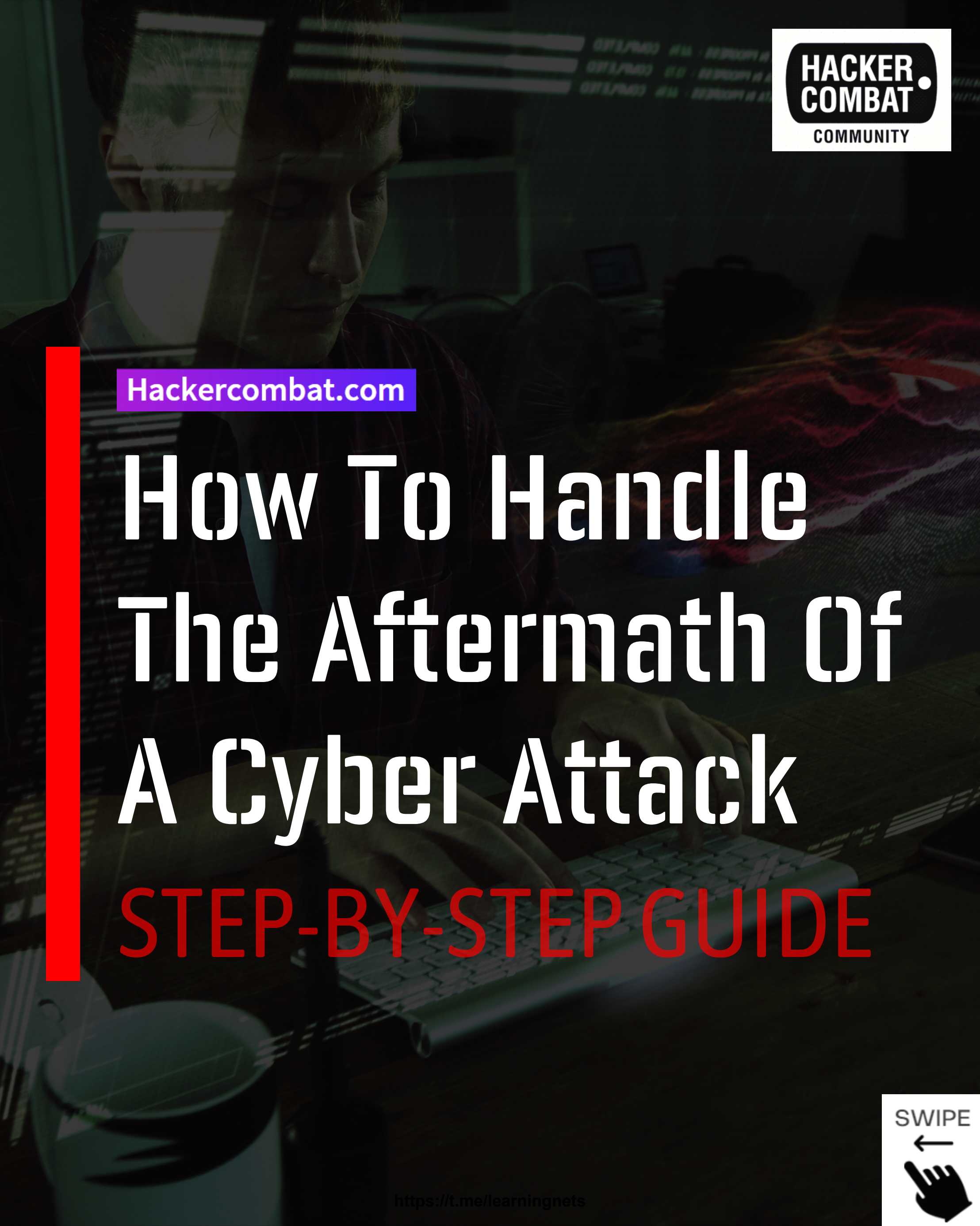

HACKER COMBAT
COMMUNITY
Hackercombat.com
How To Handle
The Aftermath Of
A Cyber Attack
STEP-BY-STEP GUIDE
SWIPE
https://t.me/learningnets

What To Do In The First Few Minutes Of A Cyber Attack

01

The employee who encounters the threat first needs to alert the IT and management teams.

When an employee encounters something irregular with their computer, they need to notify the IT team immediately. It doesn't matter if it's a false alarm, but if something is out of the ordinary, the techs need to know. There are times hackers and threat actors keep their attacks under the radar so they can steal data without issue. No one should take any irregularity for granted.

02

IT staff must disconnect the computer from the network and start documentation of the infection.

Once the tech team identifies the compromised computer, they need to remove it from the network immediately. They should start unplugging the LAN cables and move to contain the threat inside the unit. Aside from containing the threat, they will need to check nearby units for infection.

03

The company should check their backups in the cloud.

A member of the IT team needs to go to their existing backups and make sure they are not compromised in any way. The integrity of the backups will ensure the continuity of business operations after the attack is over and the team contains the bad actors.

04 The IT team on-site should start implementing cyber security protocols.

If a company creates a cyber security response plan, there should be rules and procedures for how to treat the first minutes of the discovery of a cyber-attack. If the incident response team is not yet on site, the first responders should start implementing what's stated in the plan. If the plan calls for the scene of the cybercrime to be cordoned off, the IT team should preserve the integrity of that particular part of the network.

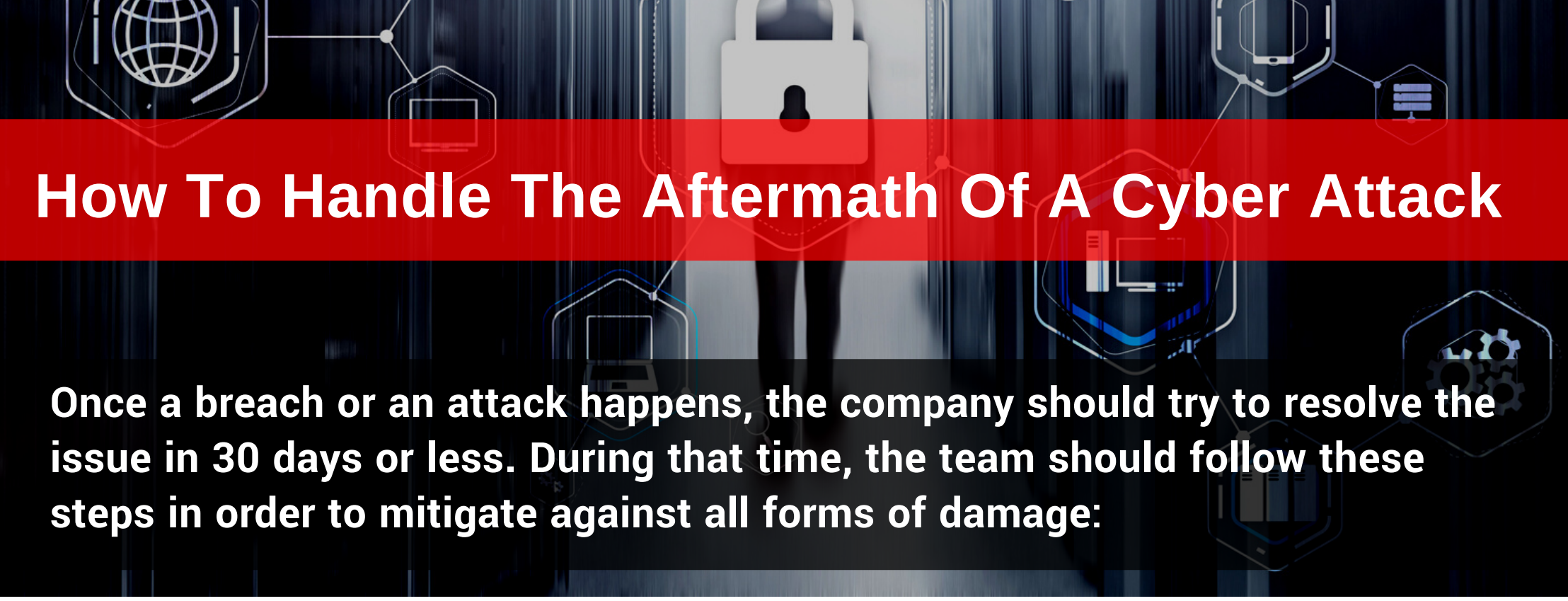
05 The IT team should call the attention of the employees and educate them about the attack or infection.

The company should immediately inform their affected employees about the cyber-attack. Human error can serve as the root cause of a breach and it can also definitely worsen a crisis. Employees need to learn how to act during such a situation in order to minimize and prevent further damage. For example, if the source of the threat is a phishing email, IT staff should immediately inform employees not to click or open a particular message to avoid any malware from spilling onto more computers.

06 Use security systems to track potential malicious assets.

Companies with security operations centers or blended solutions like Comodo Endpoint Security should definitely use their resources to make sure the threat is controlled. As we have previously mentioned, re-infection can still happen and it's best that all trace of malware or security vulnerability be controlled as soon as the issue stabilizes.

SWIPE ←



How To Handle The Aftermath Of A Cyber Attack

Once a breach or an attack happens, the company should try to resolve the issue in 30 days or less. During that time, the team should follow these steps in order to mitigate against all forms of damage:

Convene The Incident Response Team

The incident response team should be composed of an incident response manager, who may or may not be your CISO, several cybersecurity analysts and threat researchers.

They'll be at the heart of the investigation and also the ones coordinating with the representatives of the company's various stakeholders. These representatives should hail from management, human resources, risk assessors, lawyers, and public relations experts.

The internal tech team will investigate the cyber-attack while the other representatives will be there to support the work and to mitigate the kinds of damage that the company will encounter.

SWIPE ←

Cordon Off Assets and Ensure Cyber Security Integrity

The team should immediately control the scene and cut off part of the network that had been compromised. They also need to make sure that the root cause or causes of the attack or the breach aren't still lingering in the system.

Once they ascertain everything is safe and that first responders or themselves have properly documented the incident, they'll have to look at all of the assets within the company and **check for damage.** They should start consulting their detection technologies to make sure there are no additional threats within the network.

After the network has been secured, the team will need to help ensure that systems critical to business operations could be **restored immediately**. This step is crucial since stopping operations will only hurt the company more.

SWIPE ←

Document And Investigate

The investigating team will need to walk back through the incident to establish the facts. They'll have to check what happened during the discovery of the attack and how the attack unfolded later on. These investigators also need to establish the kind of attack and its root causes. Aside from reconstructing the narrative behind the cybercrime, the team should also document every step of the investigation.

The investigation should always follow the steps prescribed by the cybersecurity plan and work in alignment with existing company policies every step of the way. This is important since auditors and investigators from the government will verify and check the extent of actions the company has taken to investigate and remediate the issue.

The team will also have to be sensitive about who they share the information with. Attacks and breaches can occur because of malicious insiders within the company.

Once the team identifies who the culprit is behind the attack and who the accomplices are, the team should work with HR to ensure that the people are held accountable in accordance to company policy and the law.

SWIPE ←

Inform Law Enforcement And The Authorities

When a cyber-attack occurs, law enforcement must enter the picture as soon as possible. The problem with delaying this particular step is that it could be taken as a **sign of culpability** in the attack. Companies don't report to the law following an attack because they think investigations can put a halt to operations. Agencies like the FBI will work in a non-disruptive way and cooperate with the victims of an attack.

Notify the Public Regarding The Attack And Engage With Media

There are some breaches that your company will be able to resolve in time before they blow up and no consumers get affected. When that's the case, these breaches and attacks could be resolved without notifying the public. However, when customers will be affected by a breach, like in service businesses which actively engage with their clients, the company must make a disclosure.

When this happens, the company should own and control the narrative. The incident response team, together with the managers and people from human resources, should have a meeting before the disclosure to talk about every angle of the incident. The team should also stay in contact with a public relations expert who will help them manage how the company is portrayed in the media.

Follow Compliance Requirements After an Attack

Governments and states have become more sensitive to issues of breaches and attacks. Lawmakers have started making laws and policies which make companies accountable for any lack of preparation for the attacks carried out against their systems.

In light of these regulations, companies need to make sure they conform to every letter of these requirements to **avoid extensive** penalties.

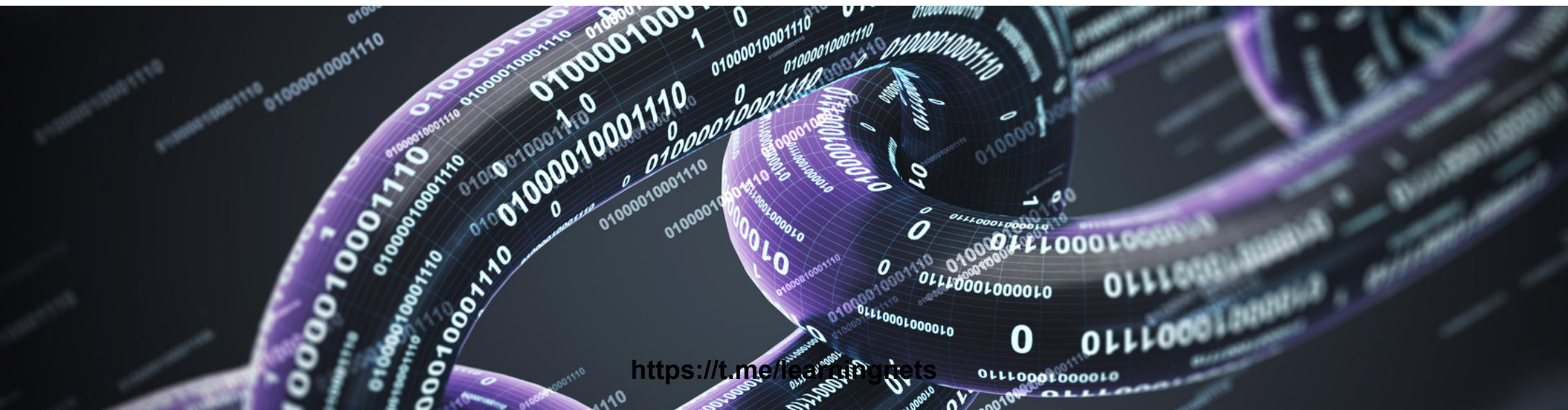
A major part of these regulations are the notification requirements. Certain laws like the European Union's General Data Protection Regulation require companies to report to their clients about the breach within a 72-hour window.

Prep For Legal Consequences

The cold hard reality about a cyber-attack is that a company will never be fully prepared for one and all an organization can do in the aftermath of an attack is to do damage control.

After your incident response team concludes its investigation, manages the story, and repairs the damage to structures within the company, they'll have to work with the company's legal team. The government or an individual will hold the company liable and there will be legal ramifications to what transpired.

The steps above should help you and your company weather the storm immediately after and within a month of a cyber-attack. This 30-day timeline is actually shorter than the actual period that a threat statistically lies dormant within a system which is around **180 days.** That's half a year that companies could actually have spent in mounting credible and proactive defenses against these threats.



Tips for Maximizing Cyber Crisis Management Efforts

Invest in Advanced Detection And Remediation Tools

The Ponemon Institute's research showed that the faster a breach is identified and contained, the lower the costs the company incurs. A company that identifies a data breach saves **$1 million** if they see the issue within 100 days. Containing the cause of the breach is another matter.

An organization that contains a breach within 30 days manages to save **$1 million** more in expenses than those that took longer. In order to meet those timetables or even avoid encountering a breach altogether, companies need to invest in advanced network and endpoint security. Advanced scanning tools found in such blended solutions have a much higher chance of catching the root cause of breaches.

SWIPE

Form an Incident Response Team

The Ponemon Institute saw a **$14 per record** cost reduction during a breach for companies that had incident response teams during the crisis.

According to the study, the average cost a company pays per member record compromised is $148. This is substantial if you think about the Equifax breach which affected at least **145.5 million users** in the US.

Based on the $148 cost per compromised record figure, Equifax should be spending around $21 billion. If Equifax had an incident response team during the time of the breach, they would have saved $2.3 billion.

Use Strong Encryption for Assets

Extensive use of encryption also saves companies $13 per member record compromised and possibly even more.

A single cyber-attack can also lead to another since the threat actors can plant their assets into the system.

These assets, like malware, can re-infect the system and open backdoors for another attack against the network.

Hackercombat.com

Follow. Learn. Share

Save For Later

Follow us!

Find us Online

Like and Comment