person's judgment about the severity of the risk (Urias, Stout, & Lin, 2016). The human factor is the underlying reason why many cyber-attacks on computers and systems are successful (Gutzwiller, Fugate, Sawyer, & Hancock, 2015). The uneducated computer user is the weakest link targeted by computer hackers attempting to break into organizations (Aloul, 2012). In response, Da Veiga (2019) concludes that schools that implement strong technological security procedures still often pay insufficient attention to human sources of vulnerability, and strongly advocates for enhanced security training. Armerding (2014) cites a report that indicates that 56% of workers who use the Internet on their jobs receive no security training at all.

In an effort to mitigate security risks, schools use the modern solution: technology-centered security measures in isolation (Peltier, 2016). However, after unsuccessful technological efforts in isolation, such solutions proved to be insufficient to mitigate risks (Ritzman & Kahle-Piasecki, 2016) caused by the 'human vulnerabilities'. These vulnerabilities are labeled as the 'human factor'. The term human factor relates to the role(s) that users play in the security process based upon their

perceptions that can either positively or negatively impact the security process (Alhogail, Mirza, & Bakry, 2015.

Preventing information technology security incidents poses a great challenge for schools where more resources are being allocated to security programs that focus on educating and training employees in an effort to reduce human misbehavior (Luo. Brody, Seazzu, & Burd, 2011). Simply stated, cyber criminals target people, not computers, in order to create a breach in the security system. Examples of user mistakes include inappropriate information security behavior, such as using a social security number as username and/or password, writing passwords on sticky paper, sharing their username and password with colleagues, opening unknown emails and downloading their attachments, as well as downloading software from the Internet (Sawyer & Hancock, 2018).

It has been reported by many researchers that the human link is the weakest in information security. Therefore, the school must have rigid security policies and need to instruct the employees in awareness and create an information security culture (Joinson & Steen, 2018). The role of humans in information security has been a neglected area of concern; security policies have been rendered useless through negligence and lack of knowledge or concern by school managers of information data (Hadlington, 2017).

A secure school environment for data security must incorporate human aspects of information security. The lack of information security awareness, ignorance, negligence, apathy, mischief, and resistance are most often the causes of users' mistakes (Thomas, 2018). According to Kearney (2010), people can only help in preventing security breaches if they are aware of the dangers, and are taught secure behaviors, yet those behaviors often result from employee apathy. Every school must promote a culture in which employees share the responsibility of defending the school against cyber-attack (Kearney, 2010).

The human ability to rapidly learn is driving the growth of a globally connected network; however, the result is an overly complex system riddled with cybersecurity holes, leaving schools susceptible to information security threats (Evans, Maglaras, He, & Janicke, 2016). These attacks are becoming increasingly more sophisticated as advanced hacker tools develop. Advanced defense tools have developed as well but are still not enough to overcome the security risk posed by employee error. In information security management, people are the weakest link in organizations and any employee who violates information security policies makes their organization vulnerable (Boss, Kirsch, Angermeier, Shingler, & Boss, 2009).

In spite of the significant budgetary expenditures in tools and systems to fight cyberattacks, there is very little comparative investment in human factors and security culture. The behavior of humans in the security system is a direct reflection of the culture of information security in the school (Conteh & Schmick, 2016).

Awareness

Since people are the weakest link in the information security chain, particular attention should be paid to the human dimension (Safa, von Solms, & Futcher, 2016). One way to help this process is to build employee awareness in information security. Information security is perceived as the degree to which every employee understands the importance and consequences of internal guidelines for information security (Lebek, Uffen, Neumann, Hohler, & Britner, 2014). Increased employee awareness of information security should minimize the risk of employee behavior since awareness and training are the two most effective mitigating measures for human activities. Increasing human information security awareness is an important part of the holistic approach to managing information security (Sawyer, Finomore, Funke, Warm, Matthews, & Hancock, 2016).

The human factor often determines success or failure in managing information security. Each security breach incident in a school is more or less dependent not only on technology but primarily on human users (Hadlington, 2017). In order to mitigate the risk of information security, the school should be required to implement an awareness program for all employees. Information security awareness is a dynamic process, and awareness of information security by human users can contribute to the promotion of a positive security culture, thereby increasing the protection of information and data (Da Veiga, 2019).

Social Engineering

Social engineering is one of the simplest methods to gather information about a school through the process of exploiting human weakness that is inherit to every school. In essence, social engineering refers to the use of deceitful techniques to deliberately manipulate human targets (Hatfield, 2018). Social engineering is primarily used to induce victims to disclose confidential data, or to perform actions that breach security protocols, unknowingly infecting systems or releasing classified information (Flores & Ekstedt, 2016). An attacker engages social engineering as an approach to use human insiders and information to circumvent computer security programs through deceit. Social engineering attacks challenge information security workers because no technical countermeasures to-date can eliminate the human vulnerability. The basis of a social engineering attack is to avoid cyber security systems through deceit, exploiting the weakest link, the people involved. Throughout the interaction, victims are unaware of the destructive nature of their actions. The social engineer exploits innocent instincts, not criminal intent (Luo, Brody, Seazzu, & Burd, 2011).

Social engineering is challenging the security of all networks regardless of the robustness of their firewalls, cryptography methods, intrusion detection systems, and anti-virus software systems. Humans are more likely to trust other humans compared to computers or technologies (Aldawood & Skinner, 2019). Malicious activities accomplished through human interactions influence a person psychologically to divulge confidential information or to break the security procedures. Due to these human interactions, social engineering attacks are the most powerful attacks because they threaten all systems and networks (Lohani, 2019). They cannot be prevented using software or hardware solutions as long as people are not trained to prevent these attacks. Cyber criminals choose these attacks when there is no way to hack a system with no technical vulnerabilities (Salahdine, & Kaabouch, 2019).

THE HUMAN FACTOR: STUDENTS

Students around the globe connect, exchange ideas and learn and schools hold online sessions to make learning accessible to the world. While schools fear break-ins to their computer systems by professional criminals, students are increasingly giving educators almost as much to be concerned about. Reports of students' gaining access to school networks to change grades, delete teachers' files, or steal data are becoming more common. The "anywhere, anytime" accessibility of many networks can be tempting to students, who can penetrate them from both their school and home computers. Online chat rooms, listservs, and Web sites that give step-by-step directions on how to hack make it easy for students to access networks rich with confidential data (Bathon, 2013).

Growing student use of digital technology has led to increased concerns about access to, and the use of, student data created and gathered by educational websites, applications, and other online services (Lewandowski, 2019). Further, current federal student privacy laws are widely seen as inadequate and outdated. BYOD, or Bring Your Own Device, is a technique to give students the opportunity to bring their device of choice to school and connect to the school internet service.

Advocated as a means to increase student engagement, BYOD is not without security risks, primarily because students choose their own devices (Hovav & Putri, 2016). As a result, network architects and administrators often have to make tough choices about securing their networks

THE HUMAN FACTOR: EMPLOYEES

Information technology has brought with it many advantages for schools, but information security is still a major concern for schools which rely on such technology at the exclusion of analysis of the human factor (Maglaras, He, Janicke, & Evans, 2016). Employees, whether with intent or through negligence, are a great source of potential risk to schools, particularly through their decision making, Cyber risk is related to decision-making: where decisions often create largely unintended consequences for others. By virtue of its interconnectivity, unintended consequences can be multiplied many times, and in the cyber environment with extremely short timeframes (Liang, Biros, & Luse, 2016). Similarly, if the software tools provided by an organization are deemed inadequate by employees, they are often perfectly comfortable acquiring others, perhaps open-source freeware and even installing them on the organization's systems (Hadlington, 2018).

Attitudes and disregard for cybersecurity cause problems to arise with employees taking for granted measures designed to protect their networks (Evans, He, Maglaras, & Janicke, 2019). Just as an individual might be nonchalant about protecting personal computers or employing simple safeguards, a worker at a small school might think, "Why would we have to be so uptight about cybersecurity? Who would want to attack our school out in the middle of nowhere?" (McCormac, Zwaans, Parsons, Calic, Butavicius, & Pattinson, 2017). However, a phishing attack on a small network could be used as a "back door" to gain access to a larger system (Marchal, Armano, Grondahl, Saati, Singh, & Asokan, 2017).

Adversaries or cyber criminals can get into school systems relatively easily: we let them in. Phishing is a common technique to lure school employees into revealing sensitive information in an effort to compromise their bank, credit card or other personal accounts. In a phishing attempt, cyber criminals send an email purportedly to be from a legitimate person, organization or person. The recipient is asked to click on a link and enter sensitive information; the cyber-criminal then hijacks that account to steal what they can or try to lure the victim's contacts into the scheme. Another consequence of clicking on a phishing attempt could be that the link directs the person to a malicious page that infects the computer (Gupta, Arachchilage, & Psannis, 2018). A more advanced version of phishing is spear phishing which could be an email addressed to someone along the lines of "Dear Valued Customer" and sent out to the masses. A spear phishing attack, in contrast, is tailored to its target. A spear phishing attempt could appear to be from a legitimate sounding source such as a bank, government entity, or even the head of the targeted school, and be addressed to an employee or employees. The employee then gives away information as requested, often sensitive data about the school or its electronic information (Ani, He, & Tiwari, 2019).

Despite the heightened awareness to phishing, an employee could easily fall prey by hurriedly or even accidently clicking on a legitimate-looking link, thus opening up the network to a whole host of problems. Hackers can access the school network if an employee opens the cyber door for them (Esteves, Ramalho, & De Haro, 2017). Once malware is in place, viruses and worms can infect the school's operating systems. Consequently, school cybersecurity needs to move to a high level of consciousness (Guo, 2013). All the training would prove useless if one employee, out of the many thousands targeted, clicks on a link with malware. Cybersecurity has become more about behavioral aspects than of a purely technical concern. While most of the research has focused on explaining technical aspects of cybersecurity, the current environment dedicates close examination

of individual behavior as a key deterrent in the fight against cybercrime (Chu, Chau, & So, 2015).

Human factors in the context of information security have begun to gain increased attention, particularly where the use of security technologies have failed to protect schools from cyberattacks (Chou & Chou, 2016). The use of technologies is negated in instances where employees fail to follow cybersecurity protocols or engage in activities that place themselves and the school at risk. Researchers have found that employees consistently underestimated the probability of falling victim to a cybersecurity breach (Furnell, Khern-am-nuai, Esmael, Yang, & Li, 2018).

Most people tend to focus on technology when cyber security is mentioned but it is people that are the weakest point. While part of this can be attributed to education and training for users, it also emphasizes the need for policies to be in place for enforcement. For example, many users continue to use weak passwords, despite the increase risk from hacking, even though they are told to strengthen their passwords. Information security management should consider users and their perceptions as important factors in a secure environment (Ben-Asher & Gonzalez, 2015). Methods of mitigating and preventing cyber security risks need to be implemented and users, intentionally or through negligence, are an important threat to information security (Marble, Lawless, Mittu, Coyne, Abramson, & Sibley, 2015). In addition, some research is currently being conducted to determine if there are significant differences in the perceptions and behaviors of school staff members compared to the behavior of faculty.

PLANNING RECOMMENDATIONS

With the variety of threats present, what should school leaders and information technology managers do to attempt to mitigate cybersecurity issues at the school level? Nearly all schools are highly dependent on technology, specifically the internet, in their daily operations. As a consequence, internet incidents can affect the school's ability to meet educational goals. Security conscious schools are aware of cyber-risks and take measures to reduce this risk (Moody, Siponen, & Pahnila, 2018). However, it is not possible nor economically feasible to protect against all eventualities. The security planning process requires a thorough understanding of a system's assets, followed by identifying different vulnerabilities and threats that can exist and create dynamic disruption to the school (Lincke, 2015).

Plan for the Worst

Schools can benefit from a mixed approach to cyber-risk management by taking into account a wide variety of risk awareness techniques and measures to reduce risk. The best way to protect a school in cyberspace is by anticipating threats, looking at trends, learning from worst-case scenarios, and evolving with the environment (Kleinberg, Reinicke, & Cummings, 2015). Taking those bold steps and real action, instead of thinking "it will never happen to me," is part of the culture change necessary to focus on the dangers that are lurking in the vast expanse of cyberspace (Heidenreich & Gray, 2014). Cyber security promises protection and prevention using both innovative technology and an understanding of the human user. However, as a realistic activity, the school leader should plan for the worst, meaning understanding what the real consequences of a major cyber attack would entail and working backwards to develop a plan for mitigating the significances of such an attack (Hasib, 2018). In addition, school leaders must develop an attitude of, "It can happen at this school."

Plan for Ambiguity

Why is cybersecurity practice and instruction in its current state in schools? Perhaps it is because of ambiguity because cybersecurity is an emerging need to which schools have been

slow to adapt. Could it because teachers do not perceive they have the skills necessary to address cybersecurity issues in the classroom? Another possibility is that cybersecurity is often perceived as a business function. That is, cybersecurity is more of a concern of policymakers and information technology managers and school leaders than it is of teachers. Unfortunately, there does not appear to be a great deal of literature on the subject of educators' attitudes towards information security (D'Arcy & Lowry, 2017). This lack of understanding about the roles and functions of all personnel in the school leads to ambiguity and clouds the judgment of the educators in the school. What is needed is clear and present discussion and training to outline the roles and responsibilities of all persons, including students, for everyone in the school. Only when everyone is aware of their role can all participants be held accountable for their behavior and responsibility to protect the school and alleviate the ambiguity (Peccoud, Gallegos, Murch, Buchholz, & Raman, 2018).

Plan for Data Security

The primary purpose of cybersecurity in schools is to protect data and information. To successfully accomplish this, a comprehensive cybersecurity plan is essential. The following elements should be considered:

1. A school should identify the types of information in its possession, custody, or control for which it will establish security safeguards.

2. A school should assess anticipated threats, vulnerabilities, and risks to the security of protected information.

3. A school should establish and maintain appropriate policies and administrative, physical, and technical controls to address the identified threats, vulnerabilities, and risks to the security of protected information.

4. A school should inform all employees and participants (students) of their responsibilities in the security of the protected information.

5. A school should address the security of protected information in its third-party relationships.

6. A school should incorporate all school district expertise to create the most efficient and efficient deterrents to enhance the security of protected information.

7. A school should respond actively and aggressively to detected breaches of the security of protected information. (Bordoff, Chen, & Yan, 2017; Davis, 2018; Seemma, Nandhini, & Sowmiya, 2018; Tsohou, Karyda, Kokolakis, & Kiountouzis, 2015)

Plan to Develop Trust

Data breaches make up 50 percent of cyber threats (Jaeger, 2013). Students, faculty, and staff place trust in their school and its leaders, and when a data breach occurs the individuals compromised begin to lose trust in not only the school, but also they question the procedures that are set in place for prevention of data breaches and their protection. Many schools have had some form of data breach at their campus involving the personal identifiable information of students, and very few have had no data breaches, so developing and maintaining the trust of faculty, students and the school public is critical to the overall security system of the school (Lankton, McKnight, & Tripp, 2015).

Plan for Policy Compliance

As the focus of information security measures shifts from technology to human factors, many have investigated the influence and effect that information security policies have on the overall information security culture of the school (Siponen, Adam Mahmood, & Pahnila, 2014). Most schools are required to have an information security policy in place; if not they should develop

a policy. This is usually mandated by a regulatory authority (federal, state, local, accreditation, or auditor) as a condition of qualification and/or certification (Ifinedo, 2016).

Policies set mandatory guidelines to influence favorable organizational behavior when using systems or working with data. All information security policies should comply with and emphasize the school's mission and objectives (Al Kalbani, Deng, Kam, & Zhang, 2017). Security policies are created to communicate security protocols, assign clear roles and responsibilities, and provide employees with guidance to ensure security behaviors during the performance of their jobs. The roles, responsibilities, and guidelines also give clarity to who should be contacted and how information security incidents are handled (Bordoff, Chen, & Yan, 2017). When policies are complex, ambiguous, complicated, vague, or difficult for users to understand, attitudes towards compliance are negatively affected. Organizations should make their policies as understandable, relevant, and accessible as possible to all employees.

Plan and Conduct Training

Training and awareness is a foundational piece of all thriving information security cultures because people are the weakest link (Hai-Jew, 2019; Hall, 2016). Employees are provided with the requisite knowledge needed for proper use of systems, compliance with policies, and handling of data. Information security managers must implement training and awareness programs focused on policies, roles, and responsibilities (McIlwraith, 2016). Schools need to devote resources towards building information security skills across all levels of personnel and management employees. Regardless of the hardware or software system investment, the untrained or unaware employee becomes the focal point for cyberattacks (Simmonds, 2018).

Long-term training is necessary to reasonably reduce human susceptibility to violating cybersecurity protocols and exposing the school to cyberattack (Joinson & Steen, 2018). However, existing training procedures may not be effective because the cybercriminals continue to develop new and more sophisticated procedures and processes. For example, adversaries launch several new phishing websites when existing ones are blacklisted. Unfortunately, many organizations fail to maintain a high level of information security awareness over a long term (Caldwell, 2016). A continuous program that focuses on information security is required to ensure that employees will be reminded of the rules.

CLOSING THOUGHTS

The best way to protect a school in cyberspace is examining trends, learning from worst-case scenarios, and evolving with the environment. Taking those bold steps and real action, instead of thinking "it will never happen to me" is part of the culture change. If a school's leadership demonstrates and instills the importance of cybersecurity and good cyber behavior, the mindset could rub off on the employees and improve the culture. School leaders cannot expect school personnel and students to behave responsibly without providing them with the knowledge and resources to be effective. Employees are the first line of defense for the school cybersecurity system (Zammani & Razali, 2016).

Conclusions

(1) Current researchers investigating mitigating risks for school cybersecurity suggest that a 'one-size-fits-all' approach to securing cybersecurity is not currently working.
(2) More work should focus on why mitigating threats from human actors within the system is critical to the long-term success of school cybersecurity.
(3) The pace of change and advancements in technology cybersecurity has been astonishing but not shared on the human side.

(4) Continuous changes have left an ever-increasing gap between cybersecurity technological improvements and the human factor.

(5) Technological aspects of cybersecurity will continue to grow and become more effective, but what of the human factor?

REFERENCES

Abomhara, M., & Køien, G. M. (2015). Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks. *Journal of Cyber Security, 4*(1), 65-88.

Akhtar, N., Azeem, S., & Mir, G. (2014). Strategic role of internet in SMES growth strategies. *International Journal of Business Management & Economic Research, 5*(2), 20-27.

Alavi, R., Islam, S., & Mouratidis, H. (2016). An information security risk-driven investment model for analysing human factors. *Information and Computer Security, 24*(2), 205–227.

Aldawood, H., & Skinner, G. (2019). Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues. *Future Internet, 11*(3), 73.

Aleroud, A., & Zhou, L. (2017). Phishing environments, techniques, and countermeasures: A survey. *Computers & Security, 68*(2017), 160-196.

Alhogail, A., Mirza, A., & Bakry, S. H. (2015). A comprehensive human factor framework for information security in organizations. *Journal of Theoretical and Applied Information Technology, 78*(2), 201- 211.

Al Kalbani, A., Deng, H., Kam, B., & Zhang, X. (2017). Information security compliance in organizations: An institutional perspective. *Data and Information Management, 1*(2), 104-114.

Aloul, F. A. (2012). The need for effective information security awareness. *Journal of Advances in Information Technology, 3*(3), 177-183

Ani, U. D., He, H., & Tiwari, A. (2019). Human factor security: Evaluating the cybersecurity capacity of the industrial workforce. *Journal of Systems and Information Technology, 21*(1), 2-35.

Arachchilage, N. A. G., Love, S., & Beznosov, K. (2016). Phishing threat avoidance behaviour: An empirical investigation. *Computers in Human Behavior, 60*(2016), 185-197

Arlitsch, K., & Edelman, A. (2014). Staying safe: Cyber security for people and organizations. *Journal of Library Administration, 54(*1), 46-56.

Armerdeing, T. (2014). Security training is lacking: Here are tips on how to do it better. Retrieved from: *http://www.csoonline.com/article/2362793/security-leadership/security-training-islacking-here-are-tips-on-how-to-do-it-better.html*.

Atkinson, S., Furnell, S., & Phippen, A. (2009). Securing the next generation: Enhancing e-safety awareness among young people. *Computer Fraud & Security*, *2009*(7), 13-19.

Bathon, J. (2013). How little data breaches cause big problems for schools. *THE Journal*, *40*(10), 26-29.

Ben-Asher N, & Gonzalez C. (2015). Effects of cyber security knowledge on attack detection. *Computers in Human Behavior, 48*(2015), 51–61.

Bialaszewski, D. (2015). Information security in education: Are we continually improving? *Issues in Informing Science and Information Technology, 12*(2015), 45-54.

Bordoff, S., Chen, Q., & Yan, Z. (2017). Cyber-attacks, contributing factors, and tackling strategies: The current status of the science of cybersecurity. *International Journal of Cyber Behavior, Psychology and Learning (IJCBPL), 7*(4), 68-82.

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & Boss, R. W. (2009). If someone is watching, I'll do what I'm asked: Mandatoriness, control, and information security. *European Journal of Information Systems, 18*(2), 151-164

Caballero, A. (2017). Security education, training, and awareness. In J. R. Vacca (Ed.). *Computer and information security handbook* (3rd ed). (pp. 497-505). Atlanta, GA: Morgan Kaufmann.

Caldwell, T. (2016). Making security awareness training work. *Computer Fraud & Security, 2016*(6), 8-14.

Chen, I. (2014). School districts stumbled on data privacy. In M. Khosrow-Pour (Ed.). *Crisis management: Concepts, methodologies, tools, and applications* (pp. 1346-1348). IGI Global.

Chen, I. L., & Shen, L. (2016). The cyberethics, cybersafety, and cybersecurity at schools. *International Journal of Cyber Ethics in Education (IJCEE), 4*(1), 1-15.

Chen, I. L., & Shen, L. (2019). Cybercitizens at schools. In A. Blackburn, I. Linlin Chen, & R. Pfeffer (Eds.). *Emerging trends in cyber ethics and education* (pp. 91-117). Hershey, PA: IGI Global.

Chou, H. L., & Chou, C. (2016). An analysis of multiple factors relating to teachers' problematic information security behavior. *Computers in Human Behavior, 65*(2016), 334-345.

Chu, A. M. Y., Chau, P. Y. K., & So, M. K. P. (2015). Explaining the misuse of information systems resources in the workplace: A dual-process approach. *Journal of Business Ethics, 131*(1), 209-225.

Coleman, C. D., & Reeder, E. (2018, March). Three reasons for improving cybersecurity instruction and practice in schools. In *Society for Information Technology & Teacher Education International Conference* (pp. 1020-1025). Washington, DC. Association for the Advancement of Computing in Education (AACE).

Conteh, N. Y., & Schmick, P. J. (2016). Cybersecurity: Risks, vulnerabilities and countermeasures to prevent social engineering attacks. *International Journal of Advanced Computer Research, 6*(23), 31.

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review, 4*(10), 13-21.

D'Arcy, J., & Lowry, P. B. (2017). Cognitive□affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study. *Information Systems Journal, 29*(1), 43–69.

Da Veiga, A. (2019). Achieving a security culture. In I. Vasileiou & S. Furnell (Eds.). *Cybersecurity education for awareness and compliance* (pp. 72-100). Hershey, PA: IGI Global.

Davis, D. (2018, March). Best practices for balancing technology use and safety in a modern school. In *Society for Information Technology & Teacher Education International Conference* (pp. 1026-1030). Washington, DC: Association for the Advancement of Computing in Education (AACE).

Esteves, J., Ramalho, E., & De Haro, G. (2017). To improve cybersecurity, think like a hacker. *MIT Sloan Management Review, 58*(3), 71.

Evans, M., He, Y., Maglaras, L., & Janicke, H. (2019). Heart-is: A novel technique for evaluating human error-related information security incidents. *Computers & Security, 80*(2019), 74-89.

Evans, M., Maglaras, L. A., He, Y., & Janicke, H. (2016). Human behaviour as an aspect of cybersecurity assurance. *Security and Communication Networks, 9*(17), 4667-4679.

Flores, W. R., & Ekstedt, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. *Computers & Security*, *59*(2016), 26-44.

Furnell S, Khern-am-nuai W, Esmael R, Yang W, Li N. (2018). Enhancing security behaviour by supporting the user. *Computers and Security*, *75*(2018), 1–9.

Gioe, D. V., Goodman, M. S., & Wanless, A. (2019). Rebalancing cybersecurity imperatives: Patching the social layer. *Journal of Cyber Policy*, *4*(1), 117-137.

Goel, D., & Jain, A. K. (2018). Mobile phishing attacks and defence mechanisms: State of art and open research challenges. *Computers & Security*, *73*, 519-544.

Goldsborough, R. (2016). Protecting yourself from ransomware. *Teacher Librarian*, *43*(4), 70-71.

Guo, K. H. (2013). Security-related behavior in using information systems in the workplace: A review and synthesis. *Computers & Security*, *32*(2013), 242-251.

Gupta, B. B., Arachchilage, N. A., & Psannis, K. E. (2018). Defending against phishing attacks: taxonomy of methods, current issues and future directions. *Telecommunication Systems*, *67*(2), 247-267.

Gupta, B. B., Tewari, A., Jain, A. K., & Agrawal, D. P. (2017). Fighting against phishing attacks: State of the art and future challenges. *Neural Computing and Applications*, *28*(12), 3629-3654.

Gutzwiller, G. S., Fugate, S., Sawyer, B. D., & Hancock, P. A. (2015). The human factors of cyber network defense. *Proceedings of the Human Factors and Ergonomics Society*, *59*(1), 322–326.

Hai-Jew, S. (2019). The electronic hive mind and cybersecurity: Mass-scale human cognitive limits to explain the "weakest link" in cybersecurity. In B. Christiansen & A. Piekarz, (Eds.). *Global cyber security labor shortage and international business risk* (pp. 206-262). Hershey, PA: IGI Global.

Hadlington, L. (2018). The "Human Factor" in cybersecurity: Exploring the accidental insider. In J. McAlaney, L. A. Frumkin, & V. Benson (Eds.). *Psychological and behavioral examinations in cyber security* (pp. 46-63). Hershey, PA: IGI Global.

Hadlington, L. (2017). Human factors in cybersecurity; Examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon*, *3*(7), 1–18.

Hall, M. (2016). Why people are key to cyber-security. *Network Security*, *2016*(6), 9-10.

Hasib, M. (2018). Cybersecurity as people powered perpetual innovation. In S, Latifi (Ed.). *Information technology-New generations* (pp. 7-10). Cham, Switzerland: Springer.

Hatfield, J. M. (2018). Social engineering in cybersecurity: The evolution of a concept. *Computers & Security*, *73*(2018), 102-113.

Heidenreich, B., & Gray, D. H. (2014). Cyber-security: The threat of the internet. *Global Security Studies*, *5*(1), 17-26.

Hipsky, S., & Younes, W. (2015). Beyond concern: K-12 Faculty and staff's perspectives on privacy topics and cybersafety. *International Journal of Information and Communication Technology Education (IJICTE)*, *11*(4), 51-66.

Hope, A. (2018). Creep: The growing surveillance of students' online activities. *Education and Society*, *36*(1), 55-72.

Hovav, A., & Putri, F. F. (2016). This is my device! Why should I follow your rules? Employees' compliance with BYOD security policy. *Pervasive & Mobile Computing*, *32*(2016), 35-49.

Ifinedo, P. (2016). Critical times for organizations: What should be done to curb workers' noncompliance with IS security policy guidelines? *Information Systems Management*, *33*(1), 30-41.

Jaeger, J. (2013). Human error, not hackers, cause most data breaches. *Compliance Week, 10*(110), 56–57.

Javidi, G., & Sheybani, E. (2018, October). K-12 cybersecurity education, research, and outreach. In *2018 IEEE Frontiers in Education Conference (FIE)* (pp. 1-5), Cincinnati, OH. IEEE

Joinson, A., & Steen, T. V. (2018). Human aspects of cyber security: Behaviour or culture change? *Cyber Security: A Peer-Reviewed Journal, 1*(4), 351-360.

Katzan, Jr., H. (2016). Contemporary issues in cybersecurity. *Journal of Cybersecurity Research, 1*(1), 1-6

Kaur, K. (2016). Information security management of an organization with a focus on human perspective. *International Journal of Computer Techniques, 3*(2), 201-204

Kearney, P. (2010). *Security: The human factor*. Cambridgeshire, UK: IT Governance Publishing

Ki-Aries, D., & Faily, S. (2017). Persona-centered information security awareness. *Computers & Security, 70*(2017), 663–674.

Kleinberg, H., Reinicke, B., & Cummings, J. (2015). Cyber security best practices: What to do? *Journal of Information Systems Applied Research, 8*(2), 52.

Kyriazis, D. (2018). Protection of service-oriented environments serving critical infrastructures. *Inventions, 3*(3), 62.

Lankton, N., McKnight, D. H., & Tripp, J. (2015). Technology, humanness, and trust: Rethinking trust in technology. *Journal of the Association for Information Systems, 16*(10), 880–918.

Lebek, B., Uffen, J., Neumann, M., Hohler, B., & Breitner, M. H. (2014). Information security awareness and behavior: A theory-based literature review. *Management Research Review, 37*(12), 1049-1092.

Lestch, C. (2015). Cybersecurity in K-12 education: Schools face increased risk of cyber-attacks. Retrieved from: *Fedscoop. http://fedscoop. com/cybersecurity-in-k-12-educationschools-around-the-country-face-risk-of-cyber-attacks*.

Lewandowski, J. L. (2019). Intentionally secure: Teaching students to become responsible and ethical users. In A. Blackburn, I. Linlin, & R. Pfeffer (Eds.). *Emerging trends in cyber ethics and education* (pp. 118-130). Hershey, PA: IGI Global.

Liang, N., Biros, D. P., & Luse, A. (2016). An empirical validation of malicious insider characteristics. *Journal of Management Information Systems, 33*(2), 361-392.

Lincke, S. (2015). *Security planning*. New York, NY: Springer International.

Lohani, S. (2019). Social engineering: Hacking into humans. *International Journal of Advanced Studies of Scientific Research, 4*(1).

Luo. X., Brody, R., Seazzu, A., & Burd, S. (2011). Social engineering: The neglected human factor for information security management. *Information Resources Management Journal, 24*(3), 1-8.

Maglaras, L., He, Y., Janicke, H., & Evans, M. (2016). Human behaviour as an aspect of cyber security assurance. *Security and Communication Networks, 9*(17), 4667-4679

Marble, J. L., Lawless, W. F., Mittu, R., Coyne, J., Abramson, M., & Sibley, C. (2015). The human factor in cybersecurity: Robust & intelligent defense. In S. Jajodia, P. Shakarian, V. S. Subrahmanian, V. Swarup, & C. Wang (Eds.). *Cyber warfare* (pp. 173-206). Cham, Switzerland: Springer.

Marchal, S., Armano, G., Grondahl, T., Saari, K., Singh, N., & Asokan, N. (2017). Off-the-hook: An efficient and usable client-side phishing prevention application. *IEEE Transactions. on Computers, 66*(10), 1717–1733.

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and information security awareness. *Computers in Human Behavior, 69*(2017), 151-156.

McGettrick, A. (2013). Toward effective cybersecurity education. *IEEE Security & Privacy*, *6*(11), 66-68.

McIlwraith, A. (2016). *Information security and employee behaviour: How to reduce risk through employee education, training and awareness*. New York, NY: Routledge

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a unified model of information security policy compliance. *MIS Quarterly, 42*(1), 285–311.

Nobles, C. (2018). Botching human factors in cybersecurity in business organizations. *HOLISTICA–Journal of Business and Public Administration, 9*(3), 71-88.

Peccoud, J., Gallegos, J. E., Murch, R., Buchholz, W. G., & Raman, S. (2018). Cyberbiosecurity: From naive trust to risk awareness. *Trends in Biotechnology, 36*(1), 4-7.

Peltier, T. R. (2016). *Information security policies, procedures, and standards: Guidelines for effective information security management*. Boca Raton, FL: CRC Press.

Rainie, L., Anderson, J., & Connolly, J/. (2014, October). Cyber-attacks likely to increase. Washington, DC: Pew Research Internet Project. Retrieved from: http://www.pewInternet.org/2014/10/29/cyber-attacks-likely-to-increase/

Rios, E. (2017, October 25). Hackers are stealing sensitive student data – And schools are paying thousands of dollars to get it back. *Mother Jones*. Retrieved from: http://www.motherjones.com/crime-justice/2017/10/hackersare-stealing-sensitive-student-data-and-schools-are-paying-thousands-of-dollars-to-get-it-back/

Ritzman, M. E., & Kahle-Piasecki, L. (2016). What works: A systems approach to employee performance in strengthening information security. *Performance Improvement*, *55*(8), 17-22.

Rock, A. (2019, February 10). Report: K-12 schools experienced 122 cyber-attacks in 2018. *Campus Safety*.

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security, 53*(2015), 65-78.

Safa, N. S., Von Solms, R., & Futcher, L. (2016). Human aspects of information security in organisations. *Computer Fraud & Security*, *2016*(2), 15-18.

Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. *Future Internet*, *11*(4), 89-106.

Sawyer, B. D., & Hancock, P. A. (2018). Hacking the human: The prevalence paradox in cybersecurity. *Human Factors*, *60*(5), 597-609.

Sawyer, B. D., Finomore, V. S., Funke, G., Warm, J. S., Matthews, G., & Hancock, P. A. (2016). Cyber vigilance: The human factor. *American Intelligence Journal*, *32*(2), 157–165

Schuesster, J. H. (2013). Contemporary threats and countermeasures. *Journal of Information Privacy & Security, 9*(2), 3-20

Seemma, P. S., Nandhini, S., & Sowmiya, M. (2018). Overview of cyber security. *International Journal of Advanced Research in Computer and Communication Engineering, 7*(11), 125-128.

Sen, R., & Borle, S. (2015). Estimating the contextual risk of a data breach: An empirical approach. *Journal of Management Information Systems, 32*, 314-341

Shen, L., Chen, I., & Su, A. (2017). Cybersecurity and data breaches at schools. In M. Moore (Ed). *Cybersecurity breaches and issues surrounding online threat protection* (pp. 144-174). Hershey, PA: IGI Global.

Simmonds, M. (2018). Instilling a culture of data security throughout the organisation. *Network Security*, *2018*(6), 9-12.

Siponen, M., Adam Mahmood, M., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management, 51*(2), 217–224

Stewart, H., & Jürjens J. (2017). Information security management and the human aspect in organizations. *Information and Computer Security 25*(5), 494–534.

Thomas, J. (2018). Individual cyber security: Empowering employees to resist spear phishing to prevent identity theft and ransomware attacks. *International Journal of Business Management*, *12*(3), 1-23.

Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, E. (2015). Managing the introduction of information security awareness programmes in organisations. *European Journal of Information Systems, 24*(1), 38-58

Urias, V. E., Stout, W. M., & Lin, H. W. (2016, May). Gathering threat intelligence through computer network deception. In *2016 IEEE Symposium on Technologies for Homeland Security (HST)* (pp. 1-6). Boston, MA. IEEE.

Whitman, M. E., & Mattord, H. J. (2016). *Principles of information security.* (5th Ed). Boston, MA: Cengage Learning.

Zammani, M., & Razali, R. (2016). An empirical study of information security management success factors, *International Journal of Advanced Science, Engineering and Information Technology, 6*(6), 904-913.