7. Security Toolkit: When you Experience an Incident

When You Experience an Incident

Every cyber incident is different if for no other reason that each provider's technology environment and user practices are different than sister organizations. The process of dealing with and responding to an incident will vary. Here, we've outlined some of the common things to consider if (or when) an incident occurs. This outline is not one-size-fits-all. Instead, you can use these bullet points to think through what questions to ask and what actions to take. This outline can help organizations develop plans before an attack has ever occurred, and it can help organizations experiencing an attack to determine what to do next.

1. Investigate whether you have been attacked/compromised immediately
    a. Helps to have a well-trained team of staff and volunteers who can serve as an early warning team on any suspicious behavior or changes to their environment
    b. Assume that any significant changes in performance, account access, or notifications from other organizations, your Internet or cloud providers that indicate strange behavior (e.g., lots of spam from your org, network congestion from your ISP, unusual Internet traffic patterns, etc.) are potentially signs of either an attack (DDOS) or a compromise (successful attack).
    c. Attacks or compromises might be seemingly limited but assume that they will grow/get worse.
    d. Move quickly to assess and act; be prepared to take action before you are certain your systems have been compromised – may have a false positive which isn’t the worse thing in the world.
    e. Before an attack, your executive team should collect and verify contact information (personal email addresses and phone numbers) for all staff members. In the initial stages of a security incident, most systems will be considered untrusted and/or locked down thus preventing normal methods of communication.
    f. Work with your security provider, your EDR vendor, your SIEM vendor or even use your firewall and system logs to help identify/confirm problems.

g. An attack with cryptoware may be noticed by users before it has completed its spread and encryption – so shutting down or cutting off access may limit damage.

2. Consult and follow your cyber security incident response policy.

3. If you don't have a cyber incident response policy, consider:
    a. Communicating with your leadership via out-of-band phone, text, chat, etc.
    b. What your IT and leadership team understand about how the attack was able to gain access the environment is tentative knowledge and may be wrong.
    c. If you have cybersecurity insurance, contact your agent.
    d. If you have cybersecurity counsel or general counsel, contact them.
    e. Designating an incident captain, coordinator, or manager - typically/ideally not someone from the IT team.
    f. Communicating with your staff as appropriate on what they can expect and what they can communicate to others.
    g. With respect to communications, despite any initial conclusions with respect to the nature of the incident and its impact, the organization should expect those conclusions may be wrong or may represent only a partial understanding of the incident.
    h. Generally, don't communicate about a potential incident publicly or with third parties until advised by your leadership or counsel.
    i. Talking to your tech team / tech partners for additional assistance.
    j. Attempting to isolate and shutdown access to systems.
        1. Where possible maintain remote connectivity for IT to manage access.
        2. Restrict inbound and outbound firewall traffic to only IT personnel/remote connectivity from trusted public Ips.
        3. Limit or stop traffic across all endpoints. For instance, on virtual servers, disable the virtual NIC.
        4. Talk with your cloud service providers about limiting or stopping traffic (case management, document management, email, etc.)
        5. Reset all passwords, including administrators, users, service accounts, temp accounts, guest accounts, etc.
        6. Review user accounts for anything that may have been suspiciously added.
        7. Talk with your cloud service providers about doing the same (case management, document management, email, etc.).
        8. Collect and backup all log information from all systems including servers, firewalls, VPNs, email, etc.
        9. If there is a ransomware note or a malicious email, get a copy of it.
        10. Take screenshots of any unusual activity, such as logins from unknown accounts, antivirus/EDR pop-ups, configuration changes, etc.
        11. Create a detailed timeline of all events from the moment you became aware of the security incident.
        12. Be careful not to alter/delete any potential evidence that can be used by the forensics company.
        13. Attempt to identify the source of the security breach. The compromise may have

occurred from malware, phishing email, misconfigured firewall rule, zero-day exploit, easily guessable password, etc. Check all servers and networking devices (i.e., firewalls, VPNs, email, etc.) for suspicious login activity.

k. If you don't have cybersecurity insurance, you will likely need to:
    i. Get IT and legal help from partners who have worked on cyber incidents.
l. Working quickly to mitigate the damage.
m. Getting outside expertise to Investigate the incident, determine the extent of the damage, determine, to the extent possible, whether there was data access or exfiltration.
n. Decide whether and how to negotiate with the criminals involved - there are firms that specialize in these negotiations.
o. Plan for and securely restore technology services:
    1. Consult with your insurance/security/legal teams before proceeding.
    2. May need to do this on alternative physical or virtual network and system environment in case confidence is low that the security breach has been identified or if you need the affected environment for forensic analysis.
    3. Will likely need to greatly expand logging and monitoring of the environment.
    4. Likely need to install EDR software.
        a. May need to prioritize which services to restore.
    5. May want to avoid restoring unnecessary or out-of-date, insecure systems or network infrastructure.
        a. Assume that accounts and access can be compromised again.
        b. Consider MFA deployment across all systems on an expedited basis.
        c. Review privileges and limit to the extent feasible.
        d. Modify password policies to be more stringent, if necessary.
        e. Consider modifying any sharing policies/configurations that were previously in place (i.e., disable sharing via anonymous links).
        f. Adjust or implement stronger email security systems to protect against malicious attachments/links and email security attacks such as phishing and business email compromises (BEC).
        g. Provide users with security awareness training.
        h. Restrict who has remote access (if that is even possible with COVID).
        i. Review firewall rules for any old/unused rules and disable them.
        j. Revise firewall rules to be more restrictive.
    6. Monitor electronically and with all users on high alert.
    7. Decide what changes to make to improve security (to avoid a repeat attack).
p. Work on communications/compliance as necessary (regulators/government entities, funders, clients, employees, and the public).

3. Complications
    a. Backups are not comprehensive, up-to-date, and accessible.
        i. Not certain whether the backups have backed-up the security compromise – might be restore access/backdoor.
    b. Not enough capacity in the environment to setup the restored environment.
    c. It may take a long time to recover massive data, especially when restoring from cloud-

based backups on slow internet connections.

d. Criminals are posting exfiltrated data on the dark web/shame sites.
e. Criminals sell reconnaissance information to other criminals. There is potential for another attack.
f. Forensic analysis is inconclusive.
g. Not enough/inaccessible IT documentation to rebuild the environment. May be missing installer packages for critical software or detailed configurations needed for certain connections/applications.
h. Outdated IT credentials to access systems or networking devices.

Have Insurance

Cyber insurance is essential in helping your organization recover after a data breach. Insurance can help with costs that can include business disruption, equipment damage, legal fees, public relations expenses, forensic analysis, and costs associated with legally mandated notifications. Insurance also helps companies comply with state regulations that require a business to notify customers of a data breach involving personally identifiable information.

Cybersecurity insurance policies can also cover customer notifications in the event of a breach, an option to monitor the information of anyone impacted for a specified period, and payment of costs incurred in the recovery of compromised data.

Identification of an Incident

Typically, most legal aid providers identify a possible incident when system performance or access issues, including access to files, becomes an issue that users bring to their IT team. It also happens that another user working for another organization in the community gets spam from the legal aid organization contacts the users they typically work with to alert them, or some law enforcement agency reaches out to inform the provider that they may be a victim of an incident. (It is important that such a notification by third parties be screened as possible cyber-attack itself.)

Generally, the earlier an incident is identified, the better. Early identification helps limit access, damage, and costs while improving the ability of forensic experts to determine the cause of the incident and the security lapses that need to be addressed. Increasingly, organizations are using more sophisticated tools, such as endpoint detection and response (EDR) software, and security services, such as third-party provided security information and event management (SIEM) services, to monitor and identify incidents earlier and intervene more quickly to stop an incident before the access or damage is more significant. Any monitoring might lead to false positives that might in term lead to unnecessary stress and response. It is important to work with your IT team/partner to tune any monitoring tools to reduce the number of false positive alerts. Typically, this work takes weeks or possibly longer after new systems are implemented. Similarly, training users on cyber security awareness will help improve the quality of user reporting on odd email and performance issues.

Common Cyber Attacks

The FBI recently released its 2022 report on 2021 Internet Crime that is worth reading or skimming to get a better sense of the prevalence of different cybercrime. Another great resource is from Fortinet, a security hardware, software and services firm, on the top 20 cyber-attack types. Visit their web page for a plain language understanding of the different attack types and what organization can do to help prevent them.

Exercise: Sample Incident and Response

Below is a fact pattern describing a typical data breach. It outlines several actions taken by a member of staff in one column, and in the second column it outlines a list of places to review from the toolkit while considering the fact pattern. Try to spot the things the member of staff has done that increase risk. Think about what you would do in that situation. Use the fact pattern as a tool for discussing security with the rest of your office.

Fact Pattern	Issues
You are working on an immigration case with a pro bono attorney at a private law firm. There is a sudden emergency that requires documents to be filed urgently. You need to get more confidential client information immediately to meet the deadline and share it back with the pro bono counsel.	• External data sharing

Fact Pattern	Issues
This has all unfolded, while at the airport with your family, as you head to your cousin's wedding. You think, "I've got time, 6-hour plane ride—I'll get it all done in no time". You log into the airport's public Wi-Fi and begin downloading the client's data and texting the client about the documentation that is outstanding.	• Wi-Fi, Encryption, Data sharing, and Personal Devices
In flight you connect to the free in-flight airplane wireless network, login to your 365 Webmail to review the document from the pro bono lawyer and save it on your laptop. You also;	• Wi-Fi and Passwords
• Remote into your firm's terminal server and find a few documents that you need to reference. • Use the email client to email those documents to your Gmail account, so that you can easily download them onto your Mac. • Your client sends MMS texts to you with copies of their documentation and additional documents are emailed from their yahoo account – you can easily airdrop the images on to your Mac.	• Remote Work • Email security • Personal devices and Encryption

Fact Pattern	Issues
Finally, you've made it through the 6-hour flight and to the hotel. You decide to wrap things up at the Starbucks in the hotel's lobby. You have a few email exchanges between the pro bono attorney and your client, and you e-fax all documents to immigration services. Now, it is time to get some rest. The next morning, while everyone prepares for the wedding, you receive an--alert your Gmail has been signed in at a different location. Congratulations, enjoy the wedding!	• Wi-Fi, passwords and MFA