**Cubicles and Compromises Incident Response Tabletop Game Scenario 3**

1. **Ransomware:**

On Monday morning the Help Desk starts getting dozens of calls as soon as they walk in the door. Users can’t access their computers, when they boot up they see this screen:



What do you do?

**Characters: Incident Master, CTO, Help Desk, Systems admin(s), CBO, Security Analysis, CISO, College President, College Board member, PR**

If you hold one of these positions you may play this character, otherwise everyone rolls the dice, highest number chooses first, then in descending order.

**For Incident Masters**: Your team doesn’t need to follow the below steps, they are for leading the discussion forward, you can suggest some of these steps to keep going forward.

**Rules:** For each action the IR team takes, roll the dice. An 11-20 is successful, 10 or less, it fails.

You get +5 if your organization has a documented procedure for the action. +2 if your organization has someone trained to do the action. For example, you role a 5, but you have a documented procedure and a person trained for the procedure, then you now have a 12 and the action is successful.

**Initial Investigation**

1. What is your first action?
2. Should the computers be shut off ASAP?
3. Should you send out an emergency message to all employees to not start their computers?

**Initial Communication**

1. Who do you call first?
2. Do you have a contact list for incidents?
   1. Do you have any third-party forensic firms on retainer, or at least have a reference for one? Should you be working this incident? For this game we will say yes, in reality probably not
3. Should you get the authorities involved and when?

**Forensic Investigation**

1. Analyze a sample machine, pull the drive, are the files really encrypted?
2. Is the malware persistent, or is it fileless?
3. Pick another machine that is on what addresses is the computer communicating with
4. Can you find the initial infection vector? How
5. Can you identify the malware variant?
6. Do your users have local administrative access?
7. How often are your systems patched?
8. Are there any servers also affected?
9. Are you still using SMBv1, is SMB signing enabled?
10. Do you patch third party applications such as Flash and Acrobat Reader, or only the OS?
11. Are the networks segmented, and firewalled, or can they all access the whole internal college network?
12. Do you have the same local administrative password on all of your systems?
13. Do you have the same local administrative password on your servers as you have on your workstations?
14. Do you have Windows 8 or above and have you set the registry key to isolate the LSASS program, that would prevent an admin from accessing cached plain text credentials?
15. Do you have windows 10 and have enabled the registry entry that protects admin users from accessing hashed passwords in LSASS?
16. Did the attacker pivot to other computers on the network? How can you tell? Which ones?
17. Do you have a separate logging server, like Splunk? Is the password the same as any of your other AD accounts?
18. Did the attacker delete any forensic data?
19. Any other steps?
20. Do you pay the ransom?
21. Do you have backups?

**Wrap up**

1. Supply a report to all of the management and key stakeholders, be sure to redact sensitive information if the document will ever be released publicly.
2. If any information was potentially compromised what do you legally need to do?
   1. In California a breach is defined as an individual’s first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: Social security number, Driver’s license number or California identification card number, Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account, Medical information, Health insurance information.
   2. You are required to notify those affected as soon as is reasonable, this can now be electronically or written.
   3. You are also required to alert the California attorney general of the breach and provide a sample notification letter that was user to notify those affected.
   4. Note that government agencies are not required to offer credit protection for data breaches, only commercial businesses are. However, it is customary.
   5. Please consult your general counsel for legal advice in the case of a real security incident.
3. How could this incident be prevented? Would multi-factor authentication have helped?
4. What security controls could have narrowed the scope of the incident?
5. Are there any tools available freely from the Security Center that could have helped?

Injects:

1. The CTO resigns suddenly, someone else will need to communicate with the major stakeholders, chose someone.
2. The board calls an emergency meeting, and requests an update from the acting CTO
3. The backup system wasn’t working properly, and all of the backups are several months old.
4. If the ransom was paid, the key doesn’t work for half of the computers