7 Steps to Recognize and Combat Cybercrime

Written by
Joseph Carson

How do you recognize and combat cybercrime?

This is one of the most talked-about topics in the media and in the boardroom in recent years. It is a major problem and challenge for many organizations. The average dwell-time (average time before a company detects a cyber breach) is more than 200 days, highlighting this as an area where companies do not do well. This is because not all cyber breaches are destructive in nature. Cybercriminals commonly stay hidden for long periods waiting for the right moment to steal sensitive information. They may sell the stolen access to other cybercrime groups who will perform more destructive actions such as deploying ransomware.

> Too often, companies only discover a cyber breach when they detect the “smoke”

Many companies are not proactively looking for cyber breaches. It’s only when they detect “smoke” do they realize the company has experienced a cyber breach. Ransomware, for example, makes the critical data on systems unavailable until the victim pays a financial fee,

typically bitcoins, to get the key that unlocks the data. **This type of cyberattack is easily detected**, like DDOS attacks (Distributed Denial of Service), as it makes part of the company's service immediately unavailable. Ransomware threats have been increasing and are about to pass 1 billion dollars in cybercrime.

Check out our guide: Ransomware on the Rise: How to Reduce Risks and Respond to Attacks
Related reading: Ransomware Mitigation: Where Do We Go From Here?

Cyberattacks can be quite inconspicuous in their destruction

Not all cyber threats are so apparently destructive, and due to this many companies do not see smoke at all. Therefore they assume that everything is okay and nothing is at risk. However, the reality is that **a malicious cybercriminal or cyber criminal is already on the network**, waiting, watching, stealing data, and committing financial fraud; typically abusing the credentials and privileged accounts of a trusted insider. This is because malicious cybercriminals, and cyber criminals for whom the motive is mostly financially motivated or intelligence-focused, the key to their hacking activities is to remain hidden. To stay undetected, and hide any trace or footprint of their activities.

These types of hacking techniques make it difficult for

companies to recognize and combat cybercrime. They're difficult to detect because everything appears to be working normally. Most attackers use the "live off the land" technique, meaning they will not introduce anything new onto the network. Instead, they use tools they find that already exist on the network.

So how can we recognize and combat cybercrime, and improve enterprise cyber hygiene?

Here are some tips and best practices that will help you and your company recognize cybercrime and combat the threats.

#1 Education and Cybersecurity Awareness

This is one of the most effective cybersecurity countermeasures and an instant win. Empower employees to become a strong cyber defense on the front line. Employees should never be afraid to ask for help or advice when they see something suspicious. The earlier an employee reports a security incident, the less significant the potential impact might be.

Educate employees to avoid and prevent suspicious activity on their computers:

• Detect suspicious applications running, popups, warning messages, etc.
• Flag suspicious emails (emails with attachments, sender

unknown, hyperlinks, and unusual requests)
• Be vigilant when browsing websites
• Stop and think before clicking on links or ads
• Ensure websites are trustworthy before entering credentials
• Limit activities when using public insecure Wi-Fi networks or use a VPN

Educating your employees on what to look for will increase your company's ability to recognize cybercrime early, and in many cases prevent it. This will not only help the company's cyber hygiene but will help employees keep their own personal data secure.

Training should start at the top of the organization, working down. It is recommended you appoint a cybersecurity ambassador within each department to assist in the detection and incident response for potential cybersecurity threats and risks. This helps expand the efficiency of any IT security team while ensuring that there is someone in the organization who is responsible and accountable for implementing and maintaining cybersecurity measures.

Speaking of incident response, don't wait until it's too late to protect your privileged accounts. Download our free, customizable **Cybersecurity Incident Response Plan Template** now, and get prepared.

#2 Collect security logs and analyze for suspicious or

abnormal activities

An important activity and best practice for companies are to make sure security logs are being collected and analyzed for suspicious activities. In many situations looking at security logs will likely identify abnormal action. For example, look for credential logins or application executions that occurred during non-business hours, or execution of tools such as psexec which could be an indicator of lateral moves. Not only can security logs help detect cybercriminal activities, but they also become hugely important when dealing with digital forensics to determine root cause analysis and help with future prevention measures.

#3 Keep systems and applications patched and up to date

Keep systems and applications up to date and apply the latest security patches—this will keep most malicious hackers and cybercriminals from gaining access to systems by using known exploits and vulnerabilities. This is not a foolproof countermeasure, but it will make a successful breach more difficult for cybercriminals.

Remote access is critical to keeping employees productive. But risks increase when employees work remotely. Check out our solutions for your remote workforce.

#4 Use strong passwords and keep privileged accounts protected

When choosing a password make it a strong password, unique to that account, and change it often. The average age of a social password today is years, and social media does not do a great job alerting you on how old your password is, how weak it is, and when it is a good time to change it. It's your responsibility to protect your account, so protect it wisely. If you have many accounts and passwords, use an enterprise password and privileged account vault to make it easier to manage and secure. Never use the same password multiple times.

If your company is giving employees local administrator accounts or privileged access then this seriously weakens the organization's cybersecurity. This can mean the difference between a single system and user account being compromised versus the organization's entire computer systems.

In all Advanced Persistent Threats, the use of privileged accounts has been the difference between a simple perimeter breach and a major data loss, malicious activity, financial fraud, or worst-case scenario—ransomware.

Organizations should continuously audit and discover privileged accounts and applications that require privileged access, remove administrator rights where they are not required and adopt two-factor authentication to

mitigate user accounts from easily being compromised.

Reward your employees with a password manager or privileged access security solution that will help reduce password fatigue and help move passwords into the background so they no longer need to worry about password reuse. This can help increase security controls, and protect passwords and privileged access

FREE TOOL: Windows Privileged Account Discovery Tool

#5 Do not allow users to install or execute unapproved or untrusted applications—stop malware and ransomware at the endpoint

Another major risk that organizations run—as a result of providing users with privileged access—is that the user has the ability to install and execute applications as they wish, no matter where or how they obtained the installation executable. This can pose a major risk allowing ransomware or malware to infect and propagate into the organization. It also allows the attacker to install tools enabling them to easily return whenever they wish. When a user with a privileged account is reading emails, opening documents, browsing the internet, and clicking on numerous links, or when they simply plug a USB device into the system, they can unknowingly install infectious or malicious tools. This enables an attacker to quickly gain

access and begin the attack from within the perimeter, or in the worst-case scenario, encrypt the system and sensitive data—then request a financial payment in return to unlock them.

Organizations must implement security controls that prevent any application or tool from being installed onto the system by using Application Allowlisting, Denylisting, Dynamic Listing, Real-Time Privilege Elevation, and Application Reputation and Intelligence. This is one of the most effective ways to prevent being the next victim of cybercrime.

> Force attackers to take more risks; the more risk they take the more noise they create, giving the defenders a chance at detecting them before a cyber catastrophe occurs

#6 Be deceptive and unpredictable
It's crucial to be deceptive, be unpredictable. Most organizations look to automation to help assist in their cybersecurity defenses, but in many cases, this lends itself to predictability: scans are run at the same time every week, patches take place once per month, assessments once per quarter or per year.

Companies that are predictable are vulnerable, so establish a mindset in which systems are updated and assessed on an ad-hoc basis. Randomize your activity. This will increase your capacity to detect active

cyberattacks and breaches.

These best practices and tips will help companies reduce the dwell time of cyber breaches as it makes it difficult for hackers and cybercriminals to remain hidden and increases the likeness of detecting active cyberattacks. It also raises awareness in the organization and engages employees in becoming an important role in detecting suspicious activities.

#7 Have a solid backup and recovery plan

For any business, today, being resilient means having a business recovery plan. In other words—a strong backup strategy. Unfortunately, many companies only do online backups using the same credentials as their production environment. This means once an attacker gains access to production it's easy for them to deploy ransomware to the backup systems as well, bringing the business to a complete stop with no way to restore. A strong backup strategy is one that also considers the techniques used by ransomware cybercriminals. Ensure your backups have offline capabilities and are also protected by privileged access security solutions so cybercriminals are unable to access them.

I hope you'll consider all seven steps in your efforts to combat cybercrime in your organization, and make use of the great tools we offer!

FREE EBOOK
Cybersecurity for Dummies

Show your employees how to protect themselves and your organization

DOWNLOAD THE BOOK