Cybersecurity for Online Learning 21-22

Schools face a myriad of challenging hazards and threats. In addition to natural hazards, technological hazards, and biological hazards, they now have to prepare for human-caused cyber threats. These incidents can be accidental or deliberate and disrupt education and critical operations; expose sensitive personally identifiable information (PII) of students, teachers, and staff; and lead to high recovery costs.

I- Threats Facing School Networks and Systems

Some of the most common types of online threats are

Data Breach: A data breach is a leak or spill of sensitive, protected, or confidential data from a secure to an insecure environment that are then copied, transmitted, viewed, stolen, or used in an unauthorized manner. Data breaches often occur with confidential information, such as students' records, that may be inappropriately viewed or used by an individual who should not have access to the information.

Denial of Service: A Denial of Service attack, also known as a Distributed Denial of Service attack, occurs when a server is deliberately overloaded with requests such that the Website shuts down. Users are then unable to access the Website.

Spoofing/Phishing: Both spoofing and phishing involve the use of fake electronic documents. Spoofing refers to the dissemination of an email that is forged to appear as though it was sent by someone other than the actual source. Phishing is the act of sending an email falsely claiming to be a legitimate organization in an attempt to deceive the recipient into divulging sensitive information (e.g., passwords, credit card numbers, or bank account information) after directing the user to visit a fake Website.

Spear phishing is a more targeted form of phishing and typically involves sending an email that appears to come from a colleague or acquaintance.

Malware/Scareware: Malware is illicit software that damages or disables computers or computer systems. Similar to malware is scareware, which is malware that uses social engineering to cause fear or anxiety so that a user buys unwanted and unneeded software, such as antivirus software. Ways that computers can become infected include through users downloading a piece of malware or scareware disguised as legitimate software from peer-to-peer file

sharing or email attachments or links. To help prevent becoming a victim from malware or scareware, users should keep their software up to date so that any critical software patches are received, and install antivirus software.

Ransomware is form of malware in which perpetrators encrypt users' files, then demand the payment of a ransom—typically in virtual currency such as Bitcoin—for the users to regain access to their data. An example of ransomware is WannaCry, which infected computers across the globe in May 2017. Ransomware can also include an element of extortion, in which the perpetrator threatens to publish data or images if the victim does not pay. The ransomware is frequently delivered through phishing/spoofing scams.

Unpatched or Outdated Software Vulnerabilities: Vulnerabilities occur when unpatched or outdated software has not been updated to include the latest software updates; thus, unauthorized users can gain access to information networks and systems.

Removable Media: Media devices that can be connected to computers, such as thumb drives, CDs, DVDs, and external hard drives, also pose challenges to cybersecurity. First, these storage devices can be easily stolen. Second, corrupted devices can be intentionally or unwittingly connected to computers. Once opened, files from the device can then infect the computer with malware.

II- Preparing for Threats

Schools can take a variety of actions to prevent, protect from, mitigate the effects of, respond to, and recover from cyber threats. These can be conducted before, during, and after an incident.

a. Before an Incident

To protect their networks and systems as part of an overall preparedness program, schools and school districts can do the following:

Develop and promote policies on responsible use. Before students, teachers, or staff access the school's networks and systems, they should be aware of any policies, rules, or laws regarding their use. The whole school is required to accept a Responsible Use Policy.

Store data securely to ensure that the whole school community's data are kept private. Ease of access to and use of cloud-based software makes this issue especially important, as this technology allows teachers and staff members to easily store and share students' personal information. Schools also need to regularly back up their data in case of accidental or deliberate corruption or destruction of data.

Create firewalls and an approved list of individuals who have access to the school's or school district's networks and systems. The list should be regularly reviewed to ensure that only those individuals who have permission to access the systems can do so.

Monitor networks continually to assess the risk from cyber threats.

b. During an Incident

Members of the school community need to know to whom they should report a cybersecurity incident, such as a data breach. In most cases, the first point of contact will likely be the school's or school district's IT manager or team. School leadership teams should then work to limit the damage and preserve sensitive information.

c. After an Incident

Once the incident has been contained, recovery may be needed for people, policies, and technology—all of which are interconnected. The response team will need to identify what people were impacted by the incident or caused the incident; in some cases, a cyber incident may have been caused by a user who conducted malicious activity. Policies may need to be revised, or new ones implemented, to prevent future cyber incidents from occurring. Finally, the school needs to identify how technology was impacted and address any issues. For example, does malicious software need to be uninstalled? Response teams should also conduct an After-Action Review or lessons learned meeting after an actual event or exercise to capture and document information from the event and make appropriate revisions to plans.

III- Preparedness at Zahrat Al-Sahra'a International School

Domain Users. Members at Zahrat Al-Sahra'a International School are registered on the school's domain as soon as they join. Through the system's secure network, identification numbers (IDs) and passwords are automatically generated and sent via personal messages to users. Passwords can only be revealed or reset by the head of IT.

Storage and Data Loss Prevention. The school's domain and files are stored on Google Cloud. Backups and updates are scheduled on a regular basis. Some backups are done on a daily basis and others are done on a monthly basis. Google Drive is used to store teacher and student files. The following link contains details about Google Drive's privacy and security measures https://support.google.com/drive/answer/10375054?hl=en

Firewall. The school has an installed firewall that prevents any user from outside the domain to access the system. Automatic reports are generated by the firewall and accessed whenever needed.

Operating Systems Update. An up-to-date operating system is required to prevent malicious content from disrupting the system. Automatic updates are scheduled regularly.

Multiple Sign-in Restriction. Users are not allowed to sign in from multiple devices at the same time or try to sign in several times in a row for security reasons.

Web Security Scanner. The school's web security system scans the network and domain for malicious content on a regular basis. Any hint of scam is reported immediately via email to the IT manager

Data Approval. Access to content is specified by the IT manager and Google Superadmin.