UNITRENDS
A Kaseya COMPANY

eBook

THE IT MANAGER'S INCIDENT RESPONSE PLANNING GUIDE

Introduction

Organizations across industries are rapidly adopting technology for smooth business operations. As technology advances, so do cybersecurity threats. With the average cost of a data breach pegged at $4.88 million per incident, and cybersecurity experts forecasting an upturn in the quantity and quality of hacks, organizations will undoubtedly seek help to ensure they are prepared to battle this threat.[1]

Cyberattacks hurt business and test customer trust, impacting revenue and reputation. To counter this, an incident response plan (IRP) can help organizations be prepared should the worst occur. However, an IRP can be an incredibly detailed, difficult and overwhelming process to manage when you're trying to quickly restore business operations.

This eBook will answer the most pertinent IRP-related questions to empower IT pros to create an effective incident response plan and prepare organizations to face an unpredictable threat landscape.

What is an incident response plan?

The National Institute of Standards and Technology (NIST) defines an incident response plan (IRP) as:

The documentation of a predetermined set of instructions or procedures to detect, respond to and limit consequences of malicious cyberattacks against an organization's information system(s).[2]

In other words, an IRP is the methodology used to detect, contain and recover from an incident. It minimizes direct and indirect costs like downtime costs, recovery costs and loss of brand reputation. Ideally, an IRP should be part of your overall business continuity and disaster recovery (BCDR) strategy.

What should an incident response plan address?

An incident response plan should address the following components:

How incident response supports the organization's overall mission

Define what a "security incident" means to the business and its potential impact. A good practice is to have the IRP align with relevant frameworks (NIST or ISO 27001) and comply with regulations that govern the industry, such as GDPR and HIPAA.

The incident response approach

Define the scope of the IRP and communicate which specific attacks and incidents this plan addresses. An organization's response to a social engineering attack and an insider threat incident may vary. Based on the organization's tolerance of risk, you should also determine how often the plan should be reviewed, updated and practiced. Your incident response (IR) plan should include:

1. Detection & analysis

Leverage solutions like antivirus and security information and event management (SIEM) systems to receive alerts, and monitor and detect potential security incidents based on predefined criteria. This step ensures quick activation of the IRP by analyzing and confirming suspicious activities.

2. Containment

This phase is critical for mitigating an incident's impact. For short-term containment, you must isolate affected systems to prevent the threat from spreading across the network. For long-term containment, set up temporary fixes or segmented environments to keep operations running during issue resolution.

3. Eradication

The eradication step focuses on identifying and completely removing the root cause and all traces of a security incident from the affected environment. This step helps to better understand the cause of an incident, security measures are strengthened and ensures the threat cannot recur or persist in the system.

4. Recovery of systems

After containing the incident and eradicating the threat, it is critical to restore affected systems to normal operations as quickly as possible. This step includes applying necessary updates, testing functionality and monitoring to confirm that the systems are secure and operational.

5. Post-incident activities

Post-incident activities are essential for gaining a deep understanding of the security incident and improving your organization's incident response plan.

What should an incident response plan address?

Lessons learned

Conduct a thorough review of the incident to analyze what went well and what could be improved. This analysis will help identify gaps in your IR process or solutions. Document key findings to improve your organization's readiness and response to future incidents.

Reporting and documentation

Create detailed reports about the incident, actions taken and outcomes. Comprehensive reporting and documentation are essential for meeting compliance requirements and justifying cyber insurance claims. These reports can also be used as a reference for future incident management.

Policy updates

Use the findings from the incident to update security policies, procedures and training materials. Ensure that any newly identified vulnerabilities are addressed and incorporate changes into your organization's incident response framework.

Testing and training

Testing and training are vital for effectively managing and mitigating cybersecurity incidents. A well-trained team can identify, contain and resolve incidents efficiently.

Simulation exercises

Conduct regular simulation exercises to mimic real-world incidents. These tests will help identify weaknesses in the response process, ensure the IRT is ready and enable you to handle actual incidents efficiently.

Ongoing training

Provide continuous training for employees and the IRT to keep them informed of emerging threats, new solutions and best practices. Regular training will ensure all team members are equipped with the skills and knowledge needed to respond to incidents effectively.

Roles and responsibilities

Mention the incident response team (IRT) members and their assigned responsibilities. Include names, roles, contact information and replacements when members are unavailable. Also include details of the person who will act as the liaison between internal and external stakeholders.

Communication methods

The IRP should include all the communication methods that will be used for internal and external communication. It should also include templates for making public statements to address an incident, damages, remediation measures taken and post-incident steps.

Key metrics

Define metrics to evaluate the effectiveness of the plan. The metrics will help report the efficacy of the IRP and whether changes need to be made to improve response time if a similar incident occurs.

Who should use an incident response plan?

Back in the day, an IRP was an optional safeguard. However, new cybersecurity compliance standards emerging in all industries have led to the high demand for IRPs to strengthen overall security. For organizations in the credit card or healthcare industries, it is mandatory to have an incident response plan in place.

Importance of an incident response plan

An IRP provides a framework to minimize the duration and damage of security incidents. It also identifies stakeholders, streamlines digital forensics, helps avoids bad press and customer churn, and improves recovery time. A lack of an IRP or a poorly crafted one leaves businesses scrambling during a crisis. Failure to have a finely tuned, orchestrated response hamstrings an organization's ability to respond, ultimately harming the business.

A thorough IRP will help your organization:

Avoid reputational damage

According to the Cost of a Data Breach Report 2024, 70% of organizations faced major disruptions to their business due to a breach.[3] Companies that have suffered a breach or failed to protect customer data in any way find business hard to come by as customers may seek out alternative providers due to lack of confidence. Publicly traded companies, while often larger and equipped with the resources to dedicate to crisis management, still lose both market value and share price following a publicized data breach. Investing in preventative measures before a breach occurs not only reduces the risk of harm, but it will likely garner a more sympathetic reaction if the organization can show an incident occurred despite ample procedures and defenses in place.

An IRP improves response time and risk management as well as facilitating PR planning in order to keep stakeholders and the public informed, ensuring brand reputation remains intact during and after an incident.

Curtail data theft

Data is the crown jewel of your business. Stolen data is highly coveted by hackers who may look to leverage it for extortion, sell it on the dark web or use stolen credentials and data for further wrongdoing. Account takeover (ATO) attacks are common cybercrimes that involve identity theft. Cybercriminals steal or buy online credentials in third-party breaches and then reuse them to gain easy access to corporate networks to steal data. ATO attacks generally lead to intellectual data theft, resulting in companies losing years of R&D investment in trade secrets or copyrighted material as well as their competitive advantage.

In recent years, extortion events have become significantly more common compared to traditional ransomware attacks involving encryption and ransom demands.

An IRP serves as a helpful resource in the event credentials are compromised, providing steps to secure accounts at risk, as well as defining gaps that may be addressed through implementation of additional controls and hardening of the security environment.

Minimize financial losses

When a business suffers a breach or a security incident, it experiences a sudden drop in revenue; critical operations may be paused or impacted, preventing an organization from transacting as usual. When an incident becomes public, cautious customers may jump ship to a competitor. Financial damages are compounded if the business ends up paying ransoms or giving in to extortion demands, having to draw from a reduced cash flow to recover stolen data in order to resume operations.

The direct cost a business incurs right after an attack can be better understood with the following equation:

TOTAL DIRECT COST =

Loss from attack (like ransomware or hardware malfunction)

+

Working hours investigating attacks

+

Loss from potential attacks

An IRP details and establishes mechanisms for proactive monitoring of users, accounts, devices, networks and more. Implementing controls for early detection and response to a cyber incident reduces the impact of an incident on a company's direct revenue.

Avert fines and penalties

Data protection and privacy laws require you to manage the security of all personal data, regardless of whether it belongs to staff or customers. With mandates such as GDPR and CCPA, the need for compliance is extended across industries, in addition to industry-specific regulations as set forth by FERPA and HIPAA. Penalties and fines are assessed to non-compliant entities and with that comes a pile of legal paperwork, court sessions and potential civil lawsuits. In many cases, the legal fees exceed the penalty itself.[4]

An IRP helps to deploy appropriate and timely response to contain and remediate an incident or breach that may lessen or avoid fines and regulatory sanctions.

Compliance legislation	Penalties
HIPAA	Fines of up to $250k and 10 years imprisonment.
GDPR	Fines of up to €20 million or 4% of the total global turnover of the previous fiscal year, whichever is higher.
CCPA	Civil penalties of up to $7,500 for each violation. The maximum fine for other violations is $2,500 per violation.

The incident response team

The incident response team (IRT) is the first point of contact when a cyber incident occurs. The team manages the incident and sets clear communication with internal and external stakeholders. An incident response team generally contains representatives from both the management and technical side.

The core responsibilities of an IRT are to:

- Create and maintain an IR plan
- Analyze the security incident
- Manage internal communications and alerts whenever an incident occurs
- Offer easy communication with stakeholders and the press whenever needed
- Mitigate the security incident
- Create a summary report to document the incident and actions taken
- Provide recommendations for improving IRT efficiency

An IRT extends beyond simply incident response information technology (IT) personnel. A well-constructed team will draw from other departments to fulfill roles, including:

Incident response manager

Supervises and prioritizes actions during detection, containment and recovery from an incident.

Cyber incident response team (CIRT)

Offers specialized technical skills to provide the right advice and threat analysis.

Security analysts

Supports and works directly with affected resources, implementing and maintaining technical and operational controls.

Threat researchers

Provides threat intelligence and context around security incidents, which help identify current and future threats.

Management

Brings top-level management buy-in, which is necessary for the provision of resources for incident response planning and execution.

Human resources

HR is involved when it is a case of malicious insiders or employee error.

Audit and risk management specialists

Develops threat metrics and vulnerability assessments while encouraging best practices across the organization.

Legal

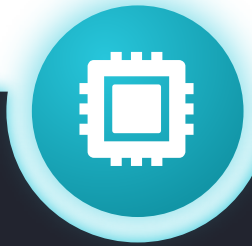
Ensures any evidence collected maintains its forensic value if the company chooses to take legal action.

Public relations

Enables communication with internal and external stakeholders.

Challenges to developing an incident response plan

Developing a perfect incident response plan is way more challenging than one might think.



The technology fallacy

Incident response planning often focuses on technology — maybe a little too much. Using tools to develop an IRP is effective only when all IRT members know how to use them. The tools might end up being underutilized or used in the wrong manner, leading to unexpected costs both at the onset and down the road.

Team dynamics

An IRT consists of different team members, from network administrators to senior management. The goal is to address technical vulnerabilities and make prompt business decisions simultaneously. This requires solid team dynamics from members who might operate with different mindsets and leadership styles.

Constant reiterations

IRP templates should be customized to adapt to the current needs of the business. In building your IRP, establish a cadence for how frequently the IRP will be reviewed. It's recommended to review your IRP at minimum any time changes are made to personnel or systems. Protocols around mission-critical infrastructure and applications may be reviewed more frequently. Unfortunately, whether struggling to keep up with the sheer volume of day-to-day projects and alerts or limited budgets and resources, IRTs aren't able to evaluate and practice as often as they should. As a result, the organization is left with an inefficient, unmanaged, untested and underutilized plan.

Incident response plan best practices

Here are some best practices to follow to deploy the most effective incident response plan.

Improve asset management

IRT members should be trained across the entire tool suite periodically. Tools should be regularly assessed to determine if they can address current threats. Maintain a centralized location and establish a process to ensure timely license renewals and functional component upgrades. This allows proper utilization of IRP tools and improves member trust with the process, leading to smooth IRP execution.

Keep communication in one place

Maintain a centralized communication platform where the IRT can post details about the current investigation, results of the investigation and the business decisions taken based on the results. Unnecessary emails and chats should be petered out to prevent missed messages, conflicting information and team tension. The platform should also clearly mention the roles and responsibilities of each member so as to improve team communication and collaboration.

Test, test, test

Frequently put your IRP into action before a real incident occurs, or in other words, test your plan. Testing your IRP avoids any rude surprises that might occur when a disaster strikes. Smart businesses have started adding testing as part of their IRP. Testing outlines the various readiness and recovery tests with corresponding steps and procedures. It provides reassurance that a business can respond to an incident on time.

Putting an IRP into action

The SANS institute outlines a six-step plan for incident response.[5] Below is a brief summary and includes the questions that need to be asked to successfully execute each of the steps.

Preparation

Preparation helps organizations determine how well their incident response team will respond to an incident. It determines policy, response plan/strategy, communication, documentation, determining the CIRT members, access control, tools and training.

Questions to ask:

- Has everyone been trained in security policies?
- Have the security policies and incident response plan been approved by management?
- Is the IR team aware of their roles and responsibilities?
- Did the IR team conduct mock drills?

Identification

Identification is the process of detecting a breach and enabling a rapid response. The IR team uses threat intelligence streams, intrusion detection systems and firewalls to classify an incident as a breach that requires prompt action.

Questions to ask:

- When did the incident happen?
- Who discovered the incident and how?
- Have any other areas been impacted?
- What is the scope of the incident?
- Does it affect operations?
- Has the source of the incident been discovered?

Containment

This process involves containing the damage and preventing further damage from occurring. It can be accomplished by taking specific sub-networks offline and spinning up system backups to ensure uninterrupted business operations.

Questions to ask:

- What's been done to contain the breach short term?
- What's been done to contain the breach long term?
- Has any discovered malware been quarantined from the rest of the environment?
- What sort of backups are in place?
- Have all access credentials been reviewed and changed?
- Does the system have the latest security patches and updates?

Eradication

Eradication is the phased removal and restoration of systems affected by the security incident to their previous state. It might involve secondary monitoring to fix vulnerabilities, if any, on the affected systems.

Questions to ask:

- Has the malware been securely removed?
- Has the system been patched up?
- Can the system be re-imaged?

Recovery

Test, monitor and validate systems, and bring those affected back into the production environment cautiously to ensure they don't lead to another incident. This requires setting timelines for full restorations as well as continued monitoring for any abnormal network activity.

Questions to ask:

- When can the systems return to production?
- Have the systems been tested and patched?
- Can the systems be restored from a trusted backup?
- How long and what parts of the affected systems will be monitored?
- What solutions will stop similar attacks from recurring?

Lessons learned

This final step helps educate and improve future incident response efforts. The IRP is updated with information that may have been missing, omitted or incomplete prior to the incident, as well as with complete documentation of remediation efforts to provide insight for a future response.

Questions to ask:

- What changes need to be made to security?
- How should employees be trained differently?
- What weakness did the breach exploit?
- How will you ensure a similar breach doesn't happen again?

The power of Unitrends Unified BCDR

Unitrends provides a range of business continuity and disaster recovery (BCDR) solutions that empower IT pros to detect, prevent and mitigate security threats.

Backup & Disaster Recovery

Unitrends provides comprehensive protection for hundreds of versions of operating systems, hypervisors and applications. Whether the infrastructure consists of physical machines or virtual servers, IT professionals can protect digital assets locally while replicating data to alternate media, such as disk, tape or cloud, for secondary and tertiary backups.

In addition, Unitrends leverages a hardened Linux architecture to strengthen security and minimize vulnerabilities, making Unitrends' backup appliances resistant to Windows-based malware. Our solutions come equipped with advanced ransomware detection features, enabling early identification and prevention of malicious activities. Unitrends also supports automated disaster recovery (DR) runbook testing, reducing the burden on the IR and IT teams by eliminating the need for manual testing. These advanced capabilities ensure streamlined, secure and efficient protection for your critical systems and data.

Dark Web Monitoring

Proactive exposure and credentials monitoring alerts admins to compromised or stolen credentials found on the dark web. IT pros can bring this to the end user's notice, hardening the account and reviewing proper cybersecurity hygiene in order to secure those accounts before any malicious activity occurs. Dark Web Monitoring reduces the risk of an ATO, protecting businesses from potential financial and competitive impacts, thereby minimizing the chance of a significant data loss incident requiring a costly, resource intensive recovery and restoration effort.

Disaster Recovery-as-a-Service

In the event your data center goes down or you're unable to reach it, you can failover invisibly into the Unitrends Cloud with Disaster Recovery-as-a-Service (DRaaS). The Unitrends team does all the heavy lifting, which includes implementation, onboarding, failover and recovery of service, and failback to your local data center once operations are ready to be resumed.

Disaster Recovery Testing

Automate testing for disaster recovery by spinning up backups in an isolated lab environment and testing against services and applications. Server performance and compliance tracking (RTO, RPO actuals) are reported to provide full visibility into what recovery looks like.

To learn how Unitrends Unified BCDR can boost your incident response strategy,

CONTACT SALES TODAY!

Sources

1. and 3. https://www.ibm.com/security/data-breach
2. https://csrc.nist.gov/glossary/term/incident_response_plan
4. https://spanning.com/resources/ebooks/best-practices-for-microsoft-365-business-continuity-ebook/
5. https://www.techrepublic.com/article/cybersecurity-incident-response-the-6-steps-to-success/

ABOUT UNITRENDS

Unitrends makes efficient, reliable backup and recovery as effortless and hassle-free as possible. We combine deep expertise gained over thirty years of focusing on backup and recovery with next generation backup appliances and cloud purpose-built to make data protection simpler, more automated and more resilient than any other solution in the industry.

UNITRENDS
A Kaseya COMPANY