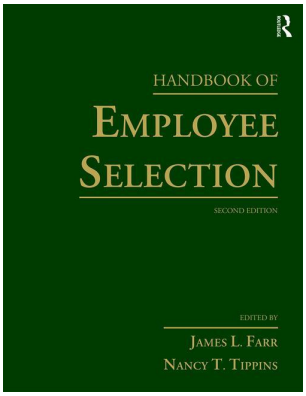

Handbook of Employee Selection

James L. Farr, Nancy T. Tippins, Walter C. Borman, David Chan, Michael D. Coovert, Rick Jacobs, P. Richard Jeanneret, Jerard F. Kehoe, Filip Lievens, S. Morton McPhail, Kevin R. Murphy, Robert E. Ployhart, Elaine D. Pulakos, Douglas H. Reynolds, Ann Marie Ryan, Neal Schmitt, Benjamin Schneider

Cybersecurity Issues in Selection

Publication details
https://test.routledgehandbooks.com/doi/10.4324/9781315690193-41
David W. Dorsey, Jaclyn Martin, David J. Howard, Michael D. Coovert
Published online on: 22 Mar 2017

41

Cybersecurity Issues in Selection

DAVID W. DORSEY, JACLYN MARTIN, DAVID J. HOWARD,
AND MICHAEL D. COOVERT

INTRODUCTION

Exponential technologies, or technologies whose performance-to-cost ratio grows faster than the pace of Moore's law, are drastically changing the modern world by propelling society forward, often with unexpected consequences (Arena, 2014; Briggs & Shingles, 2015). Examples of exponential technologies include artificial intelligence, quantum computing, and cybersecurity. These technologies challenge previously held systems in society (Briggs & Shingles, 2015). For instance, Tesla allows consumers to bypass car dealerships by selling directly to customers, while companies like Uber and Lyft are largely replacing taxi cabs.

Exponential technologies also greatly influence selection processes. The changes due to the information and telecommunications revolution in the 1980s sparked research on the role of technology in the employee selection process (see Farr & Tippins, 2010; Tippins, 2015). In many ways, technology appears to improve the selection process: online applications increase the applicant pool through greater accessibility; novel technologies facilitate the collection, storage, and analysis of assessment responses; and technology advances test development methods.

Still, the growth of exponential technologies introduces specific challenges. Namely, the rate of disruption, or the speed with which technological innovations are changing societal processes, continues to increase considerably. This indicates that no technology is stable—that is, people will continue to develop novel technologies to replace existing ones. While this does advance society, it makes it difficult for researchers and practitioners to keep up with ever-changing practices.

One constant in this era of technological change is the continuous threat of security breaches—that is, the many threats to the cybersecurity of systems that are used throughout the selection process. The aim of this chapter is to provide insight for researchers and practitioners into the challenges that are unique to cybersecurity in the selection context. Specifically, this chapter outlines the current trends in cyber attacks, cybersecurity issues within the context of current selection methods, other issues in selection, and finally, recommendations and directions for future research.

CURRENT TRENDS IN CYBERSECURITY

More than ever before, today's organizations must be aware of the threats to their internal networks and information databases. In order to defend against these attacks, it is important to know how an intruder can gain access. Attackers use several different vectors, or pathways.

These vectors include threats that occur at the personal device level, such as malware taking advantage of vulnerabilities in operating systems (e.g., Windows, Linux) and software; physical threats such as theft, unauthorized physical access, and distribution of malicious hardware (e.g., USB drives); and general network threats such as network hacking and Wi-Fi and cellular attacks. In this section, we present an overview of how attackers are able to obtain workplace information by nefarious methods and an overview of the different types of possible attacks against organizations.

Social Engineering

Before we learn some of the types of attacks intruders use to gain access to networks, it is important to understand how an attacker enters an organization's computer systems in the first place. The most common point of entry for intrusion is through social engineering. Social engineering is defined as the use of social deception, psychological tricks, and cultural ploys to help a hacker gain unauthorized access to a computer network (Abraham & Chengalur-Smith, 2010; Erbschloe, 2005). Social engineering techniques are superior to other forms of hacking because they manipulate the most vulnerable part of the system, the end user (Krombholz, Hovel, Huber, & Weippl, 2014).

It is vital to understand that no technology user is immune to social engineering tactics. Successful attacks have occurred on companies as technologically savvy as Google (Zetter, 2010), Microsoft, and Facebook (Schwartz, 2011), with social engineering methods being the initial foot-in-the-door for the attacks on all three companies. One social engineering method known as spear-phishing (i.e., receiving a targeted fraudulent e-mail that appears to be from someone you know) is an incredibly effective way for hackers to breach networks. In June 2015, this point could not be more evident as Kaspersky Labs, makers of one of the most popular antivirus programs in the market, found evidence of a nation-state spyware similar to Stuxnet and Duqu on their own internal networks, with the initial attack being traced back to a spear-phishing e-mail and zero-day exploit targeted at one of their employees in their Asia-Pacific offices (Zetter, 2015). Zero-day exploits occur when an attacker preys on a software vulnerability that is not yet known to the developer. Zero-day exploits are difficult for organizations to analyze because data on the exploit are not available until after the attack is complete (Bilge & Dumitras, 2012).

The rise of e-mail as the major form of communication in organizations gave hackers a tool to utilize social engineering manipulations. E-mail, however, is not the only method of intrusion. In 2011, the Department of Homeland Security (DHS) conducted an experiment using a technique called baiting, whereby they placed USB drives with and without the department's logo in parking lots used by government employees and private contractors. The only purpose of the USB drive when plugged into a computer was to contact the DHS experimenters to inform them that an employee had taken the bait and plugged in the USB drive that could have contained malicious code. Sixty percent of the USB drives that did not have the DHS logo were plugged into a computer. Even more shocking, 90% of the drives emboldened with the DHS logo were plugged into a PC (Rosenzweig, 2012; Schwartz, 2011).

Malware

Malware encompasses many different types of software, each designed with malicious intent to gain access to computers and networks (Hsu, Chen, Ristenpart, Li, & Su, 2006). Some of the more common examples of malware include viruses, worms, and Trojan horses (Siponen & Oinas-Kukkonen, 2007). Malware is, perhaps, the most well-known type of attack as most employees have heard of computer viruses and spyware. In fact, many employees may have anti-malware software, such as Norton Antivirus, McAfee Antivirus, or Malwarebytes Anti-Malware, installed on their personal computers. Less familiar to employees are the important differences in malware type and how each gains access to or spreads itself across a computer

network. While the end result of each type of malware is the same—to have unauthorized entry to a computer or network and execute the creator's intention—there are fundamental differences between the aforementioned malware attacks.

A virus is a program that can perform unauthorized actions on a computer and then replicate and spread itself to other computers (Cohen, 1987). Most viruses share three main components: (1) a replication mechanism allowing the virus to spread, (2) a task to perform, and (3) a trigger to execute the replication mechanism or task (Erbschloe, 2005). A worm is similar to a virus in purpose and its ability to replicate and search for other computers to infect. However, a virus requires an infected host file (i.e., carrier software) to replicate, and a worm is able to replicate without a host file and carry out its purpose as standalone software. Thus, the main difference is in how the malware travels (Cisco, n.d.; Symantec, 2015).

Trojan horses differ from worms and viruses because they do not have the ability to replicate. Instead, much like the ancient Greek horse having to be pulled into the city of Troy, digital Trojan horses rely on a user to download a file that appears to be something of interest. A well-known example is the 2001 Trojan horse that promised downloaders photos of tennis star Anna Kournikova (Glass, 2001). Once a user has downloaded the file, the Trojan horse goes into operation and infects the computer with its malicious intent. A more recent example of a Trojan horse attack occurred in November 2014, when Symantec discovered the Regin Trojan horse, malware designed to collect information on the energy, airline, hospitality, and research industries (Summers, 2014). The primary purpose of the Regin Trojan horse is thought to be espionage, and with industries now operating in an online world, it is easy to imagine the potential damage to internal systems that can be wrought by outsiders. If an employee were to download an attachment in an e-mail, and that attachment contained a Trojan horse, the creator of the Trojan horse could have unmonitored access to an organization's intellectual property.

Distributed Denial of Service (DDoS)

Distributed Denial of Service (DDoS) attacks operate in an entirely different manner from malware assaults. Traffic on the Internet is handled by web servers, and each server can only handle a set amount of traffic. DDoS attacks take advantage of a server's maximum traffic cap by flooding the server with packets of information (Kumar, 2015). In general, once a server is flooded by a DDoS attack, the server is unable to process legitimate traffic requests (e.g., an applicant attempting to access an organization's job application webpage). From the first DDoS attacks on Yahoo! and Amazon in 1999 (Bhuyan, Kashyap, Bhattacharyya, & Kalita, 2014) to the DDoS attacks that occurred over the Christmas 2014 holiday weekend that crippled the Microsoft Xbox Live and Sony Playstation Network servers (BBC News, 2014), the result remains the same: an inability to access an organization's websites or servers. As organizations move their employee application process to the online world, a DDoS attack can cripple the ability for potential applicants to begin the initial application process and also hinder the organization from accessing its own online presence.

Man-in-the-Middle Attacks (MITM)

Man-in-the-middle (MITM) attacks occur when a third party is privy to information between two unsuspecting parties and uses that access to eavesdrop on or alter the communication. An example attack could have one employee sending information encrypted with a public key[1] to another employee in the department. A third party, the attacker, could intercept the public key en route and either monitor and record the information, or the hacker might decrypt the key and control the communication between both parties. With the MITM attack in progress, the two employees believe they are communicating directly with each other (Thurimella & Mitchell, 2009), having no idea of the digital presence of the third party. An attack such as this leaves

organizations particularly vulnerable, as the two employees communicating with each other believe they are using a protected method (encryption) to transfer information.

Advanced Persistent Threat

Advanced persistent threats (APTs) are a particularly dangerous cyber attack to organizations. APTs are frequently engineered to attack a specific organization, with a target of that organization's extremely high-value data (Brewer, 2014). APTs combine multiple attack vectors, including malware, social engineering, and physical means to accomplish their objective. Three major characteristics of APTs that differentiate them from other forms of attacks are that (1) APTs repeatedly attack their target over time; (2) APTs are resistant to the target's defenses; and (3) APTs maintain the level of interaction needed to accomplish their goal (Joint Task Force Transformation Initiative, 2011). Even more troublesome is the fact that the presence of APTs on a computer network is often difficult to identify (Thomson, 2011). Intellectual property theft is a common objective of APTs, and thus any proprietary selection methods an organization creates are at risk of no longer being owned exclusively by the company that invested the resources (e.g., time, money) in developing those methods.

Anti-Forensics

An emerging trend in cybersecurity is the use of anti-forensic methods. Cyber attacks using anti-forensic methods hide their presence on a network through several different ways, including trail obfuscation, data hiding, artifact wiping, and attacks against the tools designed to detect the attack (Harris, 2006). The previously mentioned Regin Trojan horse is an example of malware designed with anti-forensic traits. While Regin's initial deployment is as a Trojan horse, the entirety of the Regin attack is polymorphic, taking place through a five-stage process. Each stage in the process is activated by the previous stage, so there is no way for digital forensics to collect complete information about the attack at any one time. The malware researchers know they are not able to see all variants of the attack on a single victim, as it only has one component (i.e., in one of the five stages) per victim at a time (Summers, 2014). Traits such as these make detection and removal of such attacks like the Regin Trojan horse difficult. Furthermore, experienced attackers are aware that slow-moving, quiet attacks are camouflaged under more "noisy" less-experienced attackers, and can employ methods to make detection akin to attempting to find a needle in a haystack.

Breach Prevention and Response

If even the employees of the DHS, Kaspersky, and Google can be deceived into falling for social engineering ploys, then how can organizations begin to prevent attacks on their systems? Organizations must be mindful that while hacker groups such as Anonymous and Lizard Squad do not have a large number of members, the relatively few hackers in existence can have disproportionate effects. Additionally, nation-states have entered into the cyber attack domain, with North Korea being responsible for the late 2014 attacks on Sony Pictures Entertainment (Niccolai, 2015), and China is now suspected of being responsible for the cyber attacks on the U.S. Office of Personnel Management, in which the personnel data for 21.5 million Americans were purloined (Banker, 2015).

One must also recognize that there is no such thing as an absolutely secure system. It is not that Target, Home Depot, Sony, JPMorgan Chase, the Postal Service, the Office of Personnel Management, and the White House simply had bad security practices when their networks were breached. To be sure, some of their security systems were better than others (e.g., Home Depot was warned of lax security policies prior to their attack; Creswell & Perlroth, 2014). However,

any threatening party putting enough time on target will get in. Attackers also benefit from the fact that there is little recourse across multiple international borders and that most companies are focused on business strategy and not on business defense (Auty, 2015).

Since there are no impervious networks, organizations must consider breach response in addition to breach prevention. In order to effectively respond to security intrusions, it is necessary to have a breach response plan in place and ready to be enacted in the inevitable event of a cyber attack (United States Department of Justice, 2015). Critical components of a breach response plan include assembling a response team prior to any security breach, fully investigating and containing the compromised computers involved, communicating and working with government and law enforcement agencies applicable to the intrusion, employing external partners such as forensic analysts and public relations firms, notifying customers who have been affected by the breach, and responding to inquiries from those customers (Experian Data Breach Resolution, 2014; United States Department of Justice, 2015). Additionally, the computers affected should be disconnected from the network and imaged for analysis, and under no circumstance should an effort be made to hack into the hackers. While this is not an exhaustive response plan, we would direct you to the Department of Justice's "Best Practices for Victim Response and Reporting of Cyber Incidents," available at http://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/04/30/04272015reporting-cyber-incidents-final.pdf, for more detailed instructions on breach response.

CURRENT SELECTION METHODS

While technological advancements facilitate the development of sophisticated cyber attacks, these innovations also encourage the growth of novel personnel selection methods. Specifically, technological evolutions recently led many companies to change the medium of selection assessment from computers to mobile devices. Moreover, companies now use technological innovation to shape selection methods through technologies involving simulation, gaming, social media, and Big Data (see Chapters 43 and 44 in this volume). This section will outline such current trends in selection methods and address the associated potential cyber threat vectors. It is essential to consider the cybersecurity issues mentioned in the previous section within the selection context because investments in test security can have huge implications for the return on investment (ROI) of organizations' hiring processes.

The selection process is now widely mediated through technology (Farr & Tippins, 2010). Applicants complete virtually all assessments (personality tests, cognitive ability tests, structured application forms) utilizing some form of technology. Specifically, applicants might complete assessments through on-site computers, personal computers, tablets, or mobile phones. Fortunately, a growing body of research suggests this transition does not always pose validity concerns, as computer-based assessment scores are often found comparable to paper-based assessment scores or at least statistically and practically comparable (Mead & Drasgow, 1993; Ployhart, Weekley, Holtz, & Kemp, 2003). However, the movement of selection assessment to technology-mediated platforms introduces several cybersecurity concerns.

Specifically, sophisticated cyber attacks—such as those mentioned in the previous section—provide the potential for unauthorized users to gain access to both the test taker's information and test content. Such information theft can result in serious issues for the organization and individual, including identity theft and the lessening of test integrity through the copy and distribution of test content. Moreover, information theft can be especially damaging to the test maker when the theft of intellectual property results in a substantial breach to test takers. For instance, Chinese students have created chatrooms in which to record as many questions from the computerized Graduate Record Exam (GRE) as they can remember after taking the exam (Hornby, 2011). This gives students who review the questions on the chatrooms a significant advantage when they complete the exam. Though the organization that produces the GRE, the Educational Testing Service (ETS), attempted to address this cheating by changing the GRE in China to paper only and retiring questions after each test, many Chinese students now fly to countries with the computerized version to complete the exam (Hornby, 2011). In addition, the

prominence of so-called braindump sites on the Internet is equally troubling. Such sites actively promote the sharing of proprietary test content. Smith (2004) demonstrated that via braindump sites, about 25% of a test item bank was exposed within three weeks of the exam being published live and with a fair amount of accuracy. After eight months, nearly the entire exam bank, more than 200 items, was posted with nearly perfect accuracy, including the answer key. Fortunately, organizations have started to evolve methodologies for combating online theft/cheating. For example, Gibson and Mulkey (2016) presented a number of techniques for using data forensics to identify stolen or compromised test material and responses. This included analyzing braindump answer keys, analyzing test response patterns to identify anomalous trends, and even using "trojan horse" items to create a test-within-a-test to detect cheating.

Another area of specific concern for cybersecurity is the growing use of mobile devices in selection. Mobile device security is simply not keeping up with the increases in mobile device usage. Survey statistics reveal that mobile devices now account for one-third of all web traffic worldwide ("StatCounter Global Stats," 2015). Furthermore, the International Data Commission (IDC) predicts that by 2017, tablets and smartphones will constitute 87% of the connected device market, with desktop and laptop PCs accounting for only 13% (Columbus, 2013). Mobile assessment in the workplace follows this global movement in that Censuswide found 78% of job applicants polled in the U.S., UK, and Australia would apply for jobs on their mobile devices (2014).

There are several reasons for the rising use of mobile devices in selection. The application of mobile devices is beneficial to organizations because it increases the applicant pool and allows for easier and faster distribution of application materials and tests, which cuts costs (Tippins, 2011). However, organizations need to be aware of the cybersecurity issues associated with mobile device usage. Mobile devices lack much of the security that PCs encompass. Specifically, mobile devices often lack firewalls, antivirus programs, and encryption (Ruggiero & Foote, 2011). The combination of widespread usage and inadequate security in mobile devices provides cyber attackers an opportunity for information theft that could result in device hijacking, identity theft, and threats to the integrity of the assessment.

Cyber attackers can compromise the security of information kept on mobile devices in several ways, including but not limited to the installation of malicious applications, "vishing," and "SMiShing" (Ruggiero & Foote, 2011; Wisenberg Brin, 2012). Vishing occurs when someone sends a fraudulent request via a voicemail message to have a person call a certain number. SMiShing occurs when a fraudulent text message is sent with a URL or phone number. Both of these methods use a message they believe will entice the user to click on the link or call back the number and ultimately give the hacker access to the device. Cyber attackers can hide malicious code that allows access to the device in seemingly innocent mobile applications (apps). Like the aforementioned phishing scams, vishing and SMiShing use social engineering to gain access to your device. However, in this case, the device is your phone.

Another way the use of mobile devices can put assessment information at risk is when mobile devices are used on public networks, which are not secure. Essentially, if a job applicant is able to access an assessment (e.g., a situational judgment test) on a public network, there is a much greater chance that the content of the assessment can be hacked. If the scenarios/questions from a test are stolen, it would compromise the integrity of the assessment and diminish the validity of the selection tool. Most attention to cybersecurity problems with mobile devices in the organizational context focuses on the potential for information or data theft from current employees' mobile devices (Wisenberg Brin, 2012). Organizations need to consider the cybersecurity implications for assessments in the selection context, as more selection procedures move to mobile devices.

In addition to the changing medium of selection assessment, organizations now utilize novel technologies in the development of selection tools. These technologies include simulation, gaming, social media, and Big Data. In practice, organizations use a wide range of simulations or virtual role plays that measure performance on tasks that closely match those that would be performed on the job. These simulations range from low-fidelity simulations, like multiple-choice text-based situational judgment tests (SJTs), to high-fidelity multimedia simulations, which present a highly realistic job scenario and encompass numerous response options. For

instance, a simulation may test piloting performance by producing a life-like scenario through flight simulator software and a hands-on-throttle-stick (HOTAS) device (Drollinger et al., 2015). Such a simulation can incorporate real-world models of physics, weather, instrument responses, and failures.

Simulations offer many advantages, such as the ability to predict a wide range of job-relevant skills with lower rates of adverse impact and a lessened susceptibility to coaching effects (Weekley, Hawkes, Guenole, & Ployhart, 2015). Conversely, research lacks clarity on which constructs simulations measure, and simulations can be costly to the organization in terms of production (Weekley et al., 2015). Moreover, it is unclear precisely what cybersecurity issues simulations may present. One concern is that simulations may become more susceptible to coaching as organizations begin to distribute the simulations via the Internet, as it is more difficult to secure the content of the test from cyber attacks. To increase the security of high-stakes assessment, Naglieri et al. (2004) recommend using a "three-tier server model" that incorporated three independent servers (an internet server, a test application server, and a database server). The authors conclude that "this configuration reduces the possibility of unauthorized intrusions into client test data" (Naglieri et al., 2004). Furthermore, the authors suggest that server traffic be actively and continuously monitored for intrusions (Naglieri et al., 2004), although this would only help with known viruses and malware. Weekley et al. (2015) also describe the likelihood for simulations to increasingly move to distribution via mobile devices, which presents some of the aforementioned vulnerability issues.

Social media represents a new and unregulated source of selection information for many practitioners. In a survey conducted by the Society for Human Resource Management (SHRM), one-fifth of respondents indicated that they use social media (i.e., Facebook, LinkedIn, Twitter, etc.) during the selection process ("Social Networking Websites and Recruiting/Selection," 2013). HR representatives find that scanning a job candidate's Facebook or LinkedIn profile is advantageous because it is a quick and cheap way to gather information on a candidate. Though there is little research on the use of social media in the employee selection process, initial examination shows mixed results in terms of the validity of the practice (Golbeck, Robles, & Turner, 2011; Park et al., 2015; Roth, Bobko, Van Iddekinge, & Thatcher, 2013; Van Iddekinge, Lanivich, Roth, & Junco, 2013).

Aside from validity issues, the use of social media in selection presents ethical and legal concerns, as most social media platforms include information about the user's age, race, gender, religion, and other information that is unlawful to use in selection. The primary cybersecurity concerns are the particular vulnerabilities presented by social engineering. Cyber attackers can profile the LinkedIn or Facebook accounts of people who work at a company to ascertain information they can employ to spoof an e-mail enticing a user to click a link that appears to be to a social media login site. By doing this, a hacker would be able to record the victim's credentials or to obtain names of coworkers, connections, or Facebook friends to use in such e-mails.

"Big Data" is a topic that has recently received much attention in organizational research and practice. As data storage costs decrease, the collection and storage of large amounts of user information increases. Certain websites, such as Facebook and Amazon, use this technology to personalize advertisements reflecting user preferences based on information gathered from previous searches, likes, and geographic location. Facebook has even used its large pool of user data to identify the times of the year when couples are most likely to break up (Gross, 2010). Evidently, the days leading up to spring break and the winter holidays offer the most distinct peaks in breakups. Given this type of data, perhaps employee posts on social media could be used to predict counterproductive work behaviors. Or perhaps certain times of the year could be identified as significantly less productive, so interventions could be introduced to alleviate this effect.

In a selection context, companies can use information from Big Data to evaluate applicants. Though this is a new area, a startup exists that can compile a comprehensive folder with all publicly available online information for a certain candidate (Preston, 2011). Because the use of Big Data in selection is still in preliminary stages, the cybersecurity implications are not yet known. However, it follows that when employers collect, store, and analyze an increasingly large amount of data, there will be greater risks for information theft, manipulation, and massaging.

As technology progresses and assessments use richer media, cyber attackers will develop new methods to gain access to test and user information. Practitioners need to be aware of the potential for cyber attacks on new and existing selection tools as these attacks have the potential to affect the psychometric standards (i.e., validity and reliability) of selection assessments. While IT departments develop preventative methods to increase cybersecurity in the workplace, increased awareness will help practitioners understand the human side of preventing breaches. Furthermore, an increased understanding of cybersecurity will aid in the development of protocols for security breach response.

ADDITIONAL ISSUES IN SELECTION

Aside from the selection methods themselves, it is essential to consider cybersecurity weaknesses in other aspects of the selection process, such as test development, applicant tracking, and the use of cybersecurity competency assessment in selection. This section gives an overview of these facets.

Many considerations accompany the development of selection assessments. For instance, organizations aim to develop assessments that have high predictive validity for job performance and positive applicant reactions. Technology enables improvement in these domains in a number of ways, such as computerized adaptive testing, computational content analysis, and new assessment validation methods. These technologies each offer ways to improve the test development stage of selection, often resulting in more valid methods that have more positive applicant reactions. On the other hand, the movement of the test development process to technology-mediated platforms introduces some cybersecurity concerns, which are important to consider, as the security of test content is essential to maintaining the validity of the assessment.

CAT technology is a method of computer-based assessment that adapts to the test taker's ability level throughout the assessment process (Wainer, Dorans, Flaugher, Green, & Mislevy, 2000). This tailored testing allows for shortened testing time without compromising the reliability of the assessment (Davison, Maraist, Hamilton, & Bing, 2012). Researchers note an increase in test security as another advantage to the CAT development method because exposure control ensures that there is minimal overlap in questions on assessments between examinees (Davey & Parshall, 1995). However, with the exponential increases in methods of information theft through cyber hacks in the last couple of decades, these controls may no longer be sufficient to ensure test security. For example, the International Test Commission (ITC) publishes guidelines on the security of tests, examinations, and other assessments that outline categories of cheating, and test theft threats now range from stealing questions during testing through digital photography to recording test content electronically (ITC, 2014). One method that provides the potential to address some of these security concerns is the development of counter-technologies, such as on-the-fly item generation (Bejar et al., 2002). Not only would this method of item development increase test security by reducing the overlap of test items, but it also prevents the storage of items, making the content more difficult to appropriate.

Another technology that could be instrumental in the development and scoring of assessments in selection is computational content analysis that allows for the automated analysis and scoring of text responses to test items (Ryan & Ployhart, 2014). The movement of essay scoring to computerized methods would presumably decrease costs while increasing the reliability. However, these methods could introduce cybersecurity concerns as the collection and storage of these large amounts of data (Big Data) for data mining electronically further invite information theft of test content, scoring algorithms, and applicant information.

A novel assessment validation method that was presented at the 2015 Society for Industrial and Organizational Psychology Conference was the use of Amazon's Mechanical Turk (MTurk) to pilot selection assessments (Beatty, Buckley, Sprenger, & Russell, 2015). MTurk is an online marketplace that essentially employs people to complete human intelligence tasks or tasks that cannot be automated (www.mturk.com). The researchers found positive indicators of data quality and participant motivation (Beatty et al., 2015). As with CAT and computerized content analysis, the cybersecurity challenges lie in the security and storage of the test content and test user data.

Organizations commonly use applicant tracking systems (ATS) to collect and organize information on candidates throughout the selection process. This software tracks the candidate from the resume search stage through phone screens and interviews (and after selection, through performance management, training, and even compensation management). The use of this technology is advantageous because it is cheaper and faster than traditional hard-copy filing systems. For instance, a standardized mass e-mail can be sent to candidates who were not selected for certain positions.

This technology introduces vulnerability in the potential for cyber attackers to access the plethora of personally identifiable information (PII) on candidates that is stored on the software. If cyber attackers get access to an organization's applicant tracking system, they would be able to find an employee's social security number, address, date of birth, phone number, and any other information that was recorded in the system throughout the selection process. The announcement that the U.S. Office of Personnel Management (OPM) was hacked for personal information from background check data, affecting an estimated 22.1 million current and former government employees, demonstrates the widespread effects that these cyber attacks on personnel data can have (Levine & Date, 2015).

Though this chapter has thus far focused on the importance of test and user information security during the selection process, another essential consideration is how selection can be used to prevent or reduce cyber breaches for organizations after employees are hired. Although test security and test user information security are important, organization-wide information theft can be much more serious. Recent examples of cyber theft for large organizations are shown in Table 41.1.

Wiederhold (2014) emphasizes that even an organization with the most cutting-edge technologies for security systems cannot prevent cyber attacks when employees fall victim to social engineering. The fact that simple mistakes (such as failing to create a strong password or sending work files to personal e-mail accounts) increase an organization's vulnerability to cyber attacks demonstrates why many refer to employees as the "weakest link" in cybersecurity (Belbey, 2015; Crossler et al., 2013; Wiederhold, 2014).

Assessing which characteristics predict cybersecurity compliance in employees could prevent some of the cyber attacks that are caused by human error. Some such assessments are in the developmental stages. For instance, Trippe, Moriarty, Russell, Carretta, and Beatty (2014) evaluated the incremental validity of a "Cyber Test" for Army personnel over technical knowledge tests for ASVAB. This test was developed for cybersecurity and information technology (IT)

TABLE 41.1
Examples of Recent Cyber Attacks

Organization	*Date*	*Estimated number of people affected*	*Information stolen*
Anthem	February 2015	80 million customers and employees	• Names • Birthdates • SSNs • Addresses • Income data
Sony Pictures	November 2014		• Contracts • Salary lists • Film budgets • Entire films • SSNs • Sensitive e-mails
Home Depot	September 2014	56 million customers	• Credit card information
JPMorgan Chase	July 2014	83 million customers	• Checking and savings account information

Adapted from Granville (2015).

positions. Still, outside of these positions, the assessment of cybersecurity competence, and specifically tests that could predict compliance with day-to-day cybersecurity procedures (i.e., locking computer, changing passwords), is particularly important for human resource and IT department positions, as those occupations typically have administrative access to all employee system login information. It is also important to note that much of today's cybersecurity activity is conducted in teams (e.g., Cyber Incident Response Teams). Accordingly, the large body of literature around the science of team formation, development, and performance has much to offer (Steinke et al., 2015), including how to select individuals into teams (also see Chapter 37 in this volume).

For most organizations, it is beneficial to consider cybersecurity compliance for all employees, yet some organizations might focus solely on cybersecurity competencies in critical positions. The obvious focus for cybersecurity competence is on positions in the IT department or other similarly technology heavy positions. The following section will address recommendations for the selection of such individuals in addition to outlining specific organizational interventions to minimize cyber vulnerabilities.

RECOMMENDATIONS

Cybercrime is a costly business for organizations. The 2013 Norton Report, published by the makers of Norton Antivirus, states that the total direct annual cost of cybercrime globally has reached US$113 billion and continues to grow (Symantec, 2013). The estimate of the total cost annually (including work-hours lost responding to cyber attacks and lawsuits as a result of security breaches) ballooned to US$445 billion annually (Nakashima & Peterson, 2014), with financial damage to organizations from intellectual property (IP) theft at US$160 billion annually (Reuters, 2014).

On a mechanical level, many steps may be taken by organizations to minimize the potential of cyber attacks on their networks. Computers used by employees should always have firewall and antivirus/anti-malware software installed, with the definitions (i.e., updates) kept current. When malware attacks are recognized by antivirus software companies such as McAfee and Kaspersky, the resolution to thwart the attacks is continuously updated in the software. Keeping antivirus software updated makes it more difficult for a hacker to breach an organization's network with a known attack. Furthermore, all operating systems (e.g., Microsoft Windows) and software (e.g., Microsoft Word, Adobe Reader, etc.) should be patched regularly to the latest version (Federal Communications Commission, n.d.; Norton, 2015). While some software updates contain fixes for software bugs, here are often patches for software vulnerabilities. Software flaws must be patched as soon as their presence is known, so hackers cannot take advantage of vulnerabilities with zero-day exploits.

Training employees in security principles is an important step to take in curbing cyber attacks. Cybersecurity training should include advising employees to avoid social engineering techniques such as "click on this link" e-mails or foreign USB sticks and guiding employees to report any suspicious e-mail or possible malware attacks (Department of Homeland Security, n.d.). Additionally, it is necessary to require employees to have strong passwords for network access and critical applications. The latest annual report from Splashdata compiles the most common passwords that were compromised by cyber attacks in 2014, a total of 3.3 million passwords. The top 25 most common passwords represented 2.2% of all passwords. The top five included "password," "qwerty," and sequential numbers such as "123456" (Martin, 2015; PRWeb, 2015). Employees who use passwords such as these leave organizations vulnerable to hackers.

Employees using non-secure passwords are not the only obstacle to adequate cyber defense. SailPoint conducted a survey among 1,000 global workers and found that 20% of employees share passwords with other employees, 56% reuse passwords, and 14% use the same password for all logins. Even more troublesome, some employees admitted they would be willing to sell their passwords for as little as US$150 (Business Wire, 2015). Recent research has shown differences in how the current workforce views security in the workplace. Duggan, Johnson, and Grawemeyer (2012) modeled password use and security among three different worker groups:

computer scientists, administrative workers, and students. Their results showed that although password security positively correlated with the sensitivity of the task, the three groups did not display the same ideology toward password use. The computer scientists viewed information security as part of their job, and passwords were a means to complete their tasks. However, administrative workers and students both felt using passwords was a cost incurred in completing their tasks. The students' and administrative workers' mindset reveals behavioral patterns and thought processes to overcome in training.

Another major aspect of cybersecurity is a focus upon security (security culture) as part of overall organizational culture. Similar to occupational health professionals analyzing safety culture and climate as part of an organizational assessment, companies must assess norms, standards, and practices that have arisen around cybersecurity. Parsons et al. (2015) reported a positive correlation between the information security culture of an organization and employees making sound security decisions. Likewise, da Veiga and Martins (2015) conducted a case study of an international financial institution over an eight-year period and found that monitoring, assessing, and influencing information security culture aided compliance with security procedures.

Furthermore, as suggested earlier, companies must focus upon cybersecurity considerations as part of employee selection. As organizations become more familiar with what constitutes a new "cyber worker," employee selection will serve as the first line of defense against cyber attacks. Currently, the field lacks a common and generally accepted definition of "cyber worker." In addition, it is unclear what specific knowledge, skills, abilities, and other characteristics drive performance in this domain. Given the seemingly infinite complexity in technologies, it is possible that the nature of technology knowledge is hierarchical, interconnected, and complex, like mathematics, thus potentially requiring different types of knowledge assessments (e.g., Davis & Yi, 2004; Dorsey, Campbell, Foster, & Miles, 1999). In addition, when focused upon specific cybersecurity skills, the typical applicant will have spent many years honing his/her knowledge and skills, thus experience (and specific types of experience) likely plays a prominent role in determining performance (Assante & Tobey, 2011). Beyond knowledge structures and deep learning over time, we need to examine the constructs that make a worker less susceptible to social-engineering tactics or indifference to password security (e.g., individuals high in the personality trait conscientiousness). Simply put, we need good predictor and criterion models that elucidate the cyber domain.

When hiring cybersecurity workers, it is important to remember that cybersecurity work requires a unique set of skills, such as reverse engineering and knowledge of domains that are not completely understood at this point. We must also ask ourselves where hackers and cybersecurity workers acquire the knowledge they use to administer or prevent attacks. Some of the most prominent hackers and cybersecurity experts in the world are high school or college dropouts (e.g., Kevin Mitnick), and currently there are few degrees available in hacking (even ethical hacking). Unfortunately, hiring professionals are currently too reliant on applicants holding technical certifications and degrees, thus many potential workers are rejected that would otherwise be excellent candidates (Yankelovich, 2013).

However, with help from the National Security Agency (NSA) and others, collegiate programs are now underway at universities across the U.S. and internationally (Dewey, 2013). Furthermore, the DHS recently created the Secretarial Honors Program, a two-year program designed to develop cyber professionals from recent college graduates (Nakashima, 2012). These advances in educational programs will help clear the ambiguity around the mysteries of the ever-changing cyber domain and thus assist in development of sound selection procedures when hiring cybersecurity employees.

Another aspect to consider in the hiring of cybersecurity employees is the difference in culture and ethos between these employees and a typical white-collar employee. Many potential cybersecurity workers tend to want to choose (1) whether to work alone (or not), (2) when they want to work, and (3) what tasks they do at any given time (Lawrence, 2014). These traits can add to the difficulty in hiring decisions. Another roadblock to the creation of well-defined hiring models for cybersecurity exists because even within the hacker community there are black hat, white hat, and gray hat hackers who have different motivations and end goals in mind when they hack. Black hat hackers are known for doing cyber attacks for their personal gain or to cause

chaos; white hat hackers are ethical hackers and generally are on the "good" side (e.g., exposing security risks in hardware, software, and websites); and gray hat hackers are a mix of the black and white (Kovacs, 2015). The picture of ethos and intent is even fuzzier when one considers growing concern over "insider threats"—those who were hired to apply cyber skills in service of the organization but who then turn and use these skills to advance a personal agenda (Azaria, Richardson, Kraus, & Subrahmanian, 2014). The challenge of insider threat is receiving increasing attention across a broad and interdisciplinary body of research, which includes contributions from computer scientists, psychologists, criminologists, and security practitioners (Azaria et al., 2014).

Although there are many obstacles to overcome in creating well-defined selection models for cybersecurity employees, the desire for these technical employees is only increasing the need for good predictors. In 2013, the demand for cybersecurity workers was 3.5 times greater than the IT worker demand overall, and 12 times the demand of the overall job market (Rosenbush, 2013). In 2014, the Pentagon announced plans to triple its cybersecurity workforce by 2016, and the Federal Bureau of Investigation announced plans to add 2,000 cyber workers that year alone (Lawrence, 2014). In 2015, after the well-publicized breaches of Target and Sony Pictures, big business's demand for cybersecurity workers can be described as "insatiable" (Anand, 2015). This increase in demand for the cybersecurity worker must be met with an equal increase in prioritization of selection methods.

The Internet of Things

In 1999, years before the current landscape of exponential technologies, Kevin Ashton foresaw the development of multiple devices connected through the Internet working together and coined the term "The Internet of Things" (Wood, 2015). Ashton proved prescient, as Gartner estimates 4.9 billion things will be connected to the Internet in 2015, up 30% from 2014. Gartner predicts the number of Internet-connected devices to reach 25 billion by 2020, with the fastest growing segment of internet-connected devices being automobiles (Gartner, 2014). Although car shoppers may be joyous that their new vehicle sports an Internet connection, organizations must be mindful that this increase in Internet-connected devices and technological advancements also grants hackers more pathways for infiltration. Thus, it is vital for companies to constantly learn, adapt, and evolve to the ever-changing technological landscape.

As mentioned previously, the ubiquity of smartphones and increase in tablet computing is the most recent technological shift impacting organizations. Gartner's (2014) survey revealed that 40% of workers use their personal smartphones at least casually for work, with 26% of workers using their personal tablets (e.g., iPad). Disturbingly, half of those users stated they perform work on their personal devices without the knowledge of their employer (Gartner, 2014). In 2014, there was a surge in malware created to breach the Android and iOS operating platforms. Malware, such as Wirelurker, preyed upon even non-jail-broken iOS devices (Epper Hoffman, 2015). An Alcatel-Lucent malware report estimated there were 15 million mobile devices infected with malware globally. The growth rate of malware infection on mobile devices was double for the first six months of 2014 as it was for the year 2013, with Android smartphones infected at the fastest rate (Alcatel-Lucent, 2014). Because of statistics such as these, policies for mobile device use, anti-malware software on personal devices used for work, and training on using personal devices for work should be a priority for organizations.

FUTURE RESEARCH DIRECTIONS

Given the nascent nature of cybersecurity research and practice, the topic of future research directions could be a chapter in and of itself. Here, we merely skim the surface of how future research might contribute to understanding cybersecurity and its role in selection systems. As a general framework for thinking about cybersecurity research, consider the three-by-three table shown in Table 41.2.

TABLE 41.2

General Framework for Cybersecurity Research Relevant to Selection

	Individual	*Team/Unit*	*Organization*
Inputs	Selecting for specific cyber skills, knowledge, attitudes, and fit Developing creative recruiting and sourcing tools to find cyber talent, including social media	Selecting for and building cyber teams	Creating organizational policies, norms, and standards around cybersecurity for individual employees
Throughputs	Predicting aspects of insider threat Providing security interventions at the level of each employee	Monitoring selection systems for exposure and compromise Countering assessment exposure with advanced adaptive testing systems	Building an internal security climate and culture
Outputs	Reinforcing security practices among external customers/end users	Building breach-response procedures and teams	Communicating an organization's cybersecurity posture externally

As shown in this table, cybersecurity is a multilevel phenomenon, affected by actions and events at the individual, team, and organizational levels. Moreover, one can consider activities, events, and interventions that are input, throughputs, or outputs of an organizational system. The entries in the cells are just a few of the myriad of possible research topics that need further exploration. We further explore just a few of these specific areas for future work as follows.

As stated earlier, one-fifth of HR professionals use social media as part of their selection process ("Social Networking Websites and Recruiting/Selection," 2013). Social media usage has skyrocketed, with Facebook alone having 1.44 billion monthly active users, and 65% of those users accessing Facebook daily (Protalinski, 2015). The amount of data being collected by these social media websites is astounding, and one potential area we commend for future research is using Latent Semantic Analysis (LSA) and related text analysis tools to understand critical cybersecurity activities and trends. Latent semantic analysis is a method of natural language processing, which employs a matrix algebra method to model combinations of words. Research has shown that cybercriminals tend to increasingly exchange cybercrime knowledge and transact via online social media (Lau & Xia, 2013); thus, text analysis of social media data could be used to understand potential threats, identify potential organizational vulnerabilities, and even to vet potential cyber job applicants.

Another fascinating and important area for research is the role of simulations, gaming, and competitions in hiring decisions, particularly as they relate to the world of cyber. The cyber worker of tomorrow might not see the value in traditional education or technical certification, but rather be self-taught in STEM fields such as computer science and programming. A traditional unstructured interview, cognitive test, or personality assessment may not motivate a person with requisite hacking skills to excel in the selection process. However, the same person might react positively when presented with a simulation scenario to prevent a new virus attack or a video game based on avoiding social engineering tactics. With the demand for excellent cybersecurity workers at an all-time high, researchers must seek creative solutions to appeal to those who are proficient in STEM skills.

Although developers and sponsors of cyber games, simulations, and competitions endorse their use, few empirical studies of their efficacy exist, and evidence from other fields such as computer science and mathematics competitions has been mixed (Tobey, Pusey, & Burley, 2014). Some research does support that cyber competitions attract experienced individuals who will remain in the profession for the long term, but future research is needed to understand how competitions may engage more diverse applicants, including those new to the field (Tobey et al., 2014).

Additionally, it is important that research continues in the cybersecurity culture domain. The applicants selected for employment become a part of the organizational culture, and that culture must promote adherence to the organization's cybersecurity policies. Although previous research has focused on defining information security culture and assessing a cybersecurity culture (Parsons et al., 2015), future work remains, such as coworker intervention studies (e.g., behavior of workers who notice another employee leaving their computers unlocked) and analysis of integrating new cyber employees into existing organizational cultures.

CONCLUSION

Exponential technologies, such as the Internet and smartphones, have forever changed the selection process for employees. Where once an applicant would have filled out a paper application and then either hand-delivered the application or mailed it through the postal service, now the applicant can seek employment by surfing the Internet on his/her smartphone, and the employer can easily collect and store the applicant's information without any physical contact. Technologies such as computer adaptive tests, social media, and high-fidelity multimedia tests have contributed to changing traditional selection methods. Although these technologies have improved the selection process immeasurably, the improvement does not come without a cost. All of the roads on the information superhighway are two-way streets, and some of the streets have "drivers" (hackers) who do not follow the rules. However, unlike a real-world traffic stop manned by the sheriff in town, it is up to organizations to police the traffic in and out of their networks and for researchers and practitioners to improve the tools used in such efforts.

NOTE

1. A public key is a value provided by a designated authority, which when combined with a private key can be used to encrypt messages.

REFERENCES

Abraham, S., & Chengalur-Smith, I. (2010). An overview of social engineering malware: Trends, tactics, and implications. *Technology in Society*, *32*(3), 183–196.

Alcatel-Lucent. (2014). *Alcatel-Lucent malware report reveals that more apps are spying on us, stealing personal information and pirating data minutes*. Retrieved July 29, 2015, from https://www.alcatel-lucent.com/press/2014/alcatel-lucent-malware-report-reveals-more-apps-are-spying-us-stealing-personal-information-and

Anand, P. (2015). *Attention, graduates: Hackers wanted*. Retrieved July 29, 2015, from http://www.marketwatch.com/story/hackers-wanted-the-ethical-ones-2015–04–22

Arena, C. (August 13 2014). *4 reasons why exponential technologies are taking off*. Retrieved August 26, 2015.

Assante, M., & Tobey, D. (2011). Enhancing the cybersecurity workforce. *IT Professional, 13*(1), 12–15. doi: 10.1109/MITP.2011.6

Auty, M. (2015). Anatomy of an advanced persistent threat. *Network Security*, *4*, 13–16.

Azaria, A., Richardson, A., Kraus, S., Subrahmanian, V. S. (2014). Behavioral analysis of insider threat: A survey and bootstrapped prediction in imbalanced data. *IEEE Transactions on Computational Social Systems, 1*(2), 135–155.

Banker, S. (2015). *The office of personnel management security breach: How does it affect our supply chains?* Retrieved July 16, 2015, from http://www.forbes.com/sites/stevebanker/2015/07/14/the-office-of-personnel-management-security-breach-how-does-it-affect-our-supply-chains/

BBC News. (December 27 2014). *Xbox and PlayStation resuming service after attack—BBC News*. Retrieved July 14, 2015.

Beatty, A., Buckley, K., Sprenger, A., & Russell, T. L. (2015). *MTurk: Piloting critical thinking items and guiding test development.* Paper presented at the Society for Industrial and Organizational Psychology's Annual Conference, Philadelphia, PA.

Bejar, I. I., Lawless, R. R., Morley, M. E., Wagner, M. E., Bennett, R. E., & Revuelta, J. (2002). A feasibility study of on-the-fly item generation in adaptive testing. *ETS Research Report Series*, 2, i–44.

Belbey, J. (2015). The Weakest Link in Cybersecurity. *Forbes*.
Bhuyan, M. H., Kashyap, H. J., Bhattacharyya, D. K., & Kalita, J. K. (2014). Detecting distributed denial of service attacks: Methods, tools and future directions. *Computer Journal, 57*(4), 537–556.
Bilge, L., & Dumitras, T. (2012). Before we knew it: An empirical study of zero-day attacks in the real world. In *Proceedings of the 2012 ACM conference on computer and communications security* (pp. 833–844). ACM.
Brewer, R. (2014). Advanced persistent threats: Minimising the damage. *Network Security*, 4, 5–9.
Briggs, B., & Shingles, M. (January 29 2015). *Tech trends 2015, exponentials*. Retrieved August 26, 2015.
Business Wire. (2015). *SailPoint Survey Confirms: Employees Will Sell Passwords for $150*. Austin, TX: Business Wire.
Cisco. (n.d.). *What is the difference: Viruses, worms, trojans, and bots?* Retrieved September 2, 2015, from http://www.cisco.com/web/about/security/intelligence/virus-worm-diffs.html
Cohen, F. (1987). Computer viruses: Theory and experiments. *Computers & Security*, 6, 22–35. doi:10.1016/0167–4048(87)90122–2
Columbus, L. (2013). *IDC: 87% of connected devices sales by 2017 will be tablets and smartphones*. Retrieved from http://www.forbes.com/sites/louiscolumbus/2013/09/12/idc-87-of-connected-devices-by-2017-will-be-tablets-and-smartphones/
Creswell, J., & Perlroth, N. (September 19 2014). *Ex-employees say home depot left data vulnerable*. Retrieved September 9, 2015, from http://www.nytimes.com/2014/09/20/business/ex-employees-say-home-depot-left-data-vulnerable.html
Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security, 32*, 90–101.
da Veiga, A., & Martins, N. (2015). Improving the information security culture through monitoring and implementation actions illustrated through a case study. *Computers & Security*, 49, 162–176. doi: 10.1016/j.cose.2014.12.006
Davey, T., & Parshall, C. G. (1995). *New algorithms for item selection and exposure control with computerized adaptive testing*. Paper presented at the Annual Meeting of the American Educational Research Association, San Francisco, CA.
Davis, F. D., & Yi, M. Y. (2004). Improving computer skill training: Behavior modeling, symbolic mental rehearsal, and the role of knowledge structures. *Journal of Applied Psychology, 89*(3), 509.
Davison, H. K., Maraist, C. C., Hamilton, R. H., & Bing, M. N. (2012). To screen or not to screen? Using the internet for selection decisions. *Employee Responsibilities and Rights Journal, 24*(1), 1–21.
Department of Homeland Security. (n.d.). *Cybersecurity 101*. Retrieved on July 29, 2015, from: http://www.dhs.gov/sites/default/files/publications/cybersecurity-101_4.pdf
Dewey, C. (2013, September 2011). *The NSA sponsors 'cyber operations' training at universities. Here's what students learn*. Washington Post online. Retrieved from: https://www.washingtonpost.com/news/the-switch/wp/2013/09/11/the-nsa-sponsors-cyber-operations-training-at-universities-heres-what-students-learn/?utm_term=.8c90e3eabc2b
Dorsey, D. W., Campbell, G. E., Foster, L. L., & Miles, D. E. (1999). Assessing knowledge structures: Relations with experience and posttraining performance. *Human Performance, 12*, 31–57.
Drollinger, S. M., Brennan, D. C., Moclaire, C. M., Olson, T. M., Vorm, E. S., & Foster, C. (2015). *Impact of gaming and simulator experience on flight performance*. Paper presented at the Society for Industrial and Organizational Psychology's Annual Conference, Philadelphia, PA.
Duggan, G. B., Johnson, H., & Grawemeyer, B. (2012). Rational security: Modeling everyday password use. *International Journal Of Human-Computer Studies*, 70415–70431. doi: 10.1016/j.ijhcs.2012.02.008
Epper Hoffman, K. (2015). Malware on the move. *SC Magazine: For IT Security Professionals (15476693), 26*(3), 16.
Erbschloe, M. (2005). *Trojans, worms, and spyware. [electronic resource]: A computer security professional's guide to malicious code*. Amsterdam, Boston : Elsevier Butterworth Heinemann, c2005.
Experian Data Breach Resolution. (2014). *Data breach response guide*. Retrieved September 9, 2015, from http://www.experian.com/assets/data-breach/brochures/2014–2015-data-breach-response-guide.pdf
Farr, J. L., & Tippins, N. T. (2010). *Handbook of employee selection*. New York: Routledge.
Federal Communications Commission. (n.d.) *Cybersecurity for Small Business*. (n.d.). Retrieved July 29, 2015, from https://www.fcc.gov/cyberforsmallbiz
Gartner. (2014). *Gartner says 4.9 billion connected*. Retrieved August 27, 2015, from http://www.gartner.com/newsroom/id/2905717
Gartner. (2014). *Gartner says 40 percent of U.S. employees of large enterprises use personally owned devices for work*. Retrieved July 29, 2015, from http://www.gartner.com/newsroom/id/2881217
Gibson, K., & Mulkey, J. (2016). *Dumping the dopes who use braindump sites: How IBM turned the tables using data forensics*. ATP Innovations in Testing Conference, Orlando, FL.
Glass, B. (May 8 2001). Know Your Enemy. *PC Magazine*, pp. 90–91.
Golbeck, J., Robles, C., & Turner, K. (2011). *Predicting personality with social media*. Paper presented at the CHI'11 extended abstracts on human factors in computing systems.

Granville, K. (February 5 2015). 9 recent cyberattacks against big businesses. *The New York Times*. Retrieved from http://www.nytimes.com

Gross, D. (2010). *Facebook knows when you'll break up*. Retrieved from http://www.cnn.com/2010/TECH/social.media/11/02/facebook.breakups/

Harris, R. (2006). Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem. *Digital Investigation, 3*(Supplement), 44–49. doi:10.1016/j.diin.2006.06.005

Hornby, L. (July 27 2011). *Gaming the GRE test in China, with a little online help (K. Wills & A. Richardson, Eds.)*. Retrieved August 26, 2015.

Hsu, F., Chen, H., Ristenpart, T., Li, J., & Su, Z. (2006, December). *Back to the future: A framework for automatic malware removal and system repair*. Paper presented at 22nd Annual Computer Security Applications Conference (pp. 257–268).

International Test Commission. (2014). ITC guidelines on quality control in scoring, test analysis, and reporting of test scores. *International Journal of Testing, 14*(3), 195–217.

Joint Task Force Transformation Initiative. (2011). *NIST Special Publication* 800-39. *Managing information security risk: Organization, mission, and information system view*. Gaithersburg, MD: National Institute of Standards and Technology.

Kovacs, N. (2015). *What is the difference between Black, White and Grey Hat Hackers?* Retrieved July 29, 2015, from http://community.norton.com/en/blogs/norton-protection-blog/what-difference-between-black-white-and-grey-hat-hackers

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2014). Advanced social engineering attacks. *Journal of Information Security and Applications, 22*, 113–122. doi: 10.1016/j.jisa.2014.09.005

Kumar, K. V. (2015). Distributed Denial of Service (DDOS) attack, networks, tools and defense. *International Journal of Applied Engineering Research, 10*(8), 20959–20971.

Lau, R., & Xia, Y. (2013). Latent text mining for cybercrime forensics. *International Journal of Future Computer and Communication, 2*(4), 368–371.

Lawrence, D. (2014). *The U.S. Government wants 6,000 New 'Cyberwarriors' by 2016*. Retrieved July 29, 2015, from http://www.bloomberg.com/bw/articles/2014–04–15/uncle-sam-wants-cyber-warriors-but-can-he-compete

Levine, M., & Date, J. (2015). 22 Million Affected by OPM Hack, Officials Say. *ABC News Network*. Retrieved from http://abcnews.go.com/US/exclusive-25-million-affected-opm-hack-sources/story?id=32332731

Martin, A. (2015). *Weakest, common passwords of 2014 revealed*. Retrieved July 29, 2015, from http://www.welivesecurity.com/2015/01/21/weakest-common-passwords-2014-revealed/

Mead, A. D., & Drasgow, F. (1993). Equivalence of computerized and paper-and-pencil cognitive ability tests: A meta-analysis. *Psychological Bulletin, 114*(3), 449.

Naglieri, J. A., Drasgow, F., Schmit, M., Handler, L., Prifitera, A., Margolis, A., & Velasquez, R. (2004). Psychological testing on the Internet: New problems, old issues. *American Psychologist, 59*(3), 150.

Nakashima, E. (2012). *Federal agencies, private firms fiercely compete in hiring cyber experts*. Retrieved July 29, 2015, from https://www.washingtonpost.com/world/national-security/federal-agencies-private-firms-fiercely-compete-in-hiring-cyber-experts/2012/11/12/a1fb1806–2504–11e2-ba29–238a6ac36a08_story.html

Nakashima, E., & Peterson, A. (June 9 2014). *Cybercrime and espionage is costing the global economy near half a trillion dollars annually*. Retrieved September 9, 2015, from https://www.washingtonpost.com/world/national-security/report-cybercrime-and-espionage-costs-445-billion-annually/2014/06/08/8995291c-ecce-11e3–9f5c-9075d5508f0a_story.html

Niccolai, J. (2015). *Code typo helps tie North Korea to the Sony hack*. Retrieved July 15, 2015, from http://www.computerworld.com/article/2885534/code-typo-helps-tie-north-korea-to-the-sony-hack.html

Norton. (2015). *Cybercrime Prevention Tips from Norton | Norton*. (n.d.). Retrieved July 29, 2015, from http://us.norton.com/prevention-tips/article

Park, G., Schwartz, H. A., Eichstaedt, J. C., Kern, M. L., Kosinski, M., Stillwell, D. J., . . . Seligman, M. E. P. (2015). Automatic personality assessment through social media language. *Journal of Personality and Social Psychology, 108*(6), 934.

Parsons, K. M., Young, E., Butavicius, M. A., McCormac, A., Pattinson, M. R., & Jerram, C. (2015). The influence of organizational information security culture on information security decision making. *Journal of Cognitive Engineering and Decision Making, 9*(2), 117–129.

Ployhart, R. E., Weekley, J. A., Holtz, B. C., & Kemp, C. (2003). Web-based and paper-and-pencil testing of applicants in a proctored setting: Are personality, biodata, and situational judgment tests comparable? *Personnel Psychology, 56*(3), 733–752.

Preston, J. (2011). Social media history becomes a new job hurdle. *New York Times*.

Protalinski, E. (April 22 2015). *Facebook passes 1.44B monthly active users and 1.25B mobile users; 65% are now daily users*. Retrieved September 9, 2015, from http://venturebeat.com/2015/04/22/facebook-passes-1–44b-monthly-active-users-1–25b-mobile-users-and-936-million-daily-users/

PRWeb. (2015). *"123456" maintains the top spot on SplashData's annual "Worst Passwords" List*. Retrieved July 29, 2015, from http://www.prweb.com/releases/2015/01/prweb12456779.htm

Reuters. (June 9, 2014). *Cyber crime costs global economy $445 billion a year: Report*. Retrieved July 29, 2015, from http://www.reuters.com/article/2014/06/09/us-cybersecurity-mcafee-csis-idUSKBN0EK0SV20140609

Rosenbush, S. (2013). *Demand for Cyber Security jobs is soaring*. Retrieved July 29, 2015, from http://blogs.wsj.com/cio/2013/03/04/demand-for-cyber-security-jobs-is-soaring/

Roth, P. L., Bobko, P., Van Iddekinge, C. H., & Thatcher, J. B. (2013). Social media in employee-selection-related decisions a research agenda for uncharted territory. *Journal of Management, 42*, 269–298. doi: 0149206313503018

Rosenzweig, P. (2012). *Thinking about cybersecurity: From cyber crime to cyber warfare*. Chantilly, VA: The Great Courses.

Ruggiero, P., & Foote, J. (2011). *Cyber threats to mobile phones*. Carnegie Mellon University Retrieved from https://http://www.us-cert.gov/sites/default/files/publications/cyber_threats-to_mobile_phones.pdf

Ryan, A. M., & Ployhart, R. E. (2014). A century of selection. *Annual Review of Psychology, 65*, 693–717.

Schwartz, M. (2011). *How USB sticks cause data breach, Malware Woes*. Retrieved July 16, 2015, from http://www.darkreading.com/risk-management/how-usb-sticks-cause-data-breach-malware-woes/d/d-id/1099437?

Siponen, M. T., & Oinas-Kukkonen, H. (2007). A review of information security issues and respective research contributions. *Database for Advances in Information Systems, 38*(1), 60. doi:10.1145/1216218.1216224.

Smith, R. W. (2004). *The impact of Braindump sites on item exposure and item parameter drift*. Paper presented at the annual meeting of the American Education Research Association, San Diego, CA.

Social Networking Websites and Recruiting/Selection. (2013). *SHRM Staffing Research*.

StatCounter Global Stats. (2015). Retrieved April 14, 2015, from http://gs.statcounter.com/

Steinke, J., Bolunmez, B., Fletcher, L., Wang, V., Tomassetti, A. J., Repchick, K. M., . . . & Tetrick, L. E. (2015). Improving cybersecurity incident response team effectiveness using teams-based research. *IEEE Security & Privacy, 13*(4), 20–29.

Summers, D. (2014). *Regin, a new piece of spyware, said to infect telecom, energy, airline industries*. Retrieved July 11, 2015, from http://fortune.com/2014/11/23/regin-malware-surveillance/

Symantec. (October 1 2013). *2013 Norton Report*. Retrieved July 29, 2015.

Symantec. (2015). *What is the difference between viruses, worms, and Trojans?* Retrieved July 14, 2015, from https://support.symantec.com/en_US/article.TECH98539.html

Thomson, G. (2011). APTs: A poorly understood challenge. *Network Security*, 11, 9–11.

Thurimella, R., & Mitchell, W. (2009). Cloak and Dagger: Man-In-The-Middle and Other Insidious Attacks. *International Journal of Information Security & Privacy, 3*(3), 55. doi: 10.4018/jisp.2009100704

Tippins, N. T. (2011). Overview of technology-enhanced assessments. In N. T. Tippins, S. Adler, & I. Kraut (Eds.), *Technology-enhanced assessment of talent* (pp. 1–18). San Francisco, CA: Jossey-Bass.

Tippins, N. T. (2015). Technology and assessment in selection. *Annual Review of Organizational Psychology and Organizational Behavior, 2*, 551–582 (Volume publication date April 2015).

Tobey, D. H., Pusey, P., & Burley, D. L. (2014). Engaging learners in cybersecurity careers: Lessons from the launch of the national cyber league. *ACM Inroads, 5*(1), 53–56. doi: =10.1145/2568195.2568213 http://doi.acm.org/10.1145/2568195.2568213

Trippe, D. M., Moriarty, K. O., Russell, T. L., Carretta, T. R., & Beatty, A. S. (2014). Development of a cyber/information technology knowledge test for military enlisted technical training qualification. *Military Psychology, 26*(3), 182.

U.S. Department of Justice. (2015). *Best practices for victim response and reporting of cyber incidents*. Retrieved August 3, 2015, from http://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/04/30/04272015reporting-cyber-incidents-final.pdf

Van Iddekinge, C. H., Lanivich, S. E., Roth, P. L., & Junco, E. (2013). Social media for selection? Validity and adverse impact potential of a facebook-based assessment. *Journal of Management, 42*, 1811–1835. doi: 0149206313515524.

Wainer, H., Dorans, N. J., Flaugher, R., Green, B. F., & Mislevy, R. J. (2000). *Computerized adaptive testing: A primer*. New York: Routledge.

Weekley, J. A., Hawkes, B., Guenole, N., & Ployhart, R. E. (2015). Low-fidelity simulations. *Annual Review of Organizational Psychology and Organizational Behavior, 2*, 295–322. doi: 10.1146/annurev-orgpsych-032414–111304

Wiederhold, B. K. (2014). The role of psychology in enhancing cybersecurity. *Cyberpsychology, Behavior, and Social Networking, 17*(3), 131–132.

Wisenberg Brin, D. (2012). *Employer beware: Spyware comes to mobile*. Retrieved from http://www.shrm.org/hrdisciplines/technology/articles/pages/spyware-comes-to-mobile.aspx

Wood, A. (2015). *The internet of things is revolutionising our lives, but standards are a must*. Retrieved August 27, 2015, from http://www.theguardian.com/media-network/2015/mar/31/the-internet-of-things-is-revolutionising-our-lives-but-standards-are-a-must

Yankelovich, M. (August 6, 2013). *Cybersecurity threats: A people problem HR can solve*. Retrieved August 27, 2015, from https://hr.blr.com/whitepapers/HR-Administration/Employee-Privacy/Cybersecurity-threats-A-people-problem-HR-can-solv

Zetter, K. (2010). *Google hack attack was ultra sophisticated, new details show*. Retrieved July 6, 2015, from http://www.wired.com/2010/01/operation-aurora/

Zeller, K. (2015). *Kaspersky finds new Nation-State attack-in its own network*. Retrieved July 12, 2015, from http://www.wired.com/2015/06/kaspersky-finds-new-nation-state-attack-network/