Readiness and Emergency Management for Schools (REMS) Technical Assistance (TA) Center

CYBERSECURITY FOR HIGHER ED FACT SHEET

Cybersecurity Considerations for Institutions of Higher Education

Background

The ability to securely connect to virtual systems is an important element within a safe and supportive learning environment. This is particularly the case within institutions of higher education (IHEs), where students are increasingly learning in digital formats; faculty, staff, and visitors are constantly accessing and sharing information online; and more infrastructure and facility functions are being managed online. To maintain their collaborative culture, colleges and universities house robust information technology (IT) networks and multilayered infrastructure systems with varied levels of access and connectivity. Unfortunately, this open environment has made IHEs around the world targets in 2017 cyber attacks, including WannaCry (U.S. Computer Emergency Readiness Team [US-CERT], May 2017) and Petya (U.S. Computer Emergency Readiness Team, July 2017), two ransomware attacks that reinforced the need for increased higher ed cybersecurity planning, education, and training.

IHEs are not new targets for malicious cyber actors and operations. Research shows that between 2005 and 2014, 562 data breaches were reported at 324 IHEs, with doctoral institutions marking the majority (63 percent) of those reported (EDUCAUSE, 2014). Hacking/malware and unintended disclosures were the most commonly reported breach types within IHEs (U.S. Department of Homeland Security [DHS], 2015). When an IHE is threatened by a cyber attack or threat, the effect goes beyond loss of student and employee personally identifiable information (PII). There can be operational, reputational, and/or financial impacts, as well as national security and privacy concerns, as some IHEs are involved in Federal defense contractor research projects. This is why cybersecurity planning, education, and training are so important in the overall framework of higher ed emergency management and in terms of ensuring compliance with state, local, and Federal laws.

There are various Federal regulations that require IHEs to ensure the privacy, security, and confidentiality of PII and/or information security in general (Wilbanks, 2016). They include, but are not limited to, the following:

- Family Educational Rights and Privacy Act (FERPA). Prevents institutions from disclosing education records or student PII without written consent;
- Federal Information Security Modernization Act of 2014 (FISMA 2014). Requires Federal data to be secure;

Learn more about how FERPA and HIPAA apply to higher ed emergency management via the REMS TA Center site. FERPA: https://rems.ed.gov/IHEFERPA.aspx. HIPAA: https://rems.ed.gov/IHEHIPAA.aspx.

Get details on state data security laws via the National Conference of State Legislatures site: http://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws-state-government.aspx

- Gramm-Leach-Bliley Act (GLBA). Requires "financial institutions," including colleges and universities, to ensure the security and confidentiality of customer PII;
- Health Insurance Portability and Accountability Act (HIPAA). Requires institutions to protect health records and other identifiable health information via privacy safeguards and by limiting use and disclosures without authorization;
- Higher Education Act (HEA). Requires IHEs with Title IV programs to have policies, safeguards, monitoring, and management practices related to information security; and
- Student Aid Internet Gateway (SAIG) Enrollment Agreement. Requires IHEs with Title IV programs to ensure that all Federal Student Aid applicant information is protected.

IHEs should keep these Federal regulations in mind, as well as state and local laws related to managing information security in the education environment, when creating cybersecurity plans, policies, and procedures for use by staff (IT, emergency management, academic, research, administrative, etc.), students, and visitors.

Threats Facings IHE Networks and Systems

Chief information security officers (CISOs) within IHEs are responsible for protecting, securing, and storing a lot of information, including financial aid applications containing student and family PII, sensitive research information, intellectual property, information within online learning portals, operational data, and more. This puts them at risk for a variety of cyber threats aimed at obtaining confidential information. It is recommended that CISOs work closely with cybersecurity teams on the internal and external levels to prevent, protect, mitigate, respond to, and recover from a variety of cyber threats to networks and systems. Common threats that IHEs face include the following:

- Cloud security. As they assess new ways to store and share information, many IHEs have adopted the use of cloud computing services that enable them to create a virtual repository of data and an invisible channel through which information can be disseminated. Although it eases collaboration in the learning environment, use of cloud computing increases an IHE's risk for data breaches, particularly if PII, operational, or financial data is stored on third-party servers that are accessible over the Internet. Cloud security "refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing" (EDUCAUSE, n.d.). It is recommended that IHEs implement and continually revise their cloud security policies to protect high-traffic networks and those managed by third-party vendors. The Higher Education Information Security Council (HEISC) developed a Higher Education Cloud Vendor Assessment Tool that IHEs can use to assess the quality of cloud computing services provided by third-party vendors (EDUCAUSE, 2016).
- Denial of Service (DoS). During DoS attacks, individuals who are normally granted access to systems or networks are suddenly denied the ability to view data or systems. This can include emails, Websites, learning accounts, etc. These types of attacks can be targeted through overall IHE technology networks, during which "an attacker 'floods' a network with information" (US-CERT, 2013); spam email messages; and individual computers and/or groups of computers.

Antivirus software, firewalls, and policies that make it easy to reduce spam can all be used by IHE information and cybersecurity departments to reduce the likelihood of DoS attacks.

- Malware. When an unrequested software is installed on an individual's computer and/or on an IHE's server, thereby restricting access and/or causing a system crash, it can be considered malware. There are various types of malware, including ransomware, viruses, worms, and adware. As recent events have shown, these malware threats are often used as a means to steal information and to commit fraud, including extortion. The Federal Trade Commission provides specific tips for avoiding, detecting, removing, and reporting malware via their site at https://www.consumer.ftc.gov/articles/0011-malware.
- Phishing. When it comes to cybersecurity, research shows that the most common threat to everyday Internet users is actually one of the oldest types—phishing (INFOSEC Institute, n.d.), which occurs when attempts at obtaining PII are made by malicious individuals or groups (US-CERT, n.d.). Phishing victims are targeted via unscrupulous email messages that hyperlink to fraudulent Websites via which users are prompted to disclose PII such as addresses, usernames, and passwords. Implementing cybersecurity training and emphasizing individual preparedness are the best defenses against phishing attacks, as they target individuals in many cases.
- Unsecure personal devices. It is no longer uncommon for IHEs to be hosts of bring-your-own-everything (BYOE) environments (EDUCAUSE, 2015), with students, faculty, staff, and visitors bringing everything from smart phones and tablets to laptops, desktops, and processing systems on campus to accommodate teaching, learning, and social needs. While BYOE enhances information sharing and digital learning, it also means that more individuals are accessing the IHE's wireless network, and that some of their devices may be unsecure, thereby making the IHE network vulnerable. Careful monitoring and regular risk assessments can support IHE efforts in managing high network traffic and the associated vulnerabilities.

When facing cyber threats, FISMA guidelines recommend that CISOs and cybersecurity mitigation and response teams identify risks and cyber threat areas; protect and implement safeguards; detect cybersecurity threats; respond to a potential incident or threat; and recover and restore capabilities. In the following sections, we will overview how to incorporate these guidelines into the preparation (prevention, protection, and mitigation), response, and recovery processes.

Preparing for Threats

Preparing for cyber threats involves implementation of a variety of prevention, protection, and mitigation strategies for use by students, faculty, and staff. It is a continuous process that requires CISOs, cybersecurity staff, and emergency management teams to constantly monitor new and emerging technologies, trends, and information security techniques. The following are some steps that IHEs can take to prepare for cyber threats that may impact higher ed networks and systems.

- Securely store data. As described in the previous section, most cyber attacks and threats target IHE data, which is why cybersecurity, emergency management, and IT staff; administrative and financial aid staff; and faculty and students must all take steps to secure data that, if breached, could negatively impact an IHE’s reputation, operations, and/or finances. A major element of secure data storage involves the performance of regular data backups. Even if a cyber attacker is successful in retrieving data, data backups can help cybersecurity teams “go back in time” in order to help confirm which systems, applications, etc. were compromised, which will in turn help IHE administrative staff communicate pertinent information to those affected.

- Create access control lists and firewalls. Controlling access is a great mitigation technique to use in the open BYOE environment on IHE campuses, and it is one that many IHEs are already using. Accessing control lists and firewalls make it easier for IT and cybersecurity staff when they are providing user and/or investigative support before, during, and after a data breach. It is recommended that lists are reviewed on a regular basis to ensure they do not include staff who have transitioned out of positions and to add new staff joining the IHE community.
- Develop policies on secure deployment, maintenance, and responsible/acceptable use. There are a lot of players in higher ed cybersecurity prevention, protection, and mitigation. They include IT staff, emergency management teams, cybersecurity professionals, as well as faculty, students, and visitors. Policies that clearly outline what to do and what not do when performing specific actions can help prevent cyber attacks. For example, IT staff should understand Federal, state, and local regulations related to ensuring information security, privacy, and the secure storage of PII before being assigned to support deployment and/or maintenance teams. Those regulations, along with procedures related to secure deployment and maintenance, can be included in policies outlined in a Cybersecurity Annex within higher ed emergency operations plans (EOPs). Furthermore, it is recommended that existing faculty, students, and visitors receive regular notifications and reminders related to responsible cyber use, and that responsible use policies are shared in the orientation packets of new faculty, staff, and students.
- Monitor networks carefully. With the recent proliferation of cyber attacks and threats, network monitoring has likely become a regular activity within IHE IT departments. Performing vulnerability scans may be one technique that IHE IT and cybersecurity staff use to assess risk and to develop courses of action to thwart potential attacks. Depending on an IHE’s size and on how connected its individual department and school networks are, network monitoring can be a time-consuming task that requires support from outside sources, such as data security firms. Consider consulting neighboring IHEs, or IHEs within cybersecurity networks, to get input on which data security firms provide the best support.

It is recommended that IHE cybersecurity and emergency management teams assess their risk and vulnerability for specific types of cyber threats and include them in a detailed list of threats within the Cybersecurity Annex of their EOPs.

Responding to Threats

The way that an IHE responds will largely be guided by the type of cyber attack or threat that is detected. For example, if financial aid data is comprised, IHEs have SAIG and GLBA reporting requirements to consider, and if operating systems are disabled, contingency plans must immediately be activated to ensure continuity of learning. In many cases, responding to a threat requires collaboration with external players as well, including other IHEs, the Federal Bureau of Investigation (FBI) and private data security firms. In 2013, the University of Delaware discovered a data breach that resulted in the PII of 74,000 current and past employees, including student employees, being stolen (University of Delaware, 2013). The university reported the breach to the FBI, initiated an investigation to determine who was responsible, made changes to their network, and consulted other universities who recently faced similar breaches to get support.

The response of Penn State University following a 2014 attack of their College of Engineering was similar. Along with collaborating with the FBI and data security firms to conduct an investigation, the university made changes to its information security protocols for faculty, staff, and students, including requiring two-factor authentication university-wide, and creating a Website that outlined steps that students, faculty, and staff could take to report incidents and reinforce security during the incident recovery phase and in general (Penn State University, 2015).

IHE cybersecurity and emergency management teams should consider how their response will be guided by similar techniques and should outline courses of action for various cyber threat types within the Cybersecurity Annex of their EOP.

Recovering from Threats

The recovery process for a cyber incident should be focused on people, policies, and technology. When designing plans for recovery, CISOs at IHEs should also consider how it involves all three areas. For example, if operating systems have been disabled, either as a result of a cyber attack and/or a protective measure, IHE cybersecurity and IT staff will need to work to restore *technology* capabilities. They will also need to notify the *people* impacted, including faculty, staff, and students, about contingency plans that will be in place until capabilities are restored. Lastly, CISOs, IT, cybersecurity, and emergency management teams should take steps to review, revise, train, and continually remind key stakeholders on *policies* that may be implemented to prevent future attacks.

The following are some questions IHEs may ask during the recovery process:

- People. Who was affected? Have those affected been informed about the incident in multiple formats? Who will manage responses to questions from students, faculty, staff, and the public about the incident?
- Policies. What changes should be made to policies to mitigate future incidents? How are these policies communicated to key stakeholders?
- Technology. Were capabilities impacted? Was data lost? Do systems need to be strengthened?

Have additional ideas for questions IHEs may ask during the recovery process? Share them via the REMS TA Center Community of Practice forum on Cybersecurity Considerations for IHEs: https://rems.ed.gov/COP/REMSCOPforum/topics.aspx?ForumID=122.

Through post-incident reports and careful monitoring following the event, IHEs can assess the success of recovery efforts and work to strengthen the recovery process in the future. It is recommended that IHE cybersecurity and emergency management teams outline plans for recovery within the Cybersecurity Annex of their EOP. In addition, plans may be outlined in a cross-cutting Recovery Annex that focuses on academic recovery, physical recovery, fiscal recovery, and psychological and emotional recovery.

Relation to EOP Development and Planning

The Federal *Guide for Developing High-Quality Emergency Operations Plans for Institutions of Higher Education (IHE Guide)* notes that “effective planning depends on a consistent analysis and comparison of the threats and hazards a particular institution of higher education faces” (“Guide for Developing High-Quality,” 2013). As core emergency management planning teams at education agencies across the country work to identify and assess the risks posed to them by adversarial and human-caused threats, they should conduct research to determine which types of cyber threats to add to their “watch lists.” Once the risks and vulnerabilities posed by those cyber threat types are understood, IHE cybersecurity and emergency management teams should incorporate them into a comprehensive Cybersecurity Annex that includes goals, objectives, and activities/courses of action for before, during, and after each cybersecurity incident type. When developing a higher ed EOP that addresses cybersecurity, planning teams should take the following actions during each step of the six-step planning process for EOP development outlined in the Federal *IHE Guide*.

Step 1: Form a Collaborative Planning Team

Designate personnel who have a role in both cybersecurity and in managing cyber incidents or emergencies to be members of your cybersecurity planning team. This may include, but not necessarily be limited to, emergency management staff, CISOs, IT personnel, cybersecurity faculty and staff, external data security experts, and Federal and national partners, including the FBI and organizations focused on supporting IHEs with cybersecurity. (See **Key Organizations** at the end of this fact sheet.) When considering who to include on the planning team, remember that individuals and teams will be needed to support every preparedness mission area, including prevention, protection, mitigation, response, and recovery. It is recommended that you continually assess human resources available to support cybersecurity against emerging threats, trends, and technologies.

The DHS National Cybersecurity Assessments and Technical Services (NCATS) team offers scanning and testing services to help identify vulnerabilities within stakeholder networks. For more information, email NCATS_Info@DHS.gov.

Step 2: Understand the Situation

During this step in the planning process, higher ed IT, cybersecurity, and emergency management teams should ensure they understand potential cyber threats that may impact their IHE community. Specifically, they should start by identifying potential cyber threats and hazards. Cybersecurity networks, as well as Federal groups including the US-CERT, can provide informational support when IHEs are looking to explore the universe of possible threats. Once potential threats are identified, planning teams should assess the cyber risk to their IHE networks and systems, and from there, identify the cyber vulnerabilities.

Steps 3 & 4: Develop Goals, Objectives, and Courses of Action

These are two important steps in the planning process, because they will form the framework for development of a Cybersecurity Annex to be included in the higher ed EOP. Using each cyber threat identified in Step 2, higher ed IT, cybersecurity, and emergency management teams can work to develop goals and objectives.

Emergency management planning teams should work to determine goals and objectives to achieve the best outcome for (1) before, (2) during, and (3) after a cyber incident occurs, as illustrated in the examples below.

- Cyber Incident Goal Example 1 (before): Prevent staff in the financial aid department from unintentionally releasing PII and IHE financial data.
  - Objective 1.1: Require all staff to take a cybersecurity training as a part of their bimonthly team meetings and/or as a security tool before accessing specific documents.
- Cyber Incident Goal Example 2 (during): Investigate the source of the security breach in collaboration with internal, private, and Federal partners.
  - Objective 2.1: Require IT staff to report all cyber incidents to the proper authorities, including the CISO.
- Cyber Incident Goal Example 3 (after): Strengthen cybersecurity procedures for financial aid staff.
  - Objective 3.1: Update bimonthly training content to provide more details on how PII and financial data can be unintentionally released.

A variety of measures should be developed to prevent cyber threats, as each threat may prevent different security issues and/or require unique responses. Highlight which action steps outlined to address cybersecurity overlap with other action steps to address other functional areas. For example, actions outlined in a Continuity of Operations Annex within a higher ed EOP might provide cybersecurity recommendations to support continuity of learning in distance learning environments serving as temporary replacements in the event of campus closure. All courses of action should be categorized, by cyber threat type, within a Cybersecurity Annex.

Step 5: Plan Preparation, Review, and Approval

When finalizing the Cybersecurity Annex, it is recommended that higher ed IT, cybersecurity, and emergency management teams address how the annex connects to state, county, and/or municipal plans. This will not only ease the approval process, but it will also ensure that IHEs are in compliance with state and local laws related to information security. (See list on pages 1 and 2.) The annex may also identify a chain of command for before, during, and after an incident, as well as roles, responsibilities, and contact information for key stakeholders in prevention, protection, mitigation, response, and recovery.

Step 6: Plan Implementation and Maintenance

Once the plan is finalized, it is important for IHEs to train stakeholders. In this case, stakeholders include faculty and staff (IT, emergency management, academic, research, administrative, etc.), students, and visitors. Consider conducting emergency drills and exercises related to cybersecurity that involve these key stakeholders, as well as other partners who will support the IHE in the event of a cyber incident, including data security firms and Federal partners. After drills and exercises are complete and after actual cyber incidents, IHEs should prepare after-action reviews in order to identify lessons learned and implement corrective actions.

On Twitter?

Get more information about cybersecurity considerations for IHEs from the REMS TA Center, the U.S. Department of Education's (ED) Office of Education Technology, and other cybersecurity partners by searching #CyberAwareCampus.

Key Organizations

Several Federal and national organizations exist to support IHEs with cybersecurity. These include:

- Computer Crime and Intellectual Property Section, U.S. Department of Justice. This center supports government agencies, the private sector, academic institutions, and foreign counterparts in preventing, investigating, and prosecuting computer crimes. Along with providing documents and reports, the Website provides access to details on how to report a computer or intellectual property crime. https://www.justice.gov/criminal-ccips
- EDUCAUSE®. This higher education technology association is comprised of IT practitioners working in the field of higher education. The organization's membership includes 1,658 U.S. and 264 international colleges and universities in 45 countries, as well as corporations, associations, and other organizations. The organization Website provides relevant resources on cybersecurity and hosts related virtual events. https://www.educause.edu/about
- HEISC. This entity leads the EDUCAUSE Cybersecurity Initiative, and also leads the Annual Campus Security Awareness Campaign. Their mission is to support the higher education community with efforts to enhance information security governance, compliance, data protection, and privacy programs. The HEISC Website offers resources and links to virtual Webinars and events. https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-initiative
- NCATS Team, DHS. This team supports key IT stakeholders with decision-making, risk management, and recommendations to support the overall cybersecurity framework. Their services are free to all stakeholders. For more information, email: ncats_info@hq.dhs.gov. https://www.us-cert.gov/ccubedvp/federal
- National Initiative for Cybersecurity Education (NICE), NIST. This initiative, which is led by NIST, is the result of collaboration between government, academia, and the private sector for

the purpose of cybersecurity education, training, and workforce development. The NICE Strategic Plan is designed to provide guidance to key stakeholders on improving the cybersecurity workforce and addressing the shortage of human resources to support cybersecurity in general. https://www.nist.gov/itl/applied-cybersecurity/nice/about

- Research Education Networking Information Sharing + Analysis Center (REN-ISAC). This international center serves as a computer security incident response team supporting the research and education communities. In collaboration with key partners, they notify IHEs of infected hosts and suspicious network traffic. Although they are a member-based organization, REN-ISAC provides a variety of public resources on their site. https://www.ren-isac.net/
- Security & Information Systems Information Analysis Center, U.S. Department of Defense. This center offers up to 4 hours of free support in response to technical assistance inquiries specific to a variety of information security topics, including cybersecurity. They utilize practices and expertise from government, private industry, and academia to also provide core analysis tasks, subject matter expert referrals, and training classes in cybersecurity and information technology. https://www.csiac.org/about/about-the-csiac/
- US-CERT, DHS. This center supports Federal departments and agencies; state, local, tribal, and territorial governments; and other key private stakeholders by analyzing data and providing information on emerging cyber threats. Through their Website, they provide secure Web-based forms that stakeholders can use to report incidents and submit evidence of malware for analysis. https://www.us-cert.gov/about-us

Key Resources

Several Federal and national publications have been created to support IHEs with cybersecurity. These include:

- An Introduction to NIST Special Publication 800-171 for Higher Education Institutions, HEISC. This publication provides an overview of NIST Publication 800-171, which outlines requirements for IHEs related to data categorized by the Federal government as controlled unclassified information. It is specifically for IHEs that have contracts via research grants or other projects with Federal agencies. https://library.educause.edu/resources/2016/4/an-introduction-to-nist-special-publication-800-171-for-higher-education-institutions
- Cyber Security Requirements for Institutions of Higher Education, ED. This presentation, from a CISO within ED's Federal Student Aid Department at the NASFAA National Conference, is designed for the student financial aid community and provides an overview of information security and data protection considerations for IHEs. http://fsaconferences.ed.gov/conferences/library/2016/NASFAA/2016NASFAACybersecurityRequirementsforIHEs.pdf
- Dear Colleague Letter on Protecting Student Information, July 29, 2015, ED. This 2015 letter from ED's Federal Student Aid Department serves as a reminder to IHEs and the third-party servicers that support their operations of their requirements, under various Federal laws,

to "protect data used in all aspects of the administration of the Title IV Federal student financial aid programs." https://ifap.ed.gov/dpcletters/GEN1518.html

- Framework for Improving Critical Infrastructure Cybersecurity, NIST. This document provides an overview of the Federal Cybersecurity Framework, which is a compilation of IT industry standards and proven practices to help organizations manage cybersecurity risks and incidents. https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf
- Information Security Guide: Effective Practices and Solutions for Higher Education, HEISC. This continually evolving guide supports IHEs with the development, implementation, and maintenance of information security and privacy programs. Along with accessing resources on a variety of topics, including but not limited to encryption, network security, privacy, and risk management, users can also submit case studies that illustrate how security solutions were solved. https://spaces.internet2.edu/display/2014infosecurityguide/Home
- Integrating Cybersecurity with Emergency Operations Plans for IHEs, REMS TA Center. This Webinar, hosted in collaboration with ED and the DHS Office of Cybersecurity and Communications, provides an overview of how IHEs can work to integrate cybersecurity into higher ed EOPs. The recommendations within the Webinar are based on the *IHE Guide*. https://rems.ed.gov/IntegratingCybersecurityForIHEs.aspx
- Toolkit for New CISOs, HEISC. This toolkit is designed specifically for CISOs who are new to their positions within IHEs. Along with providing links to various categorical resources and industry networks, the toolkit also serves as a space that new CISOs can use to assess the status of their IT department, connect with local peers, and request a mentor or coach. https://spaces.internet2.edu/display/2014infosecurityguide/Toolkit+for+New+CISOs.

References

EDUCAUSE. *Cloud Security.* (n.d.). Retrieved from https://library.educause.edu/topics/cybersecurity/cloud-security.

EDUCAUSE. *Higher Education Cloud Vendor Assessment Tool.* (2016, October 17). Retrieved from https://library.educause.edu/resources/2016/10/higher-education-cloud-vendor-assessment-tool.

EDUCAUSE. *Just in Time Research: Data Breaches in Higher Education.* (2014, May 20). Retrieved from https://library.educause.edu/resources/2014/5/just-in-time-research-data-breaches-in-higher-education.

EDUCAUSE. *Top 10 IT Issues, 2015: Inflection Point.* (2015, January 12). Retrieved from http://er.educause.edu/articles/2015/1/top-10-it-issues-2015-inflection-point.

INFOSEC Institute. *Phishing as an Attack Vector.* (n.d.). Retrieved from http://resources.infosecinstitute.com/category/enterprise/phishing/phishing-as-an-attack-vector/.

Penn State University. *College of Engineering Network Disabled in Response to Sophisticated Cyberattack.* (2015, May 15). Retrieved from http://news.psu.edu/story/357656/2015/05/15/administration/college-engineering-network-disabled-response-sophisticated.

University of Delaware. *What Happened in the July 2013 Cyberattack at UD?* (2013). Retrieved from https://www1.udel.edu/it/response/what.html.

U.S. Computer Emergency Readiness Team. *Multiple Petya Ransomware Infections Reported.* (2017, July 6). Retrieved from https://www.us-cert.gov/ncas/current-activity/2017/06/27/Multiple-Petya-Ransomware-Infections-Reported.

U.S. Computer Emergency Readiness Team. Security Tip (ST04-015): *Understanding Denial-of-Service Attacks.* (2013, February 6). Retrieved from https://www.us-cert.gov/ncas/tips/ST04-015.

U.S. Computer Emergency Readiness Team. TeamAlert (TA17-132A): *Indicators Associated With WannaCry Ransomware.* (2017, May 19). Retrieved from https://www.us-cert.gov/ncas/alerts/TA17-132A.

U.S. Computer Emergency Readiness Team. *What is Phishing?* (n.d.). Retrieved from https://www.us-cert.gov/report-phishing.

U.S. Department of Homeland Security. *Malicious Cyber Actors Target US Universities and Colleges.* (2015, January 16). Retrieved from https://intellihub.com/wp-content/uploads/2015/02/DHS-UniversityCyberThreats.pdf.

Wilbanks, L.R. *Cyber Security Requirements for Institutions of Higher Education* [NASFAA Presentation]. (2016, July 10). Retrieved from http://fsaconferences.ed.gov/conferences/library/2016/NASFAA/2016NASFAACybersecurityRequirementsforIHEs.pdf.