



Computer Network Defence Ltd

BEYOND THE BREACH

FROM CHAOS TO CONTROL

ATTACK VECTORS, INCIDENT RESPONSE & NCSC GUIDANCE

Threat Actor: Scattered Spider (Octo Tempest)

Date: April 2025

Impact: Up to £440M across UK retailers

Presented By: **Jeff Ames and Charles Bain**

EXECUTIVE SUMMARY

Critical Incident Overview

- **Target:** Marks & Spencer – Leading UK retailer
- **Attack Vector:** Multi-stage social engineering & supply chain compromise
- **Services Affected:** Online clothing orders, gift cards, customer databases
- **Customer Impact:** Personal data compromised, services suspended
- **Financial Impact:** Estimated £440 million across multiple retailers
- **Resolution:** Four arrests made in July 2025



ATTACK TIMELINE

February
2025

Initial
compromise
suspected -
Scattered Spider
gains initial
access

April
2025

Full-scale
attack
execution -
M&S forced to
suspend online
services

May
2025

M&S confirms
customer data
access - Public
disclosure

June
2025

Attribution to
Scattered Spider
confirmed -
Investigation
findings

July
2025

Law enforcement
arrests - Four
individuals
apprehended



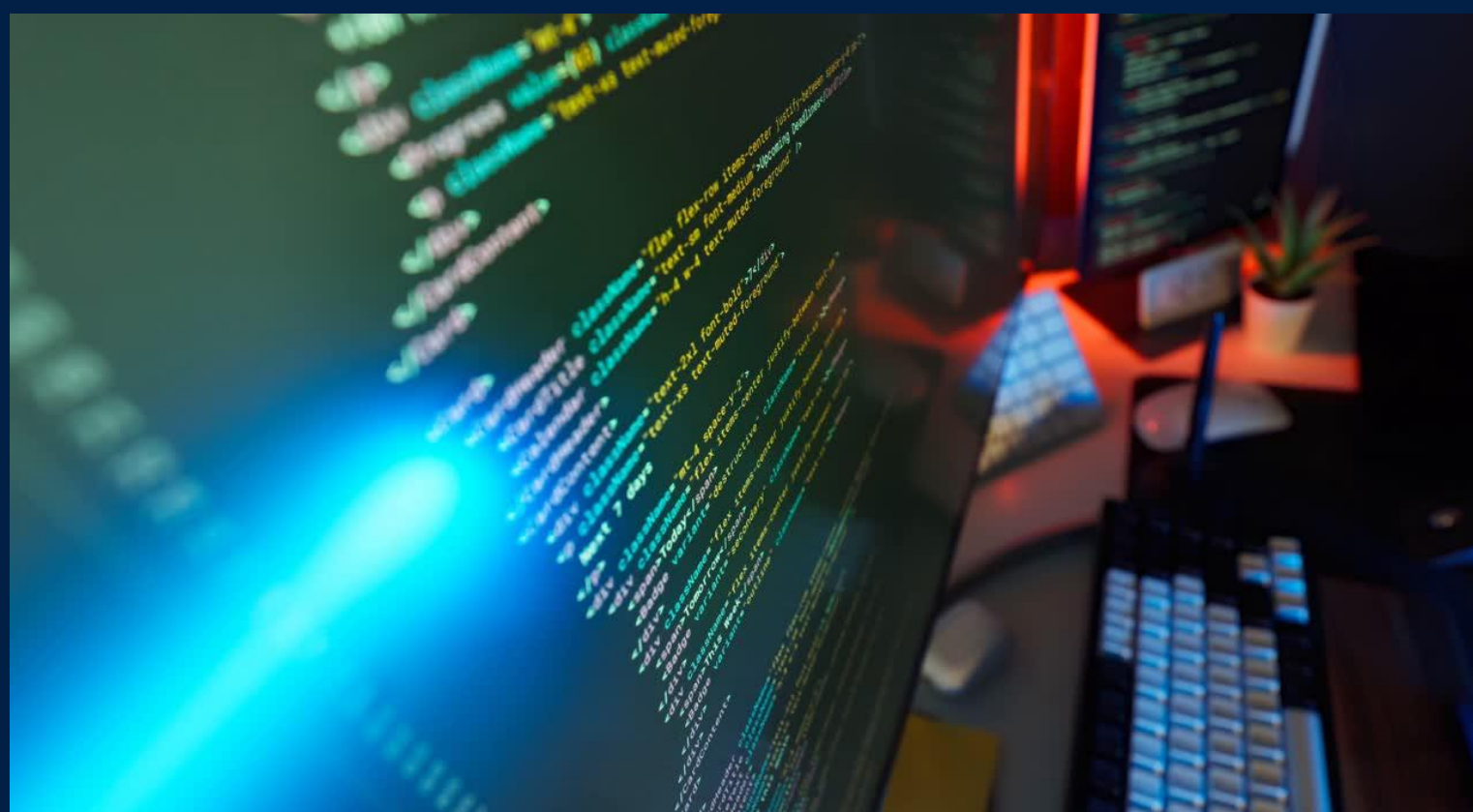
ATTACK VECTOR 1: SOCIAL ENGINEERING

Primary Techniques

- **Help Desk Impersonation:** Attackers posed as IT support staff
- **Vendor Impersonation:** Leveraged compromised TCS credentials
- **Phone-based Social Engineering:** Direct employee contact
- **SIM Swapping:** Mobile number hijacking for 2FA bypass

Technical Impact

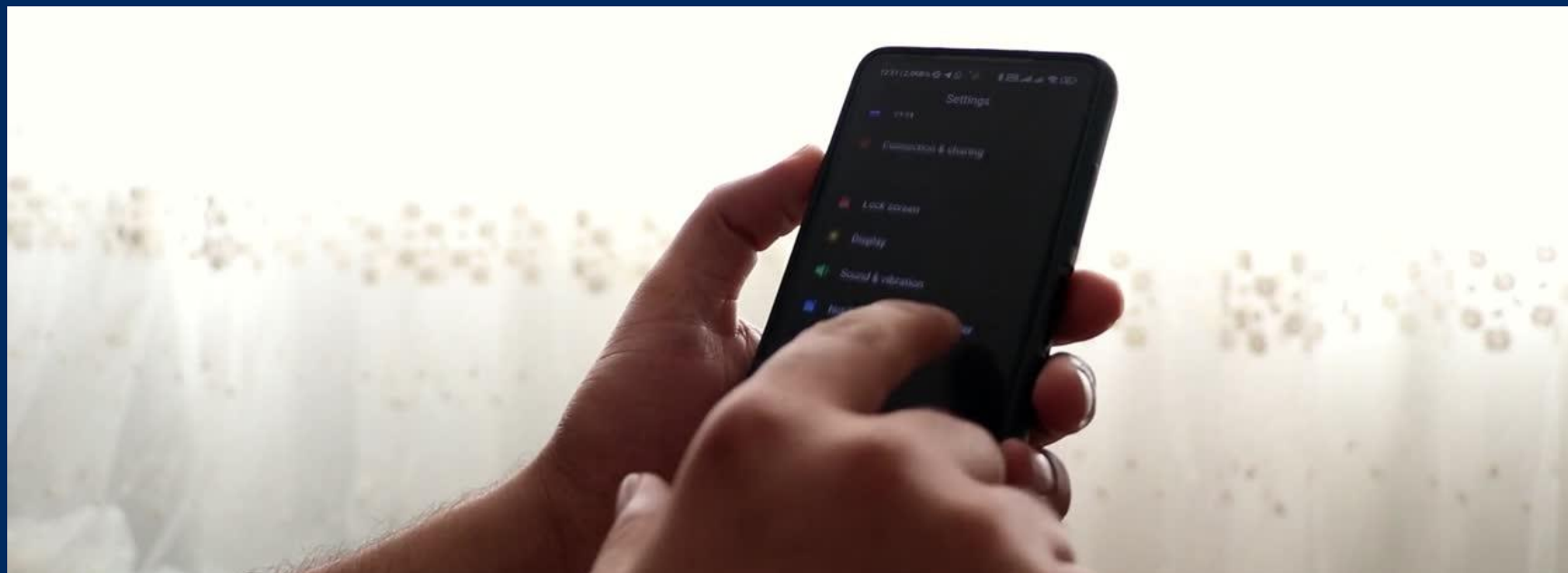
- ➔ Targeted SSO platforms through credential theft
- ➔ Exploited trust relationships with third-party vendors
- ➔ Gained administrative access through psychological manipulation



ATTACK VECTOR 2: CREDENTIAL-BASED ATTACKS

Methods Employed

- Credential Harvesting: Phishing campaigns targeting logins
- NTDS.dit Exfiltration: Windows domain database theft
- Privileged Account Compromise: Administrative access escalation



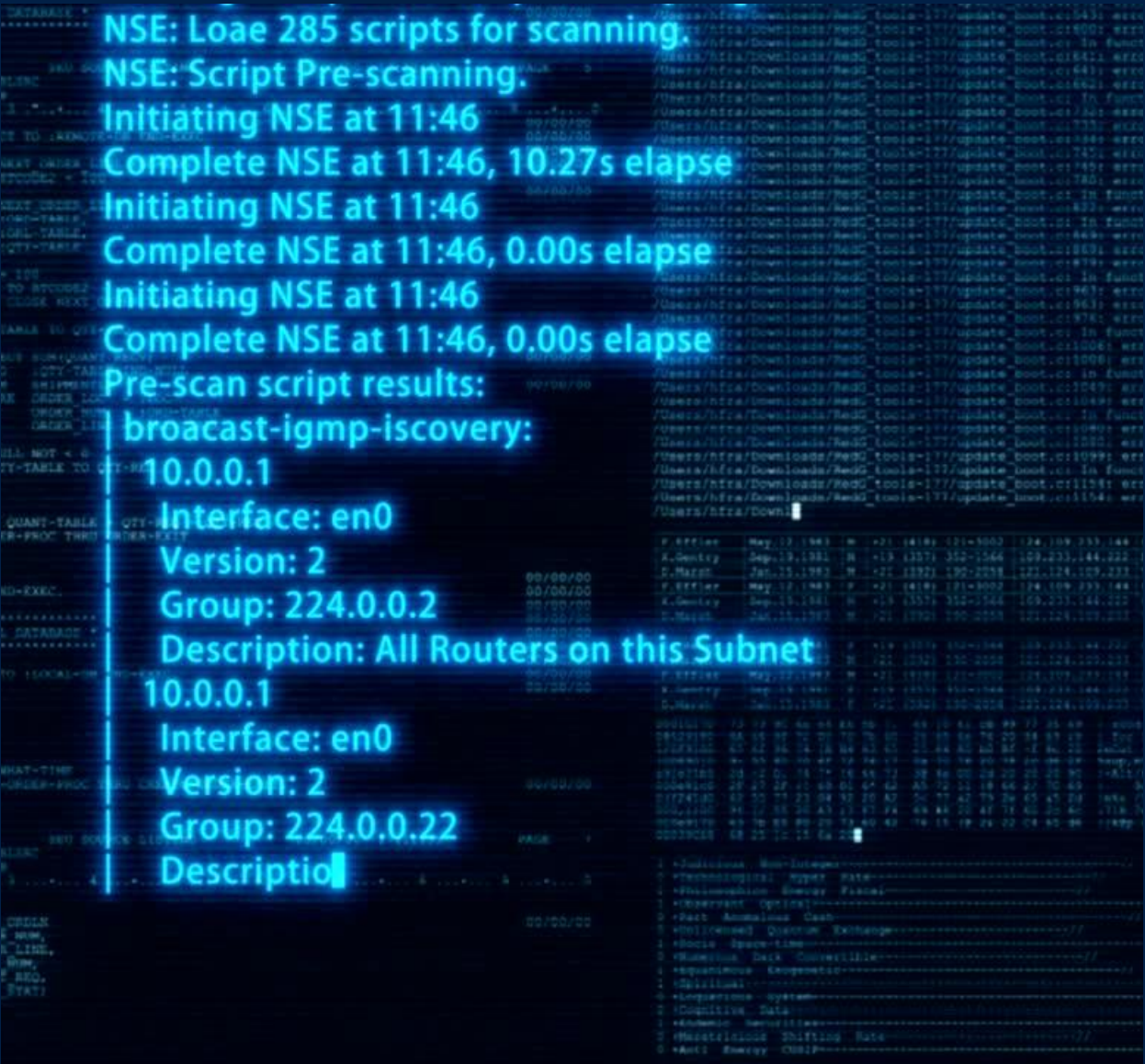
Authentication Bypass

- ➔ SIM swapping for MFA bypass
- ➔ Social engineering of help desk
- ➔ Password hash cracking
- ➔ Session hijacking techniques

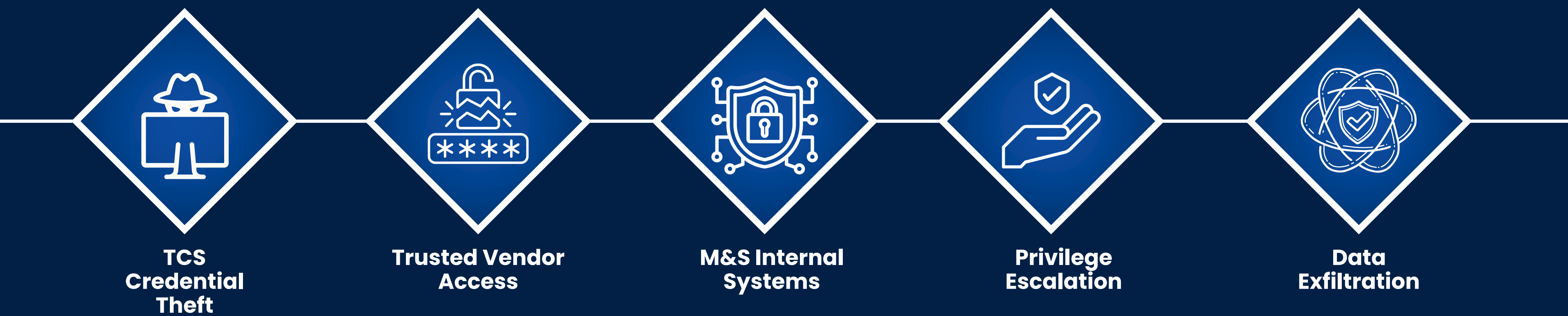
ATTACK VECTOR 3: SUPPLY CHAIN COMPROMISE

TCS (Tata Consultancy Services) Compromise

- Initial Vector: Compromised TCS credentials
- Trust Exploitation: Leveraged existing vendor relationships
- IT Outsourcing Risk: Exploited dependency on third-party services
- Legitimate Tools: Used AnyDesk, ScreenConnect for persistence



Attack Chain Progression



ATTACK VECTOR 4: TECHNOLOGY EXPLOITATION

Tools & Techniques

- Living-off-the-Land: Legitimate admin tools
- Cloud Misconfigurations: Enterprise platform exploitation
- Remote Access Tools: Persistent backdoor access
- Ransomware Deployment: Final impact payload

Key Insight

Scattered Spider specialises in using legitimate business tools to avoid detection, making their activities appear as normal IT operations.



M&S INCIDENT RESPONSE: IMMEDIATE ACTIONS



Effective Actions

- Service Isolation: Suspended affected online services
- Customer Communication: Proactive service disruption notifications
- Expert Engagement: Cybersecurity specialists consulted
- System Containment: Isolated compromised infrastructure

Areas for Improvement

- Detection Gap: February–April progression suggests delayed detection
- Third-party Monitoring: Limited visibility into vendor activities
- Early Warning: Insufficient threat intelligence integration

M&S INCIDENT RESPONSE: RECOVERY PHASE

May – June 2025 Actions

Data Assessment & Disclosure

- Confirmed customer data access through forensic analysis
- GDPR-compliant regulatory notification to ICO
- Transparent customer communication about data impact



Financial & Legal Response

Insurance Claim:

Potential £100M cyber insurance activation

Law Enforcement:

Full cooperation with investigation

Legal Action:

Support for prosecution of perpetrators

NCSC CYBER ASSESSMENT FRAMEWORK (CAF)

D1: Response and Recovery Planning

NCSC Requirement: "Capabilities exist to minimise the adverse impact of a cyber security incident"

M&S Strengths

- Structured incident response plan
- Quick service isolation
- Systematic recovery planning
- Stakeholder communication

Improvement Areas

- Early detection capabilities
- Third-party risk monitoring
- Threat intelligence integration
- Supply chain security

NCSC INCIDENT RESPONSE PROCESS

1

Preparation Phase

Establish IR capabilities, third-party risk assessment, employee training, detection systems

2

Detection and Analysis

Rapid identification, threat intelligence integration, log analysis, vendor monitoring

3

Containment, Eradication & Recovery

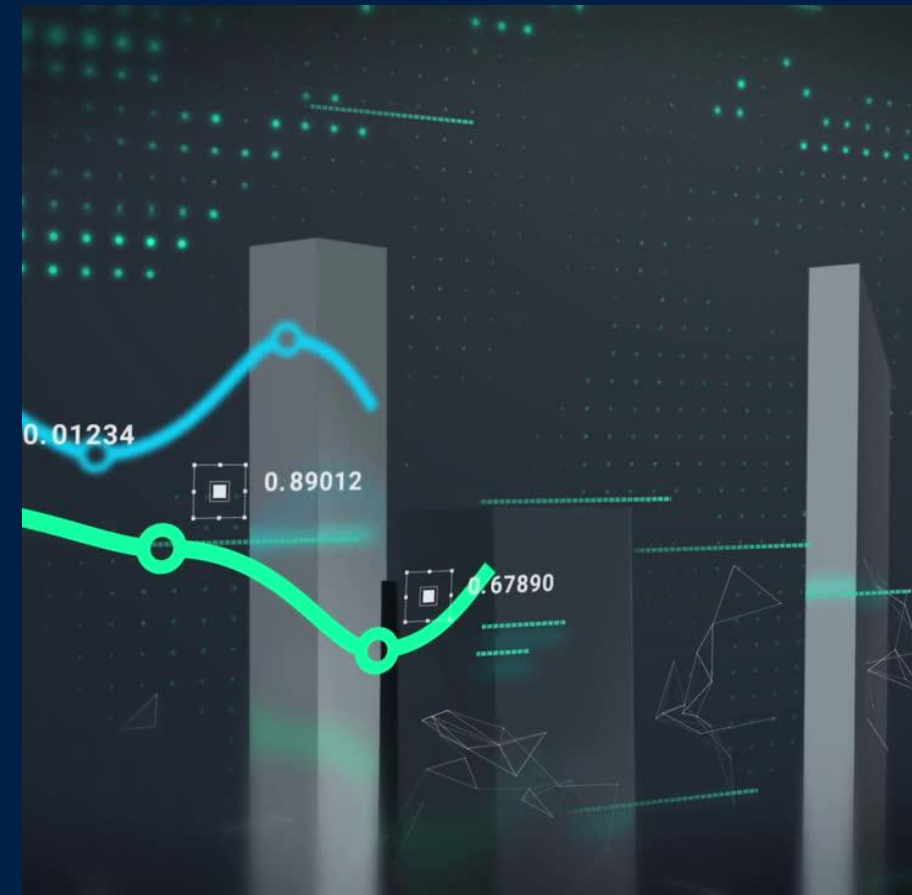
Impact minimisation, transparent communication, phased service restoration

4

Post-Incident Activities

Root cause analysis, control improvements, training updates, threat modelling

NCSC-ALIGNED IMMEDIATE ACTIONS (0-30 DAYS)



Third-Party Risk Management

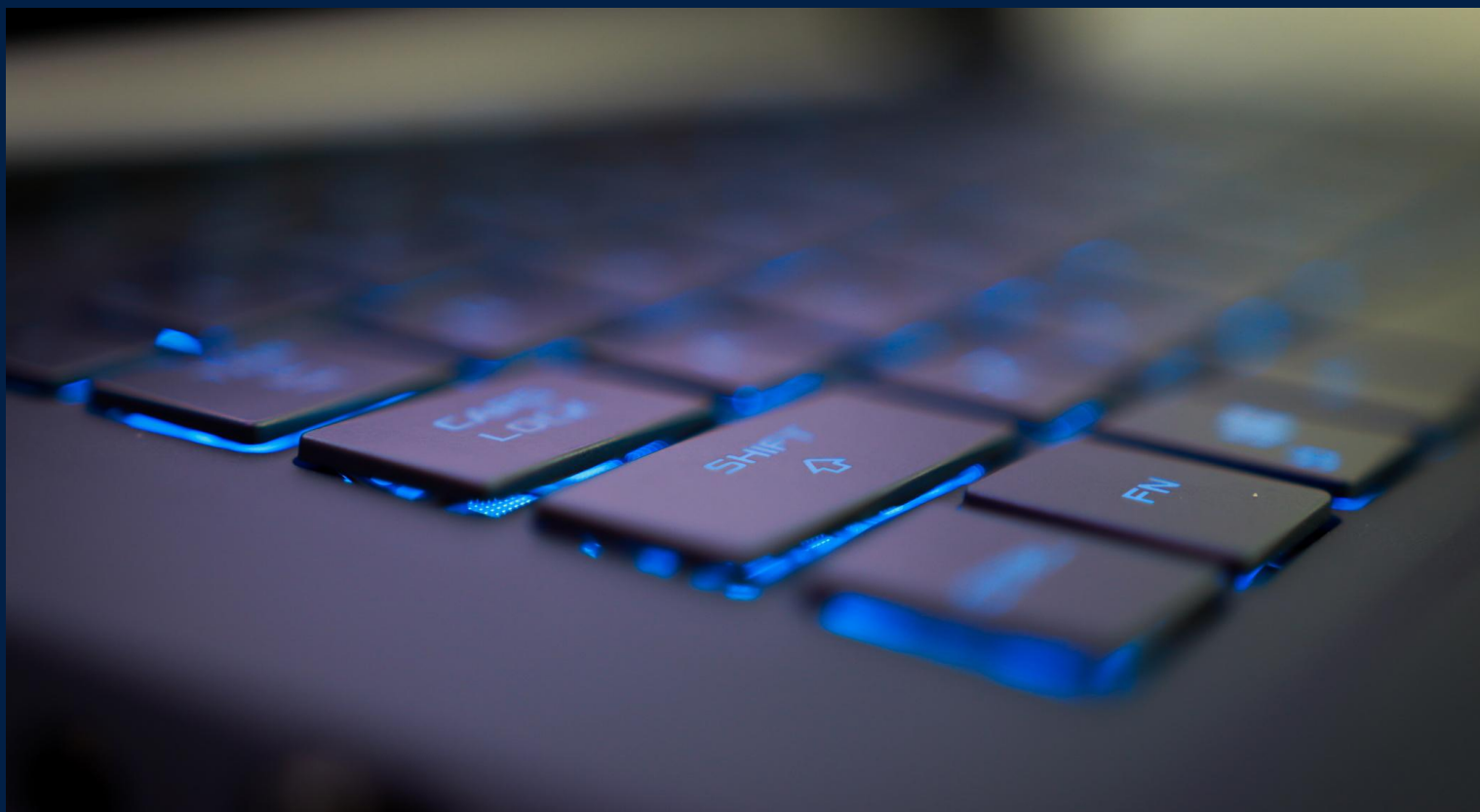
- Quarterly vendor security assessments
- Privileged access management for vendors
- Zero Trust implementation
- Real-time vendor activity monitoring

Social Engineering Defences

- Multi-factor help desk verification
- Monthly phishing simulations
- Verified IT support channels
- Simplified incident reporting

Detection & Response

- SIEM integration across all systems
- Scattered Spider IOC integration
- Automated high-risk response
- Regular tabletop exercises



MEDIUM-TERM ACTIONS (30-90 DAYS)

Architecture Security

- **Network Segmentation:** Critical system isolation
- **Cloud Security:** Misconfiguration remediation
- **Backup Strategy:** Offline, immutable solutions
- **Recovery Testing:** Regular DR exercises



Identity & Access Management

- **Phishing-Resistant MFA:** Advanced authentication
- **Just-in-Time Access:** Privileged access controls
- **Identity Governance:** Regular access reviews
- **Conditional Access:** Risk-based policies

LONG-TERM STRATEGIC ACTIONS (90+ DAYS)

Cyber Resilience Program

- **Board Engagement:** Regular cybersecurity governance reporting
- **Risk Quantification:** Financial impact modelling for cyber threats
- **Insurance Optimisation:** Coverage aligned with current threat landscape
- **Supply Chain Security:** Comprehensive third-party security program

Continuous Improvement

- **Threat Modelling:** Regular updates based on evolving threats
- **Security Metrics:** KPIs aligned with NCSC CAF principles
- **Industry Collaboration:** Information sharing with retail peers
- **Regulatory Compliance:** Proactive emerging regulation compliance

KEY LESSONS LEARNED

Attack Vector Insights

- **Human Factor:** Social engineering remains the critical weakness
- **Supply Chain Risk:** Third-party vulnerabilities require continuous monitoring
- **Multi-Vector Approach:** Combined technical and human exploitation
- **Tool Legitimacy:** Standard business tools used for malicious purposes

Key Lessons Learned

- **Communication:** Transparent, timely customer updates crucial
- **Service Balance:** Security vs business continuity
- **Law Enforcement:** Collaborative approach yields arrests
- **Financial Preparation:** Proper insurance provides resilience





CONCLUSION & NEXT STEPS

Critical Success Factors

- Comprehensive Third-Party Risk Management
- Employee Security Awareness and Training
- Advanced Detection and Response Capabilities
- Structured IR Following NCSC Guidelines

Immediate Next Steps

1. Conduct tabletop exercises based on this scenario
2. Review and update incident response plans
3. Assess third-party risk management processes
4. Implement enhanced social engineering defences
5. Schedule regular security awareness training updates

Computer Network Defence Ltd



THANK YOU

QUESTIONS & DISCUSSION

This presentation analysed the M&S cyber attack through the lens of NCSC frameworks, providing actionable insights for improving organisational cyber resilience.

Scan the QR Code for more information

www.cndltd.com

