IT Security Incident Response Plan Template

IT Security Incident Response Plan

Introduction

This template provides the starting point for creating your organization's IT Security Incident Response (IR) Plan. It's meant to help your organization be better prepared for taking action in the event of an IT security event such as a cyberattack. It incorporates industry best practices and can easily be customized to meet your organization's needs.

Note: Guidance for creating your IR Plan is italicized in the template and should be deleted once you've customized the plan to best suit your organization. Information that should be customized is highlighted.

Executive Summary

To maintain the trust of all stakeholders – employees, customers, and partners – and meet regulatory requirements, it's imperative that we to protect our organization's critical IT assets in the event of IT security event. The better prepared we are, the faster we can mitigate any threats or potential impact on our operations.

This document describes the plan for responding to IT security incidents at It explains how to detect and react to cybersecurity incidents and data breaches, determine their scope and the potential risks, respond appropriately and quickly, and communicate appropriate information to all stakeholders.

Effective incident response requires the participation of all parts of our organization, including IT, legal, technical support, finance, human resources, corporate communications, and business operations. It's important that everyone reads and understands their respective roles as well as the ways they should coordinate with others.

This plan will be updated to reflect organizational changes, new technologies and new compliance requirements that inform our cybersecurity strategy. We will conduct regular testing of this plan to ensure everyone is fully trained to participate in effective incident response.

Contact Information Chart

The IR Plan covers all personnel, including employees, temporary staff, consultants, contractors, suppliers and third parties operating on behalf of All personnel are referred to as 'staff' in the plan.

The following details the roles and responsibilities of each member of to prevent and respond to an IT security incident. *[Add additional information as appropriate.]*

IR Team Lead Responsibilities

- Making sure that the IR Plan and associated response and escalation procedures are defined and documented.
- Making sure that the IR Plan is current, reviewed and tested
- Making sure that staff with IR Plan responsibilities are trained with periodic reviews and/ or updates as appropriate.
- Leading the investigation of a suspected breach or reported security incident and initiating the IR Plan when needed.
- Reporting to and working with external parties, including business partners, legal representation, law enforcement, etc., as required.
- Authorizing on-site investigations by appropriate law enforcement or third-party security/forensic personnel, as required during any IT security incident investigation. This includes authorizing access to/ removal of evidence from site.

Incident Response Team Members

- Making sure all staff understand how to identify and report a suspected or actual IT security incident.
- Advising the IR Lead of an incident when they receive an incident report from staff.
- Investigating and documenting each reported incident.
- Taking action to limit the exposure of sensitive data and to reduce the risks that may be associated with any incident.
- Gathering, reviewing, and analyzing logs and related information from various central and local safeguards, security measures and controls.
- Documenting and maintaining accurate and detailed records of the incident and all activities that were undertaken in response to an incident.
- Assisting law enforcement, if law enforcement is involved, during the investigation. This includes any forensic investigations and prosecutions.
- Initiating follow-up actions to reduce likelihood of recurrence, as appropriate.
- Determining if policies, processes, technologies, security measures or controls should be updated.

Staff Member Responsibilities

- Making sure they understand how to identify and report a suspected or actual security incident.
- Reporting a suspected or actual security incident to the IR Lead or another member of the IR Team.
- Reporting any security related issues or concerns to line management, or to a member of the IR Team
- Complying with the security policies and procedures of

Roles, Responsibilities and Contact Information

[Customize the list that follows to meet the size, structure, and regulatory and industry requirements of your organization. Include contact information for everyone involved in incident response, both internally and externally. It should be periodically reviewed and updated. Keep a hard copy of the incident response plan and contact information accessible.]

ROLE	RESPONSIBILITIES	CONTACT INFORMATION
INFORMATION TECHNOLOGY/INFORMATION SECURITY		
CSO / CISO	Strategic lead. Develops technical, operational, and financial risk ranking criteria used to prioritize incident response plan. Authorizes when and how incident details are reported. Main point of contact for executive team and Board of Directors (if applicable).	*Name* *Phone* *Email*
Incident Response Team Lead and Team Members	Central team that authorizes and coordinates incident response across multiple teams and functions through all stages of a cyber incident. Maintains incident response plan, documentation, and catalog of incidents.	*Name* *Phone* *Email*

	Responsible for identifying, confirming, and evaluating the extent of incidents. Conducts random security checks to ensure readiness to respond to a cyberattack.	
Identity and Access Team Lead and Team Members	Responsible for privilege management, enterprise password protection and role-based access control. Discovers, audits, and reports on all privilege usage. Conducts random checks to audit privileged accounts, validate whether they are required, and re-authenticate those that are. Monitors privileged account users and proactively checks for indicators of compromise, such as excessive logins, or other unusual behavior. Informs incident response team of potential attacks that compromise privileged accounts, validates and reports on the extent of attacks. Takes action to prevent the spread of a breach by updating privileges.	*Name* *Phone* *Email*
IT Operations and Support (internal)	Manages access to systems and applications for internal staff and partners. Centrally manages patches, hardware and software updates, and other system upgrades to prevent and contain a cyberattack.	*Name* *Phone* *Email*

Technical Partners *(ISP, MSP, Hosting, Testing Partners, etc.)* *Third Party External Incident Response Teams*	Manages security controls to limit the progression of a cyberattack across third-party systems and organizations. Coordinates with IR Team to manage risks. Professional Incident response teams help ensure a solid Incident Response process is followed. It is highly recommended that the company identify and prepare an External Response Team that can be available in an emergency IR situation and provide any requested information prior to an emergency to help them become familiar with your environment.	*Name* *Phone* *Email* *Name* *Phone* *Email*
COMPLIANCE		
Legal Counsel	Confirms requirements for informing employees, customers, and the public about cyber breaches. Responsible for checking in with local law enforcement. Ensures IT team has legal authority for privilege account monitoring.	*Name* *Phone* *Email*
Audit & Compliance	Communicates with regulatory bodies, following mandated reporting requirements.	*Name* *Phone* *Email*
Human Resources	Coordinates internal employee communications regarding breaches of personal information and responds to questions from employees.	*Name* *Phone* *Email*

Regulatory Contacts	Receives information about a breach according to timeline and format mandated by regulatory requirements.	*Name* *Phone* *Email*
COMMUNICATIONS		
Marketing & Public Relations Lead	Communicates externally with customers, partners, and the media. Coordinates all communications and request for interviews with internal subject matter experts and security team. Maintains draft crisis communications plans and statements which can be customized and distributed quickly in case of a breach.	*Name* *Phone* *Email*
Web & Social Media Lead	Posts information on the company website, email, and social media channels regarding the breach, including our response and recommendations for users. Sets up monitoring across social media channels to ensure we receive feedback or questions sent by customers through social media.	*Name* *Phone* *Email*
Technical Support Lead (Internal)	Provides security bulletins and technical guidance to employees in case of a breach, including required software updates, password changes, or other system changes.	*Name* *Phone* *Email*
Technical Support Lead (External)	Provides security bulletins and technical guidance to external users in case of a breach.	*Name* *Phone*

		Email
OTHER		
		Name *Phone* *Email*
		Name *Phone* *Email*
OTHER		
		Name *Phone* *Email*
		Name *Phone* *Email*

Testing and Updates

The Incident Response Plan will be tested Testing includes walkthroughs and practical simulations of potential incident scenarios to identify process gaps and improvement areas and help ensure understanding of the incident response processes.

The IR team will record observations made during the testing, including processes that were poorly or incorrectly executed or misunderstood by participants, and identify areas requiring improvement.

The IR Lead will ensure the IR plan is updated, distributed to IR team members and reviewed with them.

IR Process Overview

The following is the six-step process defined by the SANS Institute in their Incident Handler's Handbook:

1. **Preparation**. Review and codify an organizational IT security policy, perform a risk assessment, identify sensitive assets, define which are critical security incidents the team should focus on, and build an IT Security Incident Response Team.
2. **Identification**. Monitor IT systems and detect deviations from normal operations and see if they represent actual security incidents. When an incident is discovered, collect additional evidence, establish its type and severity, and document everything.
3. **Containment**. Perform short-term containment, for example by isolating the network segment that is under attack. Then focus on long-term containment, which involves temporary fixes to allow systems to be used in production, while rebuilding clean systems.
4. **Eradication**. Remove malware from all affected systems, identify the root cause of the attack, and take action to prevent similar attacks in the future.
5. **Recovery.** Bring affected production systems back online carefully to prevent additional attacks. Test, verify and monitor affected systems to ensure they are back to normal.
6. **Lessons learned.** No later than two weeks from the end of the incident, perform a retrospective of the incident. Prepare complete documentation of the incident, investigate the incident further, understand what was done to contain it and whether anything in the incident response process could be improved.

Incident Response Checklist

[*The following is a reporting template to use for documenting the steps and documentation gathered during your review and response to a cyber incident involving privileged accounts. Make updates to reflect your approved process and the tools you use. Add a responsible party for each step now, so everyone knows what data they need to gather and steps to take when an incident happens*.]

To demonstrate and improve the effectiveness of 's IR team and security tools, requires a record of all actions taken during each phase of an incident. Supporting documentation is required, including all forensic evidence collected such as activity logs, memory dumps, audits, network traffic, and disk images.

INCIDENT PHASE	ACTION	TEAM MEMBER/ SYSTEM	DAY/TIME ACTION TAKEN
Discovery/ Confirmation	Describe how the team first learned of the attack (security researcher, partner, employee, customer, auditor, internal security alert, etc.).		
	Analyze audit logs and security applications to identify unusual or suspicious account behavior or activities that indicate a likely attack and confirm attack has occurred.		
	Describe potential attacker, including known or expected capabilities, behaviors, and motivations.		
	Identify access point and source of attack (endpoint, application, malware downloaded, etc.) and responsible party.		
	Prepare an incident timeline to keep an ongoing record of when the attack occurred and subsequent milestones in analysis and response.		

INCIDENT PHASE	ACTION	TEAM MEMBER/ SYSTEM	DAY/TIME ACTION TAKEN
	Check applications for signatures, IP address ranges, files hashes, processes, executables names, URLs, and domain names of known malicious websites.		
	Evaluate extent of damage upon discovery and risk to systems and privileged accounts. Audit which privileged accounts have been used recently, whether any passwords have been changed, and what applications have been executed. (See Appendix A for more information on Threat Classification).		
	Review your information assets list to identify which assets have been potentially compromised. Note integrity of assets and evidence gathered. (See Appendix A for more information on Threat Classification).		
	Diagram the path of the incident/attack to provide an “at-a-glance” view from		

INCIDENT PHASE	ACTION	TEAM MEMBER/ SYSTEM	DAY/TIME ACTION TAKEN
	the initial breach to escalation and movement tracked across the network.		
	Collect meeting notes in a central repository to use in preparing communications with stakeholders.		
	Inform employees regarding discovery.		
	Analyze incident Indicators of Compromise (IOCs) with threat intelligence tools.		
	Potentially share information externally about breach discovery. You may choose to hold communications during this phase until you have contained the breach to increase your chances of catching the attacker. If so, make sure this aligns with your compliance requirements.		
Containment/Continuity	Enable temporary privileged accounts to be used by the technical and security team to quickly access and monitor systems.		

INCIDENT PHASE	ACTION	TEAM MEMBER/ SYSTEM	DAY/TIME ACTION TAKEN
	Protect evidence. Back up any compromised systems as soon as possible, prior to performing any actions that could affect data integrity on the original media.		
	Force multi-factor authentication or peer review to ensure privileges are being used appropriately.		
	Change passwords for all users, service, application, and network accounts.		
	Increase the sensitivity of application security controls (allowing, denying, and restricting) to prevent malicious malware from being distributed by the attacker.		
	Remove systems from production or take systems offline if needed.		
	Inform employees regarding breach containment.		
	Analyze, record, and confirm any instances of		

INCIDENT PHASE	ACTION	TEAM MEMBER/ SYSTEM	DAY/TIME ACTION TAKEN
	potential data exfiltration occurrences across the network.		
	Potentially share information externally regarding breach containment (website updates, emails, social media posts, tech support bulletins, etc.).		
Eradication	Close firewall ports and network connections.		
	Test devices and applications to be sure any malicious code is removed.		
	Compare data before and after the incident to ensure systems are reset properly.		
	Inform employees regarding eradication.		
	Potentially share information externally regarding eradication (website updates, emails, social media posts, tech support bulletins, etc.).		

INCIDENT PHASE	ACTION	TEAM MEMBER/ SYSTEM	DAY/TIME ACTION TAKEN
Recovery	Download and apply security patches.		
	Close network access and reset passwords.		
	Conduct vulnerability analysis.		
	Return any systems that were taken offline to production.		
	Inform employees regarding recovery.		
	Share information externally regarding recovery (website updates, emails, social media posts, tech support bulletins, etc.).		
Lessons Learned	Review forensic evidence collected.		
	Assess incident cost.		
	Write an Executive Summary of the incident.		
	Report to executive team and auditors if necessary.		

INCIDENT PHASE	ACTION	TEAM MEMBER/ SYSTEM	DAY/TIME ACTION TAKEN
	Implement additional training for everyone involved in incident response and all employees.		
	Update incident response plan.		
	Inform employees regarding lessons learned, additional training, etc.		
	Potentially share information externally (website updates, emails, social media posts, tech support bulletins, etc.).		

APPENDIX A: THREAT CLASSIFICATION

[*In your IR plan, include information on how you evaluate risk. You may develop your own threat classification or risk ranking system to determine the level of incident response necessary*.]

The CIA Triad (Confidentiality, Integrity, and Availability) is a framework for incident classification that helps to prioritize the level of incident response required for a cyberattack.

- Confidentiality – Incidents involving unauthorized access to systems, including privileged account compromise. The more confidential the data or the more important the systems are to the business, the higher the potential impact.
- Integrity – Incidents involving data poisoning, including leveraging a privileged account to corrupt or modify data. The more sensitive the data, the higher the potential impact.
- Availability – Incidents that impact the availability or proper functioning of services, such as Distributed Denial of Service (DDoS) or ransomware, including use of privileged accounts to make unauthorized changes. The more critical the services to the business, the higher the potential impact.

When ranking the level of risk to the organization and the type of incident response required, you must consider the extent to which privileged accounts are compromised, including those associated with business users, network administrators, and service or application accounts. When privileged accounts are involved in the breach, the level of risk increases exponentially as does the response required.

APPENDIX B: COMPLIANCE AND LEGAL OBLIGATIONS

The following is a list of regulations that include requirements for incident response, including preparation, documentation, and reporting. Select the requirements that apply to your organization, include the appropriate contacts in the contact section of this template, and make sure the actions and tools you have in place provide the capabilities to meet your obligations.

HIPAA and HITECH

Any organization that creates, receives, maintains, or transmits electronic protected health information (ePHI) in the United States must meet HIPAA requirements for access control and data sharing.

Reporting requirements – The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information.

Similar breach notification provisions implemented and enforced by the Federal Trade Commission (FTC) apply to vendors of personal health records and their third-party service providers, pursuant to section 13407 of the HITECH Act.

Learn more – https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

PCI DSS

PCI DSS provides organizations that accept, store, or transmit credit card data with guidelines for privilege management and a framework to protect cardholder data.

Reporting requirements – PCI DSS requires entities have an incident response plan and alert affected parties immediately. PCI DSS 3.2.1, released on May 2018, marks the latest version.

You may want to set up an arrangement with an independent Payment Card Industry Forensic Investigator (PFI) to call if you need outside expertise.

Learn more – https://www.pcisecuritystandards.org/documents/PCI_SSC_PFI_Guidance.pdf

FISMA/NIST

FISMA is US legislation intended to protect the security, confidentiality, and integrity of government data systems. A FISMA audit is a test of an organization's system against the controls outlined in various NIST publications such as NIST SP 800-53, NIST SP 800-171, FIPS 199, and FIPS 200.

Reporting requirements – A FISMA audit is a test of an organization's system against the controls outlined in various NIST publications such as NIST SP 800-53, NIST SP 800-171, FIPS 199, and FIPS 200.

Learn more – https://csrc.nist.gov/projects/risk-management

NERC/CIP

The NERC Critical Infrastructure Protection (CIP) Standards apply to the cyber security aspects of the Bulk Electric System and its efficient and reliable supply.

Reporting requirements – Reliability standards require the reporting of cyber security incidents that compromise, or attempt to compromise, a responsible entity's Electronic Security Perimeter (ESP) or associated Electronic Access Control or Monitoring Systems (EACMS).

Learn more – https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

SARBANES-OXLEY (SOX)

SOX is designed to reduce corporate fraud by requiring an increase in the strength and granularity of security controls for financial auditing and reporting.

Reporting requirements – Companies must disclose failure of security safeguards and security breaches to SOX auditors.

Learn more – https://www.sarbanes-oxley-101.com/

EU GDPR

Any organization dealing with EU citizens' Personally Identifiable Information is obligated to meet standards for effective data protection, adequate security measures, and privacy by design to comply with EUGDPR.

Reporting requirements – Under GDPR, breach notification is mandatory in all member states where a data breach is likely to result in a risk for the rights and freedoms of individuals. This must be done within 72 hours of first having become aware of the breach. Data processors are required to notify their customers, the controllers, without undue delay after first becoming aware of a data breach.

Learn more – https://www.eugdpr.org/key-changes.html

NOTES