MSPs Guide to Incident Response Planning

> Give me six hours to chop down a tree and I will spend the first four sharpening the axe.
>
> — *Abraham Lincoln*

Every second matters for MSPs when responding to a security-related incident. Planning and preparation are critical for effective incident response (IR). IR is the process of preparing, detecting, containing and recovering from a data breach or cyberattack. The stakes are high for service providers since even a minor slip up has a ripple effect across your client base. Your incident response plan (IRP) should aim to optimize recovery times and mitigate collateral damage (e.g., brand reputation, employee productivity) for your clients.

To put IR into practice, your MSP needs a thoroughly documented and detailed plan to stop, contain and control an incident quickly. The IRP exists as a living, breathing document and is vital to any business continuity and disaster recovery (BCDR) strategy.

The following checklist breakdowns six key steps to creating an effective IRP:

01. **Preparation**
02. **Identification**
03. **Containment**
04. **Eradication**
05. **Recovery**
06. **Lessons Learned**

01. Preparation 

COMPONENTS	DESCRIPTION	
Policies	A documented set of principles, rules and practices that help determine whether an incident has occurred. Clear policies educate users on authorized/unauthorized actions and protect an organization from lawsuits and other legal action. Policies also ensure the organization publishes and maintains IR processes, provides workforce training, guidance and provides a secure channel to report incidents.	☐
Response Plan	Your strategy to handle a cybersecurity-related incident or data breach. Determine how you will prioritize incidents based on their perceived organizational impact. Prioritization helps determine appropriate response and helps build the case to garner management buy-in to ensure the necessary resources are being devoted to IR preparation.	☐
Communication Plan	Communication is a vital aspect of IRP. It may be necessary to contact specific individuals (client, employee) during an incident. The plan should document how employees can report an incident, who to contact, when it's appropriate to contact them, how to contact them and why. Effective communication helps minimize response time.	☐
Incident Response Team (IRT)	The IRT is composed of individuals from different disciplines to manage various aspects of incident response. At a minimum, your IRP should have the core team members including: Incident Response Team Lead (provides operational direction and oversight to the IRT, serves as the central point of contact), Incident Response Team Subject Matter Expert (SMEs assist the team lead in the creation of processes and standards, and provide technical documentation and support as needed) and an Executive Sponsor (a member of leadership who works with the IRT lead to ensure appropriate education and training is provided, the IRP &IRT is assembled, coordinated and maintained, and provides approval and oversight for all documents developed by the IRT).	☐
Access Controls and Tools	Ensure that the IRT has appropriate resources, tool and permissions (these may be a combination of digital and physical assets) to perform their roles as required. Tools also include documentation such as checklists, manuals and archives of prior incidents.	☐
Training	To identify gaps in the plan and ensure all individuals are able and prepared to perform their duties, the IRT should conduct mock drills at regular intervals. Self-assessment is critical to adjust and tweak the plan as gaps or deficiencies are uncovered during a mock or real-life incident.	☐

02. Identification

COMPONENTS	DESCRIPTION	
Monitoring	Prior to an incident occurring, you may use various tools to monitor client logs, networks, disks and firewalls. These tools are often used in combination with a security information and event management (SIEM) solution.	☐
Verification	Verify that a critical security incident has actually occurred. Determine what assets are affected (systems, networks, locations), what users are involved and the potential operational impact. The IRT should verify enough information regarding an incident to determine the appropriate response strategy.	☐
Notification/ Communication	MSPs should automate IR tasks wherever possible. Notifications is one such area. Automated notifications ensure the right owners are notified at different stages of an incident as required and contact is maintained with end users and stakeholders until the incident is resolved.	☐
Communication	MSPs should automate IR tasks wherever possible. Notifications is one such area. Automated notifications ensure the right owners are notified at different stages of an incident as required and contact is maintained with end users and stakeholders until the incident is resolved.	☐
Initial Analysis and Triage	In determining how to respond to a security incident, consider the following: • When did the incident occur? When was it discovered? • How critical are the affected systems? • What is the level of sensitivity of exposed, compromised or stolen information? • What level of unauthorized access was gained by the perpetrator(s)? • What is the apparent skill of the perpetrator(s)? • How much system and user downtime can be tolerated? • What do we estimate for potential total dollar loss? • What are the potential legal obligations? The IRT must take the necessary steps to protect the integrity of the information related to a security incident.	☐
Classification	Classification aids in formulating the appropriate response to an incident. Low-risk incidents may involve a single workstation, medium-risk incidents may impact a common application, shared network or VLAN, and high-risk incidents threaten confidential information or customer personable identifiable information (PII) and risk causing significant damage to company assets.	☐
Preservation of Evidence	Your first instinct may be to delete infected files – do not destroy evidence. Quarantine infected machines by disconnecting them from the LAN and WAN and isolating them along with any other impacted systems. Throughout this process, it will be critical to preserve all possible evidence and document all measures taken by the IRT.	☐

03. Containment 

COMPONENTS	DESCRIPTION	
Short-Term Containment	Limit the damage quickly. You may need to isolate a network segment of infected machines or takedown production servers while rerouting traffic to a failover host. Short-term containment is intended to limit the incident, avoiding further damage to the business.	☐
System Backup	Before wiping and reimaging impacted systems, it's critical to take a forensic image of the affected systems as they were during the incident. This preserves evidence in the event of criminal activity. A backup strategy must be in place to ensure client data remains accessible and safe. Best practices, at minimum, dictate three copies of data, two different formats and one copy that is offsite and immutable (such as a cloud backup copy).	☐
Long-Term Containment	This is a good time to update and patch systems. Apply security updates and harden against any discovered vulnerabilities. Review remote access protocols (2FA should be mandatory) and change all user and administrative access credentials as well as hardening all user passwords.	☐

04. Eradication 

COMPONENTS	DESCRIPTION	
Malware Removal	Once contained, all malware must be securely removed. In many cases, re-imaging systems from the default image or recovering bare metal backups will ensure no remnants remain within systems.	☐
Environmental Hardening	Once all malware has been removed, systems should again be hardened, patched and have all updates applied. New software, endpoint detection and response systems, network monitoring, etc., may be installed in the efforts to reduce future exposure.	☐

05. Recovery

COMPONENTS	DESCRIPTION	
Testing	Machines should be tested before being returned to production. The use of an isolated lab for pre-production testing ensures backups are clean before pushing machines into production.	☐
Restore to Production	The IRT will work with the client to determine a safe time and date to restore operations. System operators/owners will make the final decision to push into production based on the guidance and recommendations of the IRT.	☐
Post-Production Monitoring	Systems should continue to be monitored for a period of time to observe for abnormal behaviors. Operators should work with the IRT to determine how long systems will be monitored and what to look for while monitoring. Additional tools may be implemented (i.e., file integrity monitoring) with the goal of preventing a similar incident in the future.	☐

06. Lessons Learned

COMPONENTS	DESCRIPTION	
Debrief & Self-Evaluation	The IRT should hold an after-action meeting to discuss findings and learnings from the incident. It includes analysis of procedures, policies and documentation. Determine what worked well and where loopholes may exist. Lessons learned from mock and real-life events will help strengthen your IRT and systems against future attacks.	☐
Update Documentation	Update IR documentation or other such policies with information that may have been missing, omitted or incomplete prior to an incident. Additionally, fully document all remediation efforts to provide insight to clients and update IR archives for future use.	☐

Unitrends MSP offers enterprise-class Business Continuity and Disaster Recovery (BCDR) with a unified platform for end-to-end data protection, built-in defense against ransomware and instant recovery from any disaster.

Recovery Assurance certifies clients' runbooks and makes life easy for your technicians by automating backup testing — Unitrends spins up backups in an isolated lab environment and validates boot orders, dependencies and application-level services. Server performance and compliance tracking (Recovery Point and Recovery Time Actuals) are automatically pulled into easily exportable reports, providing complete visibility and full confidence into recovery for each and every client.