HACKTHEBOX

90-day recovery checklist for Scattered Spider incidents

Scattered Spider (AKA UNC3944) is a criminal group known for helpdesk-centric social engineering, credential theft, data extortion and ransomware recently deploying DragonForce.

This checklist is a general outline intended to guide your organization through a 90-day recovery process after a Scattered Spider incident. We've divided it into phases and by stakeholder role, and incorporates industry-specific compliance steps where applicable. We've also highlighted best practices (e.g. offline backups, phishing-resistant MFA) and regulatory timelines.

Immediate response | Days 1-3

Role/Stakeholder	Action checklist
Executive Leadership (CEO/ CISO/Board)	☐ **Activate Incident Response (IR) plan** and convene the incident command structure (CISO or designated Incident Manager) immediately. ☐ **Notify senior leadership/board** about the breach and delegate authority for rapid decision-making.
Cybersecurity/ IR Team	☐ **Confirm breach scope and contain** the attack: isolate affected networks/systems (disable compromised accounts, block malicious IPs/ domains, etc.). ☐ **Preserve evidence**: collect forensic images of affected hosts, capture live memory, preserve logs with chain-of-custody. ☐ **Escalate to authorities**: report the incident to CISA and FBI Cyber or local law enforcement as appropriate.
IT/Infrastructure Operations	☐ **Implement emergency fixes**: enforce network segmentation, disable exposed remote access (VPN/RDP), and change administrative passwords immediately. ☐ **Safeguard backups**: ensure all critical data backups are offline/ immutable (physically separate storage), to preserve clean copies.
Legal/ Compliance	☐ **Engage counsel** (internal & external) to advise on legal obligations. Identify and prioritize breach notification requirements under sector laws (e.g. HIPAA, GLBA, FISMA, state breach laws, SEC rules). ☐ **Record details**: Document the incident timeline and affected data; preserve communications and evidence for investigations and potential litigation. ☐ **Invoke** any Cyber Insurance process and requirements.
Communications & Public Affairs	☐ **Internal notification**: Inform employees and key stakeholders of the incident status with approved messaging. Prepare a “holding statement” for the press if needed. ☐ **Media monitoring**: Assign PR team to track rumors or media queries; coordinate with legal to control messaging.
Threat Intelligence/ Sharing	☐ **Collect Indicators of Compromise (IoCs)** from affected systems (IPs, domains, hashes, etc.). ☐ **Share and consume threat intel**: Report IoCs/TTPs to industry ISACs (e.g. FS-ISAC, H-ISAC), CISA AIS/JCDC and law enforcement (FBI/CISA) to seek guidance and assist collective defense. Begin coordinating with peer organizations on intelligence. ☐ **Monitor for signs** of the attackers posting about the breach on dark web sites or other forums.

Short-term recovery | Days 4-30

Role/Stakeholder	Action checklist
Executive Leadership/ CISO	☐ **Oversee full investigation and recovery**: Ensure IR team and IT have necessary resources (budget, tools, external expertise, e.g. forensic consultants or Incident Response vendors) to complete containment and remediation. ☐ **Coordinate with regulators/insurers**: Notify cyber insurers and prepare for potential regulatory reports. Update senior stakeholders (board, regulators) on progress in line with disclosure rules (e.g. SEC Form 8-K if public).
Cybersecurity/ IR Team	☐ **Forensics and eradication**: Perform deep forensic analysis to identify root cause and scope (e.g. compromised user accounts, malicious services), remove malware/ backdoors, and repoint or rebuild affected systems. ☐ **Harden authentication**: Reset all potentially compromised credentials, enforce strong, phishing-resistant MFA (FIDO/WebAuthn or certificate-based) especially for privileged accounts. ☐ **Continuous monitoring**: Enhance logs and alerts to detect any indication that the attacker has retained persistent access; resume vigilant 24×7 SOC monitoring of critical assets.
IT/Operations	☐ **Restore systems/services**: Rebuild or restore affected servers and network devices from secure backups. Verify integrity of backups before use. ☐ **Patching and configuration**: Apply critical patches (especially known exploited vulnerabilities) to all systems. Disable unnecessary services/ports. Implement network segmentation to limit future spread.
Legal/ Compliance	☐ **Regulatory notifications**: Finalize and submit required breach reports: ☐ **HIPAA**: Notify HHS OCR and affected individuals without unreasonable delay (no later than 60 days). ☐ **GLBA/FTC**: If a financial institution, notify FTC (and impacted customers per state law) within 30 days for breaches of 500+ records. ☐ **SEC**: Public companies should consider SEC rules – file Form 8-K (Item 1.05) for material incidents (or Item 8.01 if still assessing materiality) within required timeframes. ☐ **Law enforcement liaison**: Coordinate additional information requests from FBI/ CISA and comply with their investigation. Maintain a strict chain of custody documentation for evidence.
Communications/ PR	☐ **Stakeholder updates**: Provide interim briefings to customers, partners and media (if breached data is public) under guidance of legal. Use clear, factual language to maintain trust. ☐ **Messaging strategy**: Draft more detailed press release or customer notification as facts solidify. Prepare Q&A sheets for executives. Continue to monitor and correct misinformation.
Threat Intelligence/ Sharing	☐ **Industry collaboration**: Participate in ISAC/ISAO threat calls (e.g. joint healthcare or financial task forces) to share lessons learned and gather additional context on the attacker's actions. ☐ **Indicator dissemination**: Feed sanitized IoCs and TTPs into security tools and threat platforms, and share with peers (e.g. via AIS). Work with vendors (EDR, SIEM) to tune detections for Scattered Spider activity. ☐ **Continue monitoring** dark web forums

Medium-term recovery | Days 31-60

Role/Stakeholder	Action checklist
Executive Leadership/ CISO	☐ **Review incident impact:** Assess business and reputational damage. Update enterprise risk and cybersecurity strategy to reflect lessons (e.g. increased phishing resilience, helpdesk security). ☐ **Board and regulator reporting**: Provide final summaries to the board and regulators. Ensure any contractual or legal obligations (e.g. investor disclosures, audit findings) are addressed.
Cybersecurity/ IR Team	☐ **Verify full recovery**: Confirm all compromised systems have been rebuilt or cleaned and that no malware persists. Increase network and endpoint monitoring for any sign of residual compromise. ☐ **Security audit and hardening**: Perform thorough audits of account privileges and network segmentation. Implement recommended mitigations (e.g. block unapproved remote access tools, enforce policy on portable executable use).
IT/Operations	☐ **Long-term restorations:** Complete restoration of remaining systems/ services. Test applications and data access for all user groups. ☐ **Disaster recovery (DR) exercises**: Conduct DR drills using the lessons from this incident (e.g. restore operations from backups). Refine DR/BC plans.
Legal/ Compliance	☐ **Regulatory follow-up**: Submit any supplemental breach reports (e.g. annual updates for HIPAA if under 500 records). Coordinate with regulators on any required audits (e.g. HHS OCR requests, FTC inquiries). ☐ **Compliance program updates**: Review and update security policies and incident response plan based on what was learned. Ensure contracts (business associates, vendors) have appropriate incident-notification clauses.
Communications/ PR	☐ **Final communications**: If needed, issue a final public report or statement detailing incident resolution and steps taken. Highlight improvements to reassure customers and stakeholders. ☐ **Brand rehabilitation**: Plan longer-term communication efforts (e.g. customer reassurance campaigns, updated FAQs, enhanced transparency) to rebuild trust.
Threat Intelligence & Training	☐ **Lessons learned workshop**: Organize a cross-functional “lessons learned” meeting (mandatory for major incidents) to review what went well and gaps in response. Document these findings in an after-action report. ☐ **Security training**: Roll out targeted training (e.g. advanced phishing social engineering scenarios) for staff, especially helpdesk/IT personnel, emphasizing recent tactics like MFA fatigue and SIM-swapping.

Long-term recovery and resilience | Days 61-90

Role/Stakeholder	Action checklist
Executive Leadership/ CISO	☐ **Implement improvements**: Ensure all recommendations from the lessons-learned report are funded and tracked (e.g. stronger identity management, helpdesk authentication protocols). ☐ **Governance and audit**: Present a final incident review to the board/ executive committee. Verify that all regulatory and insurance requirements have been closed out.
Cybersecurity/ IR Team	☐ **Post-incident audit**: Commission an external security assessment (pen-test or red team) to validate that vulnerabilities exploited by the threat actor have been remediated. ☐ **IR plan update**: Revise the incident response plan and playbooks incorporating new threat intelligence. Conduct a tabletop exercise simulating the attack to test readiness.
IT/Operations	☐ **Backup validation**: Ensure backup/restore procedures are fully documented and tested end-to-end; encrypt and protect backup media. Maintain offline backups per best practices. ☐ **Technology upgrades**: Replace or upgrade any outdated or "living off the land" tools identified (e.g. legacy remote-admin software), and strengthen network segmentation (micro-segmentation, Zero Trust).
Legal/ Compliance	☐ **Closing compliance loop**: Finalize any remaining breach notification obligations (e.g. state laws). Prepare for potential regulatory investigations (have documentation ready). ☐ **Audit readiness**: Schedule a compliance audit (HIPAA, GLBA, FISMA, etc.) incorporating incident findings to demonstrate remediation. Review FedRAMP continuous monitoring reports if applicable.
Communications/ PR	☐ **Reputation management**: Continue engaging customers and media with updates on security improvements. Publish lessons learned or case studies (redacted) in industry forums if permitted. ☐ **Share success stories**: Highlight how the organization has become more resilient (e.g. adoption of phishing-resistant MFA) to improve public confidence.
Threat Intelligence & Training	☐ **Information sharing**: Provide anonymized incident data (e.g. IOCs, TTPs summary) to ISACs, CISA, FBI and peer organizations to strengthen collective defenses. ☐ **Ongoing vigilance**: Remain alert for Scattered Spider or similar groups leveraging discovered methods. Update threat feeds and SIEM with custom signatures for any newly identified attack patterns.