Cyber℠

PREPARE | PREVENT | MITIGATE | RESTORE

TRAVELERS INSTITUTE®

TRAVELERS

Empowering organizations to tackle evolving cyber threats.

A CYBERSECURITY GUIDE

FOR SMALL AND MIDSIZED BUSINESSES

TABLE OF CONTENTS

INTRODUCTION **1**

PREPARE – PREVENT – MITIGATE – RESTORE **2**

Know your data, systems and network 2

Focus your cybersecurity efforts 4

Validate your backup strategy 6

Plan for incident response 7

PREPARE – PREVENT – MITIGATE – RESTORE **10**

Strengthen access controls 10

Patch known vulnerabilities 12

Educate your employees 13

Adopt security-conscious policies and procedures 14

PREPARE – PREVENT – MITIGATE – RESTORE **15**

Detect incidents early 16

Execute your response plan 16

Get help when needed 19

Document your response effort 19

PREPARE – PREVENT – MITIGATE – RESTORE **20**

Remediate, restore and replace 20

Continue monitoring 21

Communicate effectively 21

Implement lessons learned 23

LEARN MORE **24**

ABOUT THE TRAVELERS INSTITUTE **24**

NOTES **25**

EVOLVING CYBER THREATS IMPACT BUSINESSES AND ORGANIZATIONS OF ALL SIZES, SECTORS AND INDUSTRIES.

INTRODUCTION

News headlines routinely feature high-profile data breaches and computer intrusions, with large corporations working around the clock to contain the damage to their business, their customers and their reputations. But research shows that cyber criminals are also attacking smaller "Main Street" businesses and organizations that are often less prepared to prevent and respond to an attack. In fact, evolving cyber threats impact businesses and organizations of all sizes, sectors and industries. There has been a steady increase during the past five years in attacks targeting businesses with fewer than 250 employees; now, over 60 percent of all targeted attacks strike small to midsized entities.[1]

Experts believe it is not a question of "if" your organization will suffer a breach, but "when." Just one resourceful hacker, one disgruntled employee or even lost physical records of customer data or your own organization's proprietary information can cause enormous financial and reputational damage. The costs of a data breach can be staggering, averaging $221 per compromised record and $7.01 million per data breach in the United States in 2016.[2] Even relatively small breaches can incur significant costs.[3] Combined with a damaged reputation, these losses can devastate an unprepared organization.

With this in mind, the Travelers Institute, the public policy division of The Travelers Companies, Inc., launched *Cyber: Prepare, Prevent, Mitigate, Restore*℠, an educational initiative convening the business community with cyber thought leaders from the public and private sectors. Working with cybersecurity experts, government agencies and insurance industry professionals, *Cyber: Prepare, Prevent, Mitigate, Restore* provides business owners with the information and resources needed to meet the challenge of cybersecurity.

In this guide, we offer fundamental safeguards that can be used by small and midsized organizations to improve their cybersecurity. These safeguards, identified by Travelers cyber risk professionals in the course of helping policyholders manage their cybersecurity risks, can help any organization be more prepared, and better able to prevent intrusions, mitigate damage and restore normal operations when the hackers come to call.

IN THIS GUIDE, WE OFFER FUNDAMENTAL SAFEGUARDS THAT CAN BE USED BY SMALL AND MIDSIZED ORGANIZATIONS TO IMPROVE THEIR CYBERSECURITY.

"By failing to prepare, you are preparing to fail."

– Benjamin Franklin

BE PREPARED:

- KNOW YOUR DATA, SYSTEMS AND NETWORK
- FOCUS YOUR CYBERSECURITY EFFORTS
- VALIDATE YOUR BACKUP STRATEGY
- PLAN FOR INCIDENT RESPONSE

PREPARE – PREVENT – MITIGATE – RESTORE

Benjamin Franklin never had to think about cybersecurity, but he understood one of its cornerstones: preparation is critical. In a world where resources are limited, you must know what systems you are running, what data you are storing and how your network is structured to allocate your cybersecurity resources effectively.

Implementing strong security controls is not enough, however, as we all know that organizations with strong security can be compromised. Accordingly, it is important to maintain regular backups of important data and to have an incident response plan in place to rely on when an incident occurs.

Know your data, systems and network

Businesses and organizations typically store many kinds of data, using a variety of computer systems, on networks that may be local, global or somewhere in between. So, the first principle of cybersecurity is "know thyself." Know what (and where) data are being created, collected and stored; maintain an accurate inventory of computer systems and software; and understand your network infrastructure.

This enables you to better:

- Identify and prioritize appropriate security controls.
- Remove unauthorized systems and software from your network.
- Patch and maintain existing systems and software.
- Recognize new vulnerabilities in existing systems and software.
- Respond more effectively when an incident occurs.

There are many kinds of data that can be found on a system or network, including the following:

Protected
Health
Information

PHI

such as health or medical records of patients or employees.

Payment
Card
Information

PCI

such as credit or debit card account numbers.

Personally
Identifiable
Information

PII

such as names, addresses, telephone numbers, Social Security account numbers or other identifying information.

Intellectual property

such as manufacturing processes, marketing strategies and other trade secrets.

Other proprietary information

including confidential information shared by a business partner.

In many cases, it may be appropriate for your organization to adopt a data classification scheme. A certain kind of data may warrant stronger security controls if it is particularly valuable to the organization, if its loss would be particularly damaging or if it merits special treatment in light of legal or contractual obligations.

Next, a systems and software inventory should be maintained to identify every device that has access to the network, including desktops, laptops, mobile devices, servers, network equipment and printers. The inventory should identify a specific person responsible for each device (by name and job title), as well as the device's network address and physical location.

Organizations should also maintain an inventory of software applications, identifying the systems (including servers, workstations and laptops) on which they reside.

Any systems or applications that are not authorized should be investigated and removed.

Finally, it is important to maintain accurate information about the structure and topology of an organization's network. This information can be used during the normal course of business to ensure that changes to the network are consistent with existing network security controls. It will also be invaluable in the course of responding to a cybersecurity incident.

WHEN BREACHES HAVE RESULTED IN INSURANCE CLAIMS

14% of the claims involved the loss of PHI

27% of the claims involved the loss of PCI

45% of the claims involved the loss of PII [4]

Focus your cybersecurity efforts

Once you understand the data, systems and network that you are trying to protect, you can focus on implementing (or improving) the security controls that would be most effective in light of your specific needs and resources. (You will also be better prepared to work with a cybersecurity consultant, if you choose to do that.)

Consider the following:

What are your "crown jewels"?

If you have adopted a data classification scheme, you will want to implement stronger security controls for the storage and transmission of data that are classified as more sensitive.

What are your vulnerabilities?

A vulnerability assessment can help identify weak spots in your cybersecurity that deserve greater attention. If your organization permits systems or network access to outside parties, such as contractors or vendors, understand that their vulnerabilities become your vulnerabilities.

What are the most likely threat scenarios?

If you understand the threats that are most likely to impact your business or organization, you can focus on minimizing those threats.

COMPLIANCE WITH A PARTICULAR CYBERSECURITY STANDARD IS NOT A PREREQUISITE TO GOOD CYBERSECURITY, BUT IT CAN BE IMPORTANT IN DETERMINING WHICH SECURITY CONTROLS TO IMPLEMENT. BUSINESSES THAT HANDLE PAYMENT CARD INFORMATION, FOR EXAMPLE, MUST COMPLY WITH THE PCI DATA SECURITY STANDARD.

Extensive information about computer and network security controls is freely available online, including comprehensive taxonomies of security controls that can help ensure that you are not omitting one that would be valuable to your organization.[5]

Here, we highlight a few fundamental security controls:

Strong passwords: Almost all systems can be configured to require users to select passwords that would be difficult for an intruder to compromise. Users should be instructed not to use passwords (or variants of passwords) that they use elsewhere (e.g., to control access to personal email or other internet accounts).

Firewalls: Firewalls are used to permit only appropriate traffic to enter and leave a system or network. Like any other security control, a firewall must be properly configured and maintained to be effective. Firewalls should only permit network traffic that is appropriate to the needs of the business or organization. For example, file transfer requests to a company's email server should probably be rejected.

Anti-virus: Anti-virus software is designed to defend your network against malicious software ("malware"). To maintain an effective defense, your anti-virus software should run in the background at all times and be continually updated. The ability to quickly install anti-virus updates on all systems is critical.

Content filtering: Content-filtering controls restrict material delivered over the internet via the Web, email or other means. They enable a company or organization to block attachments in emails or material from websites that are likely to include spyware, viruses, pornography and other objectionable content. "Spam" filters, in particular, should be used to block email messages that are unsolicited or potentially dangerous.

Encryption: Encryption can be employed to protect any data that your organization considers sensitive. Encryption should be considered both for data being stored ("data at rest") as well as data being moved or sent somewhere ("data in motion"). Many security experts believe that data are most at risk when on the move. Whenever sensitive data are transmitted externally, consider using encryption. Additionally, if sensitive data are being transmitted internally over less secure networks, consider using encryption. For laptops and mobile devices, the use of whole-disk encryption can significantly reduce the risks associated with lost or stolen devices.

Multifactor (or Two-factor) authentication: An authentication factor is an independent category of credential used for identity verification. The three most common authentication factors are often described as something you know (e.g., a password), something you have (e.g., a smartphone or access card), and something you are (e.g., biometrics such as fingerprints). Some technologies are also using location (e.g., GPS coordinates) and time of day as additional authentication factors. Multifactor authentication is often used to secure control of sensitive data or to secure remote access to a network.

Virtual private network (VPN): A VPN is a secured network that is built on a larger, underlying network. In one common scenario, a company may provide remote access to the company's network through a VPN, allowing its employees to access the company's network securely over the public internet. A VPN can also be used to provide limited access to part of a network. For example, a company might use a VPN to permit third-party vendors to access certain systems or services on its network, without providing access to the entire network.

Network and application logging: Many systems, applications and network devices have a built-in capability to generate log files that reflect user access and activity. These log files can be very helpful in the event of a cybersecurity incident, particularly for systems and applications that store and manipulate sensitive information.

Intrusion detection system (IDS): An IDS can work together with firewalls to analyze network traffic and to block traffic that matches a known or suspected attack pattern.

After deciding which security controls to focus on and implement, an organization should document its reasons as part of an overall cybersecurity plan or strategy. An organization cannot be expected to implement every possible security control, but it should have a reasonable, documented plan in place for how it is protecting its data, systems and network.

AN ORGANIZATION RUNNING AN OBSOLETE VERSION OF AN OPERATING SYSTEM OR APPLICATION (I.E., A VERSION FOR WHICH PATCHES AND SECURITY UPDATES ARE NO LONGER BEING RELEASED), SHOULD TRANSITION TO A SUPPORTED VERSION. OTHERWISE, THE VULNERABLE SYSTEM OR APPLICATION SHOULD BE CAREFULLY PROTECTED AND/OR QUARANTINED.

Validate your backup strategy

One of the most important steps that an organization can take to protect against cyber risks is to maintain regular, systematic backup copies of important data. A well-designed backup strategy will protect against system and storage failure, as well as fire or flood. In addition, ransomware is on the rise – cybercriminals are using encryption to "lock" data found on compromised computers and demanding payment to decrypt the data. Maintaining good backups can protect you from falling victim to the latest ransomware.

In evaluating your backup strategy, you will want to consider what data need to be backed up, how frequently to perform backups and where the backups should be stored. For example, maintaining remote backups in "the cloud" may be simple and cost-effective, but the backup copies may not be immediately available to you if your internet connection is down. The cost of any particular backup strategy will have to be weighed against how quickly and reliably data must be recovered if damaged or destroyed.

It will often make sense to implement a "tiered" backup strategy in which data are backed up frequently to one location, and maybe less frequently to a second location. For example, a remote backup service could be used for nightly backups, with an additional backup copy made on a local storage device every week and stored in a separate, secure location. With the growth of ransomware, at least one backup copy should be stored offline or on a more tightly secured part of your network.

Backup copies of data should be encrypted if the original data warranted encryption. The backup copies should also be tested periodically to ensure that data can, in fact, be restored if the original data have been damaged or destroyed.

Plan for incident response

Every organization should plan for the unexpected – including a data breach or cyber incident. In fact, without an incident response plan, there is a greater likelihood of making mistakes in responding to the breach or incident – for example, by failing to comply with applicable laws and regulations. Such mistakes can cause damage to the business or organization that goes beyond the damage directly caused by the attack. A well-designed incident response plan will make it easier for your organization to launch a rapid and coordinated response.

IN MORE THAN **90%** OF BREACHES, THE COMPROMISE TAKES ONLY MINUTES OR LESS

AND **99.6%** OF THE TIME, DATA ARE EX-FILTRATED WITHIN DAYS.[6]

IN GENERAL, AN INCIDENT RESPONSE PLAN SHOULD INCLUDE AT LEAST THE FOLLOWING COMPONENTS:

1. INFORMATION ABOUT THE PEOPLE INSIDE THE ORGANIZATION WHO WILL FORM THE INCIDENT RESPONSE TEAM;

2. GUIDELINES AND PROCEDURES TO ASSIST THE TEAM; AND

3. INFORMATION ABOUT EXTERNAL RESOURCES THAT ARE AVAILABLE TO SUPPORT THE TEAM.

The incident response team

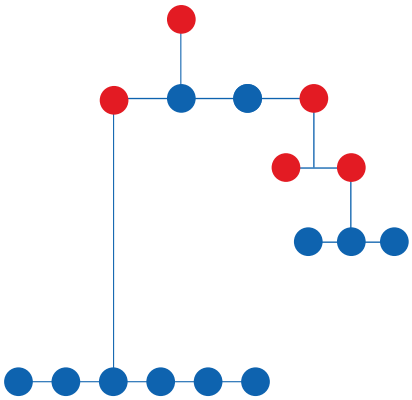
Identify team members by name and job title, together with a description of roles and responsibilities. An experienced manager, such as the Chief Information Security Officer, should serve as the team leader to help coordinate the overall response effort. Other members should include representatives from management, information technology, legal, compliance and public affairs/media relations.

Procedures and guidelines for incident response

An incident response plan should provide a framework for action so that important decisions have been considered ahead of time and are not made under pressure. In particular, it is important for the incident response plan to provide procedures and guidelines on difficult issues including identifying lines of authority and internal reporting obligations. The team should be focused on making the best possible decisions, not on figuring out how and by whom the decisions need to be made.

Clear procedures and guidelines on the following questions can greatly facilitate an incident response effort:

- Does the incident response plan even apply? Not every security incident will require invoking the plan.
- Is the business or organization insured for the incident? If so, when should the insurer be notified?
- Should the team bring in external resources? Should law enforcement authorities be notified? Who will have primary responsibility for coordinating with them?
- When should certain services or parts of the network be shut down or transitioned to backup systems, if available? There probably should be different criteria for shutting down an email server than a customer-facing website server, for example.
- What data, if lost or exposed, are subject to data breach notification laws? If notification is required, when and how should notification be made?
- What data, if lost or exposed, must be reported to government regulators? To business partners?
- Should information about the incident be communicated to employees of the organization? To the public?
- How should the team document the incident response effort, and how should it preserve records or evidence that it collects during the investigation?



It will not be possible, of course, for an incident response plan to provide detailed procedures and guidelines to cover every possible issue or scenario. The procedures and guidelines should be flexible enough to apply to a range of different cyber incidents, while providing more concrete guidance for those incidents that are considered the most likely to arise.

External resources

Depending on the nature and scope of the incident, it may be appropriate for the incident response team to seek assistance from external resources, such as a “breach coach,” a computer and network forensics expert or a crisis management consultant. Most companies do not have employees with both the experience and time to handle an incident response effort.

In the course of developing an incident response plan, it is important to identify external resources and to establish relationships with them before an incident occurs, so that they will be ready to assist when needed. It will also be more cost-effective to negotiate for these services before an incident, rather than waiting until your organization is in dire need of them.

If your organization outsources any part of its IT function, the incident response plan should also provide contact information for your IT providers. It will often be necessary to work with your IT providers to investigate and secure evidence after a cybersecurity incident.

Once you have an incident response plan in place, it is important to test it regularly — annually, if possible.

Testing the incident response plan

These "tabletop" exercises should involve the full incident response team, and the results of the exercises should be made available to senior management. It is better to address issues that might be raised by senior management about the incident response plan in connection with a tabletop exercise — not in the midst of an actual incident response effort.

Helping prevent damaging cyber incidents.

PREVENT INCIDENTS:

- STRENGTHEN ACCESS CONTROLS
- PATCH KNOWN VULNERABILITIES
- EDUCATE YOUR EMPLOYEES
- ADOPT SECURITY-CONSCIOUS POLICIES AND PROCEDURES

PREPARE – **PREVENT** – MITIGATE – RESTORE

Security controls and incident response plans are necessary, but not necessarily sufficient, for good cybersecurity. Implementing the next four guidelines will go a long way toward helping your organization effectively prevent damaging cyber incidents:

1. Strengthen your access controls;
2. Promptly patch system and application vulnerabilities;
3. Educate your employees about cyber risks and security practices; and
4. Adopt policies and procedures that integrate good security practices into your business operations.

Strengthen access controls

We are all familiar with passwords, which are among the most fundamental types of access controls. More sophisticated access controls are becoming commonplace. For example, many banks and financial institutions have begun requiring two-factor authentication for online account access, and many smartphones and computers can be unlocked using biometric identifiers, such as fingerprints. Judiciously implementing stronger access controls, like limiting the number of employees with remote network access, can be a cost-effective way to improve the cybersecurity of your organization.

Even without adopting new access control technologies, businesses and organizations can benefit if they adhere to the principle of least privilege: that is, access to data, systems and the network should be permitted only to the extent necessary for the smooth and continued operation of the enterprise. Some information may be accessible to everyone; some information may be restricted to a specific department; and some information should be accessible only by a set of key personnel.

The principle of least privilege should be applied to all users, including system administrators and other members of an IT department. Inappropriate use of administrative privileges is often found to be a major contributing factor in data breaches and other cyber incidents.

In many growing organizations, system administrators assume numerous job functions and have access to multiple systems or applications. This can present a security risk if administrative privileges are not properly controlled, making it easier for an attacker to gain full control of a compromised system. To minimize this risk, the following controls should be considered:

- Users should not be allowed local administrative privileges, even on computers provided for their exclusive use.
- Members of the IT staff should have administrative privileges only for specific systems or applications, and only to the extent necessary for the performance of their duties.
- Members of the IT staff with administrative privileges should maintain separate accounts for daily use and for use as a system administrator. The administrator account should not be used for routine access to email or the internet. The password for the administrator account should not be shared, even with other members of the IT staff, and should be different from the password for the user account.
- When wider privileges must be granted to a user or system administrator to perform a specific task, grant the privileges only for a limited time.

Finally, it is important to include physical access controls for sensitive data and systems. Providing physical security to the building exterior can be a first step to protecting against unauthorized system and network access. Protect areas such as server rooms, computer rooms and telephone equipment rooms by appropriate security measures, such as locked doors and entry controls.

FOLLOWING THE PRINCIPLE OF LEAST PRIVILEGE CAN HELP REDUCE THE RISK FROM INSIDER INVOLVEMENT, A FACTOR IN OVER 30% OF CYBER INSURANCE CLAIMS.[7]

Patch known vulnerabilities

This guideline is simple: patch your systems and software. An unpatched vulnerability is one of the easiest and most common methods of compromising a computer system or network.

Unfortunately, there can be significant obstacles to ensuring that all computer systems and software applications on a network are fully patched. First, on most corporate networks, there are a multitude of applications running on a variety of different systems. All of these applications and systems may require patches, provided by a host of third-party vendors. Second, it is a good practice to test patches before they are deployed, particularly for systems or software that are considered mission critical — introducing delay. Finally, patches are not always applied successfully, particularly to laptop computers and other mobile devices that are frequently disconnected from the network.

These difficulties can be addressed in part through the use of a patch management system. Whether using a commercial patch management system or tools that have been developed in-house, the system should:

- **Help track, obtain and validate available patches.**

  As different vendors release patches for their products, the system should identify which patches are needed in your particular environment and make them available to the IT staff for testing and evaluation.

- **Permit priority-based patching.**

  Routine patches can be applied on a predetermined schedule, but critical patches should be applied as soon as possible.

- **Perform reporting and auditing.**

  If the deployment of a patch fails anywhere on your network, information about the failure should be easily available to members of the IT staff.

PATCHES ARE NOT ALWAYS APPLIED SUCCESSFULLY, PARTICULARLY TO LAPTOP COMPUTERS AND OTHER MOBILE DEVICES THAT ARE FREQUENTLY DISCONNECTED FROM THE NETWORK.

It is also good practice for an organization to scan its systems and network regularly for vulnerabilities that may have been missed by the patch management system.

In some instances, it may be necessary to continue using a system or application with known vulnerabilities — for example, a legacy system with a vulnerability for which no patch is available. In that case, the vulnerable system should be carefully protected using other means, such as firewalls and strict access controls.

Educate your employees

Many cybersecurity incidents can be directly attributed to inadequate security awareness training. A training program designed to empower employees to recognize common cyber threats and to notify the IT staff is a cost-effective way to reduce these threats.

A comprehensive training program should:

- **Emphasize the importance of cybersecurity to the organization's success.** Employees should understand why data, systems and network security matter. A security breach can allow attackers to drain an organization's bank account; other financial and legal repercussions may follow, such as incident response costs, data breach notification expenses and loss of reputation and goodwill. If applicable, legal and regulatory requirements to protect certain kinds of data, such as personal health information (PHI), should be highlighted. The training should address each employee's responsibility to protect the organization's data, systems and network.
- **Train employees to avoid information security risks.** Risks can include phishing and other forms of social engineering, as well as improper password management, unsafe internet browsing and using unauthorized software.
- **Explain how to protect laptops, mobile devices and digital storage media.** Employees should be reminded to physically safeguard data and devices, as well as when and how to use encryption. Computers and other physical assets are lost more than 100 times more frequently than they are stolen.[8]
- **Encourage employees to report suspicious activity.** Employees should be aware of your incident response procedures and should know how to report suspicious activity, including questionable phone calls, to IT or security personnel.

Finally, employees should also receive training on policies and procedures that relate to cybersecurity. In many instances, explaining the rationale for restrictive "system use" policies will help to promote greater compliance.

The number of spear phishing campaigns targeting employees increased by 55% in 2015.[9]

Adopt security-conscious policies and procedures

Good cybersecurity will be hard to achieve if a company's policies or procedures are haphazard — a skilled hacker can compromise an entire corporate network from a foothold obtained on one vulnerable computer.

There are several areas in particular where formal policies or procedures can substantially improve cybersecurity:

WHEN NEW DEVICES ARE ADDED TO A NETWORK, THERE SHOULD BE PROCEDURES TO ENSURE THAT DEFAULT PASSWORDS ARE CHANGED; PATCHES AND UPDATES ARE APPLIED; AND UNNECESSARY SERVICES, APPLICATIONS AND NETWORK PORTS ARE REMOVED OR DISABLED.

- A "system use" policy should be in place to govern the use of the business or organization's computers and network, including appropriate restrictions on the use of electronic mail, social media, the internet, external storage devices and unauthorized systems and software.
- There should also be procedures on disposal requirements for sensitive information and data, including computer systems and storage devices that store or process such data.
- Inadequate control of changes to network equipment and systems can be a common cause of systems and security failures. Lack of a written procedure creates the risk that changes could be made without proper preparation or testing. Establish written procedures that govern and coordinate all changes to existing configurations.
- There should be a process for promptly revoking system and network access when an employee leaves a company or organization, and for changing passwords and other controls to shared accounts, if any, that the employee may have known or accessed. It may also be advisable to have employees sign a confidentiality or non-disclosure agreement, as well as a representation upon leaving the business or organization that no sensitive, proprietary or other confidential data have been taken.

Vendor management

Businesses and organizations must pay special attention to policies and procedures relating to their vendors — IT or otherwise. The cybersecurity of an organization will be seriously jeopardized if a vendor with poor cybersecurity is given access to the organization's systems or network.

In accordance with the principle of least privilege, an organization should only give a vendor the level of systems or network access that is necessary for the performance of the vendor's responsibilities. Vendors should be subject to the same password requirements as other users (or system administrators, if appropriate), and should not use the same password across different client sites. Once the organization is no longer using the vendor, policies and procedures should be in place to ensure that access credentials and privileges are promptly revoked.

The policies and procedures of the organization should also ensure that the vendor has adopted sound cybersecurity practices, commensurate with the level of data, systems and network access given to the vendor. It may be appropriate, for example, to include contract provisions that set forth cybersecurity requirements, agreements to assist with investigations, insurance obligations, indemnification provisions, etc. If the vendor is given access to sensitive data, such as personally identifiable information, additional controls may be appropriate, such as requiring third-party assessments of the vendor's cybersecurity practices.

Attackers are increasingly taking advantage of outsourcing relationships to gain access to sensitive information.[10]

Cyber incidents need not be catastrophic if properly managed.

MITIGATE DAMAGE:

- DETECT INCIDENTS EARLY
- EXECUTE YOUR RESPONSE PLAN
- GET HELP WHEN NEEDED
- DOCUMENT YOUR RESPONSE EFFORT

PREPARE – PREVENT – **MITIGATE** – RESTORE

Cyber incidents may be inevitable but need not be catastrophic if properly managed. Early detection is crucial, so organizations should review network and security logs as frequently as possible — indeed, continuous monitoring is a worthy goal.

When an incident does occur, a well-designed incident response plan will be invaluable in guiding the company or organization from the initial stages of incident response — investigate, assess and mediate — through to the eventual restoration of normal operations. It will often make sense for an organization to seek outside expertise, to contain the damage from an incident; it will always make sense to document the actions taken during the entire incident response process (as well as the reasons for doing so).

Detect incidents early

Even an organization with strong cybersecurity cannot assume that its network is impenetrable. Therefore, it is critically important to detect incidents early to minimize the damage in the event of a compromise.

Fortunately, most systems (and many applications) include some logging or monitoring capability. Network firewalls can be configured to log suspicious traffic and to issue alerts under specified conditions. Almost all computers can be configured to track unsuccessful login attempts, which are an early indicator of a potential attack. Businesses and organizations should be aware of the logging and monitoring capabilities that are already available to them; in addition, there are special-purpose network monitoring systems that can be implemented to allow for closer monitoring of network traffic.

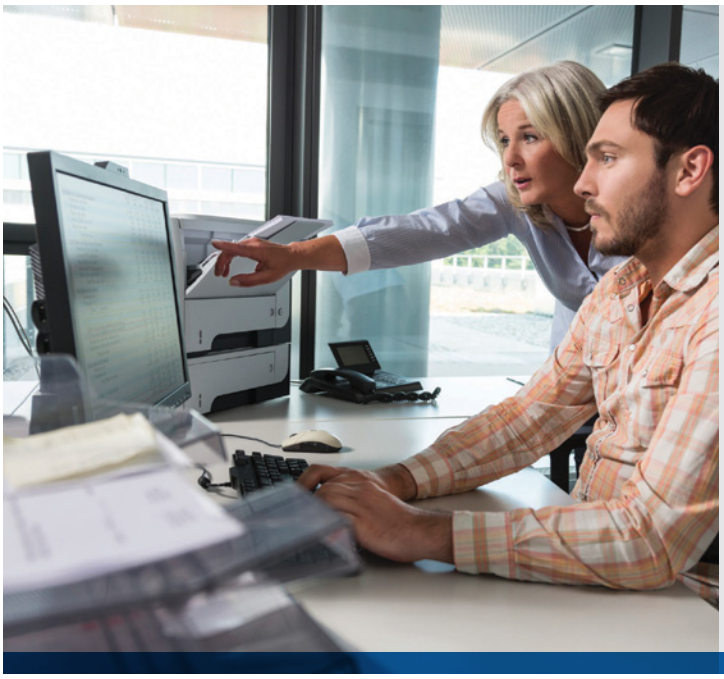
It is usually not practical, however, to have all systems and applications configured to log as much data as possible. Instead, organizations should focus their logging and monitoring capabilities on protecting their most valuable assets. For example, unsuccessful login attempts to a central database server should likely be investigated more promptly and thoroughly than unsuccessful login attempts to an average employee's laptop.

For many organizations, it will make sense to use a security incident event management system (SIEM), whether implemented in-house or provided by a vendor. Such a system operates as a centralized resource for collecting, monitoring and analyzing network logs and other security-related information. By using a SIEM, organizations can greatly reduce the risk that early indicators of a compromise will be missed.

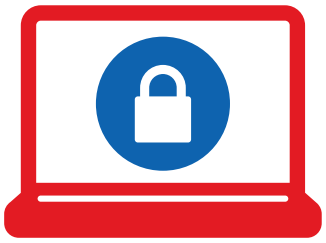
Execute your response plan

When an organization is impacted by a cyber incident, there are often a multitude of unanswered questions about what happened, what the impact will be and what to do next.

In order to answer those questions, your incident response team should initially focus on the following: investigating the incident, assessing its impact and mitigating any damage. These tasks must often be undertaken concurrently, in the middle of a situation that is rapidly changing, with information that is incomplete and sometimes inaccurate. In such trying circumstances, a well-designed incident response plan will help the team succeed by delineating areas of responsibility, facilitating information sharing and identifying pertinent guidelines or procedures — for example, when deciding whether to use a computer and network forensics consultant during the investigation.



NOTIFY YOUR INSURANCE CARRIER PROMPTLY AFTER AN INCIDENT IS DISCOVERED. CYBER INSURANCE CAN HELP COMPANIES BY PROVIDING ACCESS TO A BREACH COACH, FORENSICS CONSULTANTS AND OTHER PROFESSIONALS IN THE DATA SECURITY COMMUNITY.



Investigate the incident

The investigation of a substantial cyber incident — at a minimum, determining how the attack was conducted, which systems were compromised and what data have been lost or exposed — is likely to require substantial time and expertise. Such investigations typically involve:

- Preserving, collecting and analyzing application, system and network logs that may have evidence relating to the attack.
- Identifying any software or hardware vulnerabilities that were used to facilitate the attack.
- Identifying unauthorized changes to systems on the network, including the installation of malicious software ("malware") such as keyloggers or remote-access Trojans.
- Determining what data, if any, were stolen or exposed, including any passwords or other security controls that may have been compromised.

The investigation may have to include network devices such as firewalls and routers, not just the computers and servers that are on the network. Any significant evidence obtained during the investigation should be properly preserved, preferably in consultation with legal counsel.

The investigation may also involve interviews of employees, contractors or other third parties who may have been impacted by, or otherwise involved in, the incident. Information obtained through such interviews should be memorialized in writing, and interviews of third parties should preferably be conducted only in consultation with legal counsel.

Assess the impact

The impact of a cyber incident will typically be assessed in many dimensions: the number of impacted systems; the amount of data lost (whether measured by the volume of the data or the number of victims whose data were stolen); the magnitude of financial loss; the effect on a business or organization's operations; and the anticipated difficulty in recovering from the incident, to mention a few.

These assessments will be needed by senior management and will also be needed by the incident response team in order to make sound decisions at critical junctures. For example, the incident response plan may specify that a computer and network forensics consultant should be retained if the number of impacted systems exceeds a certain threshold, or if certain kinds of data (such as payment card information) have been stolen or exposed.

In particular, the impact of a cyber incident that involves the loss of data will be greatly affected by the kind of data involved. The loss of customer account data, for example, will likely result in a different response effort than the loss of the company or organization's own data. Whenever a cyber incident involves the loss or even potential loss of data, legal counsel should be closely involved in the incident response effort.

Mitigate any damage

Once the nature and the scope of the attack are understood, the incident response team can move toward the recovery and restoration of lost or damaged data and systems. However, if the attack is causing ongoing damage to the organization, it may be necessary to take steps to mitigate that damage even before the incident investigation and the impact assessment are complete.

The immediate impulse may be to "pull the plug" — that is, to do everything possible to disrupt the attack, such as disconnecting all systems known to have been compromised. In some cases, this can be an appropriate response.

However, other factors should be considered before deciding to "pull the plug."

First, the tactic may be ineffective. It is well known that attackers will seek to embed themselves into a compromised network, so that disabling one, or a few, compromised computers will simply cause the attackers to move elsewhere on the network. Pursuing a "whack-a-mole" mitigation effort can distract the incident response team from executing a more comprehensive recovery and restoration plan.

Second, pulling the plug may impede the investigation. If the attackers have compromised a system where encrypted data are stored, it may be more important to monitor their activities to learn if the attackers have been able to decrypt the data than to shut down the system immediately.

Finally, a mitigation effort undertaken in haste, without sufficient planning and consideration, might itself cause damage to a business or organization. It may not make sense, for example, to shut down a company's email server, if a hacker has only obtained limited access to the server without yet obtaining access to the emails.

Instead of pulling the plug, it may be preferable to mitigate damage by pursuing a strategy of containment — locking down portions of the network that the attackers have not yet compromised, or blocking egress points by re-configuring firewalls to strictly limit outbound traffic.

It can be challenging for an incident response team to investigate, assess and mitigate the damage from a significant cyber incident. Therefore, it is often appropriate for the organization to support the team with external resources.

Get help when needed

There are many outside experts and consultants who can help a business or organization respond effectively to a cyber incident. A list of these external resources should be included in the incident response plan, together with guidelines and policies that will assist the incident response team in determining when outside resources should be brought to bear.

These resources include:

A "breach coach" or other outside legal counsel. An experienced breach coach can provide guidance throughout the incident response effort, particularly on issues relating to privacy, notification requirements and regulatory compliance. In addition, aspects of the incident response effort conducted under the direction of a breach coach may be protected by privilege in the event of future litigation.

A computer and network forensics expert. Use of an outside forensics expert is necessary if internal IT personnel do not have the capacity or expertise to investigate the incident, which may require analyzing malware or examining detailed logs of network traffic. It may also be advisable to use an outside forensics expert if the incident might give rise to litigation.

A crisis management consultant. An experienced crisis management consultant can help the organization minimize any reputational injury that could result from the incident.

Law enforcement. If there is reason to believe that a crime has been committed, it may be appropriate to refer the matter to law enforcement authorities. Few cyber attacks occur in isolation; from investigating similar or related incidents, law enforcement authorities may be able to provide information about the tools and techniques that were used to conduct the attack. If the attack was financially motivated, law enforcement may be better positioned to trace the money that was stolen, if any.

Document your response effort

Throughout the incident response effort, it is important to document the steps taken by the incident response team. This will help ensure that your organization is better able to identify lessons learned, to respond to any future legal or regulatory inquiries, and to reconcile any changes made to your systems or networks after the urgency of the incident response effort has passed. The incident response plan should include forms or other guidance that will help to ensure adequate recordkeeping.

Sometimes, it may be appropriate for an attorney to be involved in documenting the incident response effort, as this may allow the organization to assert a claim of privilege over the materials in the event of future litigation.

Complete the road to recovery.

RESTORE NORMAL OPERATIONS:

- REMEDIATE, RESTORE AND REPLACE
- CONTINUE MONITORING
- COMMUNICATE EFFECTIVELY
- IMPLEMENT LESSONS LEARNED

PREPARE – PREVENT – MITIGATE – **RESTORE**

After assessing the situation, your organization will be ready to complete the road to recovery: remediating vulnerabilities; restoring lost or damaged systems and data; and replacing passwords, encryption keys and other compromised controls.

Along the way, it will be important to continue monitoring your systems and networks for signs that the attackers may have evaded your efforts to eliminate them. It will also be important to provide accurate information about the incident, if and when appropriate, to interested stakeholders, whether employees, business partners, regulators or others.

Finally, your organization can benefit from the incident by identifying and applying lessons learned from a careful examination of the incident and the incident response effort.

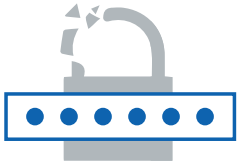
Remediate, restore and replace

Ultimately, the goal of your incident response effort is to remove the attackers from your network and to return to normal operations. To do so, you must:

- **Remediate vulnerabilities.** In most cases, the incident response team will have been attempting to eliminate vulnerabilities as they have been discovered over the course of the investigation. Any remaining vulnerabilities that compromise the security of the network should be addressed at this stage, whether through patching or other methods. If it has not been possible to identify the vulnerabilities used by the attackers and to remediate them, the recovery effort may well prove futile.

- **Restore lost or damaged systems and data.** It will be much easier to restore data from a backup copy than to re-create lost or damaged data. When restoring a compromised system, the preferred method is to re-image the operating system and applications from a clean image. If this is not possible, care must be taken to ensure that all unwanted changes to the system have been identified and repaired. Otherwise, a “back door” installed by the attackers could be used to reinfect the system and the network.

- **Replace compromised controls.** This final step is crucial, but often overlooked. When attackers have compromised a system or network, they are often able to obtain information about security controls, such as passwords and encryption keys, which can be used in later attacks. The incident response team should give thought to security controls that may have been compromised, not only security controls that have been compromised.



Passwords are stolen or exposed in nearly half of all data breaches.[11]

Continue monitoring

It is important to monitor the network closely throughout the entire incident response effort. It is equally important that monitoring continue for a time even after the recovery effort is thought to be complete. Attackers will often react to steps taken by the incident response team, and close monitoring of the network can provide insight into the attackers' goals and how they operate.

More importantly, continued monitoring of the network will help to ensure that the recovery effort was successful. It should be assumed that attackers, having once gained a foothold on a network, will have taken steps to embed themselves further in order to ensure access to the network even after the initial point of compromise has been denied to them.

Depending on the scope and duration of the incident, it may be advisable to conduct a vulnerability scan of the business or organization's systems and network. This can serve to ensure that any changes made during the incident response effort did not introduce new vulnerabilities, and can also provide added reassurance that the response effort was, in fact, successful.

Communicate effectively

When responding to a cyber incident, it can be very difficult to determine what information should be communicated both internally and externally, because the information available about the incident may be incomplete and unreliable. Providing information that later turns out to be inaccurate can significantly impair the organization's reputation in the eyes of its customers and shareholders, and can also invite the scrutiny of government regulators. Therefore, it is critical for the organization to have formulated an effective communications strategy before a cyber incident occurs.

When communicating with senior management, it is important for the incident response team to provide as much reliable information as possible about the scope of the incident, its potential impact on the organization and the anticipated duration of the response effort. It is preferable for that information to be conveyed through one or more designated points of contact, hopefully identified in the incident response plan, and not through ad hoc, informal communications with different members of the response team.

When deciding whether, when and what information should be communicated to third parties, including the public, consider the following:

Factors to consider:

Has information about the incident already been made public or is it about to be?
If so, it is probably in the best interests of the organization to make a public statement in order to maintain the trust of its customers and business partners, and to position itself as the authoritative source of information. If information about the incident is likely to become public — for example, if the incident involved the loss of data that must be reported under a data breach notification law — it is important to make a public statement.

What reliable information, if any, is available?
During the early stages of an incident response effort, there may not be much reliable information at all. In that case, if a public statement must be made, hopefully the organization can disclose when the incident was first discovered, demonstrate that it has promptly begun to investigate — including cooperating with law enforcement agencies or involving outside investigators — and describe remedial measures for affected third parties, such as credit monitoring services.

Data breach notification

Whenever data have been lost as a result of the incident, it will be necessary to determine whether notification of the breach is required by federal or state laws and regulations. Currently, 47 out of the 50 states have statutes that require notification under various circumstances when a data breach occurs. There are also situations where federal laws and regulations require notification — for example, the loss of personal health information may be governed by the Health Insurance Portability and Accountability Act (HIPAA).

Consult with legal counsel when developing your notification strategy to ensure that your notification is timely and complete. Keep copies of all notifications that are sent out, as well as any responses that are received.

Reporting obligations

In addition to notifying individuals whose data may have been compromised, there are circumstances where data breaches must be reported to state or federal authorities. For example, some state laws require that a report be made to the state's attorney general (or a similar official) when any citizen of the state is entitled to data breach notification, but other state laws do not. Federal regulators may expect reports when personal health information has been breached, when defense contractors and subcontractors have been compromised, and in other situations.

If a reporting obligation is potentially implicated by a cybersecurity incident, your organization should consult with legal counsel and contact the appropriate state or federal authority early in the incident response process. Even if the investigation of the incident is still incomplete, it is important for the organization to demonstrate that it understands its reporting obligations and is taking prompt and appropriate measures to respond to the incident.

Implement lessons learned

After recovering from a cyber incident, it is important to identify and apply any lessons that can be learned. By examining both the incident and the incident response effort, an organization has an invaluable opportunity to improve its ability to protect against and respond to future cyber incidents.

The review process should include members of the incident response team as well as personnel – employees or outside consultants – who were not involved in the incident response effort. It can be very helpful for the review process to be facilitated by an experienced manager who was not directly involved in the response effort. At a minimum, the review should cover the following questions:

REVIEW THE FOLLOWING QUESTIONS AFTER A CYBER INCIDENT:

- Are any additional changes needed to the organization's security controls, beyond those already made by the incident response team? Do remedial measures that were implemented under time pressure need to be changed or modified in the future?
- Would any changes to the organization's cybersecurity policies reduce the likelihood or severity of future cyber incidents? Would any changes to the organization's business practices as a whole (e.g., concerning what information is collected or stored) reduce the likelihood or severity of future cyber incidents?
- Would any changes to the organization's incident response plan enable the incident response team to respond more quickly and effectively in the future?
- Were outside resources used and managed well?
- Was appropriate information communicated in a timely fashion to senior management?

LEARN MORE

There is always room for a business or organization to improve its cybersecurity. Indeed, as the threat landscape evolves, organizations must pursue continuous improvement, or else risk becoming the next victim of cybercrime.

The Travelers Institute looks forward to working with businesses and organizations to help make our digital world a source of great opportunity, not unmanageable risks.

For more information about ***Cyber: Prepare, Prevent, Mitigate, Restore***, visit travelersinstitute.org/cyber or contact institute@travelers.com. Additional cyber resources can be found at travelers.com/cyber.

ABOUT THE TRAVELERS INSTITUTE

Travelers established the Travelers Institute as a means of participating in the public policy dialogue on matters of interest to the property casualty insurance sector, as well as the financial services industry more broadly. The Travelers Institute draws upon the industry expertise of Travelers' senior management and the technical expertise of its risk professionals, and other experts to provide information, analysis and recommendations to public policymakers and regulators.

NOTES

[1] Symantec Corp., 2016 Internet Security Threat Report, April 2016, Volume 21. https://resource.elq.symantec.com/LP=2899

[2] Ponemon Institute, 2016 Cost of Data Breach Study: United States. http://www-03.ibm.com/security/data-breach/

[3] NetDiligence, 2015 Cyber Claims Study. https://www.allclearid.com/business/resource/2015-netdiligence-cyber-claims-study/

[4] Ibid.

[5] National Institute of Standards and Technology, Security and Privacy Controls for Federal Information Systems and Organizations, NIST Special Publication 800-53 Rev. 4 (April 2013). http://www.nist.gov/manuscript-publication-search.cfm?pub_id=917904

[6] Verizon, 2016 Data Breach Investigations Report. http://news.verizonenterprise.com/2016/04/2016-data-breach-report-info/

[7] NetDiligence, 2015 Cyber Claims Study. https://www.allclearid.com/business/resource/2015-netdiligence-cyber-claims-study/

[8] Verizon, 2016 Data Breach Investigations Report. http://news.verizonenterprise.com/2016/04/2016-data-breach-report-info/

[9] Symantec Corp., 2016 Internet Security Threat Report, April 2016, Volume 21. https://resource.elq.symantec.com/LP=2899

[10] M-Trends 2016, Mandiant, a FireEye Company, February 2016. https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html

[11] Risk Based Security, Inc., 2015 Data Breach Trends. https://www.riskbasedsecurity.com/2015-data-breach-quickview/

TRAVELERS INSTITUTE® | TRAVELERS

travelersinstitute.org

The Travelers Institute, 700 13th Street NW, Suite 1180, Washington, DC 20005

© 2016 The Travelers Indemnity Company. All rights reserved. Travelers and the Travelers Umbrella logo are registered trademarks of The Travelers Indemnity Company in the U.S. and other countries.
M-18001 New 8-16