Final Report

Scenario

On June 18, 2025, at 11:42 a.m. (UTC+2), the organisation experienced a **security incident** involving unauthorised access to internal human resources (HR) records, including personally identifiable information (PII) and payroll data. Approximately **12,800 employee records** were affected. The estimated financial impact is **$65,000** in direct costs and potential loss due to reputational harm.

The incident began on June 16, 2025, at 9:05 a.m., when an HR specialist received an email appearing to be from the organisation's internal IT support team. The email contained a link to a fake "mandatory HR policy update" portal. Believing the email was legitimate, the employee entered their credentials into the phishing site.

Two days later, the attacker used the stolen credentials to log in to the HR system via the organisation's VPN. From there, they exported payroll and contact information for all active employees. At 2:18 p.m. the same day, the attacker sent an extortion email to the HR department demanding **€40,000 in cryptocurrency** to prevent public release of the data.

The HR director immediately escalated the incident to the Security Operations Center (SOC). A coordinated investigation and response effort was launched, which included disabling compromised credentials, reviewing VPN logs, and identifying the scope of the breach. The attack was contained within four hours of detection, and no further unauthorised access was observed.

The primary lesson learned from this incident is the importance of **multi-factor authentication (MFA)** for VPN access and improved phishing detection and response procedures.

Executive Summary

This incident was classified as a **credential compromise leading to data theft**.

- **Date/Time of Incident:** June 18, 2025, 11:42 a.m. (UTC+2)
- **Affected Data:** Employee PII and payroll data (12,800 records)
- **Attack Method:** Spear-phishing email and VPN credential abuse
- **Estimated Financial Loss:** $65,000 (direct costs and reputational damage)
- **Status:** Closed after full investigation and remediation

Recommendations to prevent recurrence:

1. Enforce MFA for all VPN logins.
2. Conduct quarterly phishing simulation training.
3. Implement anomaly-based VPN login detection.

Timeline

Date/Time (UTC+2)	Event	Details
16/06/2025 - 09:05	**Phishing Email Received**	HR specialist receives fake IT support email with malicious link.
16/06/2025 - 09:12	**Credential Theft**	Employee enters credentials into phishing site hosted at hr-policy-update[.]net.
18/06/2025 - 11:42	**Unauthorised Access Detected**	Attacker logs in via VPN from IP 91.214.44.182 using stolen credentials.
18/06/2025 - 12:05	**Data Exfiltration**	Payroll database and contact list exported (~12,800 records).
18/06/2025 - 14:18	**Extortion Email Sent**	Attacker demands €40,000 in cryptocurrency.
18/06/2025 - 14:22	**Incident Escalation**	HR Director notifies SOC; investigation begins immediately.
18/06/2025 - 15:50	**Containment**	VPN session terminated, credentials disabled, attacker IP blocked.
19/06/2025 - 08:30	**Post-Incident Actions**	Forensic analysis of logs, phishing site reported to hosting provider, MFA rollout planned.

Investigation

The SOC confirmed the attacker gained access via compromised VPN credentials stolen through a **spear-phishing campaign**. Analysis of VPN access logs revealed that the attacker authenticated from an IP address in Eastern Europe not previously associated with the employee's account.

Further investigation showed that once inside the VPN, the attacker navigated directly to the HR payroll system, executed multiple export queries, and downloaded sensitive data. No signs of lateral movement or privilege escalation beyond the stolen account's access rights were found.

Artifacts collected included phishing email headers, phishing site screenshots, VPN logs, and the exported data access logs.

Response and Remediation

- Disabled compromised user credentials and terminated active sessions.
- Blocked malicious IP addresses and domains associated with the phishing site.
- Reported the phishing site to its hosting provider, resulting in takedown within 12 hours.
- Implemented urgent VPN policy changes to require MFA for all users.
- Coordinated with PR to inform employees and provide credit monitoring services.

Recommendations

1. **Mandatory MFA for VPN Access** - Eliminate single-factor VPN authentication.
2. **Phishing Awareness Training** - Conduct targeted simulation campaigns, focusing on HR and finance teams.
3. **Anomaly Detection for Remote Logins** - Implement alerts for suspicious IP geolocations and login patterns.
4. **Rapid Incident Escalation Protocols** - Require all suspicious emails to be reported to SOC for validation before deletion.

PART 2

Appendix A – Attacker Kill Chain & Defender Response

Kill Chain Stage	Attacker Activity (TTPs)	MITRE ATT&CK Mapping	Defender Response
1. Reconnaissance	Attacker identifies HR staff via LinkedIn and scrapes public contact info.	**TA0043 Reconnaissance**	N/A - No detection; activity occurred externally.
2. Weaponization	Creates spear-phishing email impersonating internal IT support. Embeds malicious link to credential harvesting site hosted at hr-policy-update[.]net.	**T1566.002 Phishing: Spearphishing Link**	N/A - Initial delivery bypassed email security filters.
3. Delivery	Sends phishing email to selected HR specialist.	**T1566 Phishing**	Email reaches inbox; no initial user report.
4. Exploitation	Victim clicks link and enters credentials into fake login page.	**T1078 Valid Accounts**	Credentials stolen; no MFA enforcement in place.
5. Installation	Attacker stores harvested credentials for later use; no malware installed.	**T1078 Valid Accounts**	N/A - No endpoint infection detected.
6. Command & Control (C2)	Attacker logs into VPN from foreign IP address using stolen credentials.	**T1133 External Remote Services**	SOC detects unusual login location during investigation, not in real-time.
7. Actions on Objectives	Direct access to HR payroll system; executes export queries for employee data; exfiltrates ~12,800 records. Sends extortion email demanding €40,000.	**T1041 Exfiltration Over C2 Channel**	Credentials disabled, VPN session terminated, IP address blocked. Incident escalated to full investigation.

Observations from the Kill Chain

- **Key Weakness:** No MFA on VPN access allowed stolen credentials to be used without additional barriers.
- **Detection Gap:** No automated geolocation-based alerting for VPN logins from unusual IP ranges.
- **Success:** Once SOC was engaged, containment was rapid (<4 hours from detection to closure).

Additional Technical Indicators of Compromise (IOCs)

Type	Value
Malicious Domain	**hr-policy-update[.]net**
Malicious IP	**91.214.44.182**
Phishing Email Subject	**Mandatory HR Policy Update - Action Required**
File Hash (Phishing Page HTML)	**b7c8e2f9e89d4a54a6eae2714d8d6e4f23bfae3b7b55e3cceef402b6c32faae3**

Visual Summary – Kill Chain Flow

[Attacker]
LinkedIn Recon → Spear-Phishing Email → Credential Harvesting Site → VPN Login with Stolen Credentials → HR Payroll System Access → Data Export & Exfiltration → Extortion Email

[Defender]
Initial Non-Detection → User Reports Second Email → SOC Investigation → VPN Session Terminated → Credentials Disabled → IOC Blocking → PR & Employee Notification → MFA Rollout

---

Part 3

Lessons Learned - Red & Blue Team Perspectives

Red Team Perspective (Attacker Insight)

- **Recon Success:** Publicly available employee role information made targeting simple. Limiting role/title exposure on LinkedIn or public pages could reduce targeting opportunities.

- **Delivery Effectiveness:** The phishing email bypassed standard email filtering due to convincing domain spoofing and well-crafted internal branding.

- **Exploitation Opportunity:** Lack of multi-factor authentication (MFA) provided a clear path from credential theft to system access without needing privilege escalation or malware deployment.

Red Team Takeaway: Even without advanced malware or zero-days, attackers can achieve high-value data theft through minimal but strategic steps when social engineering is effective and key defenses (MFA, anomaly detection) are absent.

Blue Team Perspective (Defender Insight)

- **Detection Gap:** Initial login anomaly detection was reactive rather than real-time, allowing data exfiltration before response.

- **Process Gap:** The first phishing email was deleted by the employee without reporting it, delaying SOC engagement.

- **Response Strength:** Once escalated, containment was executed rapidly, limiting the incident's operational and reputational damage.

Blue Team Takeaway: Improve early detection and escalation protocols to engage SOC before attacker objectives are met. Pair technology upgrades (MFA, anomaly detection) with reinforced employee security awareness and mandatory suspicious email reporting.

Joint Security Posture Improvement Plan

1. **Implement MFA** for all remote access points, particularly VPN and administrative portals.

2. **Deploy Anomaly-Based Login Detection** with geolocation, time-based, and velocity-of-travel alerts.

3. **Conduct Role-Specific Phishing Drills** for HR, finance, and executive teams to simulate realistic attack vectors.

4. **Establish Immediate SOC Notification Protocols** for all suspected phishing attempts, with an easy “report phishing” button in email clients.

5. **Red Team Simulations** every six months to validate that detection and response workflows can identify and stop similar credential-based intrusions.