CYREBRO

7 Steps to Effective Incident Response

Contents

A Very Real Threat 03

Preparation – Ready for the Attack 07

Identification – Recognizing and Attack 10

- Monitor 12
- Detect 12
- Documentation 13
- Best Practices 13

Containment 14

Eradication 17

Remediation 19

Recovery 21

Post-Incident 23

Protecting Customer Networks – CYREBRO Case Study 25

CYREBRO

A Very Real Threat

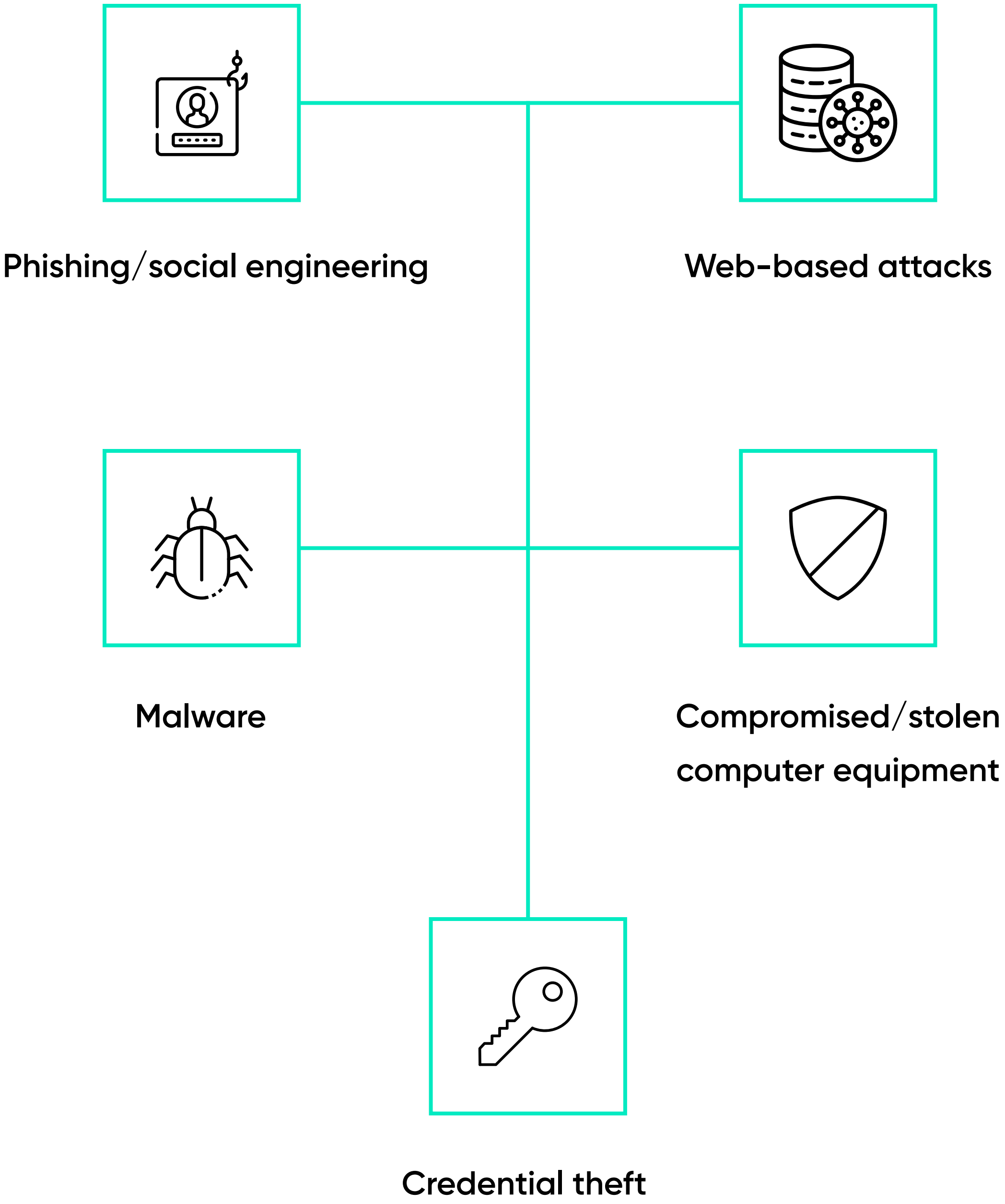
Cyberthreats wreak havoc over businesses of all sizes and forecasts expect them to cost businesses over $10 trillion a year by 2025. For many IT departments, cyberattacks aren't so much a question of if, but when.

Creating an incident response plan is the first step to ensuring you won't be blindsided when an attack happens. It lays out the steps to be taken, offering guidance when time is of the essence.

Having an incident response plan in place can limit the damage, enabling companies to remain viable. A recent **FireEye report**, based on interviews with 800 CISOs, showed that more than half of all businesses aren't ready for a cyberattack. Existing response plans ranged from having no plan at all (8%), having a plan that wasn't tested in over a year (29%), to having plans within a certain division but lacking a comprehensive, organizational plan (30%). Only one in three companies reported that they had mature, well-tested plans in place.

In a **study** by the Ponemon Institute, nearly two-thirds of all businesses experienced a cyberattack or breach in the previous 12 months. 65% of respondents said they lacked the budget to achieve a strong security posture.

Attacks on small business typically fall into one of five categories:



Phishing/social engineering

Web-based attacks

Malware

Compromised/stolen computer equipment

Credential theft

For those that experienced significant breaches, the results can be devastating. The longtail costs of data breaches can last months and even years, frequently going unnoticed. When a breach is successful, businesses suffer:

Data losses

267,277,828 records were breached in 2020 (**IT Governance**)

Businesses disruption

90% of businesses have reported downtime due to technical issues and a lack of disaster planning (**Datto**)

Revenue losses

Revenue losses - the average cost of an attack costs small businesses **$8000** a minute (**Datto**)

Brand reputation damage

40% of small businesses don't reopen after large data losses (**FEMA**)

Failing to plan for cyber-attacks can be the difference between operating and shutting down for small-to-medium-sized businesses. Without a recovery plan, your company could be closing its doors after a data breach.

CYREBRO

Preparation

Ready for the Attack

Creating an Incident Response Plan (IRP) is key to strengthening your organization's security posture. Without an IRP, an attack can throw any business into disarray. Wasting time figuring out what to do next costs time and money – it is key to your defenses.

An IRP establishes and tests a business' capability to deal with new or undiagnosed security issues. Businesses with effective IRPs in place can defend against and recover faster too. But this complex, bespoke process means that finding expert help to identify the critical components in your infrastructure and create appropriate response plans can be key to success.

BEST PRACTICES All good IRPs need five key components:

01 Identifying the baseline.

Baseline security is the minimum that a company should do to protect itself from vulnerabilities. Recommended configurations, technical solutions, and recovering actions are all contained in the baseline – it is effectively impossible to implement an IRP without one.

02 Establishing critical components.

Key parts of a company's infrastructure must be identified and protected. Companies must harden defenses around critical infrastructure and also develop plans for potential failure.

03 Diagnosing single points of failure.

Identifying single points of failures – whether at a hardware or software level – and developing plans to deal with them prevents lengthy periods of downtime. Redundant hardware and software failover features will be the difference between losing thousands of dollars and losing millions.

04 Developing communication plans.

An effective plan needs to recognize that key individuals still need to communicate. Developing a workforce continuity plan within your IRP will allow critical staff to deal with the security issue while normal company operations can continue as soon as possible.

05 Training staff.

IRPs don't work unless IT professionals understand how to implement them. Rolling out training to staff and testing the IRP should be continuous to ensure that the response is as quick as possible.

Identification

Recognizing an Attack

Recognizing an Attack

There are multiple ways to identify attacks. A business with an IDS/IPS may receive alerts from the monitoring system, malfunctions could appear for employees, or customers may send reports or complaints about a product. An unusual entry in an audit log may be the only clue that something is amiss.

Identifying precursors (a sign that something may go wrong) and indicators (a sign that there has been an intrusion) is key. Using vulnerability scanners, assessing activity logs, and working with antivirus software and intrusion detection sensors gives an organization the tools to stop attacks before they spin out of control.

Skilled security professions should also be able to identify unusual filenames or suspicious activity and implement defensive measures as soon as possible.

Monitor

Your security operations center (SOC) should have eyes on every network endpoint and vulnerability within the network. Bolstered by threat intelligence data, your monitoring system should be scanning for anomalous activity that indicates if an attack is underway.

Detect

With proper profiling and understanding of your systems, you give your organization a better chance of identifying problems.

When activity seems amiss, your SOC should detect any security incidents. Your SIEM or other security tools should issue an alert to relevant security personnel.

Documentation

Your cyberteam should document their initial findings and assign an incident classification. Retaining effective logs needs to be backed with a Log Retention Policy to help with threat analysis.

Referring to logs will then help perform event correlation, allowing for quicker and more efficient responses in the future.

Best Practices

Train employees to be on the lookout for anomalies, and report when things seem wrong. Continuous professional training will aid in preventing human errors leading to leaks and stop up to 88% of data breaches (**Kroll**).

If they are being locked out of systems that they should be able to access, or are receiving suspicious emails, create a culture where they know they need to report on the activity.

CYREBRO

Containment

Stopping the Spread

Stopping the Spread

When you need to contain an issue, you need to understand your mission-critical business systems. Limiting the attack surface will stop attackers in their tracks. Effective system hardening, rigorous updates, and continuous employee training all aid in stopping attackers from getting a foothold.

Your containment strategy should start with the information you received from the documenting analyst. Begin containment with coordinated isolation of all systems within your network that have been compromised.

The isolation must be coordinated and in accordance with your incident response policy. Communicate using established channels among all incident response personnel to coordinate the shutdown.

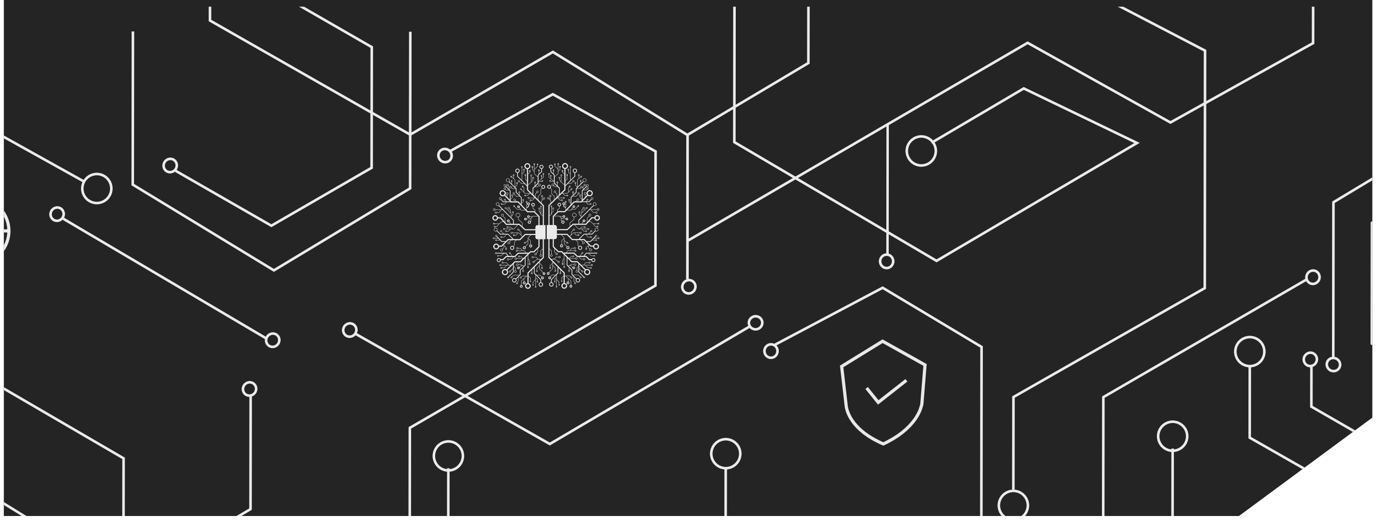
Close any gateways that enabled the breach. Find and dismantle backdoors that your attacker may have implemented to give them future access. By identifying any indicators of compromise (IOC) and searching for TTPs (Tactics, techniques, and procedures) that were used to overcome your security measures, you'll be able to contain the attack.

BEST PRACTICES

Identify the point of initial access and infection as quickly as possible. Deep and extensive technical knowledge is key for implementing the correct containment policy, depending on factors such as the potential for damage, service availability, and the duration of the solution. This will protect your network from later movement and propagation of the attack.

You need to identify outbound traffic to the attacker, as well as find and disable the command and control (C2) server, which might also be used to propagate follow-up attacks.

By identifying the point of entry, preventing late movement, and disabling the command-and-control center, you can fully contain the attack.



Eradication

Removing the Threat

Removing the Threat

Once contained, your security team will take a surgical approach to remove any malware. In extreme cases, it may be necessary to wipe out all infected devices and rebuild the operating system.

As part of the eradication process, administrators must restore systems to normal operation and ensure that systems function as expect. Continuous assessment is necessary throughout the eradication process to ensure that vulnerabilities and infections are not still present during the remediation, recovery, and post-incident phases.

BEST PRACTICES

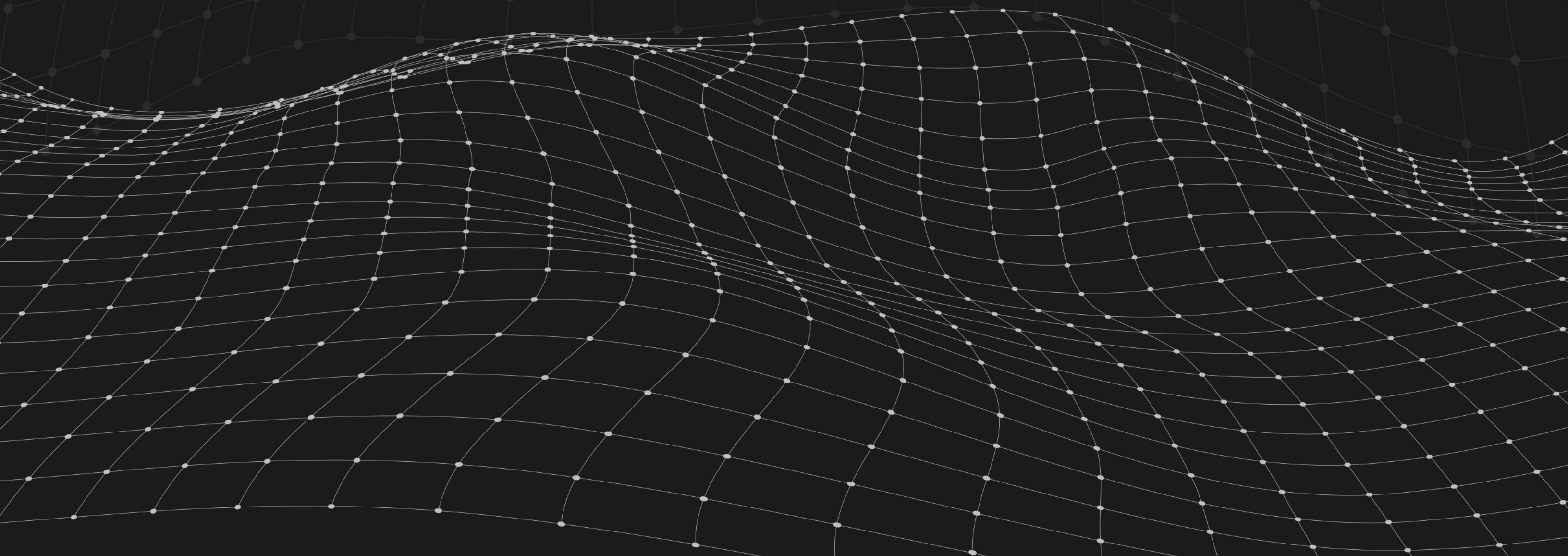
Use logs and artifacts to establish the initial time and date of the infection, so you know which versions of your system back-ups are usable. Update passwords, including any for accounts that were logged on during the breach.

Taking a higher level of logs during the eradication process is necessary to assist with future recovery processes. As known vulnerabilities are often attacked,effective logging will aid in avoiding repeated disruption to business operations.

CYREBRO

Remediation

Hardening for the Future



Hardening for the Future

Once your system is clean, you will need to ensure that your cybersecurity is up to date. Safely returning your organization to full-functionality, set aside time for updates and analysis of the incident.

Reduce vulnerabilities through system hardening, following the path that the attackers took, and closing vulnerabilities. This includes the hardening of applications, operating systems, servers, databases, and the network.

Check all configurations to ensure that there are no misconfigured settings that could be exploited by cyber-criminals, and deploy all patches.

The remediation process should be a phased approach. Small-to-medium-sized businesses may be online again within a matter of days, but large enterprises may need months to safely return to full functionality. Here is a situation when failover software and full disaster recovery (DR) plans can save businesses millions of dollars.

BEST PRACTICES

Review all your hardware to make sure that it is still receiving support and has not reached end of life. Once hardware reaches end-of-life and is no longer patched, it opens new vulnerabilities into your network.

Assess all software and ensure that all patches are applied before returning to full functionality. Failure to update software can leave known vulnerabilities such as backdoors open for cyber-attackers to strike again.

Recovery

Returning to Full Functionality

Returning to Full Functionality

During the recovery phase, your goal is to determine whether the malware can be completely removed, assess the recoverability of the compromised assets, and rehabilitate the asset, bringing it back into normal operations.

The IT team will take predefined steps as defined in the Incident Response Plan and apply the required changes and patches to the affected asset. If recovery is too complex, or if the cost of recovery is more than the value of the asset, the IT team may decide to decommission the asset.

BEST PRACTICES

Before investing resources toward recovery, review the bill of materials (BOM) in the asset.

While part of your assessment as to the recoverability of the asset should be linked to the degree of difficulty in removing the malware, you should also consider the amount of time the asset has before end of life, to determine whether it is worthwhile to try and recover.

CYREBRO

Post-Incident

Learning from the Past

Learning from the Past

With the incident in your rearview mirror, it's time to focus on lessons learned, which will be used to help prevent another attack. Post-incident activity should feed back to incident identification, containment, eradication, and recovery.

Conduct "threat hunting" operations, looking for signs of a latent breach that you missed during the Containment and Eradication stages. Threat hunting becomes immediately more effective with well-organized and detailed logs as they can inform incident response teams about known effective practices.

Document the incident and your response, noting areas where your team functioned effectively and areas that need to be improved. Determine if the issue was poor policy or poor implementation, and act accordingly.

Maintain a higher state of vigilance, as hackers may decide they want to exploit your network again, and study logs to see if there was a sign before the initial attack that you missed.

BEST PRACTICES

After analyzing the attack, review your existing security policies to see if they are adequate or need to be updated.

Additionally, continue to impress upon your employees the role that they play in keeping the company network safe. Review password policies, provide additional training, and ensure that employees know what to do when they encounter suspicious activity.

CYREBRO

Protecting Customer Networks

CYREBRO Case Study

CYREBRO Case Study

A North American financial institution approached CYREBRO after falling victim to multiple cyberattacks. The financial institution was using a remediation plan from a different cybersecurity vendor, but it was ineffective.

The CYREBRO team was asked to audit security practices that were in place. CYREBRO analyzed the network and compared its report to that of the original cybersecurity vendor. CYREBRO found a number of persistence mechanisms that had gone previously undiscovered, which served as a gateway for malware to enter the system.

CYREBRO'S team realized that the issues were coming from a third-party provider who had an open network connection. CYREBRO provided a remediation plan and was able to eradicate the threat.

About CYREBRO

The CYREBRO SOC Platform gives you strategic monitoring, threat intelligence, and rapid incident response services in one place. With a vision to take all security events and display them in one place, CYREBRO makes the complex world of information security clear and allows for the prioritization of problems.

CYREBRO turns the chaos of the complex and ever-changing world of cyber-security into clarity using its cyber-brain.

GET STARTED

www.cyrebro.io