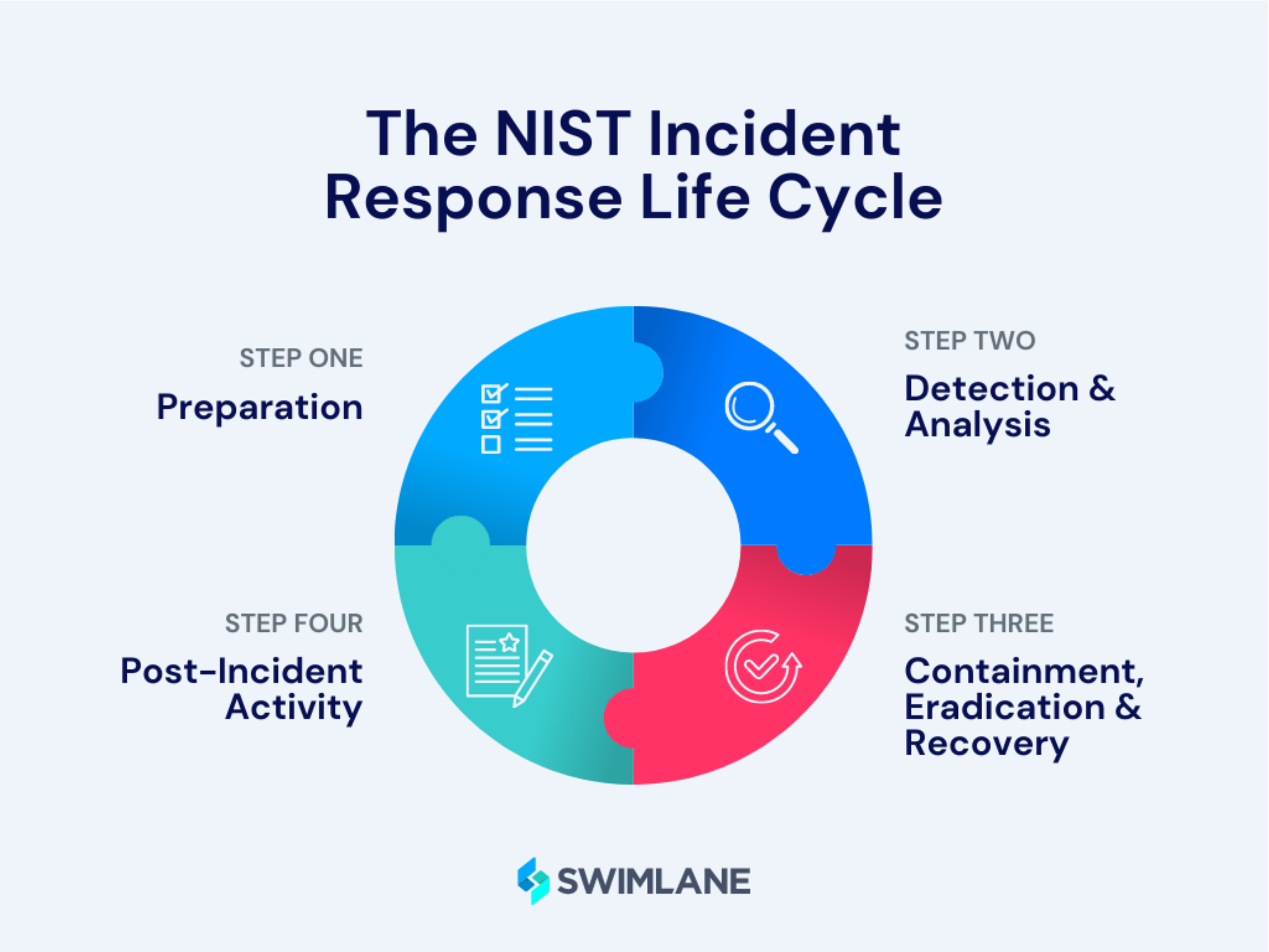
CYBERSECURITY POST-INCIDENT RESPONSE PLAN FOR ROVE HOTELS



Cybersecurity Planning/CYBR3050

Assignment #3

Scenario 5: Unknown Wireless Access Point

Gregory Stephens

Preparation

Rove Hotels would consider the presence of a rogue access point a security incident, as it potentially compromises network integrity, confidentiality, and availability, and could be an avenue for unauthorized access, data interception, or man-in-the-middle attacks. It directly affects both internal operations and potentially guest Wi-Fi, which is critical in the hospitality industry.

This activity violates Rove Hotels following policies

- **Network Security Policy** where unauthorised devices are not permitted on the network
- **Wireless Communication Policy** which governs the deployment and use of wireless devices within Rove hotels.
- **Acceptable Use Policy** this would breach acceptable use IT assets if **the** rogue access point was developed by an employee.
- **IT Asset Management Policy:** the unauthorized AP violates the approved deployment process.

Measures in Place to Prevent or Limit the Impact of this Incident

- **MAC Address Filtering and AP Whitelisting** where only approved access points can be used.
- **Wireless Intrusion Detection System (WIDS**) which detects unauthorized or rogue APs.
- **Network Access Control (NAC)** which prevents unauthorized devices from connecting to the internal network.
- **Regular Network Audits and Site Surveys**: this is very important especially in hospitality where guest and internal Wi-Fi co-exist.

Employee Security Awareness Training

- It ensures staff know not to install or connect to unauthorized devices.

Detection and Analysis

Precursors of the Incident and Potential Actions

In the case of the unknown wireless access point, Rove Hotels might have detected precursors such as:

- Unusual spikes in outbound traffic: This could indicate unauthorized data exfiltration via the rogue access point.
- Phishing emails targeting employees: Attackers may use phishing to gain credentials for deploying rogue devices.
- Weak or default passwords on network devices: These could allow attackers to exploit vulnerabilities and deploy rogue access points.
- Unpatched systems or outdated firmware: Devices with known vulnerabilities could be exploited to create backdoors for rogue access points.

Would these precursors cause action?
Yes. Detecting these precursors would prompt proactive measures such as:

- Conducting immediate phishing awareness training for employees.
- Patching systems and applying security updates.
- Enforcing strong password policies and disabling default credentials on network devices.
- Isolating suspicious systems temporarily until further analysis is completed.

Indicators of the Incident

For the unknown wireless access point, indicators might include:

- Rogue access point listed in wireless configurations: A clear sign of an unauthorized device on the network.
- Anomalous network traffic patterns: Unusual outbound traffic originating from the rogue access point.
- Unauthorized connections to guest databases: Suggests potential data exfiltration.
- User complaints about connectivity issues: Indicates interference or malicious activity from the rogue access point.

Which indicators would raise suspicion?

- The presence of an unauthorized access point would immediately suggest a critical incident requiring escalation.
- Anomalous network traffic would indicate potential data breaches or command-and-control communication.

Additional Tools Needed

To detect this particular incident, additional tools might include:

- Wireless Network Scanners: To identify rogue access points and their signal strength.
- Network Traffic Analyzers (NTA): To monitor and analyze unusual traffic patterns originating from the rogue access point.
- Threat Intelligence Platforms: To correlate detected anomalies with known threat signatures.
- Forensic Tools: For deep-dive analysis of compromised systems connected to the rogue access point.

Analysis and Validation Process

The Incident Response Team (IRT) would analyze and validate the incident as follows:

- Initial Assessment: Use SIEM to aggregate logs and correlate events related to the rogue access point.
- Forensic Investigation: Employ forensic tools to trace the attack vector and identify compromised systems.
- Root Cause Analysis: Determine how the rogue access point was deployed (e.g., physical installation, exploiting vulnerabilities).
- Scope Determination: Assess the number of affected systems, users, and the operational impact.

Personnel Involved:

- Security Analysts: Perform in-depth analysis and containment.
- IT Managers: Oversee technical remediation efforts.
- Legal Representatives: Provide guidance on regulatory obligations.
- Forensic Specialists: Conduct advanced investigations if necessary.

Reporting the Incident

The team would report the incident to:

- Internal Stakeholders: Executive leadership, IT Security Lead, Legal/Compliance Team, and HR Representative.
- External Groups: Affected guests, regulatory bodies (e.g., GDPR authorities), law enforcement (if criminal activity is involved), and cybersecurity vendors for additional support.

Prioritization of the Incident

The team would prioritize the incident based on:

- Severity: Critical incidents (Tier 3) involving sensitive guest data or financial systems would take precedence.
- Impact: Incidents affecting multiple systems or large volumes of data would be prioritized.
- Regulatory Requirements: Incidents requiring mandatory reporting within specific timelines (e.g., GDPR's 72-hour rule) would be handled urgently.

Containment, Eradication, and Recovery:

Containment strategy

- Containment is important before an incident overwhelms resources or increases damage. Most incidents require containment, so that is an important consideration early in the course of handling each incident. Containment provides time for developing a tailored remediation strategy.
- Containment strategies vary based on the type of incident. For example, the strategy for containing an email-borne malware infection is quite different from that for a network-based DDoS attack. Organizations should create separate containment strategies for each major incident type and some of the strategies that the organization should follow includes:

Immediate Isolation strategy

- Disconnect affected systems, restrict access, or shut down compromised processes to prevent spread. For example, in a ransomware attack, isolate infected servers to stop lateral movement.

Why it's preferable:

- Containing the problem early reduces the risk of escalation and helps protect customers, staff, or systems. Quick action can limit reputational and financial damage.

Short-Term Mitigation

- Apply patches, revoke compromised credentials or deploy temporary fixes.

Why it's preferable:

- For instance, If a vulnerability is exploited, apply a workaround while waiting for a permanent patch.

Selective (Targeted) Containment strategy

- Only block malicious activity while allowing normal operations.

Why it's preferable:

- Preferred if disruption must be minimized.

Aggressive (Full) Containment strategy

- Complete shutdown of affected systems (used when risk of further damage is extreme).

Why it's preferable:

- Best used when there is extreme risk like organizational sabotage.

Transparent Communication strategy

- Notify stakeholders (internal teams, legal, PR, regulators) to align response efforts.
- Report to authorities or regulatory bodies, if required.
- Acknowledge the issue and outline the steps being taken to address it.

Why it's preferable:

- Being transparent builds trust and shows accountability. Attempting to hide or downplay an incident often leads to backlash when the truth comes out.

- After an incident has been contained, eradication may be necessary to eliminate components of the incident, such as deleting malware and disabling breached user accounts, as well as identifying and mitigating all vulnerabilities that were exploited. During eradication, it is important to identify all affected hosts within the organization so that they can be remediated. For some incidents, eradication is either not necessary or is performed during recovery.

If the incident were not properly contained, the following consequences could face our organization:

- Malware or hackers could spread deeper into systems, stealing more data or shutting down operations.
- More customers could be harmed or affected by a faulty or dangerous product.
- Toxic behavior or misconduct could continue unchecked, impacting morale and safety.
- Fines and penalties from regulators.
- Lawsuits from customers, employees, or stakeholders.
- Revocation of licenses or certifications in some industries.
- Customers lose trust, which can lead to loss of business, negative media coverage, and damage to brand image that takes years to recover.
- Data recovery, legal fees, regulatory fines, public relations, and lost business opportunities.
- For public companies, share prices can go down due to lack of investor confidence.
- Employee morale may drop if they feel unsafe or left in the dark.
- Productivity can suffer due to chaos, uncertainty, or system downtime.

Some additional tools needed to respond to a particular cybersecurity incident will be:

- Intrusion Detection Systems (IDS) – to monitor for suspicious activity.
- Endpoint Detection and Response (EDR) – to isolate and investigate affected devices.
- Forensic Tools (e.g., EnCase, FTK) – to trace the source of the breach and preserve evidence.

Patch Management Systems – to fix vulnerabilities quickly.
SIEM (Security Information and Event Management) – to centralize logs and detect threats.
Encrypted backup and recovery tools – to restore systems safely.
Checklists and playbooks – clear steps for your team to follow.

Key Personnel in Containment, Eradication, and Recovery Process

The personnel involved in containment, eradication, and recovery process will vary based on the type and severity of the incident.

Key Personnel of Containment Phase:

- Incident Response Team Lead – oversees coordination and decision-making.
- IT/Security Analysts – isolate affected systems, accounts, or networks.
- Network Administrators – cut off access or reroute traffic as needed.
- Legal/Compliance Officers – ensure actions align with regulations (e.g., privacy laws).
- I'm HR/Management (for internal incidents) – may be needed if people are involved.

Key Personnel of eradication Phase:

- Cybersecurity Engineers or Forensics Specialists – investigate how the incident happened and clean it up.

- System Administrators – remove malware, reimage systems, revoke access, or apply patches.
- Application Developers (if software is involved) – fix code vulnerabilities or misconfigurations.
- Legal Counsel – ensures proper documentation and reporting, especially if customer data is involved.

Key Personnel of Recovery Phase:

- IT/Operations Teams – bring systems back online, restore backups, and test functionality.
- QA/Test Engineers – verify systems are secure and working as expected.
- Business Unit Leaders – prioritize restoration based on critical services.
- Communications/Public Relations – inform customers, partners, or employees if needed.
- Compliance Auditors – confirm recovery aligns with industry regulations.

Source of evidence

Common sources cybersecurity incident includes:

- System logs (firewall, server, endpoint, antivirus, application).
- Network traffic captures (e.g., PCAP files).
- Authentication records (login/logout, MFA failures).
- Email records (especially phishing or social engineering attempts).
- Malware samples or infected files.
- Screenshots of error messages or suspicious activity.

How Organizations Acquire Evidence:

- Use Forensic Tools: Collect digital evidence using tools that preserve metadata (e.g., EnCase, FTK, Autopsy).
- Write-Protect Storage Devices: When imaging hard drives or copying data, always write-protect the target to avoid tampering.
- I'm Chain of Custody Documentation: Record who accessed, collected, or handled each piece of evidence crucial for legal admissibility.
- Minimize Handling: Only allow trained personnel to access evidence.

Where to Store the Evidence:

- Secure, Access-Controlled Storage.
- Digital: Encrypted external drives, secure cloud storage with audit trails.
- Physical: Locked evidence lockers or safes for physical items (e.g., product samples, printed reports).

- Isolated Backups: Keep a copy of critical data for analysis, separate from main systems to prevent tampering or deletion.
- How Long should organizations Retain Evidence:
- The organization retain evidence based on factors like legal, regulatory, and business factors. For instance, and organization will retain digital logs of high-risk organization like healthcare and finance for one to three years, Legal/compliance-related evidence for seven plus years, Product defect or safety incidents for three to five years, and HR/personnel investigations for three to five years.

Post-Incident Activity

Lessons Learned Meetings are Attended by

- Incident Response Team Lead (Security Operations Manager or CISO) to evaluate the effectiveness of the incident response lifecycle, identify procedural gaps, and ensure the lessons learned are incorporated into future incident playbooks.
- Network Administrator / Network Security Engineer to provide technical account of the discovery and mitigation process. Offers insight into network vulnerabilities or misconfigurations that allowed the incident to occur.
- IT Manager / Director of IT to review the overall impact on hotel systems and operations and helps determine if changes to policy, procedures, or training are needed across IT.
- Hotel Operations Manager to assess how the incident affected staff productivity and guest services and contribute perspective on operational disruptions and communication gaps during the incident.
- Legal and Compliance Officer / Data Protection Officer (DPO) to evaluate whether data protection policies were violated and decide if reporting to regulators or customers is necessary and advises on policy revisions.
- Human Resources (HR) Representative would help assess behavioral risk and determine appropriate disciplinary or corrective actions if an employee was involved (intentionally or unknowingly). He/she also contributes to employee training improvement plans.
- Facilities Manager / Building Security Leader to investigate how a device could have been physically installed without detection and proposes physical access restrictions or additional surveillance.
- Internal Audit or Risk Manager (if applicable) to assess whether the incident exposes broader vulnerabilities in hotel operations or IT governance and may also recommend updates to risk registers or audits.

To prevent similar incidents in the future the following should be implemented:

- **Stronger Physical Security**: including restricted access to network ports or areas where devices can be plugged in.
- **Zero Trust Architecture**: any device or access request should be assumed untrusted until verified.
- **Enhanced Employee Training** especially for housekeeping, IT, and engineering staff.

The following could be done to improve detection:

- **Automated Rogue AP Detection Tools** should be integrated into the SIEM (e.g., alerts triggered by unrecognized SSIDs).
- **Frequent Wireless Scanning by Security Teams** especially in guest areas.

- **AI-based Anomaly Detection** should be implemented capture sudden changes in network topology or traffic patterns.

Follow-Ups

How many incident response team members would participate in handling this incident?

Approximately 4 to 5 core members which include:

- Incident Response Lead
- Network Engineer
- Security Analyst
- IT Manager
- Documentation Support (optional but important)

Besides the incident response team, what groups within the organization would be involved in handling this incident?

- Hotel Operations Team if guests' services are impacted.
- Legal/Compliance especially with potential GDPR or regional privacy law implications.
- Facilities Management if physical access to install the rogue AP is suspected.

- HR if internal staff misconduct is involved

To which external parties would the team report the incident? When would each report occur? How would each report be made? What information would you report or not report, and why?

Data Protection Authority:

- **When:** Only if an investigation confirms that Personally Identifiable Information (PII)—particularly guest data—was accessed or exposed via the rogue access point within **72 hours of confirmation** of a data breach (as required by many data protection regulations).
- **I'm How:** Through official reporting portals (e.g., EU GDPR online forms if Rove serves European guests).
- **What to Report:** Nature and scope of the breach (if any guest data was at risk), affected data categories (e.g., login credentials, billing info), actions taken to mitigate the breach and contact details for follow-up (e.g., DPO or Legal Counsel).
- **What NOT to Report:** Internal technical weaknesses (e.g., specific firewall configs) and employee names or internal disciplinary actions.
- **Why:** Focused disclosure maintains transparency while protecting Rove's internal security posture and employee privacy.

Law Enforcement:

- **When:** If there is evidence the rogue access point was maliciously deployed by a guest, contractor, or external attacker, if tampering with hotel infrastructure is suspected.
- **How:** Through a formal incident report submitted to the Cybercrime Unit supported with technical logs, timestamps, and forensic findings.
- **What to Report:** Device MAC address, SSID, network logs, physical location where the AP was found, any surveillance footage or badge access logs if relevant.
- **What NOT to Report:** Sensitive guest data (unless required for the case) and full internal incident response report (share summary only).
- **Why:** To assist in investigation without breaching customer confidentiality or exposing internal vulnerabilities unnecessarily.

Hotel Guests (if impacted):

- **When:** If further investigation reveals the rogue access point **intercepted or mimicked the guest Wi-Fi network**, if guests' personal or payment data were exposed or there's a risk of phishing via rogue Wi-Fi.
- **How:** Via official email communication or through the hotel app, in some cases, with on-site staff communication if guests are still in the hotel.
- **What to Report:** That an unauthorized device was detected and removed, any actions they may need to take (e.g., reset passwords, avoid suspicious emails) and contact info for support (e.g., IT security hotline or guest relations).
- **What NOT to Report:** Technical details that may confuse or alarm guests unnecessarily and internal failures or delays in detection.
- **Why:** To maintain **guest trust**, uphold **transparency**, and meet **legal obligations**, while keeping the messaging clear and non-alarming.

Rove Hotels Corporate Office / Brand Oversight (If part of a larger group):

- **When:** Immediately after incident escalation or within the first 24 hours of confirmation.
- **How:** Internal reporting protocol (incident ticketing system, secured report submission), scheduled briefing with corporate IT/security leadership.
- **What to Report:** Incident summary, potential impact, and resolution steps, policy or infrastructure gaps identified, recommendations for group-wide mitigation (if systemic issue).
- **What NOT to Report:** Individual staff performance issues unless it involves misconduct.
- **Why:** For situational awareness and to inform enterprise-wide cybersecurity strategy updates.

Insurance Provider (If Covered Under Cybersecurity Insurance):

- **When:** If the incident results in financial loss, liability risk, or triggers a clause in the **cyber insurance policy**.
- **How:** Incident report submission via the insurer's digital claims platform or through the risk management/legal liaison.
- **What to Report:** Nature of incident affected systems, downtime, and any guest claims, costs associated with remediation, investigation, or legal counsel.
- **What NOT to Report:** Non-relevant incidents or internal policy reviews.
- **Why:** Ensures claim eligibility and accurate underwriting for future premiums.

What other communications with external parties may occur?

During the incident handling process, there is also some other sort communication with external parties to manage the situation effectively and minimize impact. Those communication types can vary depending on the nature of the incident and with which external parties do the incident response team communicates such as:

- Incident escalation, requesting technical support, or troubleshooting assistance communication can be done with vendors or service providers to resolve technical issues, obtain additional resources, or get expert guidance on addressing the incident.
- Requesting expertise, advice, or assistance in managing the incident can be done with third party incident response team or consultants to bring in external expertise when the internal team does not have the necessary resources or skills to handle the incident.
- Updating partners on the status of the incident and its impact on operations can be communicated with business partners or suppliers to manage dependencies, coordinate joint efforts for recovery, and minimize impact on business continuity.
- Informing about the incident, providing updates, and managing customer concerns can be communicated with customers or clients to maintain transparency, explain the impact, and keep clients informed about steps taken to resolve the incident.

What tools and resources would the team use in handling this incident?

The general list of tools and resources that the response team might use for any kind of cybersecurity incident includes:

Tool Type	Examples	Purpose

Security Information & Event Management (SIEM)	Splunk, LogRhythm, IBM QRadar	Aggregates and analyzes logs for signs of compromise.
Endpoint Detection & Response (EDR)	CrowdStrike, SentinelOne, Microsoft Defender	Detects threats on user devices and allows for remote isolation.
Forensics Tools	FTK, EnCase, Autopsy	Preserves and analyzes digital evidence.
Vulnerability Scanners	Nessus, Qualys, OpenVAS	Identifies security gaps to remediate after an incident.
Packet Capture Tools	Wireshark, tcpdump	Analyzes network traffic to detect intrusions.
Backup & Recovery Tools	Veeam, Acronis, Rubrik	Restores systems and data from clean backups.

Additional Resources:

- Incident Response Playbooks – pre-defined action plans for different scenarios.
- Subject Matter Experts (SMEs) – for technical, legal, HR, or operations insights.
- Legal Counsel – to navigate compliance and liability.
- PR/Communications Team – for consistent and reputation-aware messaging.
- Executives or Crisis Leadership Team – for major decision-making and resource allocation.
- Incident Retrospective Templates – for learning and documenting what went well or didn't.
- Training & Simulation Platforms – like Cyberbit, RangeForce, or tabletop exercise guides.
- Policy Documents & SLAs – to guide response within regulatory and contractual boundaries.

What aspects of the handling would have been different if the incident had occurred at a different day and time (on-hours versus off-hours)?

Incident handling can vary significantly depending on whether it occurs during on-hours (regular business hours) or off-hours (nights, weekends, or holidays). Here are some key aspects that would likely differ:

Staff Availability:

On-hours:

- Full staff are typically available, including technical support, incident response teams, and decision-makers. This allows for quicker coordination, communication, and resolution.

Off-hours:

- Limited staff may be on-call or unavailable, leading to delays in identifying, escalating, or resolving the incident.

Response Time:

On-hours:

- Response is usually faster due to active monitoring and immediate access to resources.

Off-hours:

- There may be delays due to the need to wake or notify personnel,

Communication and Escalation:

On-hours:

- Easier to escalate issues up the chain of command or coordinate across teams, since everyone is generally working.

Off-hours:

- Escalation protocols might rely on paging or call trees, which can slow things down, especially if contacts are missed or delayed.

Access to Resources:

On-hours:

- Support tools, systems, and physical access (e.g., to server rooms or data centers) are more readily available.

Off-hours:

- Access may be restricted or require special approvals, which can delay response efforts.

Impact Mitigation:

On-hours:

- Mitigation might be more complex due to active users or services running, requiring careful coordination to avoid disruption.

Off-hours:

- Easier to isolate systems or take them offline without affecting a large number of users, which can speed up containment.

Communication with Stakeholders:

On-hours:

- Easier to keep stakeholders informed in real-time.

Off-hours:

- Updates might be delayed or limited to key personnel only.

What aspects of the handling would have been different if the incident had occurred at a different physical location (onsite versus offsite)?

Incident handling can vary significantly depending on the physical location where it happened, mainly either onsite or offsite. Here are some key aspects that would likely differ:

Response Time

Onsite:

- Response tends to be faster because staff are physically present and can immediately assess & act.

Offsite:

- There may be delays as responders need to travel to the location or coordinate remotely, depending on the incident type.

Access to Resources

Onsite:

- Immediate access to equipment, documentation, or support tools is typically available.

Offsite:

- Limited or no access to critical resources may hinder the response and require additional coordination to bring necessary tools or personnel to the location.

Communication and Coordination

Onsite:

- Face-to-face communication enables quicker decision-making and clearer coordination.

Offsite:

- Communication is often done via phone, email, or video calls, which can slow down the process and lead to misunderstandings.

Support from Colleagues

Onsite:

- Easier to get help or input from nearby colleagues or department.

Offsite:

- More challenging to collaborate in real-time, especially if remote teams are involved and not familiar with the location.

Familiarity with Environment

Onsite:

- Staff are usually familiar with the layout, systems, and procedures, which helps in navigating the incident efficiently.

Offsite:

- Unfamiliar environments may pose logistical issues (e.g., not knowing who to contact, where equipment is located, or how systems are set up).

Authority and Decision-Making

Onsite:

- Authorized personnel are often readily available to make quick decisions or approvals.

Offsite:

- Delays may occur if key decision-makers are not present or reachable.

Documentation and Reporting

Onsite:

- Easier to document the incident in real-time and collect evidence.

Offsite:

- May rely on remote reporting, which could be less thorough or delayed.

Scenario 5 Follow-Ups

First Major Step in Handling the Incident

The first major step would depend on the nature of the incident:

- Physical Access Point Discovery: Physically locate and disable the rogue access point to prevent further unauthorized access.
- Logical Containment: Logically isolate the rogue access point from the network by disabling its connection.

Locating the Access Point

- Fastest Way: Use network scanning tools (e.g., Nmap) to identify the rogue access point’s IP address and MAC address. Cross-reference this with physical locations using asset documentation.
- Most Covert Way: Deploy wireless sniffers discreetly to avoid alerting the attacker while gathering intelligence.

External Party Deployment of the Access Point

If the rogue access point was deployed by an external contractor:

- Verification: Verify the contractor’s authorization and scope of work.
- Coordination: Work with the contractor to understand their setup and ensure compliance with security policies.
- Removal: If unauthorized, remove the access point immediately and escalate to legal/compliance teams for further action.

Suspicious Activity on Workstations

If intrusion detection analysts report suspicious activity on workstations:

- Correlation: Investigate whether the rogue access point is linked to the workstation activity.
- Containment: Isolate affected workstations from the network to prevent lateral movement.
- Forensics: Analyze workstation logs and memory dumps for malware or unauthorized access.

Access Point Removal During Investigation

If the access point is removed before it can be located:

- Log Analysis: Review historical logs to identify its presence and usage patterns.
- Forensic Evidence: Collect residual evidence from connected devices or network traffic.
- Policy Update: Strengthen physical and logical controls to prevent similar incidents in the future.

References

1. https://hyperproof.io/resource/cybersecurity-incident-response-plan/
2. https://www.techtarget.com/searchsecurity/feature/5-critical-steps-to-creating-an-effective-incident-response-plan
3. https://purplesec.us/learn/incident-response-steps/
4. 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
5. Computer Security Incident Handling Guide (nist.gov)
6. 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
7. 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.
8. 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
9. National Institute of Standards and Technology. (2012). *Computer security incident handling guide* (Special Publication 800-61 Revision 2). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-61r2
10. Scarfone, K., Grance, T., & Masone, K. (2008). *Computer security incident handling guide* (SP 800-61 Rev. 1). SANS Institute. https://www.sans.org/white-papers/incident/
11. Smith, J. A. (2025). *Effective communication strategies during incident handling*. Crisis Response Publications. https://www.crisisresponse.com/incident-communication
12. ISO/IEC 27035-1:2016 Information security incident management – Part 1: Principles of incident management International Organization for Standardization - Search
13. Incident Handler's Handbook | SANS Institute
14. Incident Management 101 Preparation and Initial Response (aka Identification) | SANS Institute
15. SP 800-61 Rev. 2, Computer Security Incident Handling Guide | CSRC
16. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf