SECURANCE CONSULTING
Advantage of Insight AI

www.securanceconsulting.com

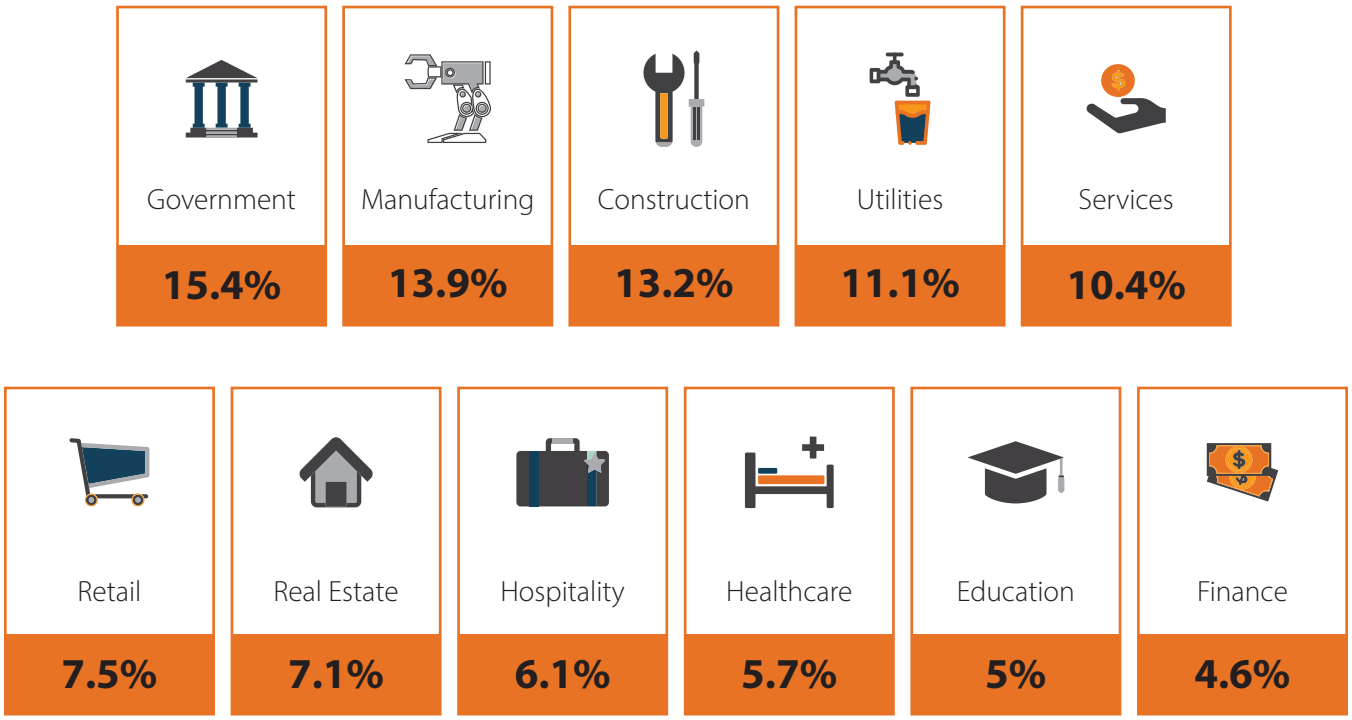
Prepared for Peril: Incident Response Solutions to Combat Ransomware and Cyber Threats

INTRODUCTION

From ransomware and phishing scams to unauthorized access from within, nearly every organization will experience a cyberattack that could impact the security of its data, networks, and | or systems. Even with every preventative measure in place, governments and businesses are increasingly susceptible to cyber threats. That is why every organization must establish, test, and regularly update its incident response (IR) strategy.

Ransomware, a form of malware that prevents businesses from accessing their computer files, systems, or networks and demands a ransom be paid for their return, is currently the most prevalent cyber threat. In 2024, ransomware groups reported 5,461 successful attacks on organizations worldwide.[1] The financial impact of these attacks has surged dramatically, with the average recovery cost for state and local government organizations increasing from $1.21 million in 2023 to $2.83 million in 2024, more than double the previous year's figure.[2]

North American Industries Reporting Ransom Attacks in the Last Year



NetLabs Global IT Services, 2021[3]

An organization may not be able to prevent a cyberattack, but it can take measures to minimize business impact and costs, and expedite the recovery process. By implementing an incident response plan (IRP), your organization will be poised to react quickly, decreasing the potential for loss.

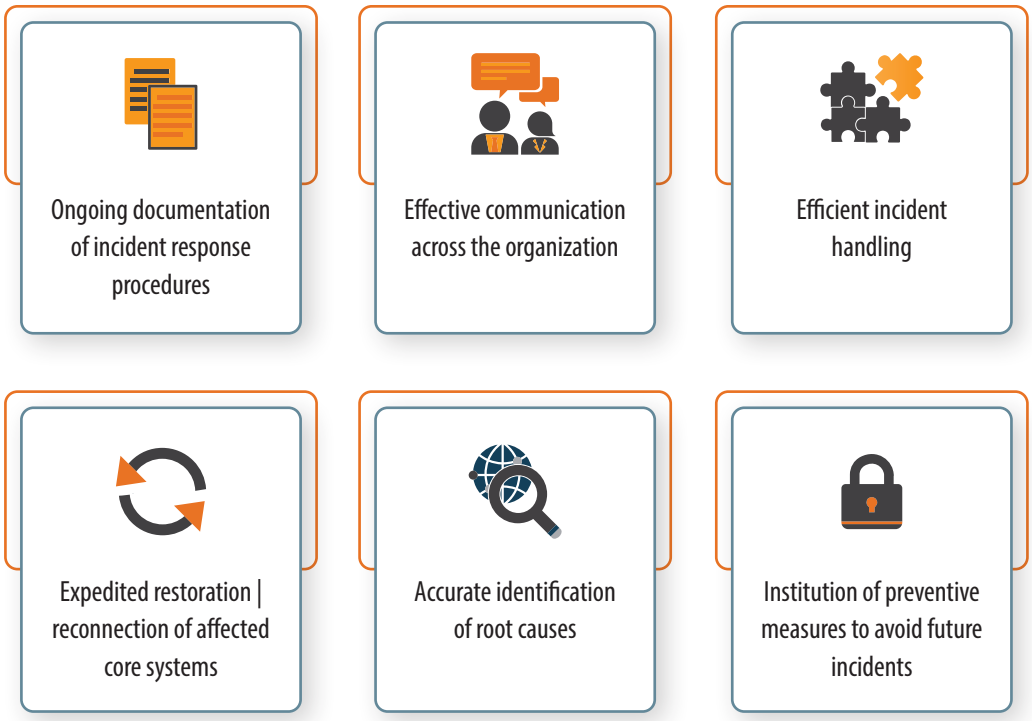
THE IMPORTANCE OF HAVING AN INCIDENT RESPONSE STRATEGY AND PLAN

Without clear guidelines in place, your organization will be unprepared for incidents and vulnerable to future attacks. Having a well-thought-out and systematic IR strategy and plan in place will allow you to react quickly and effectively to an attack or breach because you will have already defined:

- What an incident is
- The roles and responsibilities of the security team
- The tools that should be used for managing different kinds of attacks and breaches
- The steps that will need to be taken to address a security incident
- How an incident will be investigated and communicated
- What the notification requirements are following an attack

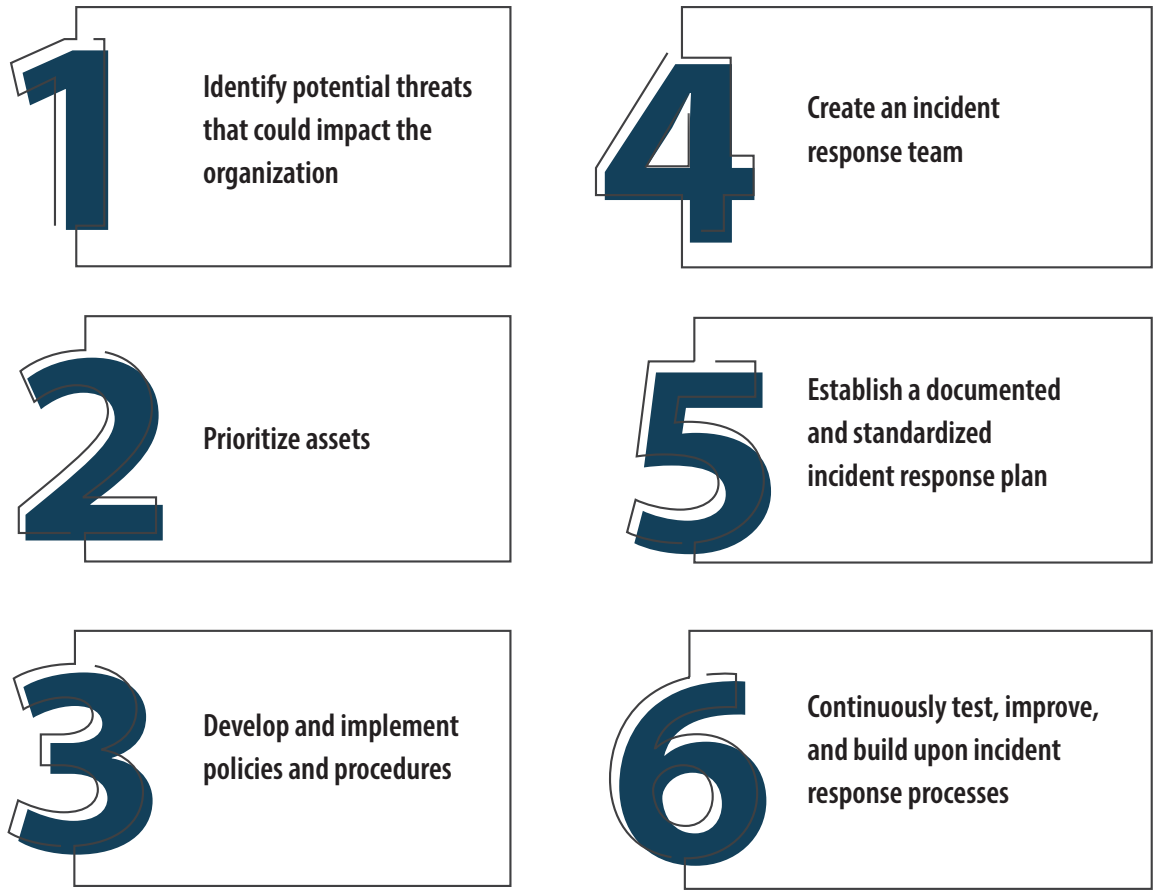
An IRP is a documented plan that details six distinct steps to ensure an organization's IT professionals and staff can recognize and deal with a cybersecurity incident, such as a data breach or cyberattack.[4] Having an IRP expedites an organization's ability to recover quickly from data and firewall breaches, denial of service attacks, outbreaks of viruses or malware, and even insider threats.

An effective IRP establishes guidelines that will ensure:



GETTING STARTED

To develop an effective IR strategy, organizations must critically evaluate their enterprise as a whole. Following these six steps will help you develop a holistic IR strategy that will support your organization's broader mission and minimize damage from cyberattacks.



Step 1: Identify Potential Threats that Could Impact the Organization

Every organization's IT environment is unique, as is its threat landscape. It is crucial to conduct research to understand your risk appetite, the cyber threats you face, and their level of severity. This may include reviewing past cyberattacks against your organization and | or looking at industry-specific threats on a broader scale. Consider not only external risks (such as phishing, Trojan worms, and malware), but internal threats (such as user error, employee skill levels, and disgruntled employees), as well. Taking a holistic approach that evaluates all aspects of organizational security is an ongoing task. As cyberattacks continue to evolve, your threat landscape will, too.

Step 2: Prioritize Assets

After documenting the types of attacks that your organization is most likely to experience, determine which assets, data, networks, systems, and resources are most critical to business operations. If damaged, lost, or stolen, what would cause the organization to undergo heavy loss? Once you have identified your essential assets, prioritize them according to their criticality.

Step 3: Develop and Implement Policies and Procedures

Businesses must have documented policies and procedures in place to ensure that all parties know what needs to be done when, where, and how, should an incident occur. These policies and procedures support the IRP and ensure it is effective. At a minimum, each policy should contain the following criteria:

- **Responsible Parties**— Assigns roles and responsibilities for the IR team
- **Purpose**— Details the intent and function of each policy
- **Scope**— Defines the environment to which each policy applies
- **Disciplinary Actions**— Describes consequences for noncompliance
- **Definitions**— Defines the meaning of each policy and its associated terms
- **References | Documents | Forms**— Provides reference material and supporting information for each policy
- **Exceptions**— Lists any exceptions to the policy

> "Nearly three-quarters of organizations don't have a consistent, enterprise-wide cybersecurity IRP. Yet, organizations with IR teams and testing had an average data breach cost **USD 2.46 million** lower than those with no IR team and no IR plan testing."[5]

Step 4: Create an Incident Response Team

Once policies and procedures have been developed and approved, it is critical to establish a dedicated IR team that will coordinate breach response efforts. When establishing your team, consider:

- **Composition**— Do you need different IR teams for different kinds of attacks?
- **Roles**— Who will be responsible for specific tasks, such as testing the IRP?
- **How to operationalize the IR policy**
- **Resources, technology, and tools available** to the IR team for identifying and recovering impacted data and systems

When developing your team, take into account all aspects of your organization, and ensure team members have a clear understanding of their roles. Establishing responsibilities beforehand reduces stress and time when responding to a security incident.

Step 5: Establish a Documented and Standardized Incident Response Plan

Establishing an effective IRP is an organization-wide effort. Both business and security leadership must make IR planning a priority and collaborate with the IR teams to execute response actions in accordance with formal policies and procedures. IRPs will only be successful if everyone involved knows their roles and responsibilities. Take time to hold regular meetings to discuss the IRP and ensure all parties involved are on the same page. By revisiting the plan frequently, your team will have a documented, systematic, and effective plan of action in the event of a cyberattack.

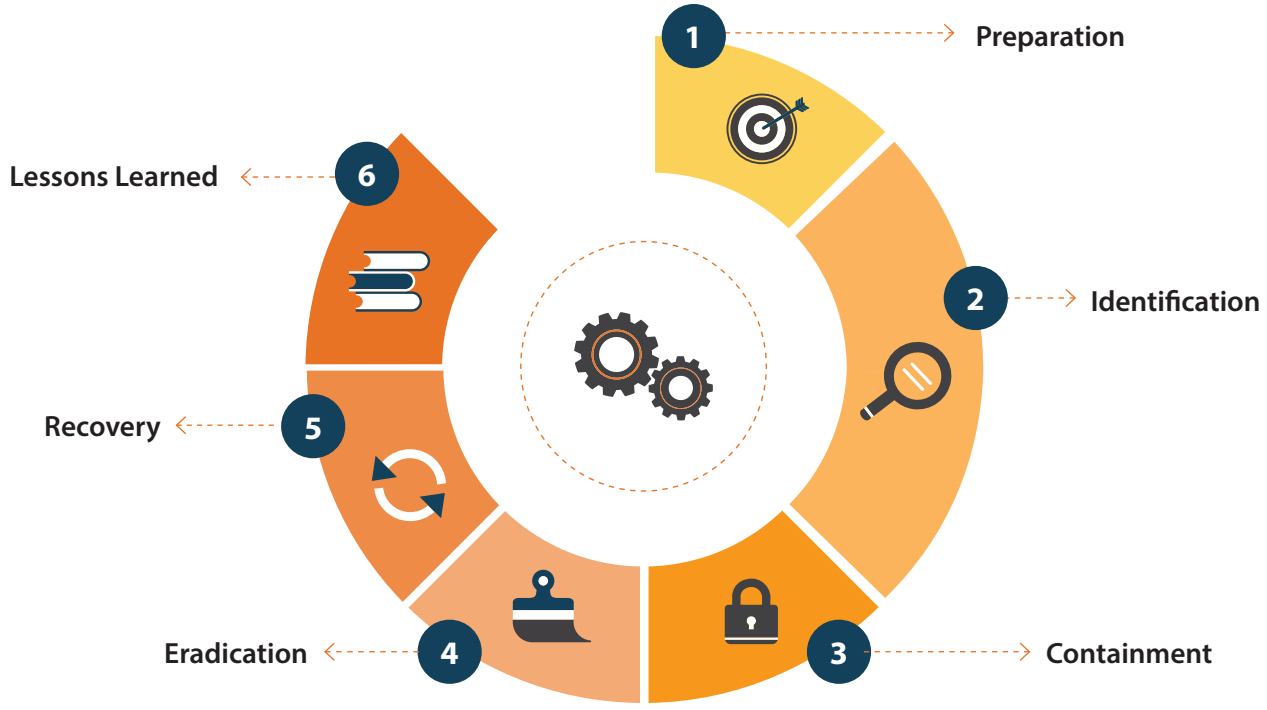
Step 6: Continuously Test, Improve, and Build Upon Incident Response Processes

Establishing an IRP is only the beginning. The major question is: does it work? Many compliance regulations, including the Payment Card Industry (PCI) Data Security Standards (DSS), IRS Publication 1075, and Federal Financial Institutions Examination Council (FFIEC) standards, require at least annual testing of the IRP to ensure the proper policies and procedures are in place and that training and security awareness are adequate to respond to security incidents. Even if your organization's compliance requirements do not include IRP testing, it is important that the plan be tested to ensure it functions efficiently and effectively in the event of an unexpected attack.

PHASES OF AN INCIDENT RESPONSE PLAN

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-61 provides guidelines on how to create effective IR strategies, how to select the best model for your organization's IR team, and best practices for operating your team.

When developing an IRP, there are six phases within the response and recovery process that must be addressed:



Phase 1: Preparation

The preparation phase for developing an IRP usually takes the most effort, but is the most crucial aspect in the development cycle, especially if a formal IRP is not already in place. This phase will include:

- Creating documented IR policies
- Defining communication guidelines
- Training employees in their roles and responsibilities
- Cyber hunting exercises
- Threat detection capabilities

The IRP must be tested in mock drills to ensure that all employees involved can perform their duties efficiently with minimal error.

Phase 2: Identification

During the identification phase, the security team must determine whether or not the organization is actually under attack. If there has been a real breach and not a false positive, the team must determine:

- When did the event take place?
- Does it impact operations?
- Has the point of entry been discovered?

Addressing important questions such as these will enable the team to determine the type of attack and what steps must be taken to get it under control.

Phase 3: Containment

In the containment phase, the plan must address how the organization can stop an attack before it spreads and causes even more damage. Containment should address solutions for both:

- Short term— to limit damage before the incident gets worse, usually by isolating network segments, taking down the hacked production server, and routing to failover systems.
- Long term— to bring production systems back online, applying temporary fixes, if necessary, removing accounts or backdoors left on systems by the attackers, and addressing root causes, such as fixing a broken authentication mechanism.[6]

Phase 4: Eradication

Once containment has been achieved, the organization needs to locate and eliminate the root cause of the breach. The most important aspect of this phase is that the organization must be thorough in eradicating all traces of the attack. If any trace of the security breach remains, your organization may still be at risk of losing valuable data.

Phase 5: Recovery

Recovery phase activities focus on implementing strategies to restore system capabilities, repair damage, and resume operational capabilities at the original or an alternate location. At the completion of the recovery phase, the systems will be functional and capable of performing their respective functions.[7]

Phase 6: Lessons Learned

Once business operations return to normal after a cyberattack, it is crucial to analyze the incident and the organization's response to it in order to improve procedures and update the plan for future incidents. Are there elements of security that need to be improved? Should staff receive additional or different training? What processes could have run more smoothly, and which ran well? The lessons learned process will strengthen the organization's systems, staff, and ability to respond to future attacks.

> "The NIST process emphasizes that incident response is not a linear activity that starts when an incident is detected and ends with eradication and recovery. Rather, incident response is a cyclical activity, where there is continuing learning and improvement to discover how to better defend the organization."[8]

NEXT STEPS

Have an incident response strategy and plan in place?

Keep your IR strategy forward-facing, your IRP fresh, and your team members trained and up-to-date. Organizations, IT environments, and staff change. We suggest conducting tabletop exercises regularly, as often as once a quarter, to ensure new team members have practice and that all team members know how to respond within the current organizational structure. Regular testing will help you to identify and close knowledge or communication gaps and will keep security awareness in the forefront. You can conduct these exercises yourself or hire an independent cybersecurity firm to facilitate them. The latter will allow all security team members to participate and will provide an unbiased opinion of the organization's strategies and response processes.

Don't have an incident response strategy and plan in place?

The amount of effort, time, and resources necessary to develop an IRP may seem daunting, but you have options. A third-party firm can bring an objective eye to the task and will work with your IT team to develop a strategy and plan that fits your IT and business requirements and objectives.

If your organization prefers to work independently, there are numerous templates available online, including the:

- CISA: Cybersecurity Incident & Vulnerability Response Playbooks[9]
- NIST: Computer Security Incident Handling Guide[10]
- AICPA: Incident Response Plan: Template for Breach of Personal Information[11]

There is no one-size-fits-all solution when it comes to IR planning. Each organization must take into account its unique threat landscape, risk appetite, and IT and business requirements, then develop procedures that support efficient response, minimize impact, and help business operations return to normal.

> "An effective incident response will start well in advance of an actual detection of any incident or crisis. The time an organization spends on preparation and planning before an incident occurs can minimize the impact and exposure during an incident."[12]

CONCLUSION

Not If, But When

Responding to security incidents is infinitely more effective with a solid plan of action, in which roles and responsibilities, detection and eradication methods, and preventive measures are clearly defined. By developing an IR strategy and plan in advance of an incident, organizations will have a clear view of their threat landscape, critical assets, and processes and procedures each department can follow to ensure that business operations return to normal with as minimal damage as possible.

As the cyber landscape continues to develop, threats will become increasingly prevalent, sophisticated, and dangerous. The question has become not if, but when your organization will fall prey to an attack. Having an effective IR strategy in place is the key to combating and minimizing the impact of any cyber incident.

ABOUT SECURANCE

Securance has two decades of experience helping organizations combat evolved cyber threats, build effective risk management programs, align with compliance standards, and increase operational efficiency. Our comprehensive approach integrates proven methodologies, dependable expertise, and each customer's unique requirements to maximize the benefits and long-term value of each assessment.

SOURCES

1. https://industrialcyber.co/ransomware/comparitech-reveals-drop-in-ransomware-attacks-in-2024-though-breached-records-may-increase/?utm_source=chatgpt.com
2. https://news.sophos.com/en-us/2024/08/14/the-state-of-ransomware-in-state-and-local-government-2024/?utm_source=chatgpt.com
3. https://www.netlabsglobal.com/protecting-your-organization-against-ransomware-attacks/
4. https://www.securitymetrics.com/blog/6-phases-incident-response-plan
5. https://www.ibm.com/security/incident-response?utmcontent=SRCWW&p1=Search&p4=43700068113287379&p5=p&gclid=c31676f6d8731cc57c1a144f05692847&gclsrc=3p.ds#citation1
6. https://www.criticalstart.com/incident-response-101-what-to-expect-before-during-and-after-a-breach/#:~:text=Short-term%20containment%E2%80%94limiting%20damage%20before%20the%20incident%20gets%20worse%2C,%28s%29%20and%20then%20wiping%20and%20reimaging%20the%20systems.
7. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf
8. https://www.cynet.com/incident-response/nist-incident-response/
9. https://www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf
10. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
11. https://www.aicpa.org
12. https://www.mcafee.com/enterprise/en-us/assets/white-papers/wp-10-ways-prepare-incident-response.pdf

Prepared for Peril: Incident Response Solutions to Combat Ransomware and Cyber Threats

SECURANCE CONSULTING
Advantage of Insight AI

13916 Monroes Business Park, Suite 102 • Tampa, FL 33635 • 877.578.0215
www.securanceconsulting.com