Working Group Chairs Meeting on COVID Lessons Learned

Cybersecurity Working Group

August 20, 2020

COVID Lesson Learned #1: Privacy

-**Lessons Learned Description:** Practice added vigilance with good privacy in a home/remote work environment by providing remote workers with established privacy guidance to follow. Guidance should include:

- Creating an established home location with the required privacy to discuss any sensitive information where children or other adults do not come into the room (closed door location, sign on door to not be interrupted).
- The established room should only contain the computing equipment that has been designated to perform work tasks. No other Internet enabled equipment should be in the vicinity.
- Discussing expectations of privacy with anyone that will be at home. Advise anyone at home of protocols for entering the designated space.
- Maintaining awareness of surroundings and concerns to safeguard the location.

-**Why it was used:** Good cybersecurity practices are further complicated with remote capabilities in the addition of a “home” office that is not well suited for secure communications. The home networks include devices in use by the children of staff members and contractors, as well as multiple IoT devices. While some secure connectivity capabilities are in place, depending on the technology used, other insecure devices can bridge the connection. Children or others at home may overhear sensitive conversations or their devices may be in an online listening mode without the knowledge of the remote worker.

-**Benefits of LL:** Protection of potentially sensitive information.

-**Any Problems/Issues:** None reported

COVID Lesson Learned #2: Good Cyber Hygiene

- **Lessons Learned Description:** Remote workers need to be cognizant of the security vulnerabilities of home computing devices and ensure that good Cybersecurity practices are used. Companies should:
  - Enhance system monitoring for early alerts to detect anomalous activities on end user devices and remote connections.
  - Use multi-factor authentication.
  - Configure endpoint firewalls.
  - Ensure devices are being “managed.”
  - Provide employees with a Virtual Private Network capability and require devices to connect regularly to obtain updated security patches, or better yet, VDI.
  - Ensure that remote management capabilities are established to maintain managed devices.
  - Consider using a Virtual Desktop Infrastructure (VDI) to further segment the environment. Ensure that employees are aware of the need to connect regularly to ensure the process occurs on schedule.
  - Consider use of a Network Access Control (NAC) that scans the machine before it allows the device to connect to the remote network.
  - Know where all government data is located and being sent and be sure that requirements surrounding that are known and followed.
  - Ensure that continuity of operations plans are up to date. Know how to get ahold of people at home.
  - Clearly communicate requirements for support to IT/Cyber staff to include how to communicate issues.
  - Update incident response plans to address remote work. Remote access software is needed and if an incident occurs, responders need to be able to segment that device in a “network jail.”
  - Require remote workers to remain vigilant of vulnerabilities and patch levels for home computing equipment, such as routers, and keep routers updated to reflect the most recent security patches. US-Cert offers has good best practices for understanding firewalls for home use: https://us-cert.cisa.gov/ncas/tips/ST04-004
  - Make sure that any issues or anything suspicious is promptly reported to the IT/Cybersecurity organization and that IT/Cybersecurity know the FISMA reporting requirements.

COVID Lesson Learned #2: Good Cyber Hygiene

-**Why it was used:**

1) Government contractors have a requirement and obligation to work in a secure and compliant environment which requires, at a minimum, a NIST-171 compliant practices for systems that obtain and process government data.
2) With the added complexities associated with remote work, data access needs and data control needs have changed for some organizations and our method of conducting business needs to evolve to accommodate those changes. The methods used for defense in depth in the office is not equal to that of a home connection.
3) The whole world, including hackers, know that we are operating in a largely remote capacity. As a result, the attack vectors have increased exponentially, and we are dealing with highly capable and motivated attackers with a playground of potentially unmanaged systems that are ripe for exploitation if we don't take the needed precautions.
4) The network boundary is now everywhere.

-**Benefits of LL:** Protection of potentially sensitive information. And, quite frankly, the cost of the data loss, network breach, and/or compromise is too high from the perspective of not just dollars to respond but also in reputation to the organization.

-**Any Problems/Issues:** The number of attack attempts are greatly increased at this time.