INFORMATION SYSTEMS EDUCATION JOURNAL

Volume 16, No. 5
October 2018
ISSN: 1545-679X

In this issue:

iscap
Information Systems & Computing Academic Professionals

The **Information Systems Education Journal** (ISEDJ) is a double-blind peer-reviewed academic journal published by **ISCAP** (Information Systems and Computing Academic Professionals). Publishing frequency is six times per year. The first year of publication was 2003.

ISEDJ is published online (http://isedj.org). Our sister publication, the Proceedings of EDSIGCON (http://www.edsigcon.org) features all papers, panels, workshops, and presentations from the conference.

The journal acceptance review process involves a minimum of three double-blind peer reviews, where both the reviewer is not aware of the identities of the authors and the authors are not aware of the identities of the reviewers. The initial reviews happen before the EDSIGCON conference. At that point papers are divided into award papers (top 15%), other journal papers (top 30%), unsettled papers, and non-journal papers. The unsettled papers are subjected to a second round of blind peer review to establish whether they will be accepted to the journal or not. Those papers that are deemed of sufficient quality are accepted for publication in the ISEDJ journal. Currently the target acceptance rate for the journal is under 40%.

Information Systems Education Journal is pleased to be listed in the Cabell's Directory of Publishing Opportunities in Educational Technology and Library Science, in both the electronic and printed editions. Questions should be addressed to the editor at editor@isedj.org or the publisher at publisher@isedj.org. Special thanks to members of AITP-EDSIG who perform the editorial and review processes for ISEDJ.

INFORMATION SYSTEMS EDUCATION JOURNAL

Editors

2018 ISEDJ Editorial Board

Cyber Security Curriculum Development: Protecting Students and Institutions While Providing Hands-On Experience

Jim Marquardson
jimarqua@nmu.edu
College of Business
Northern Michigan University
Marquette, MI 49855, USA

David L. Gomillion
dgomillion@mays.tamu.edu
Mays Business School
Texas A&M University
College Station, TX 44843, USA

Abstract

Demand for graduates with cybersecurity skills continues to increase. Many universities have developed or are in the process of developing new courses or degree programs to meet student demand and fill the skill gap in industry. Instructors face unique challenges when developing cybersecurity courses: While it is widely recognized that hands-on exercises are critical for helping students reach course learning objectives, legal, operational, and pedagogical challenges make it difficult to create safe, secure, and reusable exercises. The purpose of this article is to provide course designers principles for developing cybersecurity exercises in a way that maximizes student success while minimizing organizational risk. A matrix to help educators and administrators evaluate controls is provided, allowing for a clearer description of the risks eliminated, mitigated, and accepted. The principles provided in this article are based on the experience of developing a new cybersecurity degree program at a Midwestern university.

Keywords: Cybersecurity, Information assurance, Curriculum design and development, Computer Security, Risk assessment

1. INTRODUCTION

Cybersecurity challenges pervade the global computing infrastructure. Tens of thousands of data breaches incur millions in losses annually across the globe and across industries (Verizon, 2016). Democratic elections face hacking threats (Fidler, 2016). Fears regarding critical infrastructure have prompted governments to invest heavily in cybersecurity (Wagner, 2016). Cybersecurity concerns show no sign of abating. In such an environment, it is unsurprising that there is an increased demand for qualified cybersecurity professionals (Bernstein, 2013).

Institutions of higher education have moved quickly to create degree programs and classes to prepare students for cybersecurity careers. A common challenge that educators face is creating effective and realistic course exercises to teach cybersecurity skills without putting their institutions at significant risk. Hands-on, experiential learning has been shown to be effective in learning about information systems (Jewer & Evermann, 2015). Practicing professionals have stated that, "[t]here must be a strong emphasis on practical exposure to concepts in terms of hands-on experience for students" (Sauls & Gudigantala, 2013, p. 72).

Cybersecurity exercises, by their nature, present significant risk of causing harm, something unique to cybersecurity.

At the risk of stating the obvious, all cybersecurity exercises should be conducted legally. Passive defensive measures like firewalls, anti-virus, and updating operating systems are safe activities that stand little chance of offending the law. However, students need to learn active defensive tools and offensive hacker tools and techniques to know how to protect systems. Students must only perform these security exercises on systems with explicit authorization.

The current state of the art is to perform testing in an isolated environment, typically using virtualization and a segmented network. This is an effective step in protecting the organization, but it may not be enough. Virtualized labs suffer from limitations in scope and experience. Simulating a connection to a social media platform can pose significant challenges to instructors because of the complexity of systems behind those platforms. In addition, recognizing real threats from outside actors requires experiencing these attacks. This leads many instructors to transition away from the isolated lab towards live security testing, which can touch real networks and the internet.

With live security testing, protecting your institution's network and reputation can be difficult for two major reasons: inadvertent student mistakes and purposeful malicious use of their newly developed skills (Nurse et al., 2014). An example of an accidental breach could be a port scanning exercise. Network administrators scan open ports on network hosts to assess their systems, but hackers also scan ports to probe potential victims for exploitable weaknesses. While most security experts may not consider port scanning to be malicious, prosecution is a very real possibility. For example, Scott Moulton scanned a Cherokee County, Georgia web server and was charged with violating the Computer Fraud and Abuse Act of America (Lyon, 2008). Though Moulton was eventually acquitted, the case shows that even seemingly innocuous activities can be interpreted as malicious crimes. A classroom port scanning exercise might ask students to scan a specific internet protocol (IP) address. With an active internet connection, a mistyped IP address could cause a port scan to be conducted on a computer for which the student does not have the required authorization. It is imperative that safeguards are put in place to ensure that simple mistakes do not land students or educational institutions in legal trouble. Universities also must protect their reputation by not engaging in activity that appears to be illegal.

Malicious insiders are individuals within an organization who intentionally abuse acceptable use policies and intend to do the organization harm (Cappelli, Moore, & Trzeciak, 2012). It is essential to teach students the tools and techniques used by malicious actors; unfortunately, a portion of students may employ those tools and techniques in unauthorized ways. For example, one student used keylogging software to steal credentials that allowed him to alter his grades (Osborne, 2012). In another instance in which the present authors were made aware, a member of a student cybersecurity club learned about session hijacking and used that knowledge to view a peer's private Facebook data without permission. It is important to note that these examples occurred outside of formal classroom exercises but leveraged skills taught in the cybersecurity programs. Identity theft, Federal Educational Rights and Privacy Act (FERPA) violations, denial of service attacks, and cyberbullying are just some of the examples of what malicious actors inside campus environments might carry out. Actions taken by network administrators to protect network perimeters are often ineffective against tools and techniques initiated by insiders (Harrison, 2005).

But how can educators anticipate all the risks inherent in cybersecurity curriculum? And how can they communicate the protections put into place so that risk managers at institutions of higher learning can be comfortable with level of risk the organization is accepting? In the following sections we discuss pedagogical considerations, the risk assessment process, controls, and actions that educators can take to protect their students and their organizations. Educators can use the guidance in this paper to ensure that their universities are employing sufficient resources and attention to keeping their organizations safe while delivering value to students.

2. PEDAGOGY

Universities have chosen to create cybersecurity programs from a variety of perspectives. Cybersecurity programs are currently housed in business, computer science, computer engineering, criminal justice and other departments. Depending on the program, emphasis may be given to network administration, penetration testing, forensics, legal matters, to name just a few key areas of cybersecurity. These different perspectives provide students with diverse educational

backgrounds to provide complementary skills to the workplace. However, the distinct curriculum at institutions makes it difficult to provide one all-encompassing guide for delivering a cybersecurity curriculum. This extends to ensuring the curriculum is taught safely. Therefore, the first step to ensuring that cybersecurity exercises are done safely it to determine the scope of the curriculum.

Once the learning objectives have been identified, activities to meet those objectives must be planned. In research, tension exists between research methods. Research methods can excel in rigor, relevance, or generalizability, but not all three simultaneously (McGrath, Martin, & Kulka, 1982). A similar challenge exists in pedagogy. Internship experience is highly relevant, but those experiences may not be generalizable across industries, and due to business needs, the work may lack educational rigor. A virtual lab environment can be tuned to provide educational rigor at the expense of relevance. Instructors can focus teaching on principles that can be broadly applied in many contexts, but in so doing usually must relax rigor and relevance.

The process of developing effective and clear objectives is an important topic but beyond the scope of the current work. But once those objectives are defined, the risks of exercises used to reach those objectives must be weighed against the educational value. We provide a risk assessment process to help in identifying controls to help address the identified risks.

3. RISK ASSESSMENT

Risk assessments are key activities undertaken when information systems are deployed (Dhillon & Torkzadeh, 2006). Educators should practice what they preach and perform risk assessments on their own cybersecurity exercises. When assessing risk, educators must thoroughly assess the different ways in which an exercise could cause harm. The primary goals of risk assessments in the cybersecurity exercise context are to ensure that exercises are performed legally and prevent harm to infrastructure. Depending on the risks identified, the risk assessment may not need formal documentation and organizational sign-off, but risks should be evaluated and proper controls should be put in place. But in other exercises, the proper organizational authorizations must be obtained.

Controls must be put in place to protect institutions from both the accident prone and the malicious insider based on the risks identified. Controls such as using virtual labs or isolated network segments can prevent some accidental or malicious behaviors. But it is important to assess risk beyond the classroom for two major reasons: first, live security testing is often required to give students the knowledge, skills, and abilities they will need to be successful; and second, the knowledge and skills learned in the class can be applied outside of the classroom. While it is generally impossible to eliminate risk, based on the risk assessment, different types of controls may reduce risk to an acceptable level. Instructors and campus network administrators must work jointly to implement controls. This paper provides an overview of controls that can protect students, instructors, and institutions of higher learning and integrates the concepts into an easy-to-use matrix to help all stakeholders ensure safety and recognize risks.

4. CONTROLS

The major types of information security controls are technical, operational, and management (Baker & Wallace, 2007). These controls can have preventive, detective, corrective, or deterrent goals. A combination of these controls is necessary for optimal risk reduction, a concept known as defense-in-depth (Butler, 2002). To help educators effectively mitigate risk, identify controls that have or could be implemented, and to recognize any risks that have been accepted, administrators and educators should evaluate the institutional controls in each cell in the matrix provided in Figure 1. Each of the types and goals of controls are discussed and more details on controls are integrated into an extended matrix in Appendix A.

	Technical	Operational	Management
Preventive	✓	✓	✓
Detective	✓	✓	✓
Corrective	✓	✓	✓
Deterrent	✓	✓	✓

Figure 1: Abridged Control Matrix

Control Types

Technical controls "focus mainly on protecting an organization's [information and communications technologies] and the information flowing across and stored in them" (Baker & Wallace, 2007, p. 37). Examples of technical controls include

network and host-based firewalls, intrusion prevention systems, antivirus, and authentication. Several technical controls can be employed to protect organizations from harm. An advantage of technical controls is that they work continuously without the need for human intervention.

Operational controls are specific actions that must be carried out by personnel to proactively protect against harm or correct deficiencies (Baker & Wallace, 2007). A major difference between operational and technical controls is that operating controls are performed by people, not information systems. Vigilance is required to ensure that operational controls are being carried out properly. Examples of operational controls include awareness training, performing backups, and using secure passwords. Operational controls are typically carried out on a frequent, regular basis.

Management controls involve assessment and planning activities. Examples of management controls in a cybersecurity exercise context include performing risk assessments and vulnerability assessments. Compared to operational controls, management controls are conducted less frequently. Management controls may need to be employed whenever a major change is made to a system. Audits conducted annually help ensure that existing controls are being conducted properly.

Control Goals

Controls can have four major goals: preventive, detective, corrective, or deterrent. Preventive controls stop an event from occurring or mitigate the fallout from an event that takes place (Ko et al., 2011). Examples of preventive controls include student training, network hardening, network segmentation, and intrusion prevention systems.

Detective controls are put in place to discover when an adverse security event takes place. Detective controls are critical because "there is no absolute security that will completely prevent intrusions" (Cavusoglu, Mishra, & Raghunathan, 2004, p. 88). Examples of detective controls include intrusion detection systems, network traffic monitoring, and simply being aware of activities occurring in the classroom. Students will sometimes admit to mistakes that could have caused harm.

Corrective controls decrease the impact of an exploited vulnerability (Jones & Rastogi, 2004). It is hoped that the need to carry out corrective controls is rare, but failure to implement corrective controls can have severe consequences on the confidentiality, integrity, and availability of systems. Examples of corrective controls include backups, removing inappropriate access, and intrusion prevention systems that modify the computing environment to prevent access.

Deterrent controls attempt to prevent bad behavior "out of the perceived threat or fear of the inherent elements of sanctions" (Gopal & Sanders, 1997, p. 31). Examples of deterrent controls that can be employed in the context of cybersecurity exercises include threats of academic probation, impacts on grades, revocation of network privileges, and the possibility of legal action.

The following section describes how the risk assessment process should be driven in a cybersecurity curriculum context.

5. OPERATIONALIZATION

The burden is upon instructors to drive the risk assessment process. Instructors generally have a great deal of latitude in how they create and deliver course content to reach learning objectives. Academic freedom is one of the main drivers for choosing a career in academia (Searls, 2009). When developing exercises, instructors should follow a process for ensuring that the curriculum maximizes student success while minimizing institutional risk.

First, program curriculum and learning objectives should be defined. Syllabi should be evaluated to find activities that contain risk. For each of those activities a risk assessment should be conducted.

In conducting risk assessments, several university roles may need to be included. The instructor will be required in all cases. Programs may have dedicated lab administrators who should participate in the risk assessment when the activities impact the lab environment. Department heads and/or deans should also be included at some level, though different departments will function in idiosyncratic ways. University network administrators should be included where appropriate. Where greater risks exist, instructors should work with higher level administration. Risk management departments would need to be consulted for only the most serious risks. In some cases, even the president should be aware of risks and be asked to provide support for conducting certain exercises.

The instructor will perform the majority of the risk assessments. In many cases, instructors can implement controls themselves without needing to include others in the risk assessment process. As the risk increases or instructors are unable to implement controls, additional parties must be brought into the risk assessment process. Figure 2 shows a risk pyramid. The size of the pyramid level roughly indicates the time and effort needed to assess cyber security assessment risk.

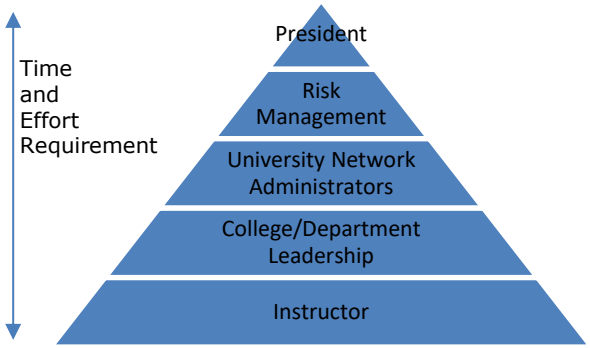

Figure 2: Risk Pyramid

To help instructors and organizations, Appendix 1 provides a sample matrix with controls that may need to be put in place depending on risk assessment outcomes. The matrix should be used as a starting point for identifying controls—not a checklist. Depending on curriculum, risks identified, risk appetite, and other factors, additional controls may be needed and some of the controls may not be necessary. However, every cell of the table should be considered carefully – from technical-preventive to management-deterrent.

An example of this process in action may be illustrative. The first time we planned to teach a course that included penetration testing concepts, we thought it would be a great experience for students to evaluate the security of local organizations. We built a relationship with one local non-profit organization and gained their buy-in. Our students and the non-profit organization were excited about the prospect of working together. As educators, we knew the students would gain valuable experience. Before beginning the engagement with the client, we drafted a legal contract with the assistance of a faculty member lawyer. The director of the non-profit was willing to sign the contract. The instructors were not legally able to sign the contract because they were not authorized agents of the university. The contract would have to be signed by a university vice president after review by the risk management department. After reviewing the scope of services proposed to conduct the security audit, the university risk management department decided the risks were too high to proceed. Despite eager students, organizations, and instructors, the project could not go forward because of risk management concerns.

The preceding story should not be considered a failure. In fact, we feel that the risk assessment process worked as intended. Risk management administrators were aware of risks and potential harm that could befall the university if something went awry. Instead of performing hands-on security evaluations of the non-profit organization, managers of the organization were invited to speak to students about the challenges they face. Virtual environments were constructed within the university to mimic the organization's infrastructure insofar as possible. Students were able to gain some of the experience they needed and learn about real-world challenges while reducing risks to the university.

6. CONCLUSIONS

No single technology or practice is the solution to the challenges of developing effective cybersecurity exercises, but whatever the exercise, care must be taken to protect the organizations from risks inherent to cybersecurity exercises. This paper provides high-level, practical guidance for organizations creating cybersecurity programs, courses, and exercises.

Some risk of harming confidentiality, integrity, or availability of systems will exist irrespective of the exercise platform. Students can make mistakes. Students can also be malicious and intentionally cause harm to systems. Risk assessments should be performed for each exercise and consider both intentional and unintentional harm that could occur. Technical, operational, and management controls with the goal of preventing, detecting, correcting, or deterring harm need to be established based on the risks identified.

The world is in dire need of qualified cybersecurity professionals. Educational institutions are working quickly to create curriculum to prepare students for challenging and exciting careers in cybersecurity. Following the guidance in this article, instruction designers can create safe cybersecurity exercises to give students the skills they need to succeed.

7. ACKNOWLEDGEMENTS

The authors would like to acknowledge the large community of software developers, educators,

and researchers working together to promote cybersecurity education.

8. REFERENCES

Baker, W., & Wallace, L. (2007). Is Information Security Under Control?: Investigating Quality in Information Security Management. *IEEE Security and Privacy Magazine*, *5*(1), 36–44. https://doi.org/10.1109/MSP.2007.11

Bernstein, C. (2013). IT Skills Shortage: The Other Critical Cliff Facing Enterprises. *EWeek*. Retrieved from http://www.eweek.com/it-management/it-skills-shortage-the-other-critical-cliff-facing-enterprises

Butler, S. A. (2002). Security Attribute Evaluation Method: A Cost-benefit Approach (p. 232). ACM Press. https://doi.org/10.1145/581339.581370

Cappelli, D., Moore, A., & Trzeciak, R. (2012). *The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud)* (1st edition). Upper Saddle River, NJ: Addison-Wesley.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). A Model for Evaluating IT Security Investments. *Communications of the ACM*, *47*(7), 87–92. https://doi.org/10.1145/1005817.1005828

Dhillon, G., & Torkzadeh, G. (2006). Value-focused assessment of information system security in organizations. *Information Systems Journal*, *16*(3), 293–314. https://doi.org/10.1111/j.1365-2575.2006.00219.x

Fidler, D. P. (2016). The U.S. Election Hacks, Cybersecurity, and International Law. *AJIL Unbound*, *110*, 337–342. https://doi.org/10.1017/aju.2017.5

Gopal, R. D., & Sanders, G. L. (1997). Preventive and Deterrent Controls for Software Piracy. *Journal of Management Information Systems*, *13*(4), 29–47.

Harrison, J. V. (2005). Enhancing Network Security By Preventing User-initiated Malware Execution (Vol. 2, pp. 597–602). Presented at the 2005 International Conference on Information Technology: Coding and Computing, Las Vegas, NV, USA: IEEE. https://doi.org/10.1109/ITCC.2005.146

Jewer, J., & Evermann, J. (2015). Enhancing Learning Outcomes through Experiential Learning: Using Open-Source Systems to Teach Enterprise Systems and Business Process Management. *Journal of Information Systems Education*, *26*(3), 187–201.

Jones, R. L., & Rastogi, A. (2004). Secure Coding: Building Security into the Software Development Life Cycle. *Information Systems Security*, *13*(5), 29–39. https://doi.org/10.1201/1086/44797.13.5.20041101/84907.5

Ko, R. K. L., Jagadpramana, P., Mowbray, M., Pearson, S., Kirchberg, M., Liang, Q., & Lee, B. S. (2011). TrustCloud: A Framework for Accountability and Trust in Cloud Computing (pp. 584–588). Presented at the 2011 IEEE World Congress on Services, Washington, DC, USA: IEEE. https://doi.org/10.1109/SERVICES.2011.91

Lyon, G. F. (2008). *Nmap Network Scanning: Official Nmap Project Guide to Network Discovery and Security Scanning* (1st ed). Sunnyvale, CA: Insecure.Com, LLC.

McGrath, J. E., Martin, J., & Kulka, R. A. (1982). Dilemmatics: The Study of Research, Choices and Dilemmas. In *Judgment calls in research* (pp. 69–102). Sage Publications Thousand Oaks, CA, USA.

Nurse, J. R. C., Buckley, O., Legg, P. A., Goldsmith, M., Creese, S., Wright, G. R. T., & Whitty, M. (2014). Understanding Insider Threat: A Framework for Characterising Attacks (pp. 214–228). Presented at the 2005 International Conference on Information Technology: Coding and Computing, Las Vegas, NV, USA: IEEE. https://doi.org/10.1109/SPW.2014.38

Osborne, C. (2012, February 8). Keylogging Student Caught Hacking College Grades. Retrieved June 13, 2017, from http://www.zdnet.com/article/keylogging-student-caught-hacking-college-grades/

Sauls, J., & Gudigantala, N. (2013). Preparing Information Systems (IS) Graduates to Meet the Challenges of Global IT Security: Some Suggestions. *Journal of Information Systems Education*, *24*(1), 71–73.

Searls, D. B. (2009). Ten Simple Rules for Choosing between Industry and Academia. *PLoS Computational Biology*, *5*(6), e1000388. https://doi.org/10.1371/journal.pcbi.1000388

Verizon. (2016). *2016 Data Breach Investigations Report*. Retrieved from http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

Wagner, D. (2016). Infrastructure Under Attack. *Risk Management*, *63*(8), 28–30.

Appendices and Annexures

Appendix A – Additional Tables and Figures

	Technical	**Operational**	**Management**
Preventive	Network Segmentation Firewalls, Network and Host-based Antivirus Authentication / Authorization Least Privilege	Physical Access Controls Training Access Review Asset Management	Risk Assessment Clean Desk Policy
Detective	Intrusion Prevention Systems Network Monitoring	Log Auditing Intrusion Detection Systems	Vulnerability Assessment
Corrective	Authorization	Backup and Restore	Business Continuity Planning Disaster Recovery Planning Incident Response Policy
Deterrent	Warning Messages	Course Policies Acceptable Use Policies (Campus and Course) Training	Disciplinary Process

Table 1: Control Matrix

Glossary of Controls

Acceptable Use Policy. All campuses should have policies that dictate appropriate use of the network. Ambiguities in the acceptable use policy do a disservice to students, instructors, and network administrators. Course policies should make clear expectations for students as to the appropriate use of security tools and techniques. Even though students are bound by public laws and campus network acceptable use policies, it is important to reinforce acceptable behavior in cybersecurity courses.

Access Review. Groups and individuals are granted access to computing resources through access control lists (ACLs). Access to resources should be periodically audited to ensure that no unnecessary access has been granted. Examples of resources that should be audited are servers, files shares, and access to administrative accounts.

Antivirus. All students on campus should run antivirus. Some cybersecurity exercises involve the analysis or creation of malware. Antivirus minimizes the risk of malware spreading across campus. Many universities choose to license antivirus so that students and faculty can install the software on their personally owned machines.

Asset Management. Computing equipment such as servers, laptops, routers, and switches should be tracked. Responsibility for maintaining that hardware must be clear.

Authentication. Campus servers, networking equipment, and other devices should be secured with strong passwords. Where appropriate, multifactor authentication should be used.

Authorization. Authorization refers to a legitimate access to a resource. When abuse occurs, authorization must be revoked. Authorization should follow the principle of least privilege—that users and services should be granted the minimal level of access required.

Backup and Restore. Data, network configurations, server configurations, and other critical data should be backed up. The backups should periodically be tested to ensure that a restore is possible.

Business Continuity Planning. Plans should be in place to ensure that the campus can still function appropriately in the case of a major outage. The business continuity plan details how work will be carried out without the use of affected computer systems.

Clean Desk Policy. People with access to sensitive information such as personal information or administrative credentials must ensure that the information is properly protected. Sensitive information should be safeguarded using locked doors and cabinets where appropriate. Multiple control points may be needed depending on the sensitivity of the information. Passwords should not be written down and kept in unguarded locations.

Disaster Recovery Planning. In case of major system outages, a disaster recovery plan details how functionality will be restored. Included in this plan is the recovery point objective and recovery time objective. The recovery point objective defines the acceptable amount of data that will be lost when restoring a system. For example, a system may only be backed up at night, so any work done after the last full backup may be lost. The recovery time objective defines the acceptable duration of restoration activities. Complex systems could take days or weeks to rebuild.

Disciplinary Process. Processes for enforcing written policies must be in place. Instructors often only have authority to enforce discipline in their classes. Discipline that exceeds classroom authority may need to be enforced by the Dean of Students.

Firewalls, Network. Network firewalls use rules to determine if network traffic can enter or leave a network segment. Network firewalls are often installed on the perimeter of a computer network. Network firewalls may also be placed between critical network segments for compliance reasons, such as protecting the cardholder data environment (CDE) for Payment Card Industry (PCI) compliance.

Firewalls, Host-based. Host-based firewalls can be enabled on individual computing devices for protection against malicious traffic. Most modern operating systems come with host-based firewalls installed and enabled by default.

Intrusion Detection System. Network administrators typically employ intrusion detection systems at the network perimeter to detect attack threats from external parties. Network administrators should consider placing intrusion detection systems where they can detect internal network traffic to identify misuse (unintentional or otherwise).

Incident Response Policy. An incident response policy defines the procedures to be carried out when a security incident takes places. The policy should include the individuals who are notified, responsibilities for communicating information about the event, and the procedures system administrators should conduct after an incident.

Intrusion Prevention System. Like intrusion detection systems, intrusion prevention systems identify malicious network traffic. Intrusion prevention systems go one step further and make changes to network configurations in an attempt to stop malicious traffic. For example, an intrusion prevention system might automatically block an IP address sending malicious traffic.

Log Auditing. Signs of hacking attempts can often be seen in computer logs. Log files should be audited to find evidence of hacking attempts, successful or unsuccessful. Log files are too large and complex to be analyzed manually. The amount of Security information and event management (SIEM) tools aid in processing logs.

Network Monitoring. Network administrators should monitor and log network traffic. Unusual system usage, such as extremely high bandwidth usage, should be questioned.

Network Segmentation. Cybersecurity exercises with the potential of causing harm may be conducted in an isolated network environment. Isolating the network prevents malicious traffic from reaching an unintended target. This can be accomplished physically (by using a separate network switch and cables), through configuration (by setting ports on a switch to an isolated VLAN), or virtually (by using virtual machines connected to an unrouted virtual network).

Physical Access Controls. Following industry best practices, telecom closets and data centers should be locked. Access to infrastructure should only be granted to authorized administrators.

Training. Network administrators should receive ongoing training that include content being taught in cybersecurity classes. Relevant topics include ethical hacking, penetration testing, and risk assessments. Because many campuses employ students, it is critical that student administrators are trained to deal with security incidents. At the beginning of teach course, students should be asked to provide assurance that they will obey all laws and abide by a standard code of ethics. This assurance can be recorded in a learning management system. Requiring students to give explicit assurance will encourage safe practices by the students and will provide the instructor some defense against organizational fallout if a student chooses to disregard course policies.

Risk Assessment. While instructors should assess the risk of individual cyber security exercises, network administrators should assess the risk to systems overall.

Vulnerability Assessments. Network administrators should periodically assess the network for vulnerabilities. Going further, penetration tests should be performed on a limited basis to ensure critical infrastructure is protected.

Warning Messages. Banner messages at login or other appropriate times can be configured to remind users about acceptable use policies and repercussions for violations.