How to react


Incident Response Cheat Sheet
Step 1
DON'T PANIC
DON'T PANIC
A cyber attack can certainly be classified as a disaster scenario, and a clear mind is needed to navigate a solution. Once you and your team adopt a problem-solving attitude, you will be able to DON'T respond to the breach in a logical and organized PANIC way.
Step 2
DO NOT PAY A RANSOM
If a cyber attacker demands a ransom, it may be tempting and easier to pay it to regain control of your network, but often times, it may lead to future attacks.
Only pay a ransom if there is no other way to recover your data. A much easier solution is to invest in an Endpoint Detection and Response solution that can stop ransomware before it can be executed.
Step 3
FORM A RESPONSE TEAM
To address any damage caused by the cyber attack, you will need a capable and experienced response team. Your team should be comprised of IT staff members, either contracted or in-house, who will investigate the attack and work to resolve it. HR should be included if your employees have been impacted by the attack. Public Relations representatives should be included to best explain the attack to your customers. Always include legal counsel since breaches can have a number of legal implications.
Step 4
USE BACKUP SERVERS
If you have backup servers available and undamaged from the attack, switch to them immediately. The biggest reason this step fails is that organizations fail to test their data restoration process.
If your organization does not have backup servers, avoid the temptation to switch off your servers and workstations. While this may seem to be a viable solution, it will not help to fix the damage.
Step 5
ISOLATE THE BREACH
If your organization is hit with a cyber breach, it is imperative that you minimize the number of affected systems. You will need to isolate where the breach occurred and stop if from infecting other systems. Once the breach has been suspended, your response team can test other portions of the network to see if they have been compromised as well.
Step 6
INVESTIGATE & MANAGE
Upon investigation, you may find that the damage affects numerous portions of your organization. HR response team members will need to be address any impact on your employees. If your customers or the public were affected, PR staff will need to control the damage done to your reputation. The attack may even cause legal ramifications, and as such your business's lawyers may need to be involved.
Step 8
CONTACT CLIENTS
The PR members on your response team need to reach out to all clients who have been impacted by the breach as soon as possible. For security purposes, your clients may need to change their passwords or PIN numbers if their private information was compromised.
Step 7
DOCUMENT
As your response team is investigating the attack, ensure that they are documenting both their process and their findings. From this evidence, you will be able to ascertain the vulnerability that allowed the attack to be successful, and thus fortify it going forward.
Step 9
PREVENT FUTURE ATTACKS
If your team is unable to effectively secure your organization's IT, you may need to partner with an outside cyber security company. Outsourcing your cyber security needs to an Managed Security Services Provider (MSSP) can be cheaper and they are often more effective than most IT teams.
Cyber Writes
cyberwrites.com

CheatSheet

incident-response-cheatsheet.pdf