CYBERSECURITY INCIDENT RESPONSE PLAN FOR ROVE HOTELS

Gregory Stephens

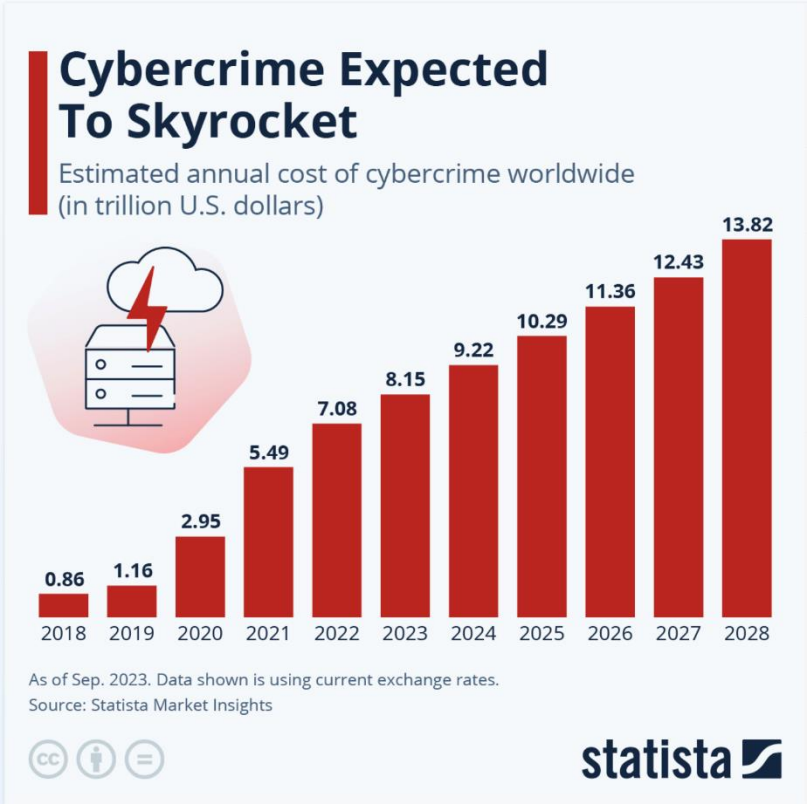
Cybersecurity Planning/CYBR3050

Submission: March 30, 2025

Introduction

Are you concerned about the increasing number of threats?

At Rove Hotels, we recognize that cyber threats are becoming increasingly sophisticated and frequent. According to a report by PurpleSec, cybercrime has risen by 600% since the start of the pandemic, with ransomware attacks alone costing businesses over $20 billion annually. As a hospitality provider handling sensitive guest information, such as personal details, payment data, and booking records, protecting this data is critical to maintaining trust with our guests and ensuring compliance with global standards like GDPR and PCI-DSS. The growing threat landscape demands a proactive approach to cybersecurity.



Source: Statista

In addition to the financial impact, cyberattacks can severely damage an organization's reputation. For Rove Hotels, where guest satisfaction and trust are paramount, even a single breach could lead to long-term consequences, including loss of customer loyalty and negative publicity. Furthermore, the interconnected nature of modern technology means that attackers often exploit vulnerabilities not just within our systems but also through third-party vendors, unsecured Wi-Fi networks, or even IoT devices such as smart locks and thermostats in guest rooms.

The hospitality industry is particularly attractive to cybercriminals due to the large volume of sensitive data processed daily. This includes personally identifiable information (PII), credit card numbers, passport details, and travel itineraries. A breach at any point in this data flow could expose thousands of guests to identity theft or fraud. Moreover, the rise of remote work and cloud-based services has expanded the attack surface, making it more challenging to secure all entry points effectively.

What is the most common source of entry for an attacker?

The most frequent entry points for attackers targeting Rove Hotels include:

- Phishing Attacks: Employees may inadvertently click malicious links in emails or messages. According to TechTarget, phishing remains the top vector for breaches, accounting for nearly 30% of all incidents.
- Weak Passwords: Guests or staff using easily guessable passwords can expose accounts. Weak credentials were responsible for 81% of hacking-related breaches in 2022 (Verizon DBIR).
- Unpatched Systems: Outdated software or hardware vulnerabilities in hotel management systems, Wi-Fi networks, or POS terminals are exploited by attackers. Hyper proof highlights that unpatched vulnerabilities account for 60% of successful breaches.
- Third-Party Vendors: Weaknesses in vendor systems (e.g., booking platforms, payment processors) can provide attackers with indirect access.
- Insider Threats: Both intentional (malicious employees) and unintentional (negligent actions) insider risks pose significant challenges.

ATTACK VECTOR TRENDS	2021	2020	2019
Cyberattacks	1,613	878	928
Phishing/Smishing/BEC	537	383	490
Ransomware	321	158	83
Malware	139	104	112
Non-secured Cloud Environment	23	51	15
Credential Stuffing	14	17	3
Unpatched software flaw	4	3	3
Zero Day Attack	4	1	n/a
Other - not specified	436	161	222
NA	106	n/a	n/a
Human & System Errors	179	152	231
Failure to configure cloud security	54	57	56
Correspondence (email/letter)	66	55	89
Misconfigured firewall	13	4	4
Lost device or document	12	5	19
Other - not specified	34	31	63
Physical Attacks	51	78	118
Document Theft	9	15	19
Device Theft	17	30	57
Improper Disposal	5	11	14
Skimming Device	1	5	4
Other - not specified	19	17	24
Unknown	12	n/a	2

Source: Darkreading

For instance, a phishing email sent to a front-desk employee might grant attackers access to the hotel's reservation system. Similarly, outdated firmware on a smart thermostat in a guest room could serve as a gateway for hackers to infiltrate the broader network. These examples underscore the importance of adopting a multi-layered security strategy that addresses both human and technical vulnerabilities.

What is the intent of this document?

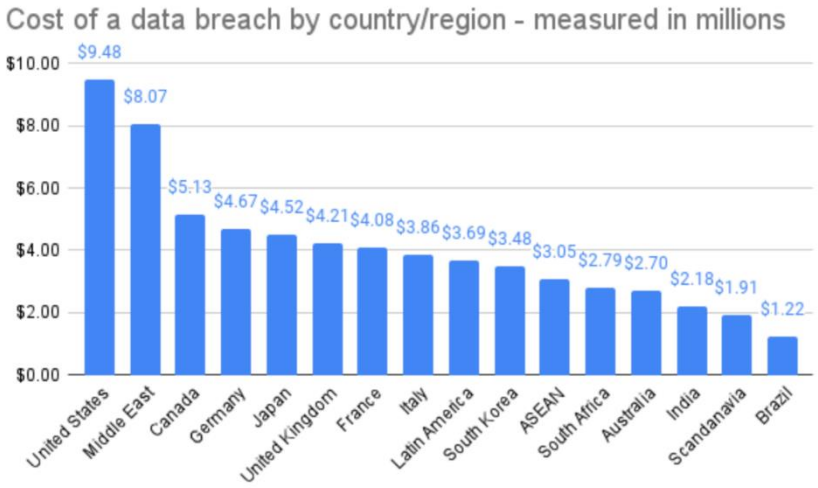
The intent of this document is to establish a clear and actionable framework for detecting, responding to, and mitigating cybersecurity incidents at Rove Hotels. It ensures that all employees, management, and stakeholders understand their roles during a security breach and provides step-by-step guidance to minimize damage and restore operations quickly.

This plan is not only a reactive tool but also a proactive one. By outlining preventive measures, training requirements, and incident simulation exercises, it aims to reduce the likelihood of breaches occurring in the first place. Additionally, the plan serves as a reference guide for legal and regulatory compliance, helping Rove Hotels meet obligations under frameworks such as GDPR, PCI-DSS, and UAE Cybersecurity Laws.

Why is the cybersecurity incident response plan required?

A cybersecurity incident response plan is vital for Rove Hotels because:

- It protects sensitive guest and employee data from unauthorized access or theft.
- It reduces downtime and financial losses caused by breaches or disruptions. According to IBM's Cost of a Data Breach Report, the average cost of a breach is $4.45 million globally.
- It demonstrates compliance with industry regulations like GDPR, PCI-DSS, and local laws.
- It safeguards the brand reputation and customer trust upon which Rove Hotels depends.
- It enhances operational resilience by preparing us for potential future attacks.



Source: Breachsense

Beyond these immediate benefits, the incident response plan fosters a culture of accountability and preparedness across the organization. Every employee—from housekeeping staff to senior management—plays a role in identifying and mitigating risks. By clearly defining responsibilities and procedures, the plan ensures that no critical steps are overlooked during high-pressure situations.

Does this document align with a specific standard/law and regulations?

Yes, this document aligns with the following standards and regulations:

- NIST SP 800-61: Guidelines for incident handling and response, which emphasize preparation, detection, analysis, containment, eradication, and recovery.
- ISO/IEC 27001: Best practices for establishing an Information Security Management System (ISMS), ensuring continuous improvement and risk management.

- GDPR: Ensures the protection of EU citizens' personal data, requiring timely notification of breaches to supervisory authorities and affected individuals.
- PCI-DSS: Protects cardholder data processed through our payment systems, mandating encryption, access controls, and regular vulnerability scans.
- UAE Cybersecurity Laws: Compliance with national cybersecurity frameworks, including the UAE's National Electronic Security Authority (NESA) guidelines.

Furthermore, this plan incorporates insights from leading cybersecurity resources such as Hyper proof, TechTarget, and PurpleSec, ensuring that it reflects the latest trends and best practices in the field. By adhering to these standards and leveraging expert recommendations, Rove Hotels positions itself as a leader in cybersecurity within the hospitality industry.

Objectives

What is the object of the incident response plan?

The primary objectives of the incident response plan for Rove Hotels are:

Define the goals of the cybersecurity incident response process:

- Rapidly identify and classify cybersecurity incidents affecting Rove Hotels' systems and data.
- Contain and mitigate the impact of incidents to prevent further damage.
- Restore affected services and systems to normal operation promptly.

Recover from a major incident:

- Ensure that critical systems (e.g., reservation systems, Wi-Fi networks, and payment gateways) are restored without compromising guest experience.
- Provide alternative solutions (e.g., manual check-ins) during system outages to maintain service continuity.

Limit the damage to information assets and resources:

- Prevent unauthorized access to guest databases, financial records, and internal communications.
- Minimize reputational harm by addressing incidents transparently and efficiently.

Gather evidence:

- Collect forensic data to investigate the root cause of incidents and support legal proceedings if necessary.
- Preserve evidence in a manner that adheres to chain-of-custody requirements.

Improve the incident response process:

- Conduct post-incident reviews to identify areas for improvement.
- Update policies, procedures, and training programs based on lessons learned.

Conclusion: The objective is all the above, ensuring that Rove Hotels remains resilient and prepared for any cybersecurity challenge.

Roles and responsibilities

Are the roles and responsibilities required for this plan?

Yes, clearly defined roles and responsibilities are essential for effective coordination. Without them, confusion and delays could exacerbate the impact of an incident. At Rove Hotels, every team member plays a part in safeguarding our digital environment.

What is the role of IT Helpdesk/IT Personnel

- Act as the frontline responders for technical issues reported by staff or guests.
- Monitor alerts from security tools (e.g., firewalls, intrusion detection systems).
- Escalate suspected incidents to the Incident Response Team (IRT).
- Assist in restoring affected systems after an incident has been resolved.

What is the role of the Incident Response Team (IRT)

- Lead the investigation into incidents and determine their scope and severity.
- Coordinate containment efforts, such as isolating compromised systems or disabling network segments. Example: If malware infects the reservation system, the IRT will isolate the infected server to prevent lateral movement.
- Eradicate threats by removing malicious code, patching vulnerabilities, or resetting credentials.
- Oversee recovery activities, ensuring systems are brought back online securely.

What is the role of Legal/Compliance Personnel

- Provide guidance on regulatory obligations, such as notifying authorities or affected individuals within specified timelines.
- Review contracts with third-party vendors to ensure they comply with Rove Hotels' security standards.
- Work with external counsel to prepare for potential litigation or fines resulting from a breach.

Who is responsible for communication (notifying the public, law enforcement, employees, etc.)

- The Communications Lead, typically part of the Marketing or PR department, manages internal and external communications.
  - Internal: Inform employees about the incident and provide instructions to avoid panic or misinformation.
  - External: Notify guests, partners, and regulators about the breach while maintaining transparency and accountability.
  - Law Enforcement: Collaborate with local police or international agencies if criminal activity is involved.

Definitions

What is an incident

An incident is any event that compromises or threatens the confidentiality, integrity, or availability of Rove Hotels' information systems or data. Examples include ransomware attacks, unauthorized database access, or DDoS attacks on our website.

Event

An event is any observable occurrence in a system or network. For instance, multiple failed login attempts might be flagged as an event but not necessarily an incident unless they indicate malicious intent.

Breach

A breach occurs when there is unauthorized access to or disclosure of sensitive data. For example, if a hacker exfiltrates guest credit card details, it constitutes a data breach.

Precursor

A precursor is an early warning sign that suggests a potential future incident. For Rove Hotels, this could include unusual spikes in outbound traffic or phishing emails targeting employees.

Indicator

An indicator is concrete evidence of a confirmed incident. For example, finding ransomware files on a server or detecting anomalous SQL queries in a database log.

Remediation

Remediation refers to the steps taken to resolve an incident and prevent its recurrence. This includes patching vulnerabilities, deleting malware, reconfiguring firewalls, or updating security policies.

Methodology

Preparation

The key to an effective cybersecurity incident response plan (CSIRP) is to have one in place well before a breach occurs. Preparation is the basis of successful incident response; the planning you do before a security incident occurs will help you respond to an incident as quickly and efficiently as possible.

For training and awareness,

- The IT team will undergo regular training sessions to get themselves familiarized with the CSIRP, which will be covering Roles, responsibilities and response procedures.
- Extended members including key business leaders will receive incidence respond training to help them triaging incidents.
- A cybersecurity awareness training program will be implemented to educate employees on identifying and reporting incidents, this includes; identifying phishing emails and social engineering tactics, recognizing unusual system behaviour indicating a possible security breach and proper procedures for reporting suspected incidents to Help desk.
- Training will include simulated phishing attacks and tabletop exercises to enhance practical response skills.

For incident handling and responsibilities,

- The IT help desk will be the first point of contact in reporting incidents.
- Incidents will be triaged based on predefined criteria and escalated as necessary
- The Incident Response Team will include Security Analysts (to perform in-depth analysis and containment), IT managers (to oversee incident responds and remediation response), Legal

representatives (to provide guidance on legal and reporting obligations), Compliance officers (to ensure regulatory compliance during incident response) and Forensic Specialist if needed to conduct advanced investigations.

For Detection Technology and policies

- Rove hotels will use detection technology such as; SIEM (for Analysing logs for threat detection), EDR (for detecting threat at endpoint devices), IDPS (for monitoring Network traffic for malicious activities), and NTA(for examining any anomalies in the Network).
- A Cybersecurity policy will be established mandating the development, use and continuous improvement of this CSIRP.

For Asset documentation,

- Network assets and dataflow documentation will be maintained to support the Incident response team. A comprehensive asset inventory with details on endpoint (workstations, servers and mobile devices), Network Infrastructure (switches, routers and firewalls) and data flow diagrams (mapping data movement to identify potential vulnerabilities) will be maintained.
- Continuous monitoring will be implemented, this includes regular log view to detect suspicious patterns, Automated alerts for unauthorized access and unusual login attempts, intelligence integration for proactive threat identification.

Detection and Analysis

The detection and analysis phase in your CSIRP is triggered when an incident has just occurred, and your organization needs to determine how to respond to it.

For SIEM and log analysis,

- A centralized SIEM solution monitored by SOC team will aggregate and analyze logs from network resources to detect Anomalies.
- Suspicious activities that are flagged by the SIEM will be investigated by the IT Security team

For Incident Analysis and Classification,

- Analysts will assess precursors, indicators and correlating information to confirm incidents.
- The scope and impact will be determined including number of affected systems and users, operational impact and compliance risks.
- Incidents will be classified into 3 tiers which include; **Tier 1-** minor issues resolved by the help desk, **Tier 2-** more complex incidents that require IT Security intervention and **Tier 3-** critical incidents which require escalations to external specialist or Law enforcement.

Notification and Communications

For internal communication and escalations,

- Initial assessment of incidents will be conducted by the Help desk.
- Incidents will be escalated to the IT Sec. manager if necessary

- Incident response lead will notify executive leadership and external specialists if an incident is beyond Tier 2 to handle.
- The Legal and compliance team will be consulted to determine regulatory reporting requirements.
- Rove Hotels will engage a cybersecurity expert through a retainer agreement for Tier 3 incidents.

For external communication,

- The Legal and Compliance team will handle public, employee and client breach notification. They will be the one to notify affected individuals, regulatory bodies within the required time frame and also coordinate public statements and press releases.
- Law enforcement will be contacted by the Chief Information Officer or a designated Security Officer if necessary.

For Reporting and Documentation,

- All incidents will be documented in an Incident Response Form, consisting of **incident type and classification, time of detection and actions taken, resolution status and follow up measures**.

A Post Incident Response Form will be completed covering root cause analysis, lessons learned, policy improvement and recommendations for enhancing detection and response capabilities

Containment, Eradication, Recovery

- Is another critical component of a cybersecurity incident response plan that focus on limiting the damage, removing the threat, and restoring normal operations.
- Organizations can minimize the impact of cybersecurity incidents and strengthen their defenses against future threats by executing the containment, eradication, and recovery activities effectively.

Containment Phase

- Involves prevention of the incident from spreading and causing further damage, and isolating affected systems, networks, or data to limit the impact.
- Key Activities under this phase are:
  Short-term Containment:
  - Immediately isolate affected systems or networks such as disconnect from the internet, disable compromised accounts.
  - Implement temporary fixes to stop the threat from spreading such as block malicious IPs, apply firewall rules.

  Long-term Containment:
  - Apply more permanent measures to ensure the threat is fully contained such as patch vulnerabilities, update security configurations.
  - Ensure business continuity by allowing unaffected systems to operate normally.

  Documentation:
  - Record all actions taken during containment for future reference and legal/regulatory compliance.

Eradication Phase

- Focuses on identifying and completely removing the root cause of the incident AND ensures the threat is eliminated and cannot reoccur.
- Key Activities under this phase are:

- Analyze the incident to determine how the attacker gained access (e.g., phishing, unpatched software, misconfigurations).
- Use forensic tools to trace the attack vector and identify compromised systems.
- Delete malware, backdoors, or unauthorized accounts.
- Clean infected systems and ensure no remnants of the threat remain.
- Apply security patches or updates to close exploited vulnerabilities.
- Strengthen security controls to prevent similar attacks in the future.

Recovery Phase

- The recovery phase involves restoring affected systems, networks, and data to normal operation while ensuring the threat has been fully mitigated.
- Key Activities under this phase are:
  - Rebuild or restore systems from clean backups (ensure backups are not compromised).
  - Reconnect systems to the network gradually to monitor for any signs of residual threats.
  - Verify that systems are functioning correctly and securely.
  - Conduct vulnerability scans and penetration tests to ensure no new weaknesses exist.
  - Continuously monitor systems for any signs of the threat returning.
  - Implement enhanced monitoring tools or techniques if necessary.
  - Inform internal teams, management, and external stakeholders (e.g., customers, regulators) about the recovery progress.
  - Provide updates on the incident resolution and steps taken to prevent future incidents.

Post-Incident Activity

- After the recovery phase, it's essential to conduct a post-incident review to improve future response efforts that includes:
  - Review the incident timeline, response actions, and effectiveness of containment, eradication, and recovery efforts.
  - Identify gaps in the incident response plan and update it accordingly.
  - Provide additional training to staff if necessary.
  - Prepare a detailed incident report for legal, regulatory, or internal purposes.
  - Share findings with relevant stakeholders to improve overall security posture.

Testing and Maintaining the Plan

How often will this plan be tested?

- Testing and maintaining a cybersecurity incident response plan (IRP) is crucial to ensure its effectiveness in the event of a real incident. A well-prepared IRP helps organizations respond quickly, minimize damage, and recover efficiently. Below are the key steps for testing and maintaining an IRP:

Testing the Incident Response Plan

- Testing ensures that the IRP is practical, up-to-date, and that the team is prepared to handle incidents. Common testing methods include:
  - The frequency of testing a cybersecurity incident response plan (IRP) can vary depending on the organization's size, industry, regulatory requirements, and risk profile. It ensures the IRP is effective, actionable, and aligned with the organization's evolving threat landscape.
  - Regular testing and updates are critical to maintaining a strong cybersecurity posture.
- Best practices recommended while testing IRP includes:
  - Conduct a full-scale annual test of the incident response plan at least once a year to ensure the plan remains effective and up to date with current threats and organizational changes.
  - Test the IRP whenever there are significant changes to the organization's infrastructure, such as new systems, applications, or network configurations, or after major cybersecurity incidents.
  - Perform tabletop exercises every 6-12 months to simulate potential scenarios and evaluate the team's readiness. These exercises help identify gaps in the plan and improve coordination among team members.
  - Conduct smaller, more frequent drills or simulations (e.g., phishing attack simulations, ransomware scenarios) to keep the response team sharp and ensure familiarity with the plan.
  - Some industries (e.g., finance, healthcare) may have specific regulatory requirements mandating the frequency of testing. For example, PCI DSS or HIPAA may require regular testing and updates to the IRP.
  - After a real cybersecurity incident, review and test the IRP to incorporate lessons learned and improve future responses.

Method Used to Test IRP

- Organizations can use one of the following or a combination of methods to ensure their incident response plan is robust, actionable, and aligned with their cybersecurity goals.
- Some of the common methods that can be used to test the IRP includes the following and each have different purpose and can provide unique outcomes. Tabletop Exercises:
  - Simulated Attacks (Red Team/Blue Team Exercises).
  - Walkthroughs.
  - Functional Drills.
  - Full-Scale Simulations.
  - Post-Incident Reviews (After-Action Reviews).
  - Third-Party Audits or Assessments.
  - Scenario-Based Testing.
  - Regulatory Compliance Testing and etc.

Purpose of the Incident Response Plan Testing

- Identifies gaps in the plan, improves communication, and ensures alignment among team members.
- Provides a realistic assessment of the IRP's effectiveness and the team's technical skills.
- Validates the effectiveness of individual procedures and tools.
- Record the outcomes of each test, including successes, failures, and areas for improvement.
- Use the insights gained from testing to refine and improve the IRP.
- Confirms the plan's accuracy and relevance.
- Provides an unbiased evaluation and recommendations for improvement.
- Ensures the IRP is tailored to address the most likely risks.
- Ensure all relevant teams (IT, legal, PR, management) participate in testing to foster collaboration.
- Stay proactive by anticipating future threats and adapting the plan accordingly.

Maintaining the Incident Response Plan

- An IRP must evolve to address new threats, technologies, and organizational changes including:
  - Review and update the IRP at least annually or after significant changes.
  - Incorporate feedback from tests, real incidents, and audits.
  - Stay informed about emerging threats, vulnerabilities, and attack techniques.
  - Adjust the IRP to address new risks (e.g., zero-day exploits, ransomware trends).
  - Provide regular training for the incident response team and employees.
  - Conduct awareness programs to help employees recognize and report potential incidents.
  - Ensure the IRP complies with relevant regulations (e.g., GDPR, HIPAA, PCI-DSS).
  - Update the plan to reflect changes in legal or regulatory requirements.
  - Maintain a version control system for the IRP.
  - Document all changes, including the rationale and date of updates.

Incident Response Team Contact Information

Internal contacts

Title/Position	Name	Email	Phone Number
Incident Manager	Mr. x		+1 780 –111-1111
IT Security Lead	Mr. y		+1 780 –111-2222
Network Administrator	Mr. z		+1 780 –111-3333
Legal Advisor	Mr. a		+1 780 –111-4444
Public Relations (PR)	Mr. b		+1 780 –111-5555
HR Representative	Mr. c		+1 780 –111-6666

External or Third-party Contacts

External/Third-party	Name	website	Phone Number

Cybersecurity Vendor	Syncsys Technology Solutions	https://www.syncsys.ca	+1 780 –111-7777
Law Enforcement	cybercrimes and fraud to the Canadian Anti-Fraud Centre (CAFC)	https://antifraudcentre-centreantifraude.ca	+1 780-423-4567
Data Breach Hotline	Government of Alberta	https://www.alberta.ca/file-a-complaint-or-report-a-privacy-breach	+1 780-427-5848 Toll free: 310-0000

Related Documents

Incident response policy

- Prior to making an Incident Response Plan, it is recommended to create an incident response policy.
- Initially creating an Incident Response Policy:
  - Classify what a security incident is.
  - Who is responsible for responding to an event?
  - Roles and responsibilities.
  - Documentation.
  - Reporting requirements.
- According to NIST: “Policy governing incident response is highly individualized to the organization. However, most policies include the same key elements.” including:
  - Provides a road map for a Statement of Management Commitment, which outlines the purpose and objectives of the policy incident response capabilities.
  - Scope of the policy (to whom and what it applies, and under what circumstances).
  - Definition of computer security incidents and related terms.
  - Organizational structure:
    - Definitions of roles and responsibilities.
    - Levels of authority.
  - Prioritization or severity ratings of incidents.
  - Performance measures.
  - Reporting and contact form.

Security awareness policy

1. General Awareness

- Understand the importance of cybersecurity in protecting organizational data and assets.
- Recognize that every employee plays a critical role in maintaining security.
- Stay informed about the latest cyber threats and trends through regular training and updates.

2. Password Management

- Create strong, unique passwords with a mix of uppercase, lowercase, numbers, and special characters.
- Avoid reusing passwords across multiple accounts or systems.
- Enable multi-factor authentication (MFA) wherever possible.
- Change passwords regularly and immediately if a compromise is suspected.

3. Phishing and Social Engineering

- Be cautious of unsolicited emails, messages, or phone calls requesting sensitive information.
- Verify the sender's identity before clicking on links or downloading attachments.
- Report suspicious emails or messages to the IT/security team immediately.
- Never share personal or organizational information over unsecured channels.

4. Data Protection

- Classify data based on sensitivity (e.g., public, internal, confidential).
- Encrypt sensitive data during transmission and storage.
- Avoid storing sensitive information on personal devices or unauthorized cloud services.
- Follow the organization's data retention and disposal policies.

5. Device Security

- Lock your workstation when leaving it unattended.
- Use only authorized devices and software provided by the organization.
- Keep operating systems, applications, and antivirus software up to date.
- Report lost or stolen devices to IT/security immediately.

6. Network Security

- Avoid connecting to unsecured Wi-Fi networks, especially for work-related tasks.
- Use a Virtual Private Network (VPN) when accessing organizational resources remotely.
- Do not plug unknown USB drives or external devices into company equipment.
- Report any unusual network activity to the IT/security team.

7. Incident Reporting

- Familiarize yourself with the organization's CSIRP and reporting procedures.
- Report any suspected security incidents promptly, no matter how minor they seem.
- Provide detailed information about the incident, including timestamps, affected systems, and actions taken.
- Cooperate fully with the IT/security team during incident investigations.

8. Physical Security

- Secure physical access to offices, server rooms, and other sensitive areas.
- Do not allow unauthorized individuals to "tailgate" into restricted areas.
- Protect printed documents containing sensitive information and dispose of them securely.
- Be mindful of discussions involving sensitive information in public spaces.

9. Remote Work Security

- Use only approved tools and platforms for remote collaboration.
- Ensure your home Wi-Fi network is secured with a strong password.
- Avoid using personal email accounts for work-related communication.
- Follow the organization’s remote work policies and guidelines.

10. Social Media and Online Behavior

- Avoid posting sensitive organizational information on social media.
- Be cautious about sharing personal details that could be used for social engineering attacks.
- Use privacy settings to control who can view your online profiles.
- Represent the organization professionally in all online interactions.

11. Third-Party Security

- Vet third-party vendors and partners for their security practices.
- Ensure contracts include clauses for data protection and incident response.
- Limit third-party access to organizational systems and data.
- Monitor third-party activities for compliance with security policies.

12. Continuous Education

- Participate in mandatory security awareness training programs.
- Complete periodic assessments to reinforce learning and identify gaps.
- Stay updated on organizational policies and industry best practices.
- Encourage a culture of security awareness by sharing knowledge with colleagues.

13. Compliance and Accountability

- Adhere to all applicable laws, regulations, and organizational policies.
- Understand the consequences of non-compliance with security policies.
- Take responsibility for your actions and their impact on organizational security.
- Support audits and reviews to ensure policy effectiveness.

14. Leadership and Culture

- Leadership should actively promote a culture of security awareness.
- Allocate resources for training, tools, and technologies to enhance security.
- Recognize and reward employees who demonstrate exemplary security practices.
- Foster open communication to encourage reporting of potential risks.

References

https://hyperproof.io/resource/cybersecurity-incident-response-plan/

https://www.techtarget.com/searchsecurity/feature/5-critical-steps-to-creating-an-effective-incident-response-plan

https://purplesec.us/learn/incident-response-steps/

PIcture 1
https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/

Picture 2
https://www.darkreading.com/cyberattacks-data-breaches/most-common-cause-of-data-breach-in-2021-phishing-smishing-bec

Picture 3
https://www.breachsense.com/blog/cost-of-a-data-breach/

Spasojevic, A. (2024, February 8). *Upgrade your cybersecurity incident response plan with a 7-step checklist*. phoenixNAP Blog. https://phoenixnap.com/blog/cyber-security-incident-response-plan

Computer Security Incident Handling Guide (nist.gov)

U.S. Department of Health and Human Services. (n.d.). *Cybersecurity incident response plans*. Retrieved from https://www.hhs.gov/sites/default/files/cybersecurity-incident-response-plans.pdf

DataGuard. (n.d.). *Incident response plan*. Retrieved October 30, 2023, from https://www.dataguard.com/cyber-security/incident-response-plan/#:~:text=A%20Cyber%20Security%20Incident%20Response%20Plan%20is%20crucial%20for%20organisations,with%20external%20partners%20for%20support.

Spasojevic, A. (2024, February 8). *Upgrade your cybersecurity incident response plan with a 7-step checklist*. phoenixNAP Blog. https://phoenixnap.com/blog/cyber-security-incident-response-plan