YOU'VE BEEN HACKED — NOW WHAT?

HOW TO RESPOND TO CYBERSECURITY INCIDENTS

LMNTRIX

BE THE HUNTER I NOT THE PREY

How to Respond to Cybersecurity Incidents

2

It's happened: You've received a breach notification — either from internal staff, an external tipster or law enforcement. Intruders have broken through your defenses and into your organization's environment. What are your next steps?

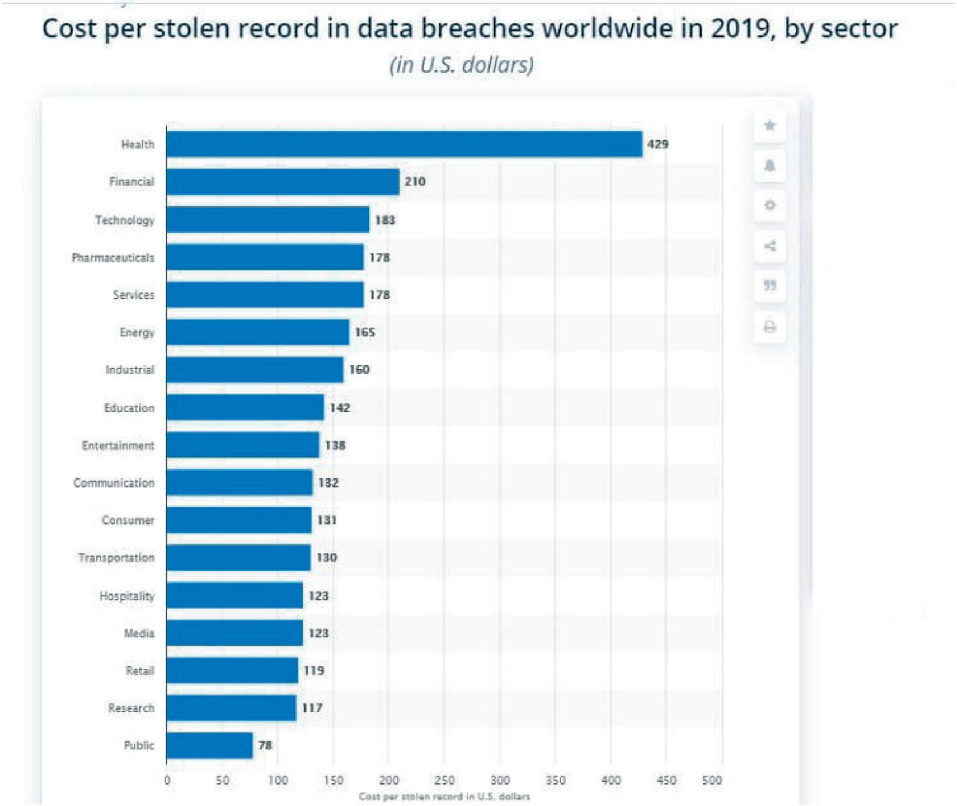
Will you respond like the Equifax CEO Rick Smith who stated that the firm would be "defined by its response" then went onto publish a website on which customers had to file a claim by entering confidential information that Equifax had already mishandled!

Or will you handle it like Uber who was exposed for an attempted payment to keep criminals from exposing a massive data breach. It's one thing to forgive the initial hack, but paying to cover it up is another thing. They even went as far as demanding the hackers signed nondisclosure agreements.

And in 2020, Travelex camouflaged a system-wide outage as a "scheduled maintenance," later admitting that the event was the result of a massive ransomware attack, ignoring the age-old wisdom that "honesty is always the best policy."

With the average cost of a record stolen in a cyber-attack topping $429 in 2019, organizations need to develop a methodology and build a strategy for responding to cybersecurity incidents. An incident response strategy combines measures to prevent threats from penetrating the perimeter with tools to respond to a cyberattack in progress and tools to manage malicious attacks.

How to Respond to Cybersecurity Incidents



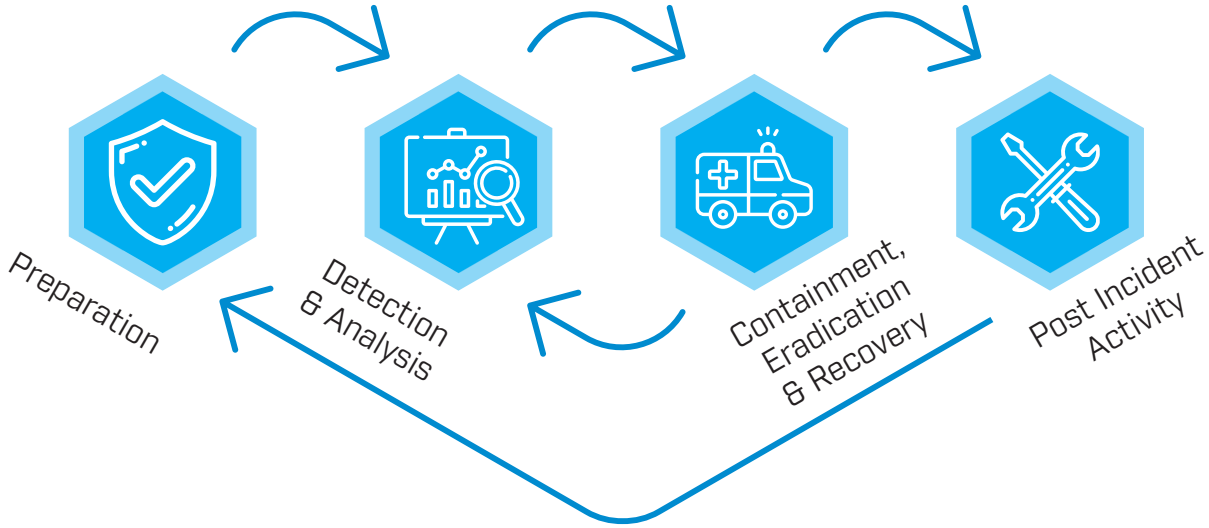
A data breach does not affect only data records containing sensitive information about customers, partners as well as critical financial information. Data breaches start a chain of destructive consequences, including stealing of intellectual property, damaging brand reputation and value, exposing customers to additional cyberattacks while making the organization vulnerable to court claims by any entity affected by the data breach.
An incident response program intends to limit the damages and restore operations to their normal states as quickly as possible. Furthermore, a feasible incident response strategy incorporates an investigative component that enables organizations to unearth the core sources of a data breach and learn from cybersecurity incidents to prevent cyber-threats from infiltrating their systems.

Six Components of Working Incident Response Plans

4

Non-government and public entities operating in the field of cybersecurity, including leading researchers at the SANS Institute (SysAdmin, Audit, Network, and Security Institute) and the U.S. National Institute of Standards and Technology (NIST) define six steps involved in the creation and implementation of a successful incident response plan.

Incident Response Lifecycle



Preparation

A key component of a feasible incident response plan is the development of policies and procedures that come into action should a cyber-incident occurs.
The organization should determine the structure and the responsibilities of the response team members and adopt procedures for alerting all stakeholders. Training the response team members to take appropriate actions depending on the kind and scope of the data breach is crucial as well as the ability to fully document the breach for extensive investigation.

Identification

Incident response is impossible without properly identifying a data breach. Only then, the response team can take quick and focused actions that eliminate the threat and prevents it from spreading across the network.
In this stage, the organization should take full advantage of advanced cybersecurity tools to identify the breach and determine its scope and specific kinds of threats it bears. Threat intelligence and threat prevention tools include software such as firewalls, antivirus applications, intrusion detection systems, and platforms for the detection of abnormal system and user behavior.
Threat intelligence is a crucial component in a working threat response and prevention plan, as organizations should take into account current cyber-threat trends and keep up with the common tactics used by nation-state actors and various hacking groups.

Containment

Containing the damage caused by a data breach to a bare minimum is of utmost importance since most modern threats are able to spread quickly and find hiding spots in different segments of a corporate network. Taking down selected sub-networks endpoints or servers plays an essential role in the process and organizations should maintain up to date and complete backups to be able to maintain operations during the stage of cleaning up the infected systems.

Eradication

Eradication is the stage and process of fully neutralizing the threat and restoring all systems to normal operation. When an organization restores its data records and puts systems back in operation, the incident response team should perform secondary monitoring to make sure an attacker is no longer able to penetrate the perimeter.
The process of extended system monitoring should continue for as long as required and until the team makes sure that none of the affected systems is vulnerable anymore.

Recovery

In this stage, the security team makes sure the cyber-threat has left no further traces of its presence on the corporate systems and no account is compromised one way or another.
During the recovery phase, the incident response team continuously monitors the entire IT ecosystem for signs of abnormal activities until all systems are restored to their pre-breach state and are operational.
Once an organization enters the recovery stage after a data breach, the internal experts will be able to calculate the cost of the damage and the associated losses.

Lessons Learned

The last stage in the incident response lifecycle is the stage of follow-up activities or 'Lessons Learned'.

The incident response team and all stakeholders should investigate the root causes of the data breach, the ways it had penetrated and spread across the perimeter, and then adopt measures that prevent future similar incidents.

During the process of follow-up, the organization could decide to tweak and update its cyber-security policies and procedures entirely or in some specific areas. Analyzing a cyber-security attack is one of the most powerful weapons an incident response team has in possession to prevent future attacks and detect unknown threats.

Each of those stages involves multiple steps and organizations need to address different issues in each of the stages.

Incident response is impossible without properly identifying a data breach. Only then, the response team can take quick and focused actions that eliminate the threat and prevents it from spreading across the network.

7

In this stage, the organization should take full advantage of advanced cybersecurity tools to identify the breach and determine its scope and specific kinds of threats it bears. Threat intelligence and threat prevention tools include software such as firewalls, antivirus applications, intrusion detection systems, and platforms for the detection of abnormal system and user behavior.

Threat intelligence is a crucial component in a working threat response and prevention plan, as organizations should take into account current cyber-threat trends and keep up with the common tactics used by nation-state actors and various hacking groups.

Steps Involved in Different Stages of Cybersecurity Incident Response

We should start by saying that not every cyber-attack is also a cyber-security attack. An organization might be a target and victim of a Denial-of-Service (DoS) or Distributed Denial-of-Service (DDoS) attack, which is aimed at paralyzing its operations and connections to external systems but such an attack does not have the organization's sensitive data as its primary target.

Hence, a cyber-security attack is one that is targeting sensitive corporate data or personally identifiable information for its customers. Another type of such an attack is a ransomware attack in which a threat actor installs a code that encrypts critical systems and data storage devices.

In the case of a cyber-security attack detection, the response actions are categorized into four stages or steps to be taken by the incident response team:

- Step 1: Identify the kind and scope of the cyber-security incident.
- Step 2: Define the specific objectives and investigate the situation in detail.
- Step 3: Take timely and appropriate action.
- Step 4: Recover systems, data and networks.

Each of the above steps involves a dynamic set of sub-steps that depend entirely on what an organization finds during an incident.

Nonetheless, during the initial stage of identifying a threat once it is detected, the IT security team should address the following issues, which are critical for further managing the incident response process.

- Who is performing the attack?
- What is the scope and extent of the attack?
- When and how did the attack occur?
- What the attacker was able to access?
- Why did they attack?

One of the most pressing issues to address following a data breach is discovering the specific point of entry the attacker had been using and how the attack is affecting operations. Another critical issue is to identify as fast as possible what information has been stolen, deleted, encrypted for ransom, or disclosed to unauthorized third parties. In other words, one of the first steps during the identification stage is to investigate what systems, networks and information assets the attackers have compromised.

Once the incident response team identifies the basic characteristics and the scope of the breach, corrective actions should be taken to contain the threat and eventually remove it. During the stage of containment, the IT security department can take actions such as:

- Block unauthorized access to resources.
- Blocking entry points such as email addresses, malicious websites or infected devices/systems.
- Close specific communication ports and mail servers.
- Change system administrator credentials, starting with systems that are natural targets for an attacker.
- Apply specific firewall filtering rules.
- Relocate website home pages and use backup hosting.
- Isolating systems and network segments as appropriate.

In the stage of containment, the IT team should take steps to update and patch all systems and endpoints while making sure they review all power-user access rights and login credentials.

Once the team manages to contain the malware, the eradication stage begins in which the security experts should find and eliminate the root cause of the breach. The process involves taking steps like:

- Identify all affected systems/devices within and outside the organization in order to remediate the threat in full.
- Perform detailed malware analysis.
- Monitoring for and analyzing any response actions from the attackers.
- Put a defense strategy in work in case the attackers develop their attack using other attack methods and malicious code.
- Make sure the network is secure and there is no follow-up attack once the initial threat is remediated.

During this process, the cybersecurity team should make every effort to keep records of all malware actions uncovered and maintain a chain of evidence for the incident.

Organizations should keep and maintain clear and precise evidence that includes the location, serial number, model number, hostname, media access control (MAC) addresses, and IP addresses of a device affected by the data breach and/or used to remediate the cyber-attack.

The recovery stage immediately follows the stage of eradication and may involve any of the steps listed below. In any case, the organization should make sure all the systems are operational and there is no immediate risk of an ensuing attack or activation of malicious code still residing within the perimeter. Some of the critical recovery steps include:

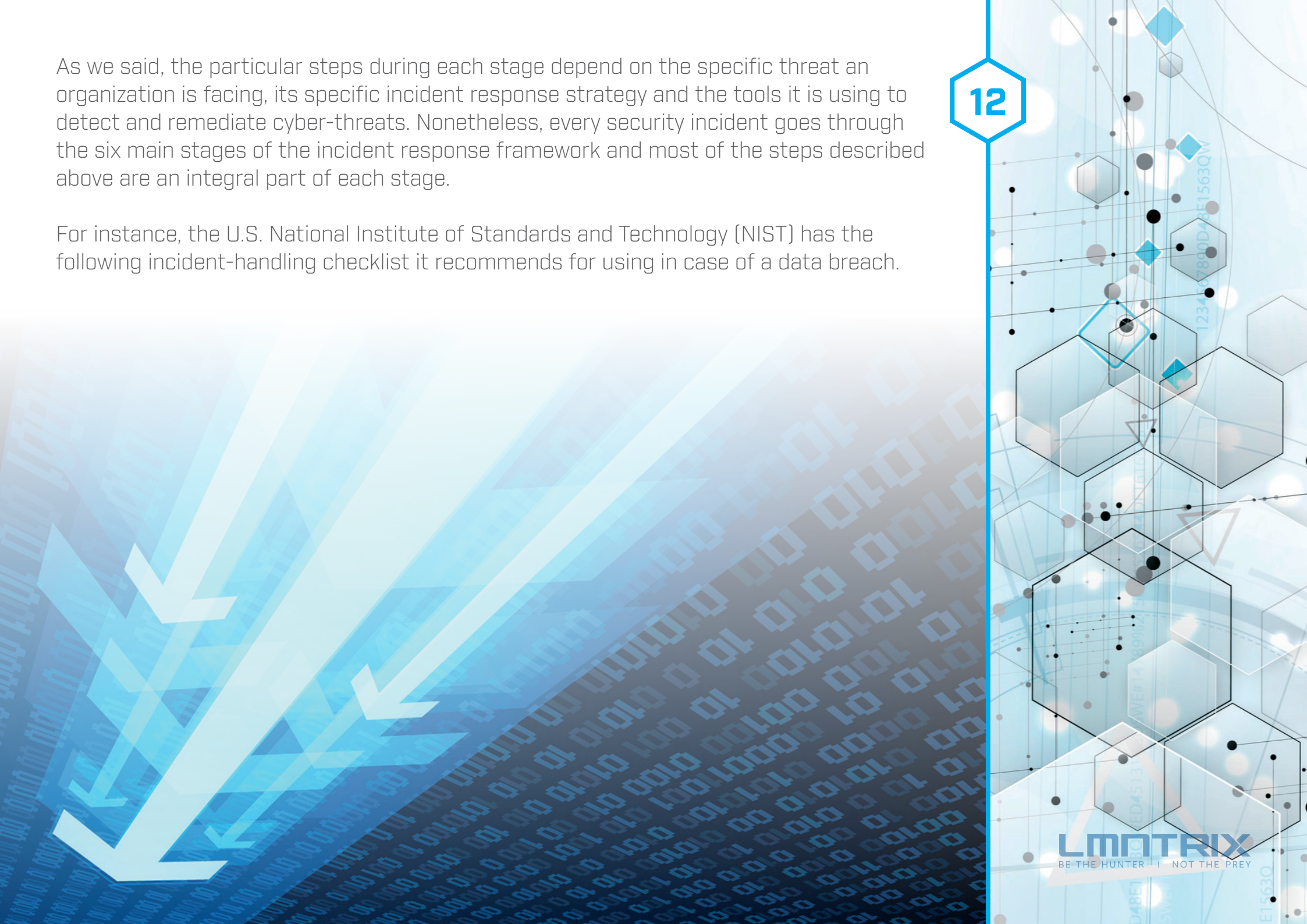
- Reinstating infected systems from backups and clean sources.
- Replacing compromised files with the latest backup versions.
- Carefully and gradually removing restrictions imposed during the containment period.
- Force-resetting passwords on compromised accounts and changing all administrator credentials.
- Installing software updates and patches and adapting firewall rule-sets.
- Running a complete security check on all systems and networks.

The organization may decide to run a penetration test and a compromise assessment to confirm the integrity of the systems and controls within the perimeter.
After all systems are back to normal operation and there is no immediate risk of a further attack, the stakeholders should perform a thorough follow-up analysis within a stage known as 'Lessons Learned'. During this phase, the organization should address a number of issues and take the respective steps. Those include:

- How did the employees and management respond to the breach and how did they follow the adopted security procedures?
- What changes need to be made to the cybersecurity policies and procedures?
- What are the weaknesses enabling the attacker to penetrate the perimeter and could that have been prevented?
- What additional training should be provided and in which areas?
- What will be the steps to prevent cybersecurity incidents from happening in the future and what are the main lessons learned during the data breach.

As we said, the particular steps during each stage depend on the specific threat an organization is facing, its specific incident response strategy and the tools it is using to detect and remediate cyber-threats. Nonetheless, every security incident goes through the six main stages of the incident response framework and most of the steps described above are an integral part of each stage.

For instance, the U.S. National Institute of Standards and Technology (NIST) has the following incident-handling checklist it recommends for using in case of a data breach.



Incident Handling Checklist

	Action	Completed
Detection and Analysis		
1	Determine whether an incident has occurred	
1.1	Analyze the precursors and indicators	
1.2	Look for correlating information	
1.3	Perform research (e.g., search engines, knowledge base)	
1.4	As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence.	
2.	Prioritize hndling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.)	
3.	Report the incident to the appropriate internal personnel and external organization	
Containment, Eradication and Recovery		
4.	Aquire, preserve, secure and document evidence	
5.	Contain the incident	
6.	Eradicate the incident	
6.1	Identify and mitigate all vulnerabilities that were exploited	
6.2	Remove malware, inappropriate materials and other components	
6.3	If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (5) and eradicate (6) the incident for them	
7.	Recover from the incident	
7.1	Return affected systems to an operationally ready state	
7.2	Confirm that the affected systems are functioning normally	
7.3	If necessary, implement additional monitoring to look for future related activity	
Post-Incident Activity		
8.	Create a follow-up report	
9.	Hold a lessons learned meeting (mandatory for major incidents, optional otherwise)	

In any case, organizations should categorize cybersecurity incidents in accordance with their severity if they are to handle data breaches properly and on time.

Prioritization is Critical for Incident Response Management

Since security incidents are now part of the routine of the IT security teams, especially in large and multinational organizations, the handling of a security incident should not be performed on a first-come, first-serve basis. Incident response should follow strict procedures for incident severity categorization based on clear criteria such as functional impact, information impact and recoverability.

Functional Impact Incident Priority

A hostile cyber-attack would typically target the business functionality of the organization's systems, aiming at disrupting the normal business operations, which in turn impacts both internal users and customers connecting to those systems.

The incident response team should immediately assess both the immediate impact of the incident and the ensuing functional impact in case the team is unable to contain the incident within a short time.

Information Impact Incident Priority

The information impact of a data breach is multifaceted and the incident may affect data aspects such as confidentiality of data, its integrity and availability. Exfiltration of sensitive information is the most common goal of a threat actor but attackers may also use ransomware or alter information stored in the databases.

The incident response team should make every effort to identify what information is affected and how the data breach affects third parties such as customers, partners or any other party involved.

Cybersecurity Incident Recoverability

An incident response strategy cannot plan for the amount of time and resources required to contain and recover from an incident and thus the severity of an incident, when recoverability is concerned, depends on the type of attack and how successful it happens to be.

Some incidents are non-recoverable since confidential information has been stolen and used in the data breaching process. In such cases, the IT security team should focus on forensic analysis, aiming at preventing future data breaches rather than trying to handle the incident in a manner that only exhausts the IT resources available.

Many incidents also require help from third-party experts to contain and recover from, as the organization does not possess the resources required to contain and eradicate a threat and then recover from the incident safely and completely.

Therefore, the incident response team should carefully evaluate the recoverability options and only then make a final decision on how to proceed with the incident handling.

Thus, prioritizing cybersecurity incidents is crucial for appropriately handling an incident and determining what resources should be set aside to deal with a specific sort of an incident.

Challenges to Incident Response Handling

Advanced persistent threats (APTs) which represent sophisticated and continuous cyber-attacks now target not only top-secret government agencies and national infrastructures but also corporations, including small and medium-sized enterprises and non-government organizations.

Malicious actors have access to similar tools and methods – including but not limited to hacking software, malicious source code and social engineering techniques. Therefore, the main difference between different cyberattacks and the resulting data breaches is whether it is a state-sponsored attack, a large organized crime syndicate or a small group of hackers.

The latter can cause a lot of damage but nation-state attackers and major hacking syndicates could stay undetected for months and even years, exfiltrating information and sabotaging an organization's operations during long periods.
There are probably a handful of organizations worldwide that are able to completely handle a major cybersecurity incident on their own and which are fully prepared to respond to all sorts of advanced cyber-threats. The problems surrounding the adequate response to a cyberattack include lack of talent, process gaps and lack of information about the latest cyber-threats and attack methods.
Furthermore, a few organizations can determine what type of attack they are facing before an external cybersecurity expert conducts a thorough investigation. The average organization cannot cope with the growing number of cyber-threats and their evolving techniques and methods to penetrate the perimeter.
Alarmingly, the overwhelming majority of organizations are unable to adopt even the most basic cybersecurity practices by leaving unpatched and not updating their business software even though those apps are well known for being a major attack vector exploited by bad actors.

Conclusion

No organization stands a chance to prevent the occurrence of a minor or major cybersecurity incident over time. The pressure is growing on Chief Information Officers and Chief Information Security Officers to both adopt preventive cybersecurity defenses and draft comprehensive incident response plans to handle a data breach.

While making it more difficult for an attacker to penetrate the perimeter is a common approach, IT security teams should also plan for actions to protect the organization's sensitive data in a compromised environment i.e. to have a feasible incident response strategy and plan.

A key component of such a strategy is to employ capabilities such as the LMNTRIX Active Defense to detect and identify a threat as early as possible and take immediate action to contain and eradicate the malicious attack. Using cybersecurity intelligence, data analytics, process analytics as well as monitoring an organization's apps and users for signs of abnormal behavior provides the pillars of a reliable IT security strategy.

Maturing from an organization that employs an established cybersecurity incident response model to an organization that has adopted a dynamic model, which in turn can respond to the evolving challenges and risks associated with cyber-threats, is a necessary strategic step for any security-conscious organization. Building a culture of cybersecurity awareness in the process is another stepping-stone for implementing a working incident response strategy.

TAKE THE NEXT STEP: CREATE OR FORTIFY YOUR PLAN

LMNTRIX Active Defense provides pre- and post-incident response services to proactively defend against and respond to cyber incidents. Both after and before a breach, our cyber defense centre intelligence experts, incident responders, threat hunters and malware researchers will help you respond to a breach, and prevent the next one. LMNTRIX has worked on some of the most challenging intrusions and malware attacks in recent years.

Call +1 888 958 4555 or visit lmntrix.com to learn more.