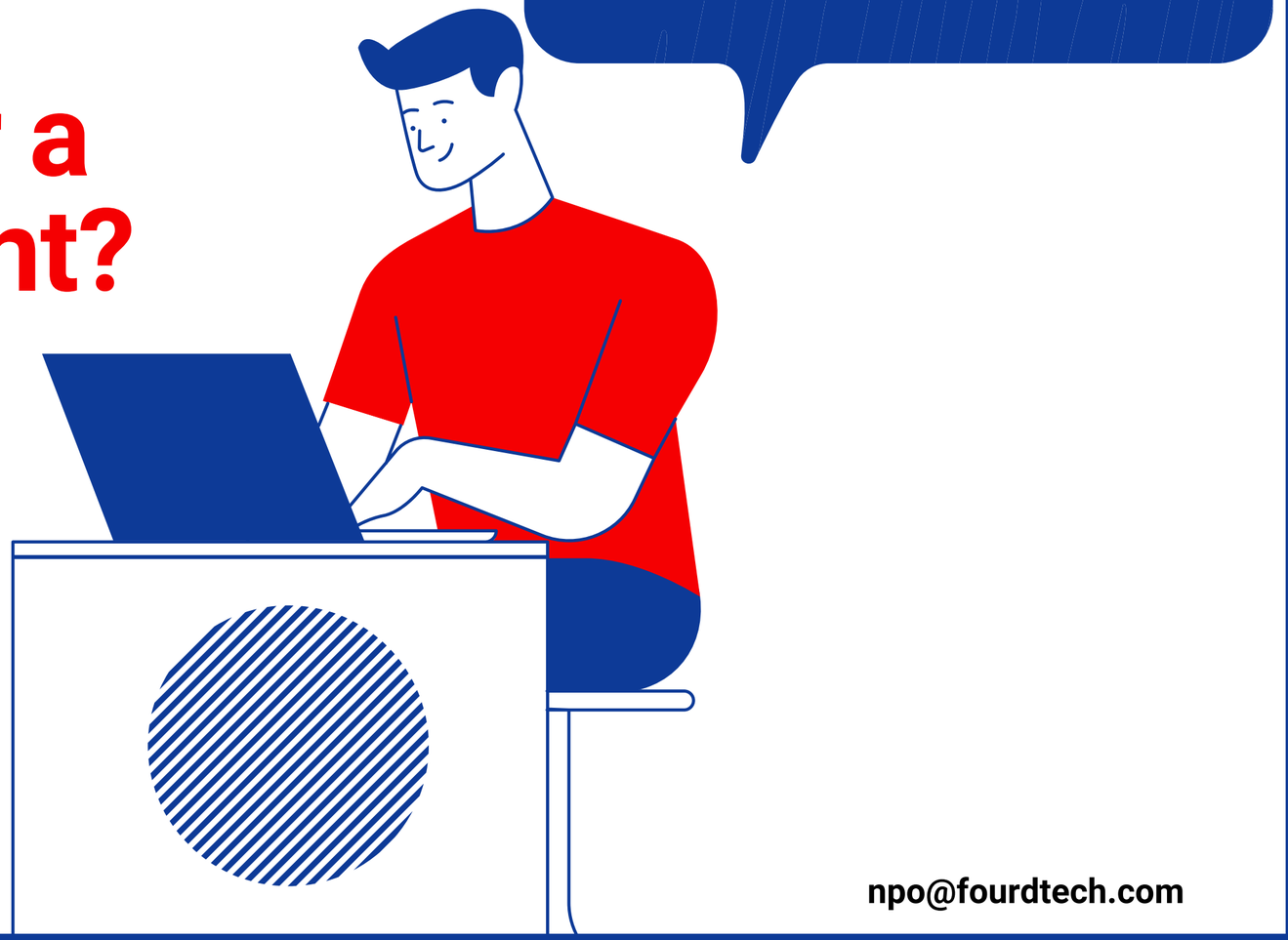
FOURTH DIMENSION
expect more

www.fourdtech.com

What Do We Do After a Cybersecurity Incident?



npo@fourdtech.com

FOURTH DIMENSION
expect more

www.fourdtech.com

Let's Start!

Even after creating a cybersecurity plan, training employees, and implementing security protocols, organizations may still fall victim to a cybersecurity attack. How should organizations respond after attacks?

What should be done after initially – and hopefully quickly – moving through the initial shock of realizing that systems have been compromised?

A critical element to effectively responding to a cybersecurity attack is a clear understanding of who needs to be involved with the response. Organizations should adopt a “stay ready so you don’t have to get ready” mindset to this.
Pre-determine who in the organization immediately needs to be notified of a security breach; that is, who on the IT team will need to involve, when executive leadership will need to be notified, and who specifically on the executive leadership team will make decisions about the broader communications.

FOURTH DIMENSION
expect more

www.fourdtech.com

After identifying a cybersecurity attack, organizations should follow these steps:

1. **Activate the Response Team**. The predetermined individuals tasked with responding to and making decisions about cybersecurity incidents should quickly assemble. In addition to IT and executive leadership, organizations should invite legal counsel to participate in discussions. Of course, if organizations have cyber insurance or third parties to manage cyber security, representatives from those organizations should help lead the response.

2. **Secure Systems**. As soon as an attack has been detected, the organization's goal should be to contain the attack and prevent further harm. Begin by changing passwords, prioritizing admin passwords on affected systems. Organizations may need to isolate and suspend portions of their IT network. Note that simply removing malware may not be enough to stop an attack.

3. **Restore Backups**. Once the attack has been contained, infected software removed, and hackers no longer have access to the system, organizations should begin repairing the system. One way to do this is to restore backups of the last point in time when an organization's systems were secure.

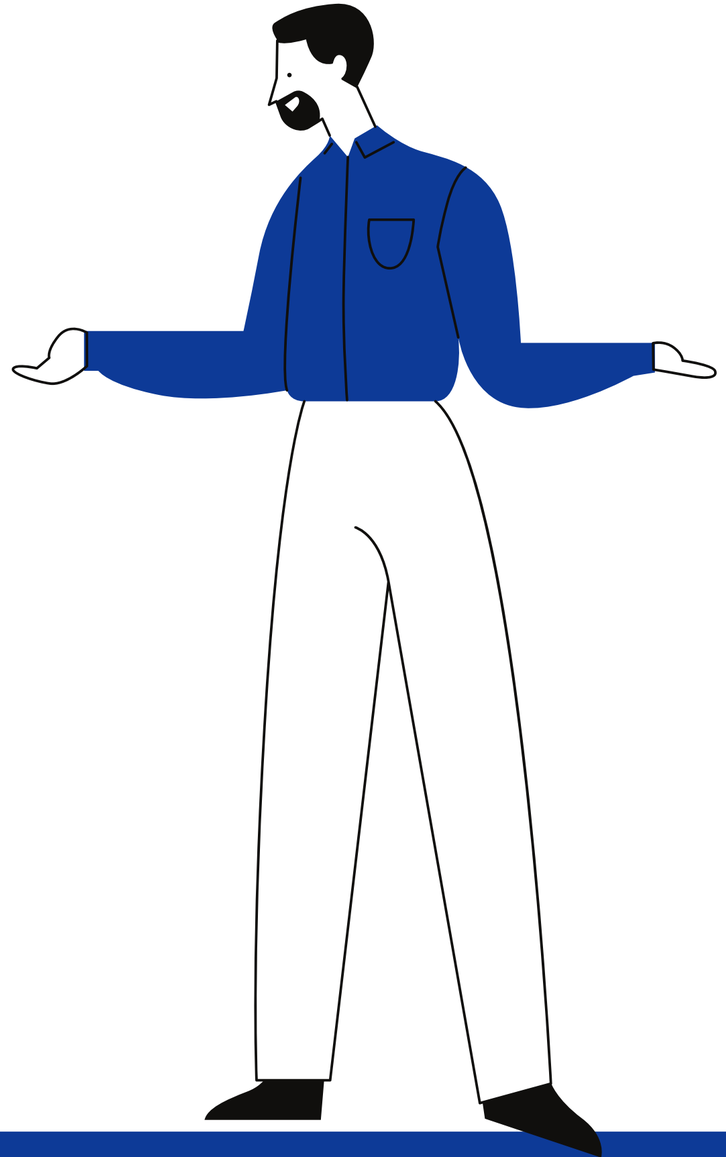
4. **Investigate**. Organizations should determine how the hackers gain access to the system. In a worst-case scenario, an organization may need to take HR action against an employee involved in the breech. The result of the investigation will drive changes to the organization's cybersecurity plan.

5. **Communicate Externally**. Depending on what data was compromised, people external to the organization must be notified. There are legal and regulatory reporting requirements for some data breeches. Organizations may want to alert law enforcement for cybersecurity attacks – both to report the crime and for possible assistance to determine who executed the attack. Finally, if Personally Identifiable Information was compromised, or users were subjected to scam communications, organizations should notify their clients, volunteers, and donors.

It is important to remember that with the rise in the number of cybersecurity attacks, “most organizations will be judged on how they respond to an attack, versus the fact that they were attacked in the first place.”

Organizations, therefore, must proactively address the concerns of relevant stakeholders throughout the response, noting, of course, that the definition of “relevant” will change with the size and scope of the cybersecurity incident.

Often, responses to cybersecurity attacks have a long tail; the attack may be quickly contained, but the recovery and communication can last significantly longer. With proper preparation, the ability to dedicate sufficient resources in the response, and a fair amount of tenacity and patience, organizations can recover from cybersecurity attacks.



FOURTH DIMENSION
expect more

www.fourdtech.com

FIVE Things You Can Do to Protect Against Cyber Attacks

1. Monitor All Money Movement – Implement Encryption and Secure Website for Online donations
2. "Protect Your Devices" Update your Software and Hardware with latest Patches
3. Look Out for Suspicious Emails
4. Keep your Cyberattack Incident Response Plan accessible
5. Change your Password regularly & Review Audit Trails once in 15 days

npo@fourdtech.com