Cybersecurity PLAYBOOK

MCNEES LAW | APPALACHIA TECHNOLOGIES | GUNN-MOWERY | INFORMATION NETWORK ASSOC

Incident Response DO's & DON'Ts

DO's

Isolate the Computer

- Wired, wireless, and cellular networks, if necessary (e.g. Airplane Mode) so that the device cannot be remotely wiped or accessed.

Enforce Chain of Custody

- Who was in possession of the device and at what time? Was the device stored in a locked/secured location while it was in custody?

Identify Other Potential Sources of Data

- USB drives, backup drives, phones, tablets, and other smart devices. Internet accounts might include cloud storage platforms like Dropbox, email platforms, or collaboration software (Slack, Microsoft Teams, etc.). Additionally, certain server-side logs may be relevant to the investigation (e.g. DHCP logs / DNS logs / Anti-Virus Monitoring logs / etc.).

Establish a Timeline of Events

- Narrow the time window as much as possible. By limiting your investigation to this short window of time, you'll be able to focus on what really matters. The window can then be expanded depending on what is found during analysis.

Identify Encryption or Passcode Recovery Keys

- If encryption or equivalent protection exists on the device (e.g. Microsoft BitLocker), it will typically be necessary for the forensic examiner to unlock that protection in order to perform forensic analysis.

DON'Ts

Change the Current State of the Device (ON/OFF)

- Doing so may alter the digital evidence on the device. If absolutely necessary to do so, document the change.

Engage Biometric Readers

- This could potentially count as an unlock attempt or alter evidence on the device (e.g. iPhone with TouchID/FaceID and wipes after 10 consecutive failed unlock attempts).

Ask Your IT Department to Review the Data

- Even the most well-meaning examination of the device will alter the data on the storage drive. Opening, reviewing, or copying files can modify crucial underlying metadata that will affect the quality of the evidence. Performing a search on the employee's device in this manner would be like trampling around in an active crime scene.

Re-Issue or Re-Assign the Device

- IT departments usually consider reallocating assets to new users when an employee quits. This could lead to the overwriting of critical evidence stored on the device. When a key employee, sales team member, or anybody with access to proprietary intellectual property leaves a firm, the former employee's device should be preserved.

Wait to Perform a Digital Forensic Investigation

- Preserving digital evidence from a device should be the most urgent priority. Once the evidence has been preserved, days or weeks of forensic preparation may be required before analysis can even be started.

Pre/Post Incident Response Checklist

What to do to prepare and protect your organization before a security incident occurs…

Preparation

Action	Completed
1. Make sure you have a trained incident response team, either employed, on retainer, or at least someone's business card so you know who to call.	
● Legal Council	
● Insurance Broker	
● Forensics Company	
● IT / Cybersecurity Company	
2. Compile a list of IT assets such as networks, servers and endpoints, identifying their importance and which ones are critical or hold sensitive data.	
3. Set up monitoring so you have a baseline of normal activity.	
4. Implement standard security controls (See "Practical Tips for Protecting Your Organization"	
5. Cyber-liability insurance	
6. Train your employees	
7. Develop and enforce policies and procedures. Review annually.	

What to do if you suspect a security incident has occurred…

Detection and Analysis

Action	Completed
8. Determine whether an incident has occurred	
● Analyze the precursors and indicators	
● Look for correlating information	
● Perform research (e.g., search engines, knowledge base)	
● As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence	
9. Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.)	
10. Report the incident to the appropriate internal personnel and external organizations	

Pre/Post Incident Response Checklist

Containment, Eradication, and Recovery

Action	Completed
11. Acquire, preserve, secure, and document evidence	
12. Contain the incident	
13. Eradicate the incident	
● Identify and mitigate all vulnerabilities that were exploited	
● Remove malware, inappropriate materials, and other components	
● If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps	
14. Recover from the incident	
● Return affected systems to an operationally ready state	
● Confirm that the affected systems are functioning normally	
● If necessary, implement additional monitoring to look for future related activity	

Post Incident Activity

Action	Completed
15. Create a follow-up report	
16. Begin notification process for affected parties, if applicable	
17. Hold a lessons-learned meeting (mandatory for major incidents, optional otherwise)	

Central PA Incident Response Team:	
Legal:	**McNees Wallace & Nurick LLC**
	Contact: Devin Chwastyk, JD, CIPP/US/E, Chair, Privacy & Data Security Group Phone: (717) 237.5482 | Email: dchwastyk@mcneeslaw.com Office Location: 100 Pine Street, Harrisburg, PA 17108-1166
Insurance:	**Gunn-Mowery, LLC**
	Contact: G. Greg Gunn, CIC, President/CEO Phone: (717) 761-4600 x3023 | ggunn@gunnmowery.com Office Location: 650 N 12th Street, Lemoyne, PA, 17043
Forensics:	**Information Network Associates, Inc (INA)**
	Contact: John Sancenito, CPP, President Phone: 717-562-7772 | Email: jsancenito@ina-inc.com Office Location: 5235 N Front St, Harrisburg, PA 17110
IT/Cyber:	**Appalachia Technologies**
	Contact: Mike Miller, vCISO Phone: (717) 918-3301 | Email: mike.miller@appalachiatech.com Office Location: 5012 Lenker Street, Mechanicsburg PA 17050