How to Manage Cyber Incidents?

Covers four examples cover containment, analysis, remediation, review and lessons learned

www.thecyphere.com

info@thecyphere.com

Let's explore how businesses handle cyber threats.

From multinational corporations facing ransomware attacks to small startups dealing with phishing attempts, these examples underscore the critical importance of having a functional incident response plan.

»

Incident Management: The 4-step process

»

01. CONTAINMENT

Limiting the impact of the attack.

02. ANALYSIS

Understanding the nature and scope of the attack.

03. REMEDIATION

Eradicate the attacker and restore normal business operations.

04. REVIEW

Learn from the incident and improve the IR plan.

»

Incident 1 - Attempted Fraud

(Suspicious email requesting £500k payment)

»

Containment

- Suspicious £500k payment request from 'CFO' detected
- IT security alerted; CFO confirms no knowledge of email
- Temporary holds placed on large payments within 30 minutes
- Incident response team assembled, lead assigned
- CFO's account credentials reset within 1 hour

Analysis

- Email origin traced to CFO's compromised account
- Unusual remote logins detected from suspicious locations
- Consistent IP ranges identified, active for several weeks
- Initial analysis completed within 4 hours of detection

Remediation

- Affected staff credentials reset; malicious mailbox rules removed
- Multi-Factor Authentication (MFA) enforced company-wide
- Remote access policy reviewed and updated
- Legal team engaged for breach assessment
- Security provider contracted for forensic analysis within 24 hours

»

Review

- Phishing campaign linked to trusted partner networks
- Internal phishing emails isolated for further investigation
- Legal team determines no notification necessary based on accessed content
- Enhanced monitoring implemented for 30 days post-incident
- Incident response effectiveness evaluated within 1 week

How the IR plan helped?

- Coordinated response prevented fraudulent payment
- Expertise-driven team assembled within 2 hours
- Log analysis revealed extent of compromise within 8 hours
- Temporary security measures limited further unauthorised access
- Social engineering techniques identified and addressed

Lessons Learned

- Incident response plan updated for BEC scenarios
- Automated alerts implemented for unusual login patterns
- Partner network security assessment process established
- Regular phishing simulations scheduled for all staff
- Financial transaction verification process enhanced

Incident 02 - Malicious code

(Malicious code was discovered on a retail website)

Containment

- Malicious code detected on retail website
- Customer reports of card fraud trigger investigation
- Website taken offline promptly by the customer IT team
- Website hosting provider engaged for immediate support (because they said they provide security support)
- Incident response team activated within 1 hour

Analysis

- Malicious code presence confirmed for 2+ weeks
- Card detail logs identified as primary target
- Data exfiltration method uncovered within 24 hours
- Extent of compromised data assessed

Remediation

- Website thoroughly scanned with advanced security tools
- Comprehensive pen testing process implemented before relaunch and updates/releases
- Continuous scanning, monitoring and alerting added to standard processes
- Website relaunched within 72 hours of initial detection

Review

- Detailed timeline of events documented
- Unknowns clearly identified for transparent communication
- Heightened monitoring conducted for 4 weeks post-incident
- Daily security reports implemented for management

How the IR plan helped?

- Coordinated response limited potential damage
- Swift containment achieved within 2 hours of detection
- Stakeholder communication maintained throughout
- Customer impact assessed: 500 potentially affected cards
- Root cause identified: outdated plugin vulnerability

»

Lessons Learned

- Incident response plan updated for e-commerce scenarios
- Procured dedicated cyber security specialists rather than relying on IT service provider for cyber security
- Regular penetration testing schedule established
- Staff training on secure coding practices mandated
- Third-party security assessments now required for all changes and before major releases

Incident 3 - Ransomware

(Three users reported damaged files)

»

Containment

- IT security team initiates rapid response, prompting shut down of user machines.
- Affected machines shutdown across regions
- Critical file servers were taken offline as a precaution
- Third-party suppliers assist with SharePoint sync issues
- Business stakeholders were informed of outage

Analysis

- The IS team employs OSINT and threat hunting techniques on ransomware to scan and detect infection routes
- Compromised admin account spreading ransomware identified through domain controller logs
- 'Sync' with SharePoint had caused issues for other file users
- Attack timeline and impact assessed within 4 hours

Remediation

- Infection routes blocked; network scanned with EDR tools
- File servers restored from air-gapped backups
- Phased approach: READ-ONLY mode implemented first
- Business continuity plans activated
- Legal team consulted on data privacy implications

Review

- Full network scan for encrypted/malicious files
- Affected accounts reset; clean machines provisioned
- Network monitored for 72 hours before full restoration
- Root cause analysis completed within 1 week

How the IR plan helped?

- Evidence was gathered, analysed, and used to understand attack timelines, objectives, root cause, and vulnerabilities.
- Normal operations were restored, data loss minimised, and critical business functions restored.
- Re-access by attackers was prevented, ensuring legal and regulatory compliance.

Lessons Learned

- Incident response plan updated for ransomware scenarios
- Enhanced monitoring implemented for privileged accounts and account and password policies reviewed
- Regular tabletop exercises scheduled for IR team
- Investment in threat detection domain in terms of established processes and toolsets

The incident response plan puts your PEOPLE, PROCESS, and TECH controls to the test, ensuring they function as intended during an event.

Get in touch to test yours and be prepared.

Contact Us

info@thecyphere.com

Incident 4 - Targeted Attack

(Targeted attack to steal client data)

»

Containment

- CISO activates IT Security and external consultants
- Network traffic and host analysis initiated within an hour
- High-risk machines isolated
- Strategic traffic blocking and account resets implemented
- Malicious activity halted within 4 hours of detection

»

Analysis

- Firewall and proxy logs scrutinised for malicious connections
- Automated connections traced back 2 months
- Logs synchronised to UTC for precise timeline analysis
- Multiple malware variants identified on affected systems
- Intrusion source pinpointed to partner company within 24 hours

Remediation

- Continuous monitoring reveals 6 additional infections
- Network-wide scanning initiated within 48 hours
- Multi-region remediation plan executed:
    - Traffic blocking
    - Machine isolation
    - Account resets
- Third-party IT systems included in monitoring scope

Ongoing Response

- New suspicious activities swiftly addressed
- Previously unknown compromised admin accounts discovered
- Access attempts from new IP ranges blocked
- Full network remediation completed within 5 days

Review

- Comprehensive incident review conducted within 1 week
- Third-party connection security enhancements proposed
- Logging capabilities significantly expanded
- Incident response processes refined based on lessons learned
- Legal and PR teams engaged for stakeholder communication

How the IR plan helped?

- Evidence gathering centralised; attack timeline established
- Lateral movement prevented through swift isolation
- Root cause identified: compromised partner access
- Legal and regulatory compliance maintained throughout
- Reputation safeguarded through proactive PR management

Lessons Learned

- Implement stricter access controls for partner companies
- Enhance network segmentation to limit lateral movement
- Conduct regular security audits of third-party connections
- Improve log retention and analysis capabilities
- Establish a dedicated threat hunting process
- Schedule quarterly tabletop exercises for IR scenarios

LIKE THIS?

- ☑ Follow 🔔 and stay updated
- ☑ Get a free consultation to discuss your security concerns:

www.thecyphere.com
info@thecyphere.com