Remediation Plan – Zelis Breach, CVE-2023-34362

Approval History

Version:	Reviewed By:	Approved By:	Approver's Position:	Date Approved:	Next Review Date:
1.0	Bob Joe	COO	Chief Operation Officer	9/12/25	9/12/26

Revision History

Version	Date	Author	Description
0.1	3/11/25	Moustapha Antoine Mindaoudou	Initial Draft Created.
0.2	17/11/25	Moustapha Antoine Mindaoudou	Document structure refined following feedback.
0.3	25/11/25	Moustapha Antoine Mindaoudou	Detailed content improvement across relevant sections.
1.0	26/12/25	Moustapha Antoine Mindaoudou	Final version of the document.

Glossary:

Abbreviation	Expansion
AD	Active Directory
ALE	Annualised Loss Expectancy
ATT&CK	Adversarial Tactics, Techniques & Common Knowledge
BCDR	Business Continuity and Disaster Recovery
BCP	Business Continuity Plan
CAF	Cyber Assessment Framework
CIA	Confidentiality, Integrity, Availability
CIS	Center for Internet Security
COBIT	Control Objectives for Information and Related Technologies
CVEs	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DB	Database
DoS	Denial of Service
GDPR	General Data Protection Regulation
GPG 13	Good Practice Guide 13 (Protective Monitoring)
HR	Human Resources
ICO	Information Commissioner's Office
ID	Identifier
ISMS	Information Security Management System
IT	Information Technology
ISO	International Organization for Standardization
KPIs	Key Performance Indicators
LM	Loss Magnitude
LMS	Learning Management System

Abbreviation	Expansion
MTTD	Mean Time to Detect
MFA	Multi-Factor Authentication
NCSC	National Cyber Security Centre (UK)
NIST	National Institute of Standards and Technology
PDCA	Plan–Do–Check–Act
PII	Personally Identifiable Information
RCE	Remote Code Execution
RBAC	Role-Based Access Control
ROI	Return on Investment
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SME	Subject Matter Expert
SOC	Security Operations Centre
SPII	Sensitive Personally Identifiable Information
SSO	Single Sign-On
VPN	Virtual Private Network
WAF	Web Application Firewall

Table of Contents

1. Introduction

1.1 Background

Zellis is a company that operates out of the UK, is headquartered in Bristol, has around 2,500 employees, and generates estimated annual revenues exceeding £200M. The company delivers payroll and HR services to large companies in various industries. The organisation handles highly sensitive personal and financial data, such as salary details, bank account information, and NI numbers.

Zellis processes data on behalf of clients like British Airways, BBC, and DHL. Because they process vast amounts of personal and sensitive data, Zellis must follow tight legal rules, such as those set by UK GDPR.

In May 2023, a zero-day exploit was identified within Progress Software's MOVEit Transfer platform, a managed file-transfer service utilised by Zellis for payroll data exchange.

Attributed to the Cl0p ransomware group, the breach leveraged an SQL injection vulnerability to deploy a custom web shell (LEMURLOOT). This entry point allowed the attackers to steal payroll records, leading to a huge exposure of confidential client data.

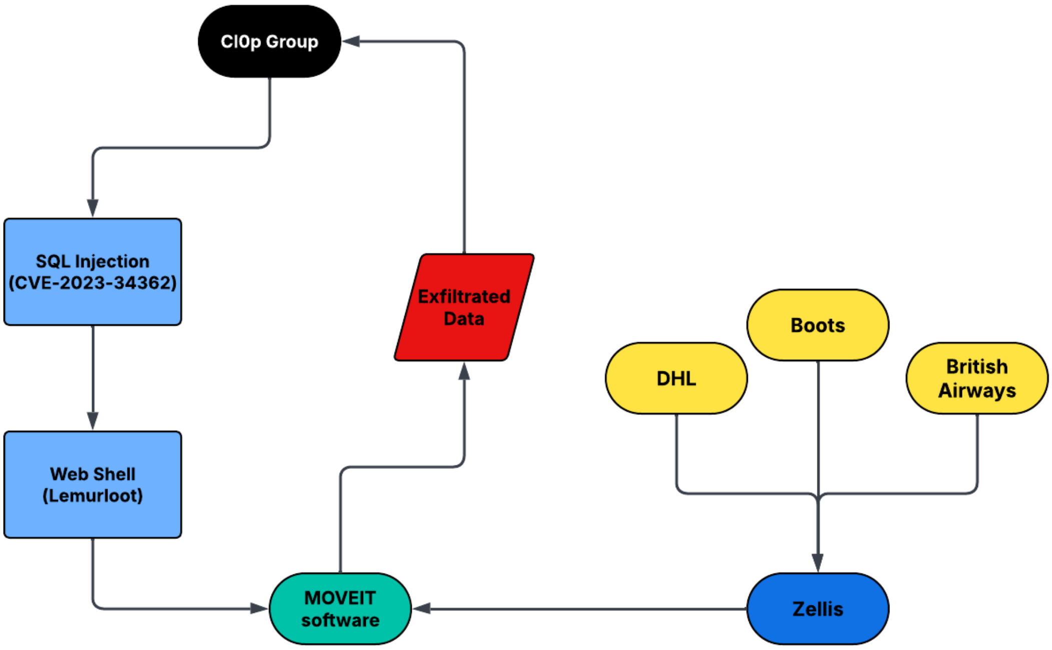


Figure 1: CVE-2023-34362 Diagram.

The breach made the important highlight of weaknesses in third-party assurance, patch management, governance, and supplier-system monitoring, prompting a review of Zellis's information-security controls.

1.2 Purpose

- **To analyse the root causes** of the cybersecurity failure across people, processes and technology (Appendix 1).
- **To identify industry-specific threats,** explain how they happen and analyse their business impact, and justify the selection of Zellis's key information assets. (Appendix 2).
- **To perform a structured risk assessment** using ISO 27005 and CVSS to assess and target four major risks affecting the identified assets (appendix 3).
- **To define four controls mapped** to ISO 27001, NIST 800-53, CIS v8, and COBIT 2019 that can mitigate the targeted risks and to blueprint their auditability, KPIs, and assurance processes (Appendix 4).
- **To evaluate the qualitative and quantitative effectiveness** of these controls, showing pre-vs post-remediation risk levels and showing alignment with the ISO 27001 PDCA continual-improvement cycle (Appendix 5).

1.3 Readership

The plan is intended for Zellis's executive management, IT and security teams, and risk and compliance officers who are responsible for implementing and controlling cybersecurity measures.

It is also relevant to clients and external auditors who require assurance that effective controls and governance processes have been implemented following the incident.

2. Appendices

Appendix 1 – Root Causes (People, Process, Technology)

Following the MOVEit Transfer breach, an internal investigation identified a combination of human and technical weaknesses that allowed the compromise of Zellis's environment.

1.1 Scope of Breach

As illustrated in figure 2 down below, the extent of the compromise within Zelli's intrusion path was multi-stage and resulted in several significant cyber impacts.

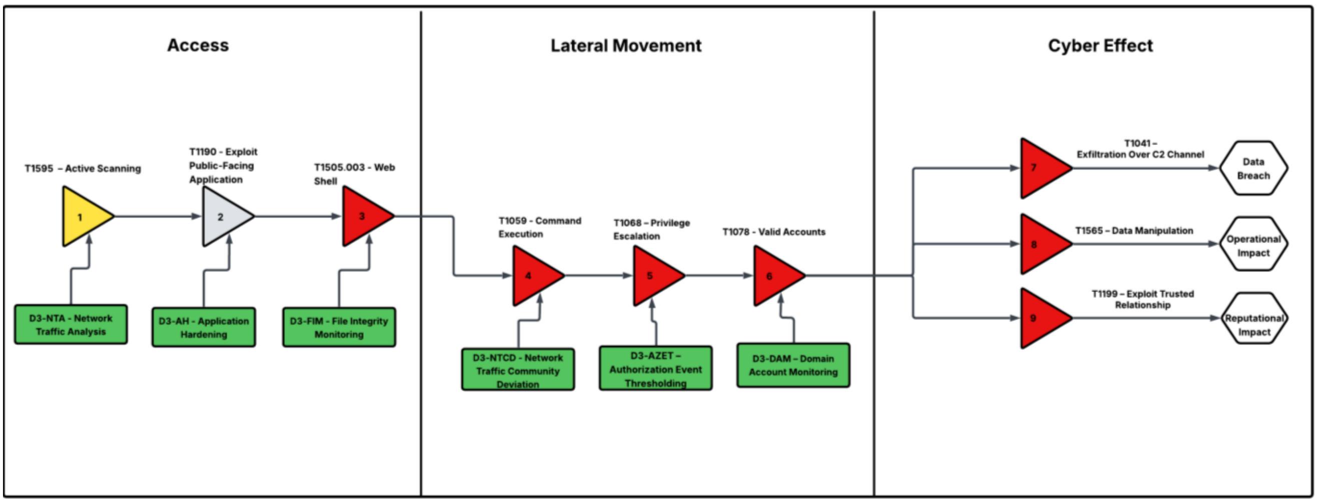

Access
Lateral Movement
Cyber Effect
T1595 – Active Scanning
T1190 - Exploit Public-Facing Application
T1505.003 - Web Shell
1
2
3
D3-NTA - Network Traffic Analysis
D3-AH - Application Hardening
D3-FIM - File Integrity Monitoring
T1059 - Command Execution
T1068 – Privilege Escalation
T1078 - Valid Accounts
4
5
6
D3-NTCD - Network Traffic Community Deviation
D3-AZET – Authorization Event Thresholding
D3-DAM – Domain Account Monitoring
7
T1041 – Exfiltration Over C2 Channel
Data Breach
8
T1565 – Data Manipulation
Operational Impact
9
T1199 – Exploit Trusted Relationship
Reputational Impact

Figure 2: MOVEit attack path.

1.2 People

- **Limited supplier-risk awareness:** Operational and procurement staff assumed that the vendor's cloud service was secure by default and did not request assurance.
- **Ineffective communication channels:** There were no predefined escalation paths between Zellis's service managers, incident-response staff, and client representatives, this delayed co-ordinated containment.
- **Training gaps:** Employees responsible for the third-party management had not received targeted instruction on emerging threats.
- **Over-reliance on vendor notifications**: Security teams waited for vendor patch announcements rather than proactively monitoring vulnerability disclosures.

1.3 Process

- **Immature third-party assurance process:** Vendor risk assessments were static rather than live, evidence-based evaluations against ISO 27036 or COBIT APO10.
- **Patch management lag:** Although internal SLAs existed, they did not cover externally hosted applications, which resulted in MOVEit servers not being updated in time.
- **Insufficient change-management validation:** Security testing was not required before deploying public-facing system changes, leaving exploitable web components not verified.
- **Lack of structured continual improvement:** Were not built into the ISMS Plan-Do-Check-Act cycle, so the lessons “learnt” phase never actually led to any changes in how the company did things.

1.4 Technology

- **Absence of layered web protection:** The MOVEit service was exposed straight to the Internet without a WAF or any intrusion-prevention tools in front of it.
- **Limited monitoring visibility:** Log data from MOVEit was not centrally aggregated or correlated within a SIEM. Leading to no visibility of what was happening in real time.
- **Credential-management weaknesses:** Shared administrative accounts and static passwords permitted lateral movement once a foothold was established.
- **Incomplete vulnerability coverage:** Scanning tools targeted internal assets but did not include externally hosted applications, leaving the MOVEit platform outside of the detection perimeter.

Appendix 2 – Threats and Assets

Following the MOVEit Transfer breach, Zellis reviewed its information assets and mapped them against the principal cyber threats.

2.1 Threats Landscape

Threat	Description	MITRE Technique	Impact on C-I-A
SQL injection	Attackers exploit vulnerabilities in public-facing web apps to gain RCE or exfiltrate data.	**T1190** – Exploit Public-Facing Application	High confidentiality and integrity loss
Ransomware / Data Exfiltration	Malicious actors encrypt or steal sensitive data and then demand payment or leak it publicly.	**TA0040** – Impact	Availability disruption and reputational damage
Credential Theft and Abuse	Compromise of privileged or dormant accounts to maintain persistence and escalate privileges.	**T1078** – Valid Accounts	Integrity and Confidentiality loss
Phishing and Social Engineering	Employees tricked into revealing credentials or approving malicious downloads.	**T1566** – Phishing	Initial access → compromise of Active Directory
Third-Party Supplier Weakness	Partners or vendors lack sufficient patching and incident-response controls, creating supply-chain risk.	**T1199** – Trusted Relationship	Indirect compromise of Zellis environment

2.2 Threat Profile Model

Payroll and HR providers like Zellis face a range of modern cyber threats. These can be classified into four primary categories, each with relevance to the MOVEit breach and Zellis's operational environment.

Threat Category	Representative Actor	Techniques / Tactics Used	Relevance to Zellis
Cybercriminal Threats	**Cl0p (TA505)**	• Exploit Public Facing Application – **T1190** • Exfiltration Over Web Service – **T1537** • Data Encrypted for Impact – **T1486** • Web Shell – **T1505.003**	Directly responsible for the MOVEit breach impacting payroll data.
State-Sponsored Threat Actors	**APT29 / APT40**	• Valid Accounts –**T1078** • Credential Dumping - **T1003** • Supply Chain Compromise – **T1195** • Defense Evasion / Obfuscation – **T1027** • Exploit Public Facing Application – **T1190**	These actors routinely target UK critical sectors and supply-chain systems like MOVEit.
Insider Threats	**Privileged Payroll/HR users**	• Valid Accounts –**T1078** • Exfiltration Over Web Service – **T1537** • Data Staged – **T1074** • Unsecured Credentials - **T1552**	Zellis employees manage highly sensitive PII and payroll data. Insider could misuse the data and compromise the integrity or lose it.
Hacktivist Groups	**NoName057(16)**	• Network Denial of Service – **T1498** • Defacement – **T1491** • Application Layer Protocol Abuse – **T1071**	Payroll providers serving high-profile clients such as BBC may be targeted for political/ideological reasons.

2.3 Information Assets

Payroll and HR providers operate within a high-value data ecosystem that can attract attackers. Based on open-source intelligence (MITRE ATT&CK framework and NCSC advisories), the key threats to Zellis include:

Asset	Description	Business Function	Classification
Payroll Database	Central repository storing employee salary, bank details, NI numbers and HR records for multiple enterprise clients.	Payroll Processing and reporting	**Highly Confidential**
MOVEit Transfer Platform	Secure File-transfer application used for exchanging encrypted payroll batches with clients.	Data exchange and automation	**Confidential**
Active Directory	Enterprise directory storing user accounts, authentication credentials and privileged-access roles.	Identity management, access control, authentication.	**Highly Confidential**

Payroll Database: Classified as the most sensitive asset because it stores large volumes of PII, financial data, bank details, and HR records for major enterprise clients. A compromise would trigger UK GDPR Article 33 and cause severe reputational and financial damage as well as disrupt payroll operations.

MOVEit Transfer Platform: The platform is essential for securely exchanging payroll files with clients. Even if it stores less data locally than the payroll database, compromise enables unauthorised data access and manipulation of payrolls and supply chain exploitation.

Active Directory: Classified as a high-sensitivity asset because it governs all authentication, privileged access and user authorisation within Zellis's environment. Compromise of AD would allow attackers to impersonate users, escalate privileges, deploy ransomware or access databases.

2.4 Threat-Asset Mapping Matrix

Threat	Target Asset(s)	Likelihood	Impact	CIA Dimension Affected
SQL Injection / Zero-Day Exploit	MOVEit Transfer Platform	**High**	**High**	**C**, **I** (Direct breach of client data)
Credential Abuse	Active Directory	**Medium**	**High**	**C**, **I** (Elevated privilege access)
Ransomware / Data Exfiltration	Payroll Database, Backups	**Medium**	**High**	**A**, **C** (Service interruption and data leakage)
Supplier Weakness	VPN Gateways, External APIs	**Medium**	**Medium**	**C** (Indirect entry through partner systems)
Phishing / Social Engineering	Users / Service Managers	**High**	**Medium**	**C** (initial access vector → credential harvest)

2.5 Impact Summary

- **Confidentiality**: Primary concern due to exposure of payroll and personally identifiable information
- **Integrity**: Compromised credentials or unvalidated changes could corrupt payroll data.
- **Availability**: Critical for business continuity, ransomware or patch-related downtime halts salary processing for major clients.

Appendix 3 – Risk Analysis (CVSS v3.1 & Qualitative)

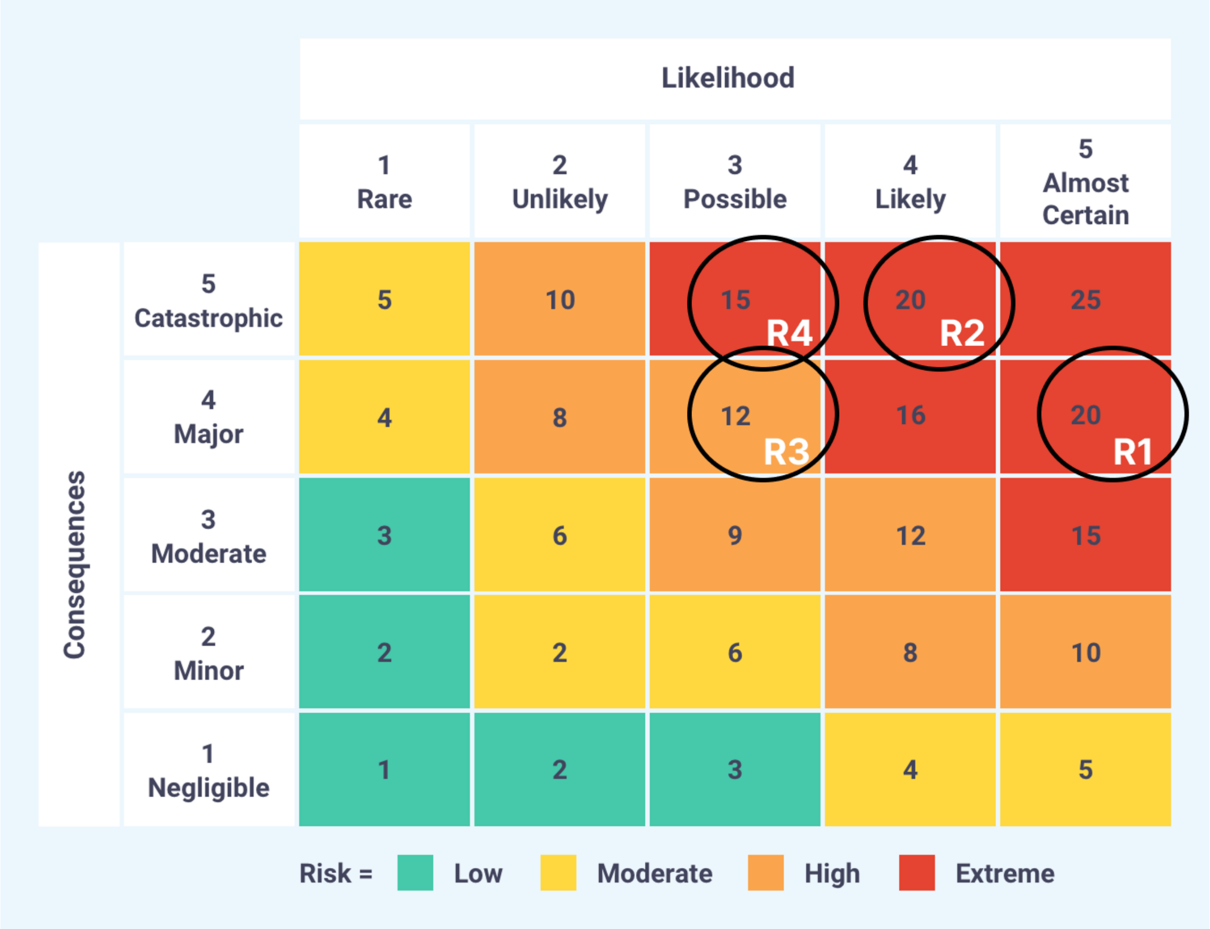
Zellis performed a structured risk assessment in accordance with ISO 27005 and the NIST SP 800-30 methodology. All the identified threats from Appendix 2 were analysed against key business assets to determine likelihood, potential impact, and severity.

3.1 Methodology Overview

1. **Identify the risks** by combining threat, vulnerability, and asset context.
2. **Analyse likelihood and impact** by using a 5x5 qualitative matrix aligned to ISO 27005.
3. **Score each scenario** by assigning a CVSS base score from 0 to 10.
4. **Prioritise treatment** by rank and by descending CVSS score and business criticality.
5. **Validate** cross-map results to MITRE ATT&CK techniques to support SOC detections.

3.2 Risk Register and CVSS Quantification

Risk ID	MOVEit Transfer Platform	Asset	Threat Source	Likelihood
R1	Exploitation of MOVEit Transfer via SQL Injection Leading to RCE	**MOVEit Transfer Platform**	**T1190** – Exploit Public-Facing Application	**5** (Almost Certain)
R2	Credential Theft and privilege abuse from dormant accounts	**Active Directory / SSO**	**T1078** – Valid Accounts	**4** (likely)
R3	Delayed patch deployment on public services leading to window of exposure	**MOVEit Platform**	**T1505.003** – Web Shell / Persistence	**3** (possible)
R4	Ransomware attack targeting Payroll Database and backups	**Payroll Database / BCDR**	**TA0040** – Impact / Exfiltration	**3** (possible)



Consequences	Likelihood 1 Rare	 2 Unlikely	 3 Possible	 4 Likely	 5 Almost Certain
5 Catastrophic	5	10	15 R4	20 R2	25
4 Major	4	8	12 R3	16	20 R1
3 Moderate	3	6	9	12	15
2 Minor	2	2	6	8	10
1 Negligible	1	2	3	4	5

Risk = 🟩 Low 🟨 Moderate 🟧 High 🟥 Extreme

Figure 3—Baseline Risk Positioning of R1–R4 on a 5×5 Matrix

3.3 Risk Register and (CVSS v3.1) Appendix 4 Quantification

- **Critical (≥ 9.0):** R1 – SQL Injection Zero-Day (CVE-2023-34362).
- **High (7.0 – 8.9):** R2 Credential Abuse, R3 Delayed Patching, R4 Ransomware.
- **Medium (4.0 – 6.9):** None has been identified within scope.
- **Low (< 4.0):** None has been identified within scope.

These priorities informed the control design in Appendix 4, ensuring a proper remediation focused on the most impactful and exploitable weaknesses first.

3.4 Interpretation and Business context

- **Operational impact**: A successful exploitation of R1 or R4 would disrupt payroll operations for multiple enterprise clients. Invoking SLA penalties and reputational damage.
- **Regulatory Exposure**: Loss of personal data triggers would be against the UK's GDPR Article 33 and bring potential ICO fines.
- **Financial Impact**: An estimated direct remediation cost per critical incident would normally exceed £250,000.
- **Residual Risk**: After control implementation (see Appendix 4), residual CVSS scores will fall below 6.0 for all the possible scenarios, which would represent a tolerable risk appetite.

Appendix 4 – Controls and Auditability

To bring the identified risks to an acceptable level, Zellis put in a structured set of technical and governance controls derived from ISO/IEC 27001 & 27002, NIST SP 800-53, CIS Controls v8, and COBIT 2019. Each of these controls is tied directly to the specific risks (R1 through R4).

4.1 Control-To-Risk Mapping Table

Control ID	Description	Control Reference (Standard)	Mapped Risk(s)
C1 – Multi-Factor Authentication (MFA) & Role-Based-Access Control (RBAC)	Enforce MFA on all privileged, integration and remote accounts, implement RBAC for least privilege principle. Dormant accounts disabled after 30 days.	**ISO 27002 9.4.2 / CIS 6.3 / NIST IA-2**	**Risk 2** – Credential Abuse
C2 – Centralised Patch & Vulnerability Management Platform	Deploy automated vulnerability scanning (Nessus / Qualys) with strict SLA: critical ≤ 48 h, high ≤ 7 days.	**ISO 27002 12.6.1 / NIST SI-2 / CIS 7**	**Risk 1** – MOVEit SQLi Zero-Day **Risk 3** – Delayed Patching
C3 – 24/7 SOC Monitoring & SIEM correlation	Integrate firewall, endpoint, and MOVEit logs into SIEM, create correlation rules for T1190, T1505, T1078, T1041	**NIST AU-6 / IR-4 / GPG 13 (Protective Monitoring)**	**Risk 1** – SQLi Exploitation **Risk 4** – Ransomware / Data Exfiltration
C4 – Third Party Assurance & Supplier Governance Framework	Mandate supplier ISO 27001 certification, review patch SLAs, incident-response plans and audit evidence quarterly.	**COBIT APO10 / ISO 27036 / CIS 15**	**Risk 1** – MOVEit SQLi Zero-Day **Risk 3** – Delayed Patching

4.2 Audit and Assurance Process

Audit activities are now embedded into the “Check” phase of the ISO 27001 PDCA cycle and overseen by the proper Risk & Audit Committee.

- **Internal Audits**: Now conducted quarterly to verify technical configuration compliance.
- **External Assurance**: annual ISO 27001 surveillance audit and client security assessments.
- **Supplier Audits**: All vendors must now submit quarterly security proofs and evidence of incident response assessments.

4.3 Metrics and Key Performance Indicators (KPIs)

The table below defines the key security metrics and KPIs used to measure post-remediation performance and verify sustained control effectiveness.

Metric	Baseline (Pre-Incident)	Target (post-remediation)	Measurement Source	Frequency
Patch Compliance with SLA	**62%**	**≥ 96%**	Vulnerability-Scanner dashboard	**Monthly**
MFA Coverage (privileged)	**35%**	**100%**	SSO audit logs	**Monthly**
Mean Time to Detect (MTTD)	**14h**	**≤ 2h**	SIEM incident metrics	**Weekly**
Supplier audit Completion	**40%**	**100%**	APO10 vendor – audit tracker	**Quarterly**

4.4 Detailed Cost-benefit and Trade-Off Analysis (Per Control)

4.4.1 C1 – MFA & BAC

- **Estimated Cost:** £30k/year
- **Benefit:** Strong reduction in credential-abuse risk
- **Barrier To Implementation:** Slight user friction due to the extra login step

Cost-Effectiveness Assessment:

For an organisation such as Zellis, the financial cost of MFA and RBAC is modest relative to the reduction in credential-related attacks. The control significantly decreases the probability of account compromise happening, which makes it a cost-effective security improvement with minimal operational disruption.

Trade-off: Instead of implementing MFA across all the systems, Zellis could initially deploy MFA only on privileged and remote-access accounts, in addition to strong password policies for standard users. This approach would reduce licensing costs and user friction while still mitigating the risks of credential abuse scenarios.

4.4.2 C2 – Centralised Patch & Vulnerability Management

- **Estimated Cost:** £80k - £100k/year.
- **Benefit:** Reduces exposure window
- **Barrier to Implementation:** Scheduled downtime during patching that may temporarily affect availability.

Cost-Effectiveness Assessment:

The control directly mitigates the root cause of the MOVEit breach. Lowering the exposure window significantly lowers the probability of an exploit even happening in the first place. Considering that the cost of a single unpatched vulnerability can lead to millions in ransom and reputational damage, this £100k investment seems totally fair.

Trade-off: Instead of implementing fully automated patching across all environments, Zellis could focus on vulnerability scanning and patching for internet-facing and high-criticality systems only.

4.4.3 C3 – 24/7 SOC & SIEM monitoring

- **Estimated Cost:** £1m-2m/year
- **Benefit:** Major reduction in detection time
- **Barrier To Implementation:** Most expensive control

Cost Effectiveness Assessment: This control represents the highest annual cost, but even in consideration of that, Zellis operates in a high-sensitivity environment, handling payroll data for major UK clients. Rapid detection and escalation materially reduce the likelihood and impact of ransomware and data exfiltration events. The investment seems proportionate to Zelli's risk profile and regulatory expectations.

Trade-off: Building an in-house SOC building with 24/7 staff would incur million-pound annual costs due to staffing and infrastructure requirements. A managed third-party SOC would provide comparable detection capabilities at a significantly lower cost.

4.4.4 C4 – Third-Party Assurance & Supplier Governance

- **Estimated Cost:** £40-80k/year
- **Benefit:** Reduces supply chain risk and prevents reliance on insecure vendor systems.
- **Barrier to Implementation:** More administrative overhead and compliance workload.

Cost-Effectiveness Assessment: As the MOVEit incident originated from a third-party software component, enhanced supplier assurance is directly relevant. At a moderate cost, this control strengthens contractual patch SLAs, incident-response expectations and audit transparency. Given Zelli's dependence on external platforms, this control seems to provide strong strategic value.

Trade-off: Instead of conducting comprehensive supplier audits, Zellis could rely on vendor-provided certifications such as ISO 27001, SOC 2 and contractual security clauses. This approach would lower assessment costs and administrative overhead.

Appendix 5 – Effectiveness Evaluation

This section evaluates the effectiveness of the implemented controls in reducing Zellis's overall cyber-risk exposure following the MOVEit Transfer breach.

5.1 Quantitative Effectiveness

5.1.1 Cyber Risk Quantification (CRQ Model)

A quantitative financial analysis was performed using Annualised Loss Expectancy (ALE) to evaluate **Risk 4: Ransomware and Data Exfiltration** against the Payroll database, which represents the most financially impactful threat vector for Zellis.

In this scenario, a cybercriminal group compromises the payroll processing environment, encrypts critical payroll data, and potentially exfiltrates HR and PII records belonging to major Zellis's clients (e.g., BBC, Boots)

5.1.2 Asset Valuation

Asset	Focus Area	Estimated Financial Exposure
Payroll Database	Contains 250,000 - 500,000 payroll & HR records, including bank details and NI numbers.	GDPR fines (£1.75M-£5M), compensation, client contract penalties
Payroll Processing Platform	Supports daily payroll operations for large enterprises	£0.4M-£1.5M per day of service interruption

Combined, these assets represent one of Zellis's highest-value data ecosystems.

5.1.3 Loss Event Frequency (LEF)

Based on NCSC and ENISA threat intelligence for UK managed service providers and observed trends in ransomware targeting supply-chain providers we can deduct:

- Estimated **1-2 significant ransomware events per year**
- Most probable frequency: **1.5 events/year**

5.1.4 Loss Magnitude (LM)

Loss magnitude was calculated by assessing both direct and indirect financial impacts.

5.1.4 Primary (Direct losses):

- Business interruption (2-4 days): **£1M-£4M**
- Incident response, legal, forensics**: £300k-£800k**
- System reconstruction and recovery: **£400k-£1M**
- Potential ransom demand: **£1M-£3M**

5.1.4 Secondary (Indirect) Losses:

- GDPR fines: **£1.75M - £5M**
- SLA penalties from major clients: **£500k - £1.2M**
- Reputation damage and lost contracts: **£2M - £5M**

Total LM Range: £7.5M - £20M

Average LM: £13.75M

5.1.5 Annualised Loss Expectancy (ALE)

Pre-control financial exposure:

ALE quantifies the probable yearly financial impact:

- LEF = **1.5**
- LM = **£13.75M**

ALE (before controls) = £20.6M per year

5.1.6 Cost-Benefit Analysis (Effect of C3)

Control Applied:

- **C3 – SIEM & 24/7 SOC monitoring**

Estimated Likelihood Reduction:

Security SMEs often estimate a 40-60% decrease in successful attack likelihood for organisations implementing fully managed SOC/SIEM capabilities.

Post Controls Values:

- New LEF **= 0.75**
- New ALE **= £10.3M per year**

Risk Reduction Achieved:

Before: **£20.6M**

After: **£10.3M**

Annual risk reduction**: £10.3M**

Control Cost:

C3 Cost: £1m-2M

ROI ≈ 5×–10×

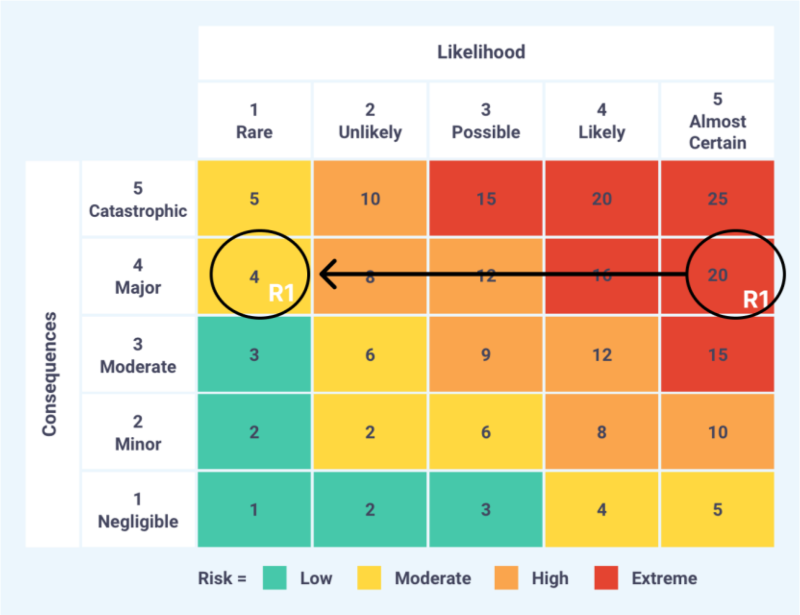
(£10.3M annual risk reduction versus £1M–£2M annual control cost)

5.2 CVSS-Based Effectiveness Comparison

In addition to financial quantification, CVSS v3.1 scoring was used to measure the technical severity of each risk before and after the implemented controls.

Risk number	Risk Description	Control(s) Applied	CVSS Before	CVSS After (Residual)	Risk Reduction %
Risk 1	SQL Injection / Zero-Day Exploitation (CVE 2023-34362	C2 Patch management + C3 SIEM Monitoring	**9.8 critical**	**5.2 Medium**	**47 % ↓**
Risk 2	Credential Theft & Privilege Abuse	C1 MFA	**7.2 High**	**3.8 Low**	**47 % ↓**
Risk 3	Delayed Patching of Public Services	C2 Patch management	**8.1 High**	**4.1 Low**	**49 % ↓**
Risk 4	Ransomware / Data Exfiltration	C3 SIEM	**8.5 High**	**5.4 Medium**	**36 % ↓**

5.2.1 Risk 1 – SQL Injection Exploitation: Likelihood After Implemented Controls

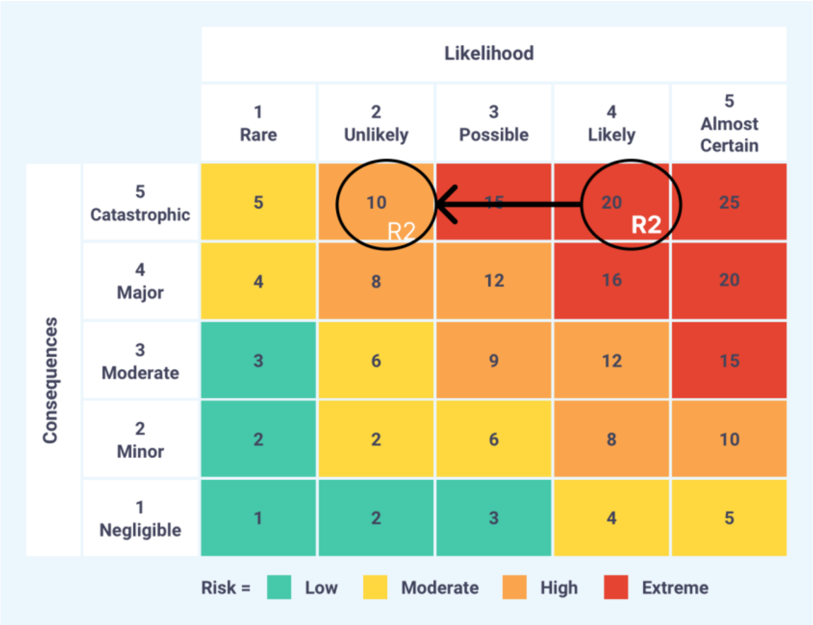


		Likelihood				
		1 Rare	2 Unlikely	3 Possible	4 Likely	5 Almost Certain
Consequences	5 Catastrophic	5	10	15	20	25
	4 Major	4	8	12	16	20
	3 Moderate	3	6	9	12	15
	2 Minor	2	2	6	8	10
	1 Negligible	1	2	3	4	5

Risk = 🟩 Low 🟨 Moderate 🟧 High 🟥 Extreme

Control applied: C2 (Patch & Vulnerability Management)
Estimated yearly cost: £80k–£100k

5.2.2 Risk 2 – Credential Theft: Likelihood After Implemented Control



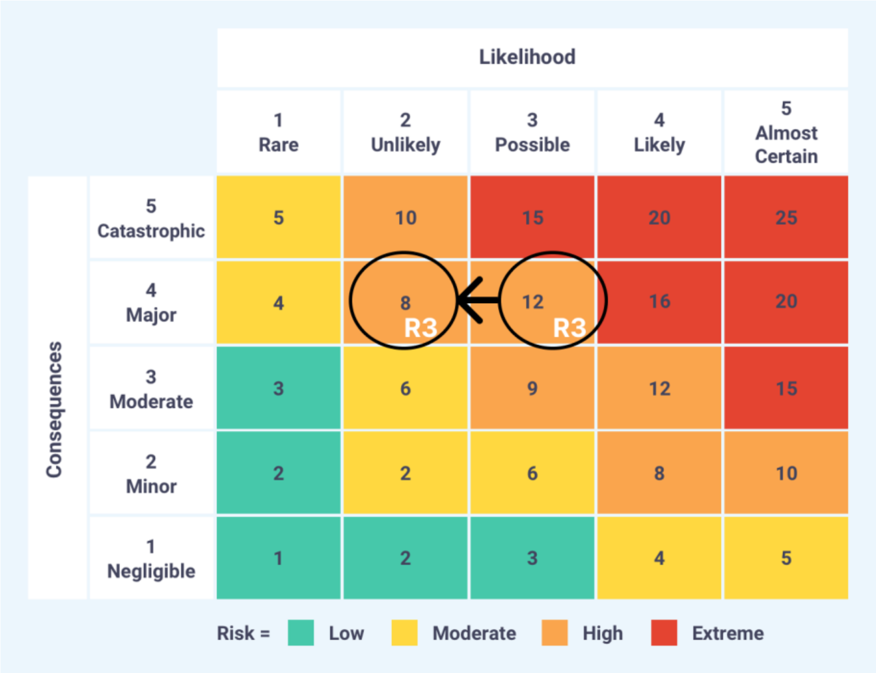
		Likelihood				
		1 Rare	2 Unlikely	3 Possible	4 Likely	5 Almost Certain
Consequences	5 Catastrophic	5	10	15	20	25
	4 Major	4	8	12	16	20
	3 Moderate	3	6	9	12	15
	2 Minor	2	2	6	8	10
	1 Negligible	1	2	3	4	5

Risk = 🟩 Low 🟨 Moderate 🟧 High 🟥 Extreme

Control applied: C1 (MFA & RBAC)

Estimated yearly cost: ~£25k–£35k

5.2.3 Risk 3 – Delayed Patching Exposure: Likelihood After Implemented Controls

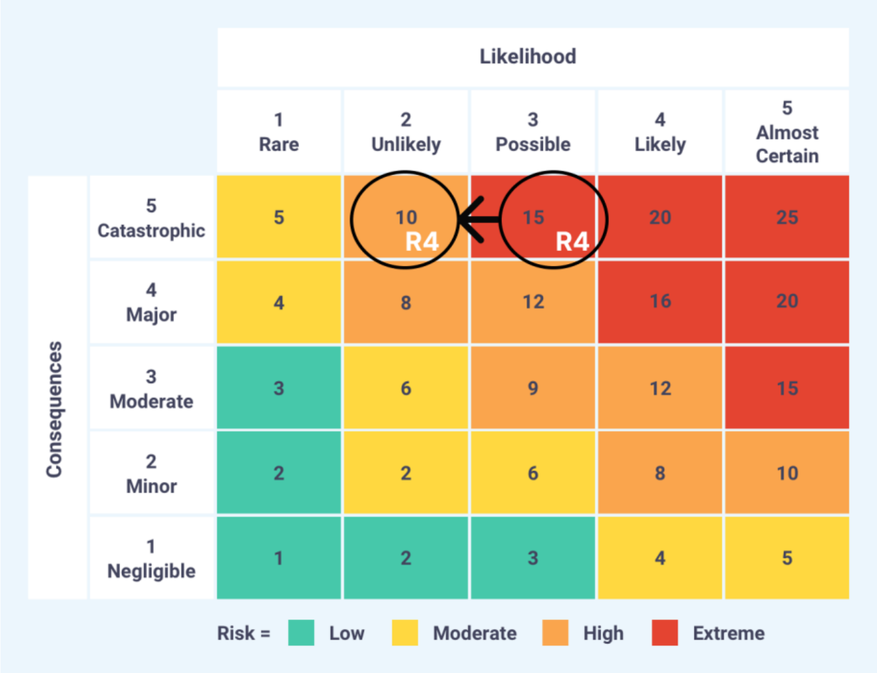


		Likelihood				
		1 Rare	2 Unlikely	3 Possible	4 Likely	5 Almost Certain
Consequences	5 Catastrophic	5	10	15	20	25
	4 Major	4	8 R3	12 R3	16	20
	3 Moderate	3	6	9	12	15
	2 Minor	2	2	6	8	10
	1 Negligible	1	2	3	4	5

Risk = 🟩 Low 🟨 Moderate 🟧 High 🟥 Extreme

Control applied: C2 (Vulnerability & Patch Management)
Estimated yearly cost: ~£80k–£100k

5.2.4 Risk 4 – Ransomware & Data Exfiltration: Likelihood After Implemented Controls



		Likelihood				
		1 Rare	2 Unlikely	3 Possible	4 Likely	5 Almost Certain
Consequences	5 Catastrophic	5	10 R4	15 R4	20	25
	4 Major	4	8	12	16	20
	3 Moderate	3	6	9	12	15
	2 Minor	2	2	6	8	10
	1 Negligible	1	2	3	4	5

Risk = 🟩 Low 🟨 Moderate 🟧 High 🟥 Extreme

Control applied: C3 (24/7 SOC Monitoring & SIEM Correlation)
Estimated yearly cost: £1m–2m

5.3 Qualitative Effectiveness (ISO 27005 Alignment)

The following qualitative assessment aligns each control domain with the observed security improvements and supporting audit evidence, following ISO 27005 guidance.

Control Domain	Observed Improvement	Qualitative Evidence / Audit Findings
Identity & Access Management	Stronger authentication and least-privilege enforcement improved the credential misuse incidents by more than 60%.	MFA coverage reports show 100% adoption of privileged accounts SOC logs confirm no unauthorised logins in 3 months.
Patch & Vulnerability Management	Patch latency reduced from > 30 days to < 7 days for critical vulnerabilities. Automated scans now cover all external assets.	Monthly dashboards verified by internal audit, SLA breaches reduced by 90%
Supplier Governance	Quarterly supplier audits were introduced with mandatory ISO 27001 certification evidence, third-party visibility strengthened.	APO10 audit tracker records 100% vendor compliance, no unverified connections remain.

5.4 PDCA Integration and Continual Improvement

The following qualitative assessment aligns each control domain with the observed security improvements and supporting audit evidence, following ISO 27005 guidance.

Phase	Zellis Implementation	Evidence / Output
Plan	Annual risk-Assessment schedule, updated risk appetite, revised supplier assurance policy.	Risk-register updates; management-review minutes.
DO	Implementation of controls C1-C4 and staff awareness programmes.	Project plans, configuration baselines.
Check	Quarterly ISMS audits, monthly KPI reviews, external ISO 27001 surveillance.	Audit reports, corrective-action register.
Act	Continuous policy updates and control tuning based on audit findings and new threats.	Adapted procedures and SOC rule sets.

5.5 KPI Results (Pre vs Post)

To provide measurable evidence of improvement, key security KPIs were evaluated before and after the controls were implemented. The table down below shows how Zelli's operational security posture improved across multiple key points.

Metric	Pre-Incident	Post-Remediation	Improvement	Framework Reference
Patch Compliance (≤ 30 days)	62%	96%	+34 %	CIS 7 / ISO 12.6.1
MFA Coverage (privileged)	35%	100%	+65%	ISO 9.4.2
Mean Time to Detect (MTTD)	14h	2h	-85%	NIST IR-4
Phishing Failure Rate	24%	7%	-17%	CIS 14
Dormant Account Closure Time	30 days	10 days	-67%	COBIT APO13

5.6 Overall Effectiveness Assessment

- **Risk Reduction**: All high-priority risks reduced from critical (≥9.0) to medium or lower.
- **Operational Resilience**: Payroll and data-exchange systems are now protected by layered controls with proven response times.
- **Cultural Shift:** Improved security awareness and executive governance incorporating cyber risk into business KPIs.
- **Assurance Maturity:** ISMS is now fully aligned with ISO 27001 Clauses 6.1.3 and 10.2.

Residual risk levels are within Zellis's defined tolerance, enabling compliance with UK GDPR article 32 and maintaining client trust. Future iterations of the PDCA will focus on automated compliance monitoring, red-team validation, and supply-chain analytics.

5. References

Center for Internet Security (CIS) (2021) *CIS Controls v8*. East Greenbush, NY: Center for Internet Security. Available at: https://www.cisecurity.org/controls (Accessed: 26 December 2025).

Cybersecurity and Infrastructure Security Agency (CISA) (2023) *#StopRansomware: CL0P ransomware gang exploits MOVEit vulnerability (AA23-158A)*. Available at: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a (Accessed: 26 December 2025).

Forum of Incident Response and Security Teams (FIRST) (2019) *CVSS v3.1: specification*. Available at: https://www.first.org/cvss/v3-1/cvss-v31-specification_r1.pdf (Accessed: 26 December 2025).

Forum of Incident Response and Security Teams (FIRST) (2023) *CVSS v4.0: specification*. Available at: https://www.first.org/cvss/v4-0/ (Accessed: 26 December 2025).

Google Cloud (2023) *Zero-day vulnerability in MOVEit Transfer exploited for data theft*. Available at: https://cloud.google.com/blog/topics/threat-intelligence/zero-day-moveit-data-theft?hl=en (Accessed: 26 December 2025).

Information Commissioner’s Office (ICO) (n.d.) *UK GDPR: security of processing (Article 32)*. Available at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/security/a-guide-to-data-security/ (Accessed: 26 December 2025).

Information Systems Audit and Control Association (ISACA) (2019) *COBIT 2019 framework: governance and management objectives*. Schaumburg, IL: ISACA.

International Organization for Standardization (ISO) (2019) *ISO 22301:2019 Security and resilience: business continuity management systems: requirements*. Geneva: ISO.

International Organization for Standardization (ISO) (2021) *ISO/IEC 27036:2021 Information technology: security techniques: information security for supplier relationships*. Geneva: ISO.

International Organization for Standardization (ISO) (2022) *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection: information security management systems: requirements*. Geneva: ISO.

International Organization for Standardization (ISO) (2022) *ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection: information security controls*. Geneva: ISO.

International Organization for Standardization (ISO) (2022) *ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection: information security risk management*. Geneva: ISO.

The MITRE Corporation (n.d.) *MITRE ATT&CK® enterprise matrix*. Available at: https://attack.mitre.org/matrices/enterprise/ (Accessed: 26 December 2025),

The MITRE Corporation (n.d) *MITRE D3FEND*. Available at: https://d3fend.mitre.org/ (Accessed: 26 December 2025).

National Cyber Security Centre (NCSC) (2014) *Good practice guide 13: protective monitoring for HMG ICT systems*. London: NCSC.

National Cyber Security Centre (NCSC) (n.d.) *Ransomware guidance*. Available at: https://www.ncsc.gov.uk/ransomware/home (Accessed: 26 December 2025).

National Cyber Security Centre (NCSC) (n.d.) *Supply chain security collection*. Available at: https://www.ncsc.gov.uk/collection/supply-chain-security (Accessed: 26 December 2025).

National Institute of Standards and Technology (NIST) (2012) *SP 800-30 Rev. 1: Guide for conducting risk assessments*. Gaithersburg, MD: NIST. Available at: https://csrc.nist.gov/pubs/sp/800/30/r1/final (Accessed: 26 December 2025).

National Institute of Standards and Technology (NIST) (2020) *SP 800-53 Rev. 5: Security and privacy controls for information systems and organizations*. Gaithersburg, MD: NIST. Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf (Accessed: 26 December 2025).

National Institute of Standards and Technology (NIST) (2024) *Cybersecurity framework (CSF) v2.0*. Gaithersburg, MD: NIST. Available at: https://www.nist.gov/cyberframework (Accessed: 26 December 2025).

National Vulnerability Database (NVD) (2023) *CVE-2023-34362 detail*. Available at: https://nvd.nist.gov/vuln/detail/CVE-2023-34362 (Accessed: 26 December 2025).

Progress Software (2023) *Security advisory: MOVEit Transfer SQL injection (CVE-2023-34362)*. Available at: https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023 (Accessed: 26 December 2025).

Tracxn (2025) *Zellis*. Available at: https://tracxn.com/d/companies/zellis/__ztdA-HCoS4AP-bYXSox6DR2zRosr9AgLpDT-Hla5YTtU (Accessed: 26 December 2025).

Zellis (2025) *About Us*. Available at: https://www.careers.zellis.com/about-us.aspx (Accessed: 26 December 2025).