Assignment 5 – Communications Strategy

During a Cyber Incident

Name – Yash Sanjaybhai Patel

Student ID - 134094184

Course – CYT145 – Cybersecurity and Threat Management Program

Professor – Ionut Anghelache

Date – 27th November 2025

Table of Contents

Organization Selected: Zellis

1. Introduction

This report explains the communications strategies that Zellis, a UK based payroll and HR services provider, should follow before, during, and after a cyber incident. Zellis is a well-known company in supply chain because many large organizations depend on it for payroll processing, including British Airways, BBC, Boots, Aer Lingus, and government agencies. Although Zellis was not the main target of the MOVEit breach, they were directly impacted because they used the MOVEit Transfer software in their environment.

I selected Zellis because it clearly shows how a single software weakness in a vendor (Progress Software) can lead to a major breach affecting Zellis, and then spread further to their customers, and even fourth-party service providers. This incident teaches an important lesson about supply-chain dependency and why communication planning is critical. My previous assignments covered the MOVEit breach and the technical details behind CVE-2023-34361, which helps build a stronger foundation for this communication strategy.

2. Summary of the Incident

In May 2023, Progress Software, the vendor behind the MOVEit Transfer, find out that threat actors had exploited a zero-day vulnerability in their software. This flaw, later identified as CVE-2023-34362, was a SQL injection vulnerability that allowed attackers to send harmful database commands to MOVEit servers.

Technical Breakdown -

- The attackers entered harmful SQL code into MOVEit's database forms.
- This let them bypass normal authentication rules and act like a trusted system user.
- After accessing the database, they installed a custom web shell named LEMURLOOT.
- Attackers belonged to the ransomware group CL0P (TA505)
- This web shell gave the attackers remote access, letting them steal files, increase privileges and exfiltrate large amounts of sensitive data.

Timeline of Events -

- May 27 – First suspicious activities reported by privately by researchers and some customers.
- May 31 – Progress Software publicly confirmed vulnerabilities and released emergency advisories
- June 1 – More advisories were released, and the security teams confirmed exploitation by CL0P.
- June 5 – Microsoft officially attributed the attack to the CL0P group and provided indicators of compromising.

Impact on Zellis

Zellis used MOVEit Transfer to collect and share payroll files for many well-known companies, Once CL0P exploited this vulnerability, they were able to access Zellis MOVEit system and also downloaded sensitive employee data which belonged to Zelli's clients. The attackers indirectly accessed: Names, Addresses, Nation Insurance numbers, birth dates, banking and salary data. This made the breach a multi-layer supply chain incident.

This incident caused serious public concerns because lots of employees knew that their personal and financial data has been compromised even though they never directly interacted with MOVEit or Zellis.

Also, Zellis quickly disabled their MOVEit system, and started investigation, informed clients and started working with Progress Software and cybersecurity teams to understand the full scale of the breach. Government agencies in the UK and Europe also got involved because personal data laws required immediate reporting.

3. Best Communication Practices and Plan

To handle a cyber incident effectively, Zellis needs a strong communication strategy that begins before an attack happens and continues through the incident and after it is resolved. Because Zellis sits in the middle of a complex supply chain between their vendor and their major clients such as British Airways, BBC, and boots their communication should be clear, honest and well-organized. Each phase requires its own type of communication, and the company must be prepared in advance so they can act quickly when a real incident occurs.

i. Phase One -Before an Attack

Before any cyber incident occurs, Zellis must build a strong structure that supports quick decision-making and good information flow. This begins by creating a dedicated incident response team that includes senior management, IT security, operations, communications staff, HR, legal advisors, and vendor management. These different groups must understand their roles and know how to coordinate with each other. Preparing this team in advance ensures that when something goes wrong, everyone knows exactly whom to contact and how to respond to it.

A key part of preparation is have knowledge what information assets the company relies on. For Zellis, databases, HR files and file-transfer systems such as MOVEit are the highest risk systems because they contain extremely important information. These systems must be protected with strong encryption, two factor authentication and monitoring continuously. Lower-priority systems, such as internal communication and backups, must also be protected but may not require the same level of urgency during an attack. By clearly ranking all data and systems before an incident, Zellis can communication internally about what assets requires immediate attention.

Another important part of communication before a breach involves identifying stakeholders who would need information if something happened. Because Zellis handles data belonging to millions of people, employees of client organizations who are affected by a breach must also be considered stakeholders. Knowing all of these groups helps Zellis to prepare message templates, contact lists and responsibilities for the teams and who can communicate and what information to share.

To reduce the chance of breach, Zellis should also implement strong technical safeguards. These includes web application firewalls, vulnerabilities scanning and testing, strong access controls, and strict patch management procedures. Since SQL injection was the core issue behind CVE-2023-

34362, Zellis should adopt secure coding standards and regular penetration testing to detect similar weaknesses. Another essential safeguard is continuous vendor risk assessment and also communication with vendors is specially important because Zellis depends on timely warning when vulnerabilities appear in their-part software now.

Finally, Zellis should create a simple and accessible internal communication process for reporting suspicious activity. Employees and contractors should know exactly how to alerts the security team if they notice anything unusual. Encouraging open communication inside company is important because early reporting can prevent as small issue from turning into a major incident.

ii. Phase Two – During the Attack

When an attack happens, communication becomes even more critical, and Zellis must act fast and follow a well-organized process. In this case, the breach was caused by a zero-day SQL injection vulnerability in MOVEit Transfer, which allowed attackers to access and bypass authentication, install the LEMURLOOT web shell, and steal sensitive payroll data. Communication this cause internally helps IT and security teams to decide what systems to isolate and what immediate actions are needed.

During the attack, Zellis must also focus on collecting and preserving evidence. Preserving evidence is crucial because it supports the investigation, helps understand the attacker's behavior, and provides information regulators. In this phase, communication with external cybersecurity partners, clients, and legal teams must be handled carefully to avoid spreading incomplete or incorrect information. Everything communicated should be verified by the technical team.

The communication plan created before the incident would greatly benefit Zellis during the attack. If the company had a clear checklist, they would know when to shut down systems, who must

approve each step, and how to notify each client. This plan would help Zellis respond faster, stay legally compliant and avoid confusion between teams. A well-prepared plan includes a formal incident report, time-stamped actions, and consistent updates to all internal and external stakeholders. With this kind of plan, Zellis would be far better prepared to contain damager and maintain trust with clients throughout the crisis.

iii. Phase Three – After the Attack

Once the attack has been contained, Zellis enters a phase where communication focuses on rebuilding trust, meeting legal obligations and improving future security practices. The company must monitor many sources of information, by carefully monitoring how the stolen data is being used or shared, Zellis can adjust its communication and respond to new developments quickly. If new evidence shows that more data was exposed, Zellis must update clients and regulators as soon as possible.

Psot incident communication must also comply with legal requirements. Because Zellis handles personal data, they must submit detailed reports to regulators such as the ICO and follow GDPR's rules for notifying affected organizations, this requires proper communication. Legal communication must be described that what happened, what data was affected, and what steps Zellis has taken to reduce risks. The legal team must prepare statements for the public and for customers, good legal communication helps reduce risk of lawsuits and shows regulators that Zellis is cooperating fully.

Finally, Zellis must review and update all cybersecurity policies, vendor agreements, training programs, and technical controls. This is an important part of communication plan because the company must inform employees, vendors, and clients about changes to prevent future incidents.

For example, Zellis may introduce stricter vendor reporting requirements so that vulnerabilities like CVE-2023-34362 are communicated earlier. They may update detection tools or add new monitoring systems. Communicating these improvements helps rebuild customer confidence and shows that Zellis is taking meaningful steps to prevent another breach.

4. Conclusion

The MOVEit breach shows that one weakness in a vendor's software can quickly move down the supply chain and affect hundreds of organizations. In Zellis case, even though they did not create the vulnerability, they still suffered a major impact because hey relied on MOVEit for payroll data transfers. This makes strong communication planning extremely important.

The main lessons are stay prepared before an attack, maintain strong relationships with vendors, respond quickly during the attack, and communicate honestly with clients and employees afterward. Clear and simple communication helps reduce panic, maintain trust, and support legal compliance. A strong communication plan also helps organizations recover faster, reduce long-term damage, and improve future security.

5. Information Sources

[1] Progress, "MOVEit Transfer and MOVEit Cloud Vulnerability," *Progress.com*, Jul. 05, 2023. https://www.progress.com/trust-center/moveit-transfer-and-moveit-cloud-vulnerability

[2] C. Condon, “Observed Exploitation of MOVEit Transfer Vulnerability CVE-2023-34362 | Rapid7 Blog,” *Rapid7*, Jun. 01, 2023. https://www.rapid7.com/blog/post/2023/06/01/rapid7-observed-exploitation-of-critical-moveit-transfer-vulnerability/

[3] C. Page, “Microsoft says Clop ransomware gang is behind MOVEit mass-hacks, as first victims come forward | TechCrunch,” *TechCrunch*, Jun. 05, 2023. https://techcrunch.com/2023/06/05/microsoft-clop-moveit-hacks-victims/

[4] National Cyber Security Centre, “MOVEit vulnerability and data extortion incident,” *www.ncsc.gov.uk*, Jun. 07, 2023. https://www.ncsc.gov.uk/information/moveit-vulnerability

[5] GOV.UK, “Data Protection Act 2018,” *legislation.gov.uk*, 2018. https://www.legislation.gov.uk/ukpga/2018/12/contents

[6] B. Wolford, “What is GDPR, the eu’s new data protection law?,” *GDPR.EU*, 2025. https://gdpr.eu/what-is-gdpr/