AVERTIUM®

eBook

CREATE AN EFFECTIVE INCIDENT RESPONSE PLAN

Everything you need to know

TABLE OF CONTENTS

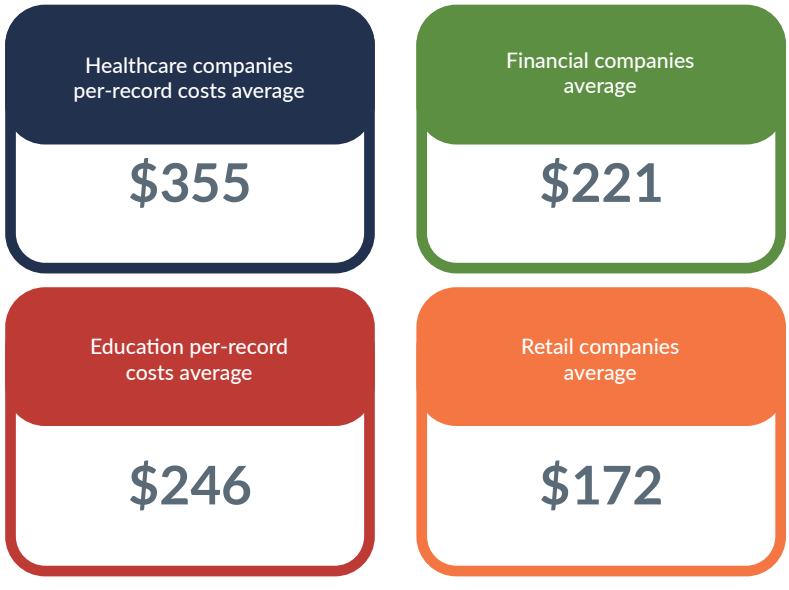
Creating an Incident Response Plan Introduction

If your network hasn't been threatened yet, it will be. If your network has been breached, you know the chaos that can ensue. Whether the event is virtual in the form of a security breach, or physical in the event of power outage or natural disaster, losing functionality or data can have a crippling effect on your organization. A rigorously developed incident response (IR) plan will prepare you to quickly mobilize around minimizing the impacts.

There are countless examples of well-known companies whose data was stolen, compromised or otherwise exposed. The last decade has seen high profile security events that resulted in fines, loss of reputation and settlements that cost hundreds of millions of dollars. These included Equifax ($575 million), British Airways ($230 million), Uber ($148 million), Marriott ($124 million), and Target ($252 million), just to name a few.

The Cost of a Data Breach

According to the Ponemon Institute, the average cost of a data breach of companies worldwide is $3.92 million with an average data breach of over 25,000 records per incident. If your company is based in the U.S., that average number rises to $8.92 million. The cost of breach also has an important time element meaning that a breach could cost you much more depending on how long it takes to detect it and respond. The same study found that it takes companies roughly 197 days to identify a breach and 69 days to contain it. Companies that contain a breach within 30 days can save more than $1 million dollars in comparison with those who take longer.



Source: IBM 2019

Companies also face the additional risk of lawsuits from consumers and other regulatory entities. Just to notify customers of a breach costs almost $800,000 on average.

It Pays to be Prepared

Crisp, timely and well-coordinated response is critical, and only achievable through an incident response plan relevant to the unique nuances of your business, and that has been tested and refined. In incident response, practice makes perfect, and since (hopefully) an incident is a very rare occurrence, it is easy to fall out of practice.

The cost of a data breach varies across industries with a significant year-to-year increase. Here are a few examples from IBM's annual data breach report (2019):

- Healthcare companies per-record costs average $355.
- Education per-record costs average $246
- Financial companies average $221
- Retail companies average $172

Additionally, organizations can face a number of fines when data is stolen or otherwise exposed. For example, according to the Payment Card Industry Security Standards Council, their penalties alone can include merchant processor fines (up to $50,000), card brand compromise fees (up to $500,000), forensic investigations ($100,000 or more), quality security assessment fines ($100,000 or more) as well as additional fees such as credit monitoring, card re-issuance, security updates, lawyers' fees, repairs and more. If you're following PCI DSS requirements, you should already have an IR plan while also having employees trained to quickly deal with a data breach. If you don't, you are non-compliant and at risk of facing the types of fines described above.

These fees alone are enough to bury an organization. Your data is one of your most valuable assets. How you prepare for, detect and respond to an incident could be the difference between the life and death for your organization.

A well-executed IR plan minimizes the impact of a breach, reduces fines, protects an organization's reputation, and helps resume operations more quickly. If there is no plan, your team is forced to scramble, which leads to costly mistakes. You may be able to "stop the bleeding" for the short-term, but in the rush to deal haphazardly with the breach, you may inadvertently remove important evidence that could have provided valuable insight to protect you from future incidents.

An IR plan is designed to be a proactive and well-documented blueprint to help your organization prepare for, recognize and deal with a cybersecurity incident like a data breach or cyberattack. Having a plan is critical, not only for the protection of your network and data, but possibly for the future of your organization.

Here we take a deep dive into what constitutes a rigorous, relevant and responsive IR plan and review the critical components to ensuring your data is kept safe.

What is an Incident Response Plan?

An IR plan is a set of instructions for your staff to follow in the event of a security breach. IR plans address data loss, theft, cybercrime, and outages that threaten your organization's operations.

An effective IR plan is a balancing act, incorporating many sometimes-competing needs. Building one must incorporate elements of business continuity and disaster recovery while focusing efforts on a specific type of risk. The plan needs to support not only rapid recovery, but also responsible evidence retention. It needs to be detailed enough to provide structure, but flexible enough to give the response team the ability to handle many types of cyber incidents.

A security incident can lead to significant breaches of your network and data that could impact your organization for hours, days, or even months. Your organization needs a thorough and detailed plan to help staff to detect, contain, and eradicate the threat quickly.

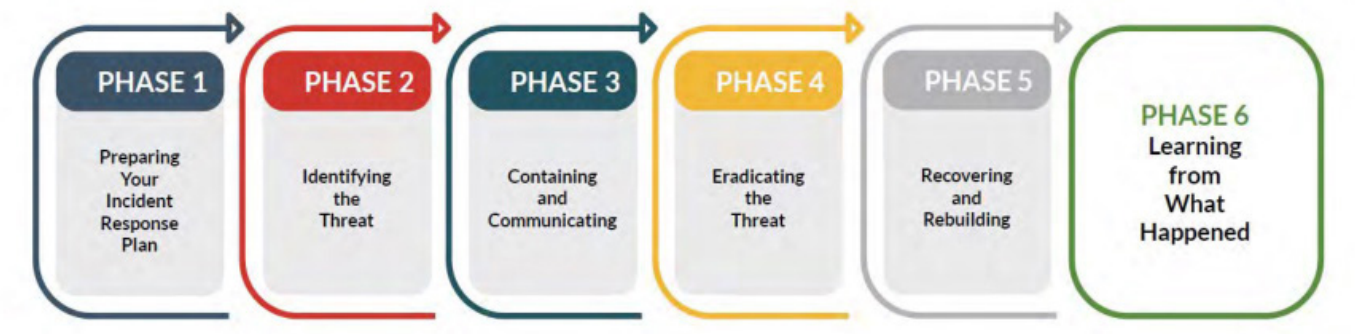
Communication is key when mobilizing an incident response plan. Therefore, identification of roles and responsibilities, as well as communications planning between the members of the incident response team, is paramount to documenting and training.

A relevant plan strengthens your organization by putting it in a position to apply rigor to preventing, detecting, responding to, and recovering from network breaches.

Six Phases of an Incident Response Plan

An IR plan should be set up before an attack so your organization can respond immediately once a breach occurs. We've identified several phases to help you create your IR plan, along with specific areas you should consider.

Six Phases in Developing an Incident Response Plan



PHASE 1: Preparing your Incident Response Plan

When it comes to an IR plan, preparation is half the battle. This phase often takes the most time and effort in your incident response planning, but this is the most crucial step in the initiative to protect your organization.

Your preparation should consider your organization's current and future states by identifying the stakeholders, "crown jewels" of data, existing weaknesses, likely threats and recovery techniques. This ensures the plan is relevant to your organization and enables rapid response – critical elements to your ability to respond.

When determining your IR plan, it's important to consider that an incident could potentially impact all aspects of your business. A comprehensive IR plan should take into account that security involves more than just your IT department. There are compliance matters to consider, third-party vendors, and regulatory entities that may be involved. Thorough preparation will provide the time needed to consider all the potential parties that need to be involved or protected in the event your data is compromised.

Preparing your incident response plan includes the following steps:

Step 1. Perform a risk assessment and prioritize security issues

All data is not created equally. Some assets are more sensitive than others. Some may be critical for business continuity. It is these critical elements that need to be considered first when determining how to protect and respond to threats. Start by locating and documenting where your organization keeps its crucial data assets. You need to assess what would cause your organization to suffer heavy losses if this information were stolen or damaged.

After discerning critical assets, prioritize them according to importance and highest risk, quantifying your asset values. This will help justify your security budget and show executives what needs to be protected and why it's essential to do so. You'll also want to recognize what controls you already have in place, their effectiveness and whether there are any potential areas of weakness.

Once you've prioritized your data and determined areas of vulnerability, your next step is to build a risk assessment matrix to identify the probability and impact of such incidents and, both in terms of financial impact as well as reputation.

Step 2. Determine Stakeholders

Time is of the essence when it comes to responding to an incident. Responding quickly could mean the difference between containment and suffering an all-out disaster. That's why it's important to identify stakeholders and their role ahead of time.

Building a rigorous and relevant IR plan takes into account all aspects of the business. Just as you practice a fire drill, an effective IR plan helps everyone know where to go and what to do when an incident occurs.

The first thing you want to do as you determine stakeholders is to designate your Computer Security Incident Response Team (CSIRT) and then define what their roles and responsibilities will be. For example, senior leadership may each have certain duties to carry out in the event of an incident - from approving financial decisions to communicating with partners and customers.

Including departments company-wide is also important for creating a strong IR plan. Devising a plan in a vacuum will almost certainly prove to be inadequate in the event of a breach. Other stakeholders to consider include finance, communications, legal, operations and human resources. You should determine the role that each department plays and design those aspects of the plan accordingly.

Third parties must also be considered. This may include your Internet Service Provider as well as any MSPs that host your data center resources. It's important to have a plan to communicate with all service providers including your cloud providers and critical SaaS applications that could be affected.

These providers should have their own incident response plans in place that your organization needs to consider as part of your plan. Collect them from your critical vendors, and have discussions with them about incident notification, communication in an incident, and delineation of responsibility.

Outside counsel is also a component of your incident response team. A best practice in incident response is to include your attorneys on all communications amongst the incident response team to provide the protection of client-attorney privilege in the event litigation may be involved. Privilege is a tool available to you through counsel, so plan to use it.

Also, you need to engage your insurance provider and ensure your coverages include cyber breach insurance. Most do not unless you've specifically selected this coverage. Failing to do so until the day of the incident will leave you uncovered and liable for potentially huge costs.

Determining stakeholders and how to engage with third parties before an incident occurs will save you valuable time and resources later.

Step 3. Identify and procure incident response tools

As you prepare your IR plan, it's essential to take advantage of all the tools at your disposal and automate as much as possible. This will save you critical time later so that you're prepared when an incident does occur. Your response tools should include software and hardware to detect the initial threat as well as actions to be taken by certain stakeholders, such as the need for quarantine or the reimaging of devices.

A note of caution when it comes to incident response tools: **Off-the-shelf security tools rarely consider the unique assets and needs of your business.** Free downloadable fill-in-the-blank plans won't allow for the nuances of your organization. A comprehensive response plan helps identify your company's unique needs ahead of time, saving you critical time later.

Step 4. Build a communication plan

Building a viable communication plan considers all internal and external parties that touch your business. Here are a few to consider:

- **Internal parties:** Regular communication with internal parties, in general, helps keep data security top-of-mind at all levels of the organization. Communicating regularly with your team on best practices for responding to phishing attacks and other security incidents is important. This should include social engineering and strong password creation, for example. Regarding incident response, you'll also want to have a plan for communication when a security incident does happen and communicate any necessary actions to be taken.

- **CSIRT:** A rigorous IR plan presents your CSIRT team with different scenarios so that you can respond quickly and adequately. It's critical to first communicate with your CSIRT team to identify whether your most valuable assets have been breached.

- **Business stakeholders:** A data breach could potentially affect all levels of your organization so it's important that all stakeholders play a role in preventing and responding to a breach. Your plan should make each stakeholder aware of their role and communicate how they will be held accountable for their response.

- **External parties:** A breach affects more than just internal stakeholders. There are likely several outside parties to consider, especially if a breach involves customer data. You should have a plan for communicating transparently with customers that clearly states the degree to which they've been affected, if at all. Law enforcement is another third party to consider – developing a relationship with your local FBI field office via the FBI Infragard program is a good step towards preparedness.

- **Third party service providers:** Each organization has external parties that are unique to their business. It's important to have a communication plan for all of them. This also involves your cloud service providers, SaaS providers of critical business applications and any document repositories. Know who to communicate with, and how to engage them in the event you need their help. Similarly, understand how they will communicate with you in the event they have an incident that impacts you.

- **Outside counsel:** Partnering with outside counsel in advance helps you save valuable time and money when a breach occurs. It's important to protect yourself and establish a plan well ahead of time to avoid costly legal expenses during an attack. Outside counsel will help you to determine the best course of action to protect your assets and respond adequately in the event of an incident. This allows you to consider the potential legal ramifications of a breach. You may wish to prosecute against a malicious actor. Or perhaps your organization will face lawsuits as a result of an incident. Preparing for the legal consequences allows you to contain the fallout from an incident.

- **Insurance providers:** The cost of a breach could possibly deal a critical blow to your organization's bottom line. Determine what role insurance will play in order to protect your business and familiarize yourself ahead of time when and how to report a breach to your provider. Most coverages do not include cyber breach insurance unless it is specifically selected. Inspect your existing coverage and purchase appropriate coverage for cyber risks in advance of the incident.

- **Media:** Negative media coverage could severely damage your company's reputation. On the other hand, a transparent and solution-based response could help establish trust and build your brand reputation. Establishing a media crisis communication plan that highlights your company's security efforts can go a long way in preventing a sustained publicity disaster. It's important to proactively engage with the media in order to retain control of your external message. You should highlight the steps you've taken to prepare for an event and note what you're doing to contain the attack and prevent future incidents.

Step 5. Train through practice

Thinking through the various scenarios your company may face can be an invaluable exercise. Once you have established various realistic situations, table-top exercises and penetration testing to play out different possibilities will help you to establish a plan for action. Role playing is a best practice and many "eye-opening" experiences have happened as a result of practicing various scenarios. This can be done by a variety of means:

- **Red team/blue team exercises:** This is an exercise where "red teams" test the effectiveness of a security plan. These teams emulate the behaviors and techniques of likely attackers, designed to be as realistic as possible. The "blue team" is the internal security team that is charged with stopping these simulated attacks. The aim of these exercises is to test an organization's security maturity as well as its ability to detect and respond to an attack.

- **Tabletop sessions:** In a tabletop exercise, your team meets to discuss their roles during an emergency and their response to a security breach. A facilitator guides the group through different scenarios, allowing you to think practically through the role and response of your security response team.

- **End user training sessions on detecting and reporting suspicious activity:** Data security is a team effort. Your end users are your first line of defense against malicious attacks. Communicate regularly with your team so that even the most non-technical among us can identify when something looks… phishy.

Planning involves identifying your most important assets, stakeholders, and tools as well as having a robust communication plan that is well-rehearsed. Everyone should know their role. Good planning will help you contain or prevent an attack and save you invaluable time and help to mitigate the damage.

A Stronger IR Plan Requires a Show-no-weakness Approach

Prevention is your best line of defense when it comes to a security incident. More rigorous processes, automation and authentic human intelligence are keys to a show-noweakness approach.

While prevention won't make you totally immune to an attack, it's important to account for your business's specific needs and have the tools in place to protect your most valuable assets.

IBM found that companies that fully deploy security automation have an average breach cost of $2.88 million whereas companies without automation have an estimated cost of $4.43 million. Automating security tasks saves time and money in several ways. It quickly completes timeconsuming tasks that keep security and IT personnel from other higher-level assignments. Automation also eliminates the chance of human error and increases your chances of detecting a security threat.

As you implement controls to prevent attacks, you'll want to do things like:

- **Inventory your hardware and software assets.** Your first-line defenses against an attack include the hardware and software you already have. It's important to know what protectionary controls they have built-in, if you're using these capabilities and if you're certain they are enough to protect you. Perhaps it might be worth bringing in an outside consultant who has worked with other companies like yours to identify potential blind spots.

- **Map your network and keep the map current.** Changes in your network introduces the possibility of vulnerabilities. Keeping an updated network map helps you to identify potential areas of weakness and allow you to pinpoint controls you need to have in place.

- **Identify connections to third parties.** End users may be connected to third-party applications and tools that allow access to your network. Many attacks occur "through the front door." That means that hackers are looking for vulnerabilities in places where your end users have access through firewalls in places like your web browsers or email.

- **Scan for and remediate vulnerabilities.** There are "bad actors" out there who can penetrate your safeguards faster than you can find areas of vulnerabilities. It's critical to have the tools in place to scan these areas and find areas of weakness.

- **Continuously monitor the security of your environment.** Drawing together event log and network telemetry and correlating that data together against quality threat intelligence can alert you to a potential incident before it becomes a big problem.

When it comes to protecting your data, the most relevant data sources to monitor are:

- **Data from firewalls:** Your firewall monitors traffic into and out of your environment, providing visibility into the type and source of traffic. These devices are designed to stop connections from suspicious networks by inspecting source addresses, destinations and the destination ports of connections, and decide if these networks are trustworthy. This protects your systems from internal and external sources and acts as a resource to your security team who use the firewall as a means of tracking how a breach penetrated your network. Firewall logs offer insight into source and destination IP addresses, protocols, and port numbers. Firewall logging is useful for determining if your firewall rules are working well and for helping to ascertain how to debug them if they do not work well. Firewall logs are also useful for:
    - Discovering any malicious activity within your network and offering information on how to isolate the source of malicious activity
    - Identifying repeated attempts to access your firewall from single or multiple IP addresses, allowing you to create rules to stop connections from those addresses.
    - Identifying connections from internal servers that may be using your system as a launchpad for attacks against computers on other networks from your system.

- **Endpoints:** Data from your endpoints, including anti-virus, anti-malware, event logs, and Endpoint Detection and Response (EDR) tools are vital sources of information. This data can give your security team a granular view of risks and hone your containment and response efforts.

- **Email:** Review your email and email gateway logs to identify phishing attacks, malicious attachments and other links that hackers use to steal your information. If a breach has occurred, look at where the attack initiated, which IP addresses were initially affected, the resulting scope of the incident and any other devices impacted. Addressing the infection point is critical for a timely response.

- **Web browsers:** Review what users are interacting with on the internet. You should also note any malicious domains and block them while also monitoring incoming and outgoing traffic logs to detect any new threats.

- **Data that is publicly accessible:** Protect web applications that process or store data as well as review logs from these web apps and from servers that host them.

- **Dynamic Host Configuration Protocol (DHCP):** Review your DHCP and associated IP addresses to determine the scope of an incident and which devices were affected.

- **Database Logs:** Conduct a thorough review of your environment and unique data sets to be aware of the security features you already have in place as well as recognize areas where your controls are lacking and need more protection. It's important to prioritize the critical, must-have data sets and your controls over those.

You can then pinpoint threats and procedures hackers use to identify incidents much faster. This allows you to correlate all the data together and greatly enhance your detection capabilities.

PHASE 2: Identifying the threat

In the event you experience an incident, you must identify the threat in order to address it. The first step here is detection, the process of determining whether you've been breached by looking for deviations from normal activities and operations. An organization typically learns of a breach in one of four ways:

1. The breach is discovered internally via intrusion detection logs, alerting systems, system anomalies or anti-virus scan alerts
2. The victim's bank informs the business of a possible breach based on reports of credit card fraud
3. Law enforcement discovers the breach while investigating a crime
4. A customer complains that the organization was the last place they used their card before they noticed fraudulent charges

Despite your best efforts, data breaches will still occur. That's why detection is so important. Having tools and personnel in place to identify breaches will help you respond quickly. Here are ways you can detect potential attacks:

>> Implement processes and technology to detect security incidents

Cyberattacks are more varied than ever before. Knowing the key symptoms of a breach helps keep your systems and data safe. Here are some of the most common types of security incidents:

- **Unusual behavior from user accounts:** Anomalies in the behavior of a user can indicate that someone is using it to gain entry into a company's network.

- **Traffic anomalies:** Organizations should monitor incoming and outgoing traffic. Users could be uploading content to personal cloud databases, downloading large files to external devices or sending large numbers of attachments to destinations outside the company.

- **Threat Intelligence:** A device inside your network communicating with an Internet-based IP with a reputation for spamming, hosting malware, etc., is an indicator that you need to act swiftly. Threat Intelligence tracks these reputations and should be incorporated into your detection strategy.

- **Excessive consumption and suspicious files:** An increase in the performance of hard drives of server memory may mean an attacker is accessing or sending data illicitly. This may also be the case if you find a suspicious file that is trying to remain hidden. Suspicious file names, sizes, and locations may indicate data or logs that have been leaked.

- **Configuration changes:** You may recognize changes that have not been approved. This could include firewall changes, malicious startup programs, reconfiguration of services or the addition of scheduled tasks.

- **Abnormal browsing behavior:** Unexpected redirects or repeated popups could indicate malicious activity. Look for changes in browser configuration or the addition of third-party add-ons or extensions that could be used to access information.

- **Suspicious registry entries:** This occurs mostly when malware has infected an operating system and is one of the main ways it remains in the infected system.

There are processes and technology you can put in place to detect the most common symptoms of a breach. Here are a couple of examples to consider:

- **Security Information and Event Management (SIEM):** There are a number of software applications that offer a window into the health of your security. These typically track applications, business processes, and network intrusion detection systems (IDS). However, these usually only see IP addresses, packets, and protocols. Individually these options cannot indicate what is happening in real time within your network. SIEM, on the other hand, includes both products and software that helps companies manage security events and information. SIEM goes beyond log management and comprises many security technologies, making each individual security component more effective by aggregating the data and creating a singular way to view and analyze all your network activity.

  The most effective SIEM products can aggregate, analyze and report log output from networks, operating systems, databases and applications. An effective SIEM also offers applications that manage access and verify identify, provide vulnerability management and provide forensics data as well as threat notifications.

- **Engage a 24/7/365 Security Operations Centers (SOC) as a Service Provider:** Many organizations don't have the requisite tools, training or staff to withstand the ever-present threat posed by security vulnerabilities. This is where managed security services can assess your environment and provide protection that would otherwise take months or years to put in place. Spending large amounts of time and resources to put these processes and practices in place could make you vulnerable in the meantime and may expose you to blind spots that a security professional could otherwise solve outright.

>> Train your users to report suspicious or anomalous activities

Having an IR plan isn't enough when it comes to cybersecurity. Individuals at all levels of your organization should be trained to spot malicious activity. The most vulnerabilities are through phishing attacks, malicious websites, or email attachments that contain malware. Employees need to understand their role in maintaining company security. You can test your employees through simulated exercises and real-world scenarios presented by a facilitator. Although these exercises cost time and money, they play a vital role in making sure your staff is prepared for a breach. This helps your employees with their particular roles by testing through various scenarios.

By testing employees, you can identify and address weaknesses in the plan and recognize areas for improvement, with no actual risk to your organization.

PHASE 3: Containing and communicating

Once you've detected an attack, containment and communication to the proper channels is critical. The various internal and external stakeholders you've identified ahead of time should each know what their role is and be prepared to take action.

[ ] Activate the incident response plan

Having an IR plan will help you know what to do next. There are certain best practices you need to be aware of and recognize the role that various departments in your organization will play. Working with a dedicated security organization can reveal areas you haven't thought of and provide invaluable insights from organizations of similar size within your industry.

[ ] Alert the CSIRT and stakeholders to the confirmed incident

You've identified the CSIRT team and all third parties that need to be contacted. Be certain you've captured answers to the following questions:

[ ] Communicate with third parties

You should have already identified all third parties your organization uses so that you have a plan for communicating with them when the time comes.

- **Service Providers:** If you experience a breach ask yourself if it is necessary to contact your internet service provider to determine the source of attack or to contain it. Determine what role will your managed service providers play, especially your security provider, in containing the threat.

- **External IR Team:** These could be any outside party needed to identify or contain the attack, including law enforcement professionals or data security experts.

- **Outside Counsel:** Ideally you have already engaged with your outside counsel and they know how to advise you on next steps. You don't want to wait until an incident occurs before you've contacted them. This could end up costing you more time and money. Your priority at this point is how to contain the incident and work the plan you already have in place.

- **Customers:** Your customers can either be your biggest fans or your greatest adversaries depending on if you communicate well or if you botch the communication. That's why it's best to be transparent about the nature of the attack, who was affected and possible ramifications. You should also inform them of any action they should take, such as changing passwords. This is also a good time to highlight your many efforts to protect them.

- **Media:** Your public image could take a hit from a publicized breach. Knowing how you will manage a potential public relations crisis could help you prevent one.

[ ] Apply containment strategies

As you're communicating with all the necessary parties, you'll want to simultaneously take steps to contain the attack. Some actions need to be taken immediately in order to identify the threat vector and isolate the attack. You may need to take immediate action to quarantine one or multiple devices and perform network segmentation or take devices offline to reduce the potential infection of other devices.

A divide-and-conquer approach can be very effective. This means that different individuals and departments are assigned a variety of tasks to execute simultaneously in order to avoid overloading one person or department with all the work. This approach also ensures the work is completed in a timely manner.

Containing the incident also entails implementing a fix while you rebuild. Oftentimes, it's much more beneficial and reliable to reimage devices as opposed to removing malware or resetting registry keys. Working with a dedicated security professional can assess your unique environment and point out time-saving methods to help you stop an incident in its tracks.

PHASE 4: Eradicating the threat

After a cyberattack has been contained you must eradicate all traces of the security incident (e.g. removing the attack from the network, deleting malware and disabling breached user accounts), as well as identify and mitigate vulnerabilities that were exploited.

Identify the root cause of the incident. Eradicating the threat involves removing all traces of infection or threat vector from the network. It is critical to have very clear data to identify the scope of the attack and put safeguards in place to contain it. That's why it is essential to know your network and identify those vulnerable areas in advance.

The process of eradicating the threat may include:

- Identifying all affected hosts within (and sometimes beyond) your organization, so that they can be fixed.
- Locating the source of the attack in order to remove all instances of the software.
- Carrying out malware analysis to assess the damage and discover catalogue indicators of compromise that will reveal other machines that have been affected by the same malware or intruders.
- Checking to see if the attacker has responded in any way to your actions.
- Anticipating a different form of attack and developing a response.
- Allowing sufficient time to ensure that the network is secure and that there is no response from the attacker.

Eradication must be carried out swiftly to prevent attackers from launching a new initiative. Attackers will often come back when they know that they are being investigated and have been discovered. Therefore, it is important to ensure that all elements of the attack have been eradicated and that the attackers cannot carry out further attacks.

Close gaps and correct weaknesses which enabled the incident. Keep a detailed written log of every action taken during the investigation to assist in responding to future attacks and developing a plan of action to stop events from happening again.

Remove all traces. You will also need to find and eliminate or alter policies, procedures, or technology that led to the breach. Whether you or a third party do this, you need to be thorough. If any trace of malware or security issues remain in your systems, you may still be losing sensitive data, with your liability increasing.

No network is exactly alike. There may be areas of vulnerability you're not aware of. Having a team of dedicated security specialists who are able to assess your environment and provide further insight to protect your organization helps expose potential blind spots.

PHASE 5: Recovering and rebuilding

The goal of recovering efforts is to restore normal operations. It's a good idea to define specific recovery goals for your systems, processes, and business. Your goals should be to minimize disruption to normal operations. Many security incidents are limited in scope and you will be resolving them in parallel with regular business operations. Recovery efforts should have minimum impact on work elsewhere within your organization. Recovery is often performed in stages, so you should clearly define the order of recovery for systems and processes. Consider both the technical requirements as well as the business aspects. Technical requirements will help identify what systems are necessary to bring other areas back to operation while some business aspects will be more urgent than others.

Recovering from a data breach entails restoring and returning affected systems and devices to your business environment. It's important to apply lessons learned to construct more rigorous controls to get your systems and business operations running again in a way that reduces the threat of another breach.

Your team can restore compromised assets in a number of ways. In some cases it's possible to simply wipe and replace the storage drives of affected devices and download any data lost from a backup. In other cases, activating entire cloud-based replicas of your network environment may be possible to quickly restore your organization's network to normal while you work to investigate the breach.

How you restore the assets on your network depends largely on the business continuity and disaster recovery plans you have in place. These plans are an important part of your incident response in order to have fail-safes so that if one of your assets is down, you have a means of keeping your business going. Be sure to catalog which assets have been taken down and determine what is supposed to be on your network. That way, you can be sure you haven't missed anything.

- **Restore systems to normal operations.** Once the cause of the breach has been identified and eradicated, ensure all systems have been hardened, patched, replaced, and tested before you consider re-introducing the previously compromised systems back into your production environment. Determine a time frame for when systems can be returned to production and how long you should monitor affected systems as well as what to monitor them for. Based on the type of breach, assess tools, such as file integrity monitoring and intrusion detection and protection, to help you ensure similar attacks will not reoccur.

- **Verify normal operations through communication with stakeholders.** Once you've implemented all steps to restore normal operations and prevent a future incident, you should communicate with stakeholders. This will help you verify that all systems are stable and functional. Monitor closely for validation of normal operations and be prepared to act quickly in the event of a problem.

PHASE 6: Learning from what happened

While you might be tempted to move on after the chaos of a security incident, it's important not to skip the step of learning from the incident. An investigation into the attack can provide valuable lessons.

- **Lessons learned session with CSIRT within 2 weeks of incident.** It's advisable to hold an after-action meeting with all CSIRT members to discuss what you've learned from the data breach. This is where you will analyze and document everything about the breach. Lessons learned from both mock and real events will help strengthen you for future events.

- **Complete an incident report.** It is essential to study the attack method and find out how the attackers got in and identify gaps in your cybersecurity and how to close them.

- **Performing a root cause analysis could expose further areas of vulnerability.** Note successes as well as failures. Making improvements enhances your response time for future incidents and minimizes the downtime and disruption that an attack can cause.

- **Identify where the CSIRT was effective and where improvement is needed.** Identify departments or individuals you may have overlooked in your initial IR plan. Perhaps further input would have been helpful to contain the incident more quickly.

- **Identify where the IR plan worked and didn't work and revise as needed.** Make a comprehensive list of areas where your IR plan worked and areas where it failed or could be improved. Then note where these areas fit into the overall plan.

Managed Security Services Providers

Shrinking IT budgets and ever-increasing security threats put many organizations in a bind. A cost effective solution to accurately and consistently monitor logs is the use of a managed security service provider (MSSP). An MSSP can help you to make your incident response more rigorous by doing the following:

Getting the Help You Need

Many businesses lack the resources to dedicate to developing, testing and organizing an effective incident response plan. Partnering with an outside consulting firm that has experience with different types of breaches across many industries can provide peace of mind in knowing you have a plan to deal with unexpected security incidents.

Working with experienced professionals can take the burden of preparation off you, and make a complex undertaking simple.

What to Look for in a Partner

Security consultant firms can provide much-needed expertise and relief, becoming a trusted extension of internal operations. It's important to choose a reputable firm with an extensive history of helping companies to achieve and maintain a comprehensive IR plan. Rigorous IR plan development services should include the following:

- Incident response plan development
- Incident response policy development
- Incident response breach notification proceducres (if applicable based on industry requirements
- Semi-annual facilitated incident response scenario-based tabletop exercises designed specifically for your environment
- Executive summary of table top exercises with maturity-based scoring
- Incident response training
- Risk profile assessment and report
- Incident response retainer for related services including forensics, eDiscovery, root cause analysis, and other related services

Creating Your IR Plan

An effective plan ensures that every person knows their role during a breach, which enables detection, response and containment in a timely manner. This provides peace of mind in a crisis since each step is carefully laid out and tested. By using an IR plan as a strategy for action to combat breaches when they occur, an organization diminishes their impact.

If you don't already have an incident response plan in place, creating one, practicing it regularly and reviewing it should be a top priority. With regular tabletop exercises and simulation training, your staff can make better decisions and contain the consequences of future events. A data breach can be one of the most stressful situations in an organization, but it doesn't have to spell doom. By following your IR plan, you can preserve your brand image, learn valuable lessons, and continue to grow.

ABOUT AVERTIUM

Avertium is the security partner that companies turn to for end-to-end cybersecurity solutions that attack the chaos of the cybersecurity landscape with context. By fusing together human expertise and a business-first mindset with the right combination of technology and threat intelligence, Avertium delivers a more comprehensive, more programmatic approach to cybersecurity - one that drives action on the ground and influence in the boardroom.

That's why **over 1,200** mid-market and enterprise-level organizations **across 15 industries** turn to Avertium when they want to be more efficient, more effective, and more resilient when waging today's cyber war. **Show no weakness.®**

CONNECT WITH US

AVERTIUM®

Cyber Fusion Centers of Excellence
Arizona • Colorado • Tennessee

Contact Us | www.Avertium.com

SHOW NO WEAKNESS®