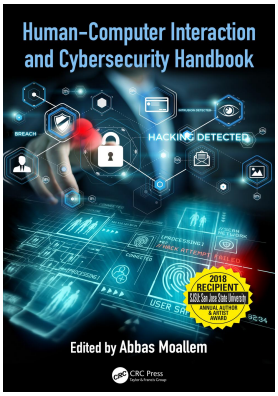

Human-Computer Interaction and Cybersecurity Handbook

Abbas Moallem

Enterprise solutions and technologies

Publication details
https://test.routledgehandbooks.com/doi/10.1201/b22142-18
Michael Cook
Published online on: 24 Oct 2018

chapter eighteen

Enterprise solutions and technologies

Michael Cook

Contents

18.1 Introduction 330
18.2 Challenges of securing the human 330
18.2.1 Phishing 330
18.2.2 E-mail accidents 332
18.2.3 Physical security 333
18.2.4 Record retention and disposal 333
18.2.5 Procurement 334
18.2.6 Human resources 334
18.2.7 Employee awareness programs 335
18.2.8 Special considerations for software and web developers 335
18.3 Role of enterprise information technology teams 336
18.3.1 Making the right solutions easy and available 336
18.3.2 Technology from the home to the office: Preparing for the Internet of things 337
18.4 Impact of controls and tools on the enterprise 338
18.4.1 Essentials 338
18.4.2 BYOD 340
18.5 Special considerations for universities, schools, public entities, libraries, and enterprises supporting intellectual and academic freedom 341
18.5.1 Compliance 342
18.5.2 HIPAA 342
18.5.3 Credit cards 343
18.5.4 FERPA 343
18.5.5 Divide and secure: Microsegmentation 344
18.5.6 BYOD for universities 345
18.5.7 Physical security 345
18.5.8 Facilities and systems 346
18.5.9 Procurement for universities 346
18.5.10 Personal tools and making the right solution the easy solution 347
18.5.11 Centralization 347
18.6 Conclusion 348
References 348

18.1 Introduction

In the enterprise, cybersecurity programs exist to protect the confidentiality, integrity, and availability of the information of the business. Some cybersecurity programs on the surface may be striving to maintain confidentiality of intellectual property, others focus on the availability of information systems, and others focus on maintaining compliance with privacy regulations in their given field. Regardless of its focus, however, the ultimate goal of any cybersecurity program is to allow the organization to effectively conduct operations while sufficiently reducing financial, reputational, or functional risk. Enterprise solutions involve a widespread array of technical tools including protections for hardware, software, databases, and physical security to reduce this risk, but the most important aspects of any cybersecurity program are the organic pieces between the seats and the keyboards, e.g., the users.

18.2 Challenges of securing the human

The employees an organization can make or break the cybersecurity program. There is very little information in this world which cannot be transmitted, copied, photographed, reproduced, recorded, or stored by both high-tech and low-tech methods. While the news is full of romantic reports of hackers in dimly lit rooms exploiting vulnerabilities in software to get their hands on private data, the reality is that the most frequent causes of exposure within organizations today are inadvertent or naive actions from within. Each year, IBM conducts a Cybersecurity Intelligence Index, which increasingly cites employee error as the source of a breach. The 2014 report in particular cites that as many as 95% of the incidents referenced in the study involve human error [1].

18.2.1 Phishing

As discussed in our chapter on social engineering, phishing is the practice of a malicious third party sending fraudulent communications to employees of the enterprise in an attempt to coerce them into revealing their system passwords or to introduce malware to the systems of the enterprise. Phishing messages often take the form of mimicking an information technology (IT) department indicating that an account is about to expire or a mailbox is full or posing as a real person the individual knows. These messages often demand a username and password to ensure that service continues uninterrupted or provides a link to download a file containing malware. These sorts of attacks work, based largely on volume, and the numbers are alarming. Phishing expert Cofense published the results of a 13-month eight million message phishing campaign across 23 industries in the United States, which did not practice phishing awareness training. The results on average indicated that the campaigns produced a 20% response rate [2], an alarming number considering that it only takes one point of entry to cause a substantial security breach.

The individuals behind these attacks are very good at what they do. Real websites and logos are duplicated, and domain names similar to the those of the organization are registered, making it extremely challenging to detect a fraudulent message. Attackers research their targets on social media and corporate websites, and they write code that alters itself to avoid detection. More advanced phishing techniques, sometimes referred to as whaling, mimic the e-mail accounts of a chief executive officer (CEO) or Chief Financial Officer requesting a wire transfer. Other attacks include phoning into accounts payable departments posing as a vendor to be paid or asking for a bank account update and more.

The following example was received by the chief financial officer of San Jose State University (SJSU) in January 2017 from a malicious third party posing as the university president:

> From: **President's Correct Name and Work E-Mail Address**
> Date: Fri, Feb 10, 2017 at 10:25 AM
> Subject: Re: REQUEST
> To: Chief Financial Officer
>
> Kindly process a domestic wire transfer now on the beneficiary details below and reply with payment confirmation when completed.
>
> Beneficiary Name: J & D Express
> Account Name: 111810823
> Routing Number: 325070760
> Bank Address: 921 Alder Ave Sumner WA 98390
> Beneficiary Address: 24843 45th Ave South R302 Kent, WA 98032
> Amount: $67,678.00 USD
>
> Best regards
> Sent from my iPad

The shock factor of receiving a message from the president of the university is intended to cause the recipient to ignore warning signs, such as an incorrect reply-to address, and complete the transaction. While this particular attempt was caught without incident, Coastal Carolina University was tricked into wiring payment to a false bank account [3].

Some of the largest reported incidents in history can be traced to phishing. In 2014, Sony Pictures incurred an estimated $100,000,000 in damages when targeted e-mails were sent to employees tricking them into trusting the wrong people exposing the credit card numbers of thousands of customers. A few months later, another group of hackers gained access to as many as 80 million medical records belonging to Anthem, one of the largest health insurance providers in the United States. The breach occurred when employees were tricked into installing malware on trusted enterprise systems [4].

What can be done about phishing? The ability to discern a fraudulent message, website, or link from a legitimate source is critical to combat phishing. Enterprises should invest in training and awareness programs which bring attention to common mistakes made by malicious third parties including missing or incorrect secure sockets layer certificates and poor spelling/grammar, and utilize URLs which are not part of the domain of the organization. Reporting phishing attempts should be easy for the employees as well. Products such as Cofense allow cybersecurity teams to send messages to their own employees in a safe controlled environment, providing employees with learning opportunities. For less than $1 per employee per year, there is a strong return on investment argument to be made when a single breach could cost a company hundreds of thousands.

In addition to nontechnical campaigns, cybersecurity programs should take a layered approach to combat phishing. Multifactor authentication (MFA) tools ensure that disclosed usernames and passwords alone do not harm the organization by requiring a one-time key, token, fob, fingerprint, cell phone app, or another "factor" aside from a username and password to sign in. While cumbersome, MFA is becoming easier to live with every day, but many organizations still do not have this technology deployed

widely due to cost and complexity of support. Antivirus and antimalware applications prevent known malicious applications from installing or spreading, but often, the individuals behind these attacks are writing code faster than antivirus vendors can write definitions to detect it. Today's advanced firewalls and e-mail filters can prevent data from being sent to known malicious addresses and can even detect and prevent new threats. Encryption technology also helps prevent the impact of a breach if an exposure were to occur. On the extreme side of the spectrum, some organizations prevent direct electronic communication outside the organization or only permit access to e-mail from known trusted networks and devices. The key is security in layers. Assess the risk to phishing, the business needs of the organization, and the budget available to deploy as many tools as practical.

18.2.2 E-mail accidents

The act of not reviewing who is in the "to" field of an e-mail or not double checking the content of a message is one of the most common forms of information disclosure within organizations. This particular challenge is exacerbated by modern e-mail clients, cell phones, and tablets, which often hide previously read portions of messages, try to predict message content, and auto-fill in recipients. In 2016, the City of Calgary investigated an incident resulting in a breach of over 3700 employees' personal data due to a member of the organization forwarding sensitive content as part of a technical support request [5].

How does an organization reduce e-mail accidents? The inadvertent transmittal of information to third parties can only be prevented through education and awareness programs. Google has recently begun integrating into their Gmail suite a reminder whenever an e-mail address outside the organization is included on a message, but this feature has yet to see widespread adoption and could easily be overlooked (Figure 18.1). In situations where communications with outside entities are required, a strong awareness campaign is really the only option.

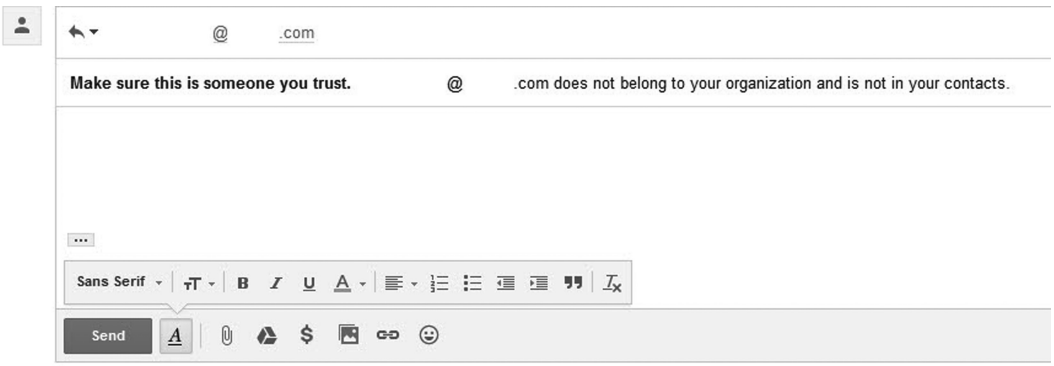

Figure 18.1 Example of an e-mail application that identifies and warns users when responding to an unknown user outside your organization.

18.2.3 Physical security

The 2014 US State of Cybercrime Survey, a joint effort by PricewaterhouseCooper, Carnegie Mellon University, CSO magazine, and the US Secret Service, reported that "only 49% of companies have a plan to address and respond to insider security threats—even though 32% of the same companies agree that crimes perpetrated by insiders are more costly and damaging than those committed by outsiders" [6]. If insiders can walk into your data center and grab a removable hard drive, they have no need to remotely break into your servers, yet physical security is often an overlooked function of an enterprise cybersecurity program [7].

Surprisingly, the Montana Department of Administration and even the Internal Revenue Service received audit findings for inadequate visitor and contractor safeguards [8]. While no two organizations are identical in the aspect of physical security the concept of open lobbies, relying on humans to be the gatekeepers to secured spaces, inadequate locking mechanisms, and unmonitored facilities are all too common, especially for small businesses and public entities.

How do companies improve physical security? Do not overlook the importance of physical security. A strong cybersecurity program should not only include extensive controls, procedures, incident response programs, and audit mechanisms for sensitive areas, but should also include controls for general-purpose spaces. Require name badges for visitors, empower employees to approach unknown parties in their workspaces, encourage clean desk policies, lock up sensitive information, and remind employees of their role in physical security at regular intervals.

18.2.4 Record retention and disposal

A lesser discussed aspect of cybersecurity is the proper retention and disposal of information. *Psychology Today* cites that there is anxiety associated with the disposition of records, especially at work, as it is all too easy to think of a scenario where a particular document type may be needed as reference in the future. This contrasts with the organizational need to destroy records at the end of their retention period in order to reduce risk and improve employee productivity. Organizations not only need to establish schedules of how long each of the document types they keep on file must be stored, but also ensure that at the end of their retention period, documents are destroyed securely. No sensitive information should be stored without establishing first how long it should be stored for and how the documents will be identified and securely destroyed following their retention periods. A strong, widely publicized, and well-known record retention and disposal program will not only reduce the risk of an organization to data exposure or discovery in legal proceedings, but also the impact of any data disclosures.

What is the right way to address record retention? Retention policies should be set with legal and operational priorities in mind, and reminders should be sent to employees regularly including procedures and retention schedules. Managers should make it part of the procedures of their departments to complete review cycles and ensure compliance. On the technical side, some document management solutions such as Hyland OnBase and ImageNow include retention management software based on document type. Other areas, especially files stored on traditional file servers, offer little in terms of real document creation dates, document types, and other needed information. Departments should establish naming conventions and procedures to ensure compliance in these more challenging scenarios and consider utilizing a more advanced document management system.

18.2.5 Procurement

A 2013 study by Trustwave, one of the world's most prominent cybersecurity firms, revealed that an estimated 63% of data breaches occurred due to some form of third-party involvement [9]. Cybersecurity programs must develop procedures for evaluating and securing agreements with third parties including evaluations of technical solutions, contract verbiage, designation of liability, background checks for employees of third parties, compliance, and other necessities. Perhaps the most famous of these incidents relates to the inadequate cybersecurity practices of Target Stores in 2013. The private network of Target, which was intended to protect over 40 million customer credit card numbers, was compromised by a heating, ventilation, and air-conditioning (HVAC) vendor, who was credentialed to have access. The vendor's credentials were used to circumvent security resulting in as many as 1.1 million credit card numbers being disclosed in 2013. Following the resignations of both the chief information officer and CEO, the $162 million breach was publicly announced [10]. Adding complexity to the challenge is the need to address all methods of procurement including purchase orders, petty cash, procurement cards, personal reimbursements, and donations. Identifying which purchases require security evaluations can be challenging; hardware, software, and software as a service purchases may all require a security evaluation.

How can procurement be improved? With the ever-growing business of software-as-a-service applications and cloud computing, storage of or access to sensitive data should be reviewed to ensure compatibility, security, compliance, and appropriate language in agreements in order to reduce the liability of the organization to exposure, fines, and other damages. Procurement personnel and the individuals requesting purchases are unlikely to be cybersecurity professionals, so a cybersecurity program must work hand in hand with the procurement department(s) of the organization to ensure that requests are sufficiently evaluated prior to purchase. Evaluations are often a conversation between the requestor, procurement, and information security teams to gain a better understanding of what types of data will be involved and how that will be transmitted or stored in order to get a better sense of what security controls may be required. Organizations such as the Cloud Security Alliance have developed comprehensive questionnaires and certification processes, which set standards and provide guidelines by which a third party's security practices can be evaluated [11]. Factors such as the third party's geographical location of data centers, disaster recovery protocols, data encryption practices, and internal security training procedures should be evaluated to ensure that the third party is held to the same standards as is the enterprise itself. The role of the cybersecurity program in procurement should pose alternatives when a requested purchase does not meet standards, consider the risks and the data types involved with the third party, be collaborative, and ensure that constituents understand why or why not a purchase was approved.

18.2.6 Human resources

Human resources departments can be a strong ally for cybersecurity programs. Human resources is the gatekeeper for who is being trusted to be privy to sensitive information within the organization. Always ensure that human resources requires appropriate criminal background checks for employees not only on the job they will be performing, but also the physical access they will require to complete that job. The same rules should apply for volunteers, interns, contractors, and anyone else who will ultimately supplement the workforce in one way or another.

18.2.7 Employee awareness programs

With so much risk placed on the employees of an organization, cybersecurity programs have a strong emphasis on employee awareness programs. Legal departments, auditors, lawmakers, and sanctioning bodies alike have made their mark on information security awareness campaigns. Regulations such as the Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI-DSS), and US Department of Justice require annual training for all employees with access to data. There is a temptation to utilize online training, training during orientation, and other easy-to-administer solutions to meet required awareness standards and satisfy the needs of auditors. This approach risks compromising the real goals of these awareness programs. The focus should be less on appeasing auditors and more on ensuring that each employee is aware of the unique aspects of their job in which information security may become relevant and know when and who to ask for help when an issue arises.

The timing and length of delivering training is critical for employees to retain the information needed to securely operate within the enterprise. The employee on-boarding process often includes information about medical benefits, signing of confidentiality agreements, emergency preparedness information, facility tours, and more. With so much information conveyed during an employee's first few days of work, security awareness may not be effectively retained. Furthermore, lengthy online trainings make security training a chore and more likely to be passively completed than other solutions. According an extensive 2007 study regarding the effectiveness of cybersecurity awareness programs in universities, factors such as cultural assumptions, regulatory agencies, beliefs, attitudes toward work, trust in leadership, and others determine the effectiveness of training. With so many variables and so many employees with differing feelings toward the work environment, there is no one-size-fits-all program approach to eliminate employee cybersecurity risks. For some employees, open forums may be successful, while for others, brief updates can be made in monthly staff meetings; for some, fliers and newsletters are effective, while for others, a brief training as part of the password reset process may be sufficient. No two organizations are alike, and no two individuals learn in the same way, so a strong cybersecurity training program needs to cover as many learning methods as possible. Instilling a culture of information security takes time; celebrate the victories, discuss thwarted phishing whaling attacks, learn from mistakes, and let the incidents of the past be an educational tool for the future. Real, relevant examples will always be a great ally. Be realistic about employees' knowledge of policies, laws, and standards [12].

18.2.8 Special considerations for software and web developers

Enterprises that develop their own applications are exposed to a whole new world of threats which must be mitigated. While the security of applications is a topic beyond the scope of this chapter, it is important to mention that there are real risks that must be addressed by programmers within the enterprise. SQL injection, where an attacker can inject malicious code into web-based applications, is perhaps the most popular of dozens of exploits which programmers need to be aware of. Heartland Payment Systems, which at the time provided credit card payment processing solutions for 175,000 customers, was fined $145,000,000 after a hacker was able to breach their security controls through SQL injection [10]. Cybersecurity programs should include special training elements for developers. Developers should be well versed in techniques attackers use to exploit software vulnerabilities including SQL injection, cross-site scripting, and web and application server configuration vulnerabilities.

The Open Web Application Security Project publishes a top 10 list of vulnerabilities, which all developers should be aware of [13]. Consider sending programmers to secure development training courses or bringing a trainer on site to keep programmers up to date on vulnerabilities. Cybersecurity and development managers should keep in mind that developing secure code is more work than developing code simply for functionality. With ever-increasing demands, it is easy for a developer to be so focused on meeting functionality goals that security is overlooked, so it is always helpful to integrate a peer code-review as part of the release management process. Make security code reusable, review it regularly, and make use of automated tools for testing. The concept of ethical hacking or penetration testing allows enterprises to test their applications using techniques developed by hackers. For environments where a live resource is not feasible, there are tools available as well, which can test for some of the most common vulnerabilities. Qualysguard Web Application Security, Trend Micro, Accunetics, TrustWave, VeriCode, and countless others offer testing applications and services to identify vulnerabilities.

18.3 Role of enterprise information technology teams

18.3.1 Making the right solutions easy and available

Enterprises today are facing the challenge of a world where technology touches every aspect of an employee's life, and technology is more obtainable than it ever has been before. Many of the employees within the enterprise are armed with technical knowledge and tools through their interactions with home computers, networks, and devices, and of course, this knowledge is often used to present ideas at work. This poses a challenge, as often technology designed for ease of use and the security demands of a home environment do not nearly meet the requirements of the enterprise. This puts IT teams in the position of having to listen more and explain why things are not as simple as they are at home.

With technology solutions at everyone's fingertips, IT teams must make the solutions of the enterprise as easy to obtain and as simple to work with as they are with their competition. Low and no-cost solutions can be readily found by any member of the organization armed with a web browser. Software-as-a-service, platform-as-a-service, and infrastructure-as-a-service providers are easy to obtain and frequently offer free trials or no-cost low transaction volume environments. Free and low-cost providers are often able to provide these services because they are accessing, sharing, and even selling the information stored in the systems which poses a significant risk to the enterprise. Even industry giant Google is utilizing information it collects from your accounts for other purposes:

> We use the information we collect from all of our services to provide, maintain, protect and improve them, to develop new ones, and to protect Google and our users. We also use this information to offer you tailored content—like giving you more relevant search results and ads.

Under the guise of tailored content, this privacy statement for Google's Gmail application is actually making their users aware that they are selling e-mail and browsing habits to the highest bidder to deliver customized advertisements. Furthermore, servers provided by third parties do not come by default with appropriate security controls such as antivirus, patch management, encryption, and strong password controls often required by enterprise cybersecurity programs. Amazon Web Services, for instance, clearly states the end user's responsibility for security in their Terms of Service:

> You are responsible for properly configuring and using the Service Offerings and otherwise taking appropriate action to secure, protect and backup your accounts and Your Content in a manner that will provide appropriate security and protection, which might include use of encryption to protect Your Content from unauthorized access and routinely archiving Your Content.

When individual contributors sign up for these services, security controls and system administration tasks are put into their hands. This means they can turn off or improperly administer firewalls, forget to install antivirus, not meet password complexity requirements, etc. In spring 2017, a server was created on Amazon Web Services for free using a personal account belonging to a SJSU faculty member. The server was used to store confidential Family Educational Rights and Privacy Act (FERPA)-protected data and compile 4-month-long projects for students in a class. When the improper configuration of the firewall of the server was combined with a weak administrator password, a malicious third party not only accessed the FERPA-protected records, but also installed ransomware encrypting the contents of the server and stopping the course dead in its tracks. The result was not only a violation of a federal law, but also a loss of the hard work of an entire semester. The underlying cause of this incident, deeper than the lack of controls, is that a problem needed to be solved, in this case, a server was needed, and the secure way to solve it was not easily obtainable. While data loss prevention (DLP) tools such as CloudLock can assist in identifying data in private clouds and tools such as Layer 7 decryption and inspection can block data from leaving a corporate network, these technologies lack the maturity to be totally effective. IT teams must therefore focus on making the right solutions easy to obtain, cost-effective, and available, or their users may be tempted to obtain their own solution. The cybersecurity program should work in concert with the IT teams to ensure that users are aware of the risks associated with finding their own solutions and know where to go in order to solve business problems in alignment with the security goals of the organization.

18.3.2 Technology from the home to the office: Preparing for the Internet of things

Among the challenges faced by IT professionals today is the expectation that the computing environment at work should be similar to that of the home. Employees today often expect to be able to wirelessly project from their laptop, expect to wirelessly print from their mobile tablets and bring any new gadget being sold online into the office. This introduces new complexities for IT professionals as not only do many of these tools rely on technologies which might not exist in the enterprise such as peer-to-peer communication or a lack of a virtual local area network segmentation to operate, but also that many of these technologies are designed for the home environment where confidential data is not stored on networks and where the risk of intrusion is far less than that in the workplace. Some organizations address these risks by enforcing policies which prevent the use of these technologies. This leaves service desk and desktop support personnel, often the primary technology interface for individuals within the organization, to explain complex security and compatibility issues. Unfortunately, the answer to "why doesn't my Apple Airplay work on the Wi-Fi?" involves explaining both why receiving an Internet protocol (IP) address in the same subnet as the AppleTV cannot be guaranteed and the intricacies of the Bonjour protocol. However, employees are typically not looking for a lecture on enterprise wireless, but rather simply want to share their screen with a projector without any wires. It is a lose–lose situation. The employee does not get what they want, and the IT team is perceived as less than helpful. Nevertheless, these situations can be turned into

win–wins. IT personnel can address many of these security risks by finding secure alternative solutions. For example, in the case of the AppleTV, a Crestron screen-sharing device will meet the need or through microsegmentation, they can create environments for known nonsecure devices to function without impacting the security of the enterprise.

The concept of the microsegmentation of networks, involves breaking networks into small segments of devices with similar access needs. In this design, for example, network-enabled HVAC devices coexist in their own network, while the public connecting to the guest Wi-Fi are in another network, and developers needing to access intellectual property are in another isolated network. Microsegmentation, especially in Wi-Fi networks, is becoming a go-to solution to support untrusted devices and improve security within the enterprise.

Network access software can identify the type of device connecting to the wired or wireless network and place it in an appropriate area of the network of the organization where it can do what it needs to do (transmit video, access the Internet, etc.) without being able to access irrelevant and unneeded sensitive resources. This allows the IT team to accommodate the request without putting any sensitive assets at risk. The 802.1x solutions such as Cisco's Identity Services Engine and Aruba's Clearpass can ensure that personal laptops have the latest antivirus definitions and operating system patches through posture evaluation. They can even make security decisions based on who is connecting and what software is installed on the device and the last time it received updates using the 802.1X protocol.

18.4 Impact of controls and tools on the enterprise

Organizations widely vary by the policies and controls that they implement and must balance risk and controls with the need to efficiently operate. The nature of the business of an organization, value of its confidential assets, its leadership, culture, regulatory agencies, and governing bodies all influence what can and cannot be written in policy and implemented using technology. In the defense or banking industries, the value of confidential assets is extremely high. It makes perfect sense for these organizations to employ strict controls, blocking communication to/from the Internet, scanning and decrypting all network traffic with the strictest of policies, requiring multiple forms of authentication, and ensuring that the only systems which can access sensitive data are owned and secured by the organization. On the opposite side of the spectrum, in the education space, the concepts of intellectual freedom, open research, and experimentation dominate the business objectives that IT departments must deliver on. Cybersecurity controls are often a detriment to mobility and rarely serve to improve the user experience. Cybersecurity programs must therefore walk a fine line between risk mitigation and business outcomes.

18.4.1 Essentials

Some organizations have the ability to take extreme measures such as blocking e-mail from untrusted devices and inspecting all web traffic; others must learn to secure their environments with little restriction. No matter what the environment, there are some basic security practices that are easy to implement, affordable, and effective in just about any organization. No enterprise today should be operating without policies and tools to ensure basic patch management and antivirus for all endpoints, firewalls to secure networks, physical security policies, and policies to assess and retire or secure dated systems.

The Center for Internet Security collaborates with cybersecurity giants such as the SANS Institute and the US Department of Defense to publish the *Critical Security Controls for Effective Cyber Defense*. While some organizations may not be able to implement in entirety, this top 20 list of essential cybersecurity controls it is a strong starting point for any cybersecurity program (Table 18.1) [14].

Table 18.1 Center for Internet Security: 20 critical controls

Critical control	Enterprise system type	Examples
CSC 1: Inventory of authorized and unauthorized devices	Endpoint management applications, inventory applications, and dynamic host configuration protocol applications	Microsoft SCCM, Jamf Casper, IBM BigFix, manual inventories, active directory, TrackIt Isupport, and Infoblox
CSC 2: Inventory of authorized and unauthorized software	Application whitelisting, antivirus/antimalware, and software inventory tools	Lumension, AppLocker, removal of administrator rights, Sophos, Symantec, Intel/McAffee, and IBM BigFix
CSC 3: Secure configurations for hardware and software on mobile devices, laptops, workstations, and servers	Endpoint management applications	Microsoft SCCM, Jamf Casper, and IBM BigFix
CSC 4: Continuous vulnerability assessment and remediation	Vulnerability scanning	Qualysguard, Rapid 7, Symantec, and Sophos
CSC 5: Controlled use of administrative privileges	Desktop configuration and MFA	Microsoft Windows, Apple OSX, Microsoft Active Directory, DUO, and Okta
CSC 6: Maintenance, monitoring, and analysis of audit logs	Log management	Splunk, LogRhythm, and Intel/McAffee
CSC 7: E-mail and web browser protections	Mail and web filters and endpoint management application	Cisco Ironport, Palo Alto Networks, Gmail, Microsoft SCCM, Jamf Casper, and IBM BigFix
CSC 8: Malware defenses	Antivirus/antimalware	Symantec, Norton, Sophos, and Intel/McAfee
CSC 9: Limitation and control of network ports, protocols, and services	802.1x authentication, port security, and firewalls	Cisco ISE, Aruba Clearpass, Cisco, HP, Palo Alto Networks, and Juniper
CSC 10: Data recovery capability	Backup and replication tools	Symantec, Veeam, IBM Spectrum Protect, Netapp, and EMC
CSC 11: Secure configurations for network devices such as firewalls, routers, and switches	Switch, network and firewall administration tools	Vendor specific
CSC 12: Boundary defense	Next-generation firewalls	Cisco, HP, Palo Alto Networks, and Juniper
CSC 13: Data protection	Encryption and DLP	Microsoft BitLocker, Apple FileVault, Netapp, EMC, Cloudlock, and Identity Finder
CSC 14: Controlled access based on the need to know	Network segmentation	Cisco, HP, Palo Alto Networks, and Juniper
CSC 15: Wireless access control	802.1x authentication	Cisco ISE and Aruba Clearpass
CSC 16: Account monitoring and control	Directory and automation tools	Microsoft Active Directory, Okta, and Phisher Identity

(*Continued*)

Table 18.1 (Continued) Center for Internet Security: 20 critical controls

Critical control	Enterprise system type	Examples
CSC 17: Security skills assessment and appropriate training to fill gaps	Information security awareness program	Skillport, LawRoom, SANS, custom solutions, in-person trainings, and Cofense
CSC 18: Application software security	Penetration testing software and ethical hackers	BURP, Qualysguard, and Rapid 7
CSC 19: Incident response and management	Policies and procedures	
CSC 20: Penetration tests and red team exercises	Penetration testing software and ethical hackers	BURP, Qualysguard, and Rapid 7

18.4.2 BYOD

Bring your own device, or BYOD, is a relatively new concept in the cybersecurity discussion. As the availability and sophistication of private services (social media, online banking, web e-mail, etc.) increases and the proliferation of work e-mail on cell phones, text messages for business communications, virtual private networks (VPNs), and telecommute programs expands, the line between work and home is blurred. At the same time, portability, the ability to customize, and the cost of personal computing devices continue to improve for the consumer, leading many individuals, when given the opportunity, to opt to use their personal devices for work tasks. After all, why carry and manage two or three or four devices when a single device is capable of getting the job done?

There is, of course, a real risk involved in allowing personal devices onto enterprise networks. BYOD means that the individual employee owns, manages, and controls the security on the endpoint. The employee is responsible for ensuring that their accounts have appropriate permissions and run without administrator rights. They are also responsible for antivirus, in control of the password policies, and in control of patch management. Some organizations, especially those in high-risk environments, simply opt to disallow unknown devices from connecting to the networks, and truly, this is the most secure method of addressing the matter; but for other organizations, BYOD is a fact of life. Enterprises should consider employing and educating employees regarding minimum security requirements for personal computers (PCs) and implementing tools to reduce the risk.

The concepts of microsegmentation and posture assessment prove useful in the BYOD space. Through posture assessment, Wi-Fi and wired networks and VPN can identify when a computer does not have antivirus installed or is not current on patches. Networks can allow BYOD on to low-risk segments, while protecting protected information. Virtual desktop infrastructure allows BYOD devices to connect to a private, secured, and organization-controlled environment to access sensitive data. Technology has adapted to the times.

The management of organization-owned devices is changing as well. The concept of immediately wiping out the manufacturer-installed copy of Windows or OSX to replace with a locked down corporate version with no authorization to change the screen saver, let alone install software is changing. Tools such as Microsoft SCCM and Jamf Casper are developing new ways of configuring, deploying, and securing devices without significantly

impacting the user experience. PC giant IBM has recently embraced this change in technology by deploying Jamf Casper to secure Apple computers as the standard-issue device for its employees. The shift has automated system deployment, while improving the security of the organization [15]. The tools today are ever changing, so before making a decision regarding BYOD, you must first understand your risk and do your homework on what tools are available to mitigate those risks while accomplishing the business objectives.

18.5 *Special considerations for universities, schools, public entities, libraries, and enterprises supporting intellectual and academic freedom*

Academic and other related enterprises have their own unique set of cybersecurity challenges. While in a corporate setting, it may be relatively straightforward to implement strict controls regarding device security and access to information, universities must balance risk avoidance with the concept of intellectual freedom. Intellectual freedom, according to the American Library Association, is "the right of every individual to both seek and receive information from all points of view without restriction." For cybersecurity professionals in a university setting, intellectual freedom means that many techniques, such as whitelisting, web traffic inspection, and e-mail monitoring, directly conflict with the university mission. Information should be able to be accessed from any device, from anywhere, without anybody watching. While primarily focusing on the university setting, the concepts in this chapter can easily be applied to cities, libraries, and other enterprises operating in an environment where risk avoidance controls may carry an intellectual freedom or political price tag.

As in other types of organizations, the biggest threats to cybersecurity in a university setting are the very people cybersecurity programs are designed to protect, the students, faculty, and staff. Universities operate much like small cities performing the work of a wide range of businesses. For example, universities house research institutes, libraries, day care centers, restaurants, construction companies, automotive repair facilities, power plants, police departments, hospitals, professional sports teams, custodial crews, Internet service providers, and computer software development teams and, of course, execute the primary mission of teaching and learning. Each area has its own set of cybersecurity challenges and regulations and unique set of users. With such a diverse environment, especially the diversity of technical skill sets belonging to individuals who have access to sensitive data, it is no surprise that the vast majority of information breaches in universities occur due to the actions of a person rather than a piece of equipment. A typical university responds to employee-created incidents vs. those from external sources at a rate of 8:1. This, coupled with the often conflicting objective of free and open learning, makes risk reduction uniquely challenging and requires extra attention to designing a multifaceted cybersecurity awareness program that appeals to all audiences, mediums, and technical skill sets.

Universities have an operational need to support intellectual freedom across an enormous number of domains and, hence, are often precluded from filtering or block content, ports, or IP addresses. There are legitimate use cases where individuals may need to access the content of questionable ethical or legal nature. Pornographic content, hacking, malware, and black-market content are all legitimate research subjects. While universities may be able to justify blocking some unwanted content such as known command and control servers and known illegal protocols (such as BitTorrents) using Layer 7 inspection on firewalls, chances are that sooner or later, an exception will need to be made if

restrictions are placed where they will have widespread impact (such as on an Internet border firewall).

Universities serve as peoples' homes as well and must function essentially as an Internet service provider. The number one consumer of bandwidth in universities is not web traffic for classes, but is often video streaming demands from dormitories. Universities must be prepared to handle large volumes of streaming traffic and be prepared to respond to or block attempts at illegal downloading from the Recording Industry Association of America and more.

18.5.1 Compliance

All universities must secure student information, and many, depending on size, have health centers, hospitals, and police departments. All universities in the United States must comply with the Family Rights and Privacy Act to protect student information and must comply with the PCI-DSS for the processing of credit cards. As such, security in each area should be as unique as the business tasks that take place in them. Each set of regulations is large enough in scale to serve as its own area of expertise. While it is beyond the scope of this chapter to explain how to comply with each regulation, there are some common pitfalls that every organization should watch out for. When working with protected information, it is always advisable to seek counsel with industry experts, legal departments, audit departments, and make use of all the resources available at your disposal as there are significant consequences for noncompliance in all cases.

18.5.2 HIPAA

The HIPAA specifies strict controls for the protection of electronic and paper information for people. In a university setting, there are typically two areas where these rules may apply, in human resources, where employees are privy to and store information regarding medical insurance, and in hospitals/health centers, which may treat faculty, staff, and students. A university may have one or many human resources departments or healthcare providers, especially universities that operate auxiliary organizations. HIPAA requires annual training for staff with access to medical records, firewalls to segment all network traffic, specific requirements for data centers, and complex contractual language to be added to all agreements with third parties among dozens of other regulations.

It is not uncommon for departments on campus that focus on accessible education or provide other clinic-type services to operate under the impression that they are a HIPAA-covered entity, when in reality, they are not. While it never hurts to have end users wanting to go the extra mile to protect data, HIPAA breach reporting requirements can be quite strict, and a cybersecurity program should identify the appropriate incident response mechanism for each area. In fact, following the HIPAA incident response protocol, which includes notification to the local media, for non-HIPAA-covered entities would pose fairly significant public relations risk for the university and its reputation. HIPAA is a complex law with specific rules regarding the transaction types and transmission/storage methods that necessitate HIPAA compliance. It is strongly advised that legal counsel, the cybersecurity office, and the administrator of each potential HIPAA-covered entity within the organization work together to determine for sure if an area is considered part of HIPAA, especially when designing incident response protocols and deploying security tools.

18.5.3 Credit cards

Credit card processing is becoming more and more available to members within any organization, and there are two areas which need to be analyzed closely and regularly: (1) financial controls and (2) the PCI-DSS. Established by the Payment Card Industry Security Standards Counsel, and composed of some of the world's largest card issuers, the PCI-DSS provides security requirements that organizations must comply with. In the past, the cost and availability of credit card processing technology made obtaining it virtually infeasible for smaller departments and individuals. However today, services such as Paypal and Square offer low or no-cost credit card processing technology. Now the flower stand on campus during graduation, the food truck driving through during lunch hour, and the vendor selling hotdogs in the stands at a football game can accept credit cards. Department managers need to be aware of their responsibilities to comply with PCI-DSS and know where to go for help. Compliance requirements may turn up in unexpected places including student clubs, supplemental applications for graduate school, and one-time fund raisers. Real headline news has been made when poor financial control decisions were made by university administrators, staff, faculty, or students leading to the misplacement of university funds, embezzlement, and other abnormalities [16].

As with traditional enterprises, an exposure of credit card information or improper processing of cardholder data has resulted in some of the most public and heavily fined exposures. What makes universities different, however, is that they often operate hundreds of distinct units with their own cardholder data environments (CDEs), whereas corporations are more likely to have one or a few explicit and extensively secured environments. University cybersecurity and credit card processing authorities have a responsibility to remain aware of changes to PCI standards and ensure compliance wherever cards are accepted. Depending on resource availability, all enterprises are advised to seek the aid of outside qualified security assessors or train internal security assessors to ensure compliance with the PCI-DSS. PCI-DSS requires extensive segmentation of networks in certain scenarios, training for card handlers, penetration testing of the CDE, annual reporting, and more. In a world where each department has its own set of applications custom tailored to their business needs, it is critical to establish standards. Each time a new method of card processing is introduced, new training and compliance programs must be established. Establish standards for the campus and minimize the number of merchant identifications used for processing to reduce efforts needed to comply with this complex set of regulations.

18.5.4 FERPA

Unique to educational organizations is the FERPA of 1978. This US federal law protecting student information was passed decades before tools such as modern enterprise resource planning applications such as Oracle's Peoplesoft, SAP, and Workday were extensively integrated into university operations but, nonetheless, significantly impacts cybersecurity today. FERPA protects every aspect of student information up to and includes information such as a student's name, grades, and class roster. FERPA breaches are the most common form of exposure in many universities and can lead to real consequences including loss of federal funding and accreditation. For example, universities are required to establish contracts ensuring total ownership and control of student information with all third parties, limit information available to parents, and more. In the

university setting, FERPA should be at the forefront of the information security awareness campaign.

- Department of Justice—The systems involved in university police operations have special considerations due to their role not only in the safety of lives on campus, but also in the sensitive nature of the data that can be accessed.
- Digital Millennium Copyright Act (DMCA)—The DMCA protects the intellectual property of digital works including, but not limited to, television, movies, and music. Universities should be aware of and prepared to handle inquiries from various entities attempting to locate those who have illegally obtained or reproduced material. A typical letter may demand the removal of the illegal content or threaten to impose fines:

> You are being contacted on behalf of NBC Universal and its affiliates ("NBC Universal") because your Internet account was identified as having been used recently to illegally copy and/or distribute the copyrighted NBC Universal motion picture(s) and/or television show(s) listed at the bottom of this letter. This notice provides you with the information you need in order to take immediate action that can prevent serious legal and other consequences. These actions include:
>
> 1. Stop downloading or uploading any motion pictures or TV shows owned or distributed by NBC Universal and/or its affiliates without authorization; and
> 2. Permanently delete from your computer(s) all unauthorized copies you may have already made of such films and/or TV shows.
>
> The illegal downloading and distribution of copyrighted works are serious offenses that carry the risk of substantial monetary damages and, in some cases, criminal prosecution.
>
> Copyright infringement also undoubtedly violates your school's policies governing acceptable use of campus network resources and could lead to serious disciplinary action.

University students, often for the first time, are being provided with commercial Internet speeds when connecting on campus, and the temptation to download illegally obtained content through BitTorrent or other services is high. Universities must require authentication for wired and wireless network ports and maintain adequate logs of IP address assignment to users. Often, the IP address and timestamp are the only pieces of information the third party will have available upon discovery of a breach to their systems. Universities must also consider blocking known ports, sites, applications, protocols, and IP addresses such as BitTorrent and PirateBay.

18.5.5 Divide and secure: Microsegmentation

The individual parts of the whole in a university setting have different business objectives. The concept of microsegmentation, or the segmenting of large networks into small, more manageable pieces that can be individually secured, is becoming increasingly popular.

By utilizing the strengths of modern multicontext firewalls, universities can start to think about security in a different way, in alignment with business needs: Most institutional research involves data which is not in any way sensitive or secret. The network traffic in dorms does not have any reason to communicate with the ERP system in human resources. The network connecting the point-of-sale systems in campus dining has to be on its own segment in order to maintain PCI compliance. Microsegmentation allows universities to implement a security strategy as unique as are the departments within the organization. Identify the areas of campus which have no need to communicate with sensitive systems, e.g., the dorms, the guest Wi-Fi, and research. Then, identify the areas of campus that have strict compliance rules, e.g., police departments and health centers, and for each area, create a unique network segment. The security of legacy HVAC, electrical control networks, and other devices with historically very poor security designs is now possible by allowing them to exist in a portion of the network unavailable to the outside world. Securing the university is not an insurmountable task but rather a process of collecting unique networks with their own unique business objectives and, as a result, security configurations.

18.5.6 BYOD for universities

Universities have little choice but to embrace and support BYOD with some estimating the impact of the Internet of things causing the number of devices on campus to double by 2020 [16]. Many universities rely on personally owned devices belonging to their faculty to support classes as well. As a result, Virtual Desktop Infrastructure, 802.1x, posture assessment when connecting to networks and strong policies and awareness programs, reminding individuals that they are responsible for their device meeting security standards, are all key pillars of a cybersecurity program. A strong responsible use policy reminding constituents that they are responsible for ensuring that personal devices meet security standards is a must as well. Universities often benefit from the generosity of their vendors. Antivirus, password vault, and patch management applications frequently offer free licenses for students or faculty use alongside the purchase of licensing for the enterprise-owned systems. Make getting the right tools into the hands of those who need them as simple as possible.

18.5.7 Physical security

An interesting aspect of universities, especially public universities, is the concept of open physical access to facilities. Libraries, classrooms, and administrative buildings are typically unlocked during regular business hours, are open for public use, and do not discriminate as to who is allowed to enter the facility. Most department offices on campuses, even police and healthcare departments, regularly employ student assistants and interns. The result is a highly open and collaborative environment for business operations, teaching, and learning. But the openness of university buildings and offices also results in an inherent information security risk. Where a typical company may employ security checkpoints, security guards, badges, biometrics, electronic access to facilities, facial recognition, and other controls, universities frequently choose not to, or cannot, implement these controls due to resource constraints or intellectual freedom. Adding to the challenge is that employees, especially student employees, are rarely required to wear name badges, so self-policing of physical parties in areas where confidential data (physical or electronic) are infrequent, and inventorying access to physical and electronic data, is even more rare. Solving this issue is primarily a matter of changing the culture. University cybersecurity programs must include a piece to empower employees to question visitors in secure spaces, encourage departments to require

name badges, lock doors or drawers which control access to sensitive data, encourage the installation of electronic door locks in lieu of hard keys, and employ name badge programs for visitors. A discernable percentage of security incidents, even thefts, involve not hackers breaking into systems, but rather a lack of a culture of physical security.

18.5.8 Facilities and systems

Seldom talked about are the unique manners in which universities receive funding and their impact on their extremely diverse facilities. Universities operate power plants, police departments, residential buildings, commercial buildings, restaurants, and more. In many universities, the term *deferred maintenance* is the vernacular term for resource constraints which result in facilities having not been upgraded in years, sometimes decades. From a cybersecurity perspective, there are a couple things that have impact. The first is that often, buildings are constructed with one-time funding using building technology that was cutting edge at the time of construction. The result is many universities are running building management systems, supervisory control and data acquisition (SCADA) systems, door lock control systems, and security camera systems which are dated and possibly plagued with information security vulnerabilities. SCADA systems, used for power management within buildings, cogeneration facilities, and in power plants, are notoriously built on dated technologies and are thus easy to compromise. Security camera systems are often procured and installed by individual contributors and departments and as part of building projects. Due to the low cost and ease of implementation, it is not uncommon for departments to purchase and install these devices without the knowledge of requirements for video retention, regular functionality testing, or the ability for the cameras to be accessed by security personnel. Regardless of the system or environment, facilities pose a myriad of challenges where upgrades may be necessary or where, in some cases, microsegmentation is the only feasible solution; the key is to be inclusive with facilities services departments and have an open dialog and an accurate inventory of the devices that they manage so that risk can be assessed and remediated as needed.

The second aspect of facility management may not be so obvious, but it centers on strategizing and setting standards. Companies that manufacture technology for facilities are good at what they do and often practice rather rapid development. They are very good at sales as well. Great care needs to be taken to ensure that compatibility and security standards are established for not just things such as network, telephony, and Wi-Fi in facilities, but also the specific facility technology which runs the building. This will not only ensure that procured systems follow laws and policies, but it also avoids duplication and unwanted diversification of systems as well. It is not at all uncommon to find multiple incompatible building management systems, multiple door access control systems, or other related services of varying degrees of compatibility and security within universities. SJSU, for instance, has three building access control systems, administered by five different departments. A strong cybersecurity program includes inventory and security methodologies for facilities management and standards for future procurement so that when decisions are made to build new buildings or procure new technology, they are done so in a fashion that helps better align security, facilities management, and the business needs of the organization.

18.5.9 Procurement for universities

Procurement can be especially challenging in a university setting as universities often do not have a single procurement office, but may have several or dozens to serve the needs

of student organizations, campus dining, facilities, athletics, research, and other operations of the campus, each with their own procurement procedures all equally contributing to risk. A strong cybersecurity program will address all procurement mechanisms used within the university including auxiliaries and individual members of the organization who may be taking advantage of reimbursements or other easy-to-use services. Irrespective of how technology is procured and what its purpose is, research or otherwise, it needs to be inventoried and properly secured by the IT staff.

18.5.10 Personal tools and making the right solution the easy solution

University employees can be quite resourceful. In the absence of availability, or barriers to make use of a service, it is not uncommon to find individuals contributing their own equipment, utilizing personal accounts for university business, or taking advantage of free programs offering services to universities. This can range from bringing in personal equipment, such as servers, to utilizing personal Hotmail accounts to communicate with students, to standing up servers in Microsoft Azure. While most organizations allow BYOD to occur and have policies requiring certain security measures, these policies are often forgotten or improperly implemented. Cybersecurity programs have an obligation to identify and address the risks associated with these practices.

The use of personal systems, personal e-mail accounts, and personal cloud services (i.e., Dropbox, Microsoft One Drive, etc.) for university business causes a number of concerns. When an individual without signing authority for the university signs an agreement for a cloud service, the security of the data stored there is immediately in jeopardy. As soon as university data make their way onto a system not controlled by the university, there could be a lack of security controls, intellectual property could be brought into question, Public Records Act queries cannot be fulfilled, administrative investigations cannot be completed, and more. Cybersecurity is not something that can always be accomplished quickly or easily and often the motivation needed to properly set up a service according to university standards is outweighed by the need to provide a solution. University IT teams must find ways to identify the types of services being provided personally, work with the individuals who have the needs, and find a way to make the right decisions easier than their less secure counterparts. Many universities have passed policy restricting the usage of personal e-mails, servers, and cloud services. Others provide no-cost virtual services to faculty. If the right service is not as easy to get as Amazon Web Services, for instance, the audience will continue to gravitate toward the easy-to-obtain solution.

IT teams do have some tools available to them to help address many situations, but they are no substitute for education, outreach, and making the right choices easy. VPN services, switches, and other network-enabling technologies now have the ability to block or permit access based on compliance. Services now exist, albeit often rather costly, that can scan cloud services within the scope of the university to perform DLP or identify sensitive data being stored in a cloud service that is not compliant with their standards. There is also a dramatic increase in cloud service providers, such as Dropbox and LucidChart, that are working with IT organizations to prevent the creation of unauthorized personal accounts using university e-mail addresses.

18.5.11 Centralization

Universities often struggle with challenges associated with decentralization and shadow IT. In some situations, departments have created their own technology teams; in others,

hobbyists have set up services that become integral parts of the organization. Some universities have 1 active directory; others have 50, with hundreds of administrators. While the discussion of centralized vs. decentralized is still a topic of debate among university administrators, the fact is that things are easier for cybersecurity programs when a single team can be the authority for configuration, compliance, and product selection. In the case of decentralized IT, individual departments customize their technology to their specific needs, and cybersecurity programs may not have as much authority to specify solutions. In these environments, cybersecurity programs need to rely on setting achievable standards and providing incentives for compliance. By offering low or no-cost tools to decentralized teams, and being openly collaborative about decisions made in the technology departments, some decentralized departments will not want to have to reinvent the wheel and will come on board. Leverage audits help auditors see where decentralized controls do not meet security standards. Finally, employ at least annual internal risk assessments to identify issues and make sure that those issues are made visible to not only technical personnel but also relevant administrators as well.

18.6 Conclusion

Enterprise systems are an ever-growing and ever-changing world. There is no shortage of new tools and services to keep any cybersecurity team busy, but it is important to not get distracted and lose focus on the human side of the cybersecurity program. A cybersecurity program needs to spend as much time on educating and building solutions with the employees in mind as it does on technology. Cybersecurity is never an easy job and often demands the support and attention of professionals in enterprise environments. Remember to communicate with stakeholders early and often and gain buy-in from business leadership and technology partners alike as new controls are implemented. Celebrate the successes, learn from the mistakes, and always remember the systems will only ever be as secure as the people who use them.

References

1. International Business Machines. 2014. *IBM Threat Force Intelligence Index*. International Business Machines, New York, https://www.ibm.com/security/data-breach/threat-intelligence-index.html.
2. PhishMe.com. 2016. *Enterprise Phishing Susceptibility Report*. PhishMe.com, Leesburg, VA, https://phishme.com/project/enterprise-phishing-susceptibility-report/.
3. Brown, Jo. 2016. Coastal Carolina University scammed out of more than $1M. *WBTW News*, http://wbtw.com/2017/03/22/coastal-carolina-university-scammed-out-of-more-than-1m/
4. Sporck, Lauren. 2016. *8 of the Largest Data Breaches of All Time*. January 18. OPSWAT, San Francisco, CA.
5. Von Ogden, Jacqueline. 2016. *8 Examples of Internal-Caused Data Breaches*. October 18. Cimcor: Merrillvile, IN.
6. Pricewaterhouse Cooper, Carnegie Mellon University, CSO magazine, US Secret Service. 2014. *US State of Cybercrime Survey*. United States Department of Homeland Security, Washington, DC.
7. Covington, Robert. 215. *Physical security: The Overlooked Domain*. Computer World, Framingham, MA, http://www.computerworld.com/article/2939322/security0/physical-security-the-overlooked-domain.html.
8. Knapp, Kenneth; Denney, Gary; and Barner, Mark E. 2011. *Key Issues in Data Center Security: An Investigation of Government Audit Reports.* August 27. Elsevier: New York, NY.

9. Ashford, Warwick. 2013. Bad outsourcing decisions cause 63% of data breaches. February 15. Computer World, Framingham, MA, http://www.computerweekly.com/news/2240178104/Bad-outsourcing-decisions-cause-63-of-data-breaches.
10. Amerdlng, Taylor. 2017. *The 15 Worst Data Security Breaches of the 21st Century*. June 14. CSO, Framingham, MA, http://www.csoonline.com/article/2130877/data-protection/data-protection-the-15-worst-data-security-breaches-of-the-21st-century.html.
11. Cloud Security Alliance. 2017. *STAR Self Assessment*. Cloud Security Alliance, https://cloudsecurityalliance.org/star/self-assessment/. Seattle, WA.
12. Resgui, Yacine. 2007. *Information Security Awareness in Higher Education: An Exploratory Study*. December 18. Elsevier: New York, NY.
13. Open Web Application Security Project. 2017. *WASP Top Ten Project*. Open Web Application Security Project, https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project. Maryland, US.
14. Center for Internet Security. https://www.cisecurity.org/controls/. East Greenbush, NY. January 19, 2017.
15. Madden, Brian. 2016. *Jamf and IBM Are Showing How Mac in the Enterprise Is Changing*. October 25. http://www.brianmadden.com/opinion/Jamf-and-IBM-are-showing-how-Mac-in-the-enterprise-is-changing. Techtarget, Newton, MA.
16. American Library Association. 2017. *Intellectual Freedom and Censorship Q & A*. American Library Association, Chicago, IL, http://www.ala.org/advocacy/intfreedom/censorship/faq.
17. *News and Observer*. 2016. Former NCSU professor charged with embezzling from agriculture student groups. February 11. http://www.newsobserver.com/news/local/crime/article59740506.html.