Scenario :

Day 1

It has been one year since the developer of your current operating system announced that it will no longer develop security patches for your operating system. The final security patch was installed last week. This vulnerability was identified in your recently completed annual risk assessment.

Day 2: 8:00 a.m.

An employee reports to his manager that his work laptop was stolen from his car overnight. The computer contained sensitive information.

Day 4: 3:00 p.m.

A Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) Alert is released regarding a new ransomware variant. This ransomware is being used in a campaign targeting state, local, tribal, and territorial governments and private sector firms.

Day 6: 10:00 a.m.

A system administrator from the Information Technology (IT) Department receives an email from the personal email account of a human resources (HR) employee. The system administrator and HR employee are connected via professional networking websites. The email notes that the HR employee recently noticed some discrepancies in their 401K withholdings and recommends that the system administrator review their own account information. The system administrator clicks on the link in the email and is re-directed to what appears to be the legitimate 401K website. The IT employee does not believe the email to be suspicious.

Discussion Questions

Discussion questions included in each module may be modified as desired. Additional questions can be found in Appendix A.

1. Would any of the events described in this module be identified as cybersecurity incidents or events? If so, how would they be handled?
2. What sources of cybersecurity threat intelligence does your organization receive? For example, information from CISA, Federal Bureau of Investigation (FBI), open source reporting, security service providers, or others?
   a. What cyber threat information is most useful?
   b. Is the information you receive timely and actionable?
   c. Who is responsible for collating information across your organization?
3. Does your organization provide basic cybersecurity and/or IT security awareness training to all users (including managers and senior executives)?
   a. How often is training provided?
   b. Does the training cover:
      i. Review of organizational acceptable use and IT policies,
      ii. Awareness of prominent cyber threats,
      iii. Password procedures, and
      iv. Whom to contact and how to report suspicious activities?
   c. Is training required to obtain network access?
   d. What security-related training does your organization provide to, or contractually require of, IT personnel and vendors with access to your organization's information systems?

    e. How often do they receive the training?

4. How do employees report suspected phishing attempts?
    a. What actions does your department take when suspicious emails are reported?
    b. Are there formal policies or plans that would be followed?
    c. Does your organization conduct phishing self-assessments?
5. Has your organization conducted a cyber risk assessment to identify organization-specific threats and vulnerabilities?
    a. What are your most significant threats and vulnerabilities?
    b. What are your highest cyber security risks?
6. Does your IT department have a patch management plan in place? If so,
    a. Are risk assessments performed on all servers on the network?
    b. Are processes in place to proactively evaluate each server's criticality and applicability to software patches?
    c. Does this plan include a risk management strategy that addresses the following considerations?
        i. The risks of not patching reported vulnerabilities,
        ii. Extended downtime,
        iii. Impaired functionality, and
        iv. The loss of data?