GMU's Cyber Security Protocol and Policies Fact Sheet

Compiled, written, and edited by Ricardo Silvestri, IT Director at Global Ministries University, June 2023

Threats Facings IHE Networks and Systems

Chief information security officers (CISOs) within Institutions of Higher Education (IHEs) are responsible for protecting, securing, and storing a lot of information - including financial aid applications containing student and family PII - personally identifiable information, 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.

- 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.

- Unsecured personal devices. It is no longer uncommon for IHEs to be hosts of bring-your-own- everything (BYOE) environments (EDUCAUSE, 2015). While BYOE enhances information sharing and digital learning, it also means that more individuals are accessing the IHE's 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.

Preparing for Threats - GMU's Implementation

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 steps that GMU has already taken to prepare for cyber threats that may impact its 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 GMU'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 is imperative that faculty and staff use the provided email communication system to avoid leaking sensitive information. In other words, use the official GMU email. Furthermore, existing faculty, students, and visitors receive regular notifications and reminders from its CISO 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. Fortunately, GMU's monitoring extends to automatic scans implemented by its CISO.

Emergency Scenarios

If there is a breach, GMU's recovery process for a cyber incident should be focused on people, policies, and technology: Who is affected, what are the policies we have for responding, and which technology should we employ to combat the situation? Please note that all of the steps below are currently part and parcel of GMU's plan:

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. 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.

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.

Summary

The advantages of GMU as an online school are evident in its baked-in cybersecurity on the backend. Indeed, its current infrastructure is premised and built with and reliant on the latest tools to keep its students, faculty, and administration safe. Its main pillars are the main website, its email and storage infrastructure, and its Learning Management System (LMS); the latter of the three is split between Moodle and Google Classroom. All three employ the latest in cybersecurity, which is interdependent with GMU's CISO. However, all this is not to say that GMU is invulnerable. Careful monitoring of faculty and staff usage of its tools, coupled with precautionary measures outlined above, can keep Global Ministries University safer as we continue to extend our international outreach.

References

More information can be found at the United States government website REMS, or Readiness and Emergency Management for Schools.

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.

U.S. Consumer Phishing Scam Information: https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams#recognize