Ransomware Disaster Recovery Plan

Jurassic University

Prepared by: Group 6 -- *Business Continuity Specialists*
A dedicated consulting team committed to ensuring business continuity and resilience

Professor - Claude Sam-Foh

Date – 13th August 2025

CSCL1060 Business Continuity in the Cloud

Contents

Group Details:

Group 6

Team Members:

- **(232)Sahil Panjwani — Team Captain**
- **(261)Xuanyu Zhu — Assistant Team Captain**
- **(239)Kaustubh Patil— Business Systems Analyst**
- **(216)Pooja Rameshbhai Gadge— Business Systems Analyst**
- **(251)Faheem Salim Shaikh — Communication Coordinator**
- **(258)Mohammed Mubeen Uddin — Communication Coordinator**

Executive Summary

Jurassic University, a renowned leader in emerging technologies, is increasingly at risk from ransomware attacks that could disrupt its most essential operations. This report presents a comprehensive plan to safeguard the institution's critical systems - namely Workday, Moodle, and SAP - and ensure they can be restored within two hours in the event of an attack. The strategy relies on encrypted cloud backups, a coordinated cross-functional response team, and a clear framework built on Business Impact Analysis (BIA), Business Continuity Planning (BCP), and Disaster Recovery Planning (DRP). By adopting this roadmap, the university will be better equipped to minimize downtime, maintain vital functions such as teaching and payroll, and strengthen its long-term resilience through technical safeguards, coordinated departmental actions, and continuous improvement measures.

Purpose of the Report

The purpose of this report is to guide Jurassic University in preparing for and recovering from a ransomware incident. It lays out a strategy for identifying and prioritizing critical systems, defining clear continuity and recovery procedures, and creating a roadmap that balances immediate recovery with long-term readiness. It also offers recommendations to improve the university's overall preparedness against future threats.

Introduction

Ransomware has become one of the most disruptive cyber threats facing higher education institutions today. Universities, with their sprawling IT environments, distributed

decision-making, and wealth of sensitive data, are prime targets. Jurassic University - an internationally recognized institution specializing in emerging technologies - must take proactive steps to protect its operations, reputation, and community from such risks.

This report has been developed by a consulting team with expertise in both business and digital transformation. Working under the guidance of the Executive Steering Committee (ESC), our mission was to create a tailored BIA, BCP, and DRP that align with the university's unique needs. The approach draws on lessons from real-world ransomware incidents and best practices from across the industry.

Our team has collaborated closely with both IT and business units to shift the institution's stance from reactive recovery toward proactive resilience. This includes identifying mission-critical systems, setting recovery time and recovery point objectives, and defining clear escalation paths. The sections ahead will present an in-depth look at the current state of operations, the potential impact of a ransomware event, and the recommended strategies for rapid recovery and long-term continuity. Recommendations also extend to future enhancements such as cloud migration, regular simulation drills, and centralized backup management.

Enterprise Highlights

About Jurassic University

Jurassic University offers a wide range of programs - undergraduate, graduate, and postgraduate - in fields such as generative AI, cloud computing, and advanced medical sciences. Its academic structure spans faculties in engineering, arts, computer science, and business management, complemented by a Continuing Education Department that caters to corporate clients and distance learners. The institution operates under the governance of a Board of Governors, a President, a Senate, and several academic committees. Its reputation for innovation and technology leadership, while a strength, also makes it an attractive target for cybercriminals.

IT Department and Operations

The university's IT division, led by Chief Information Officer Elisapie Ray, is organized into six specialized units: Enterprise Architecture, Compliance, and Governance (EACG); Project Management Office (PMO); Infrastructure and Operations (IAO); Cybersecurity (CS); Service Management Office (SMO); and Application Development/DevOps (DO). Each unit plays a vital role - from maintaining infrastructure and applications to ensuring security compliance and supporting service delivery.

Despite its technical capabilities, the IT organization has historically operated in silos, which has slowed collaboration and response times. With growing demands for faster delivery and reduced time-to-market, the need for integrated continuity planning has never been more urgent.

Critical Systems

Jurassic University depends on a handful of enterprise systems that are fundamental to both academic and administrative operations. At the heart of this infrastructure are Workday, Moodle, and SAP - classified as Tier 1 systems because of their direct role in payroll, teaching, and financial transactions. Tier 2 systems such as ServiceNow and Monday.com support service management and project coordination. The protection and swift restoration of these platforms form the backbone of the continuity strategy outlined in this report.

Key Systems List

Jurassic University relies on several enterprise systems critical to its operations:

Tier 1	Moodle, Workday	Most urgent – essential for teaching and payroll
Tier 2	SAP	Important – financial operations, but less urgent than Tier 1
Tier 3	ServiceNow, Monday.com	Lower priority – restore after core operations are stable

Incident Overview & Problem Statement

At 2:03 AM on a quiet Saturday morning, the glow of the server room at Jurassic University hid an unfolding crisis. The cybersecurity dashboard lit up with alerts – unusual data spikes, unexplained file renaming, and processes running that no one had authorized. Within ninety minutes, the university's three most essential systems - Workday, Moodle, and SAP were no longer accessible. Payroll cycles froze, students logging in for weekend coursework hit error screens, and the finance department watched as if their tools simply went dark.

The attack was swift, calculated, and costly. By the end of the day, operations had stalled across multiple departments, and the estimated financial toll was already surpassing **half a million dollars**. For a technology-forward institution known for cutting-edge research and innovation, the reputational risk was as damaging as the operational disruption. The event became a wake-up call – not just to recover from this attack, but to design resilience into the very DNA of the university's systems.

Business Impact Analysis (BIA)

The Business Impact Analysis for Jurassic University assesses how ransomware-driven downtime affects teaching operations, administrative workflows, financial processes, and the institution's reputation. The analysis focuses on determining criticality, acceptable downtime (RTO), and acceptable data loss (RPO) for each major system, ensuring resources are deployed where they matter most during recovery.

Tier 1 - Mission-Critical Systems

These systems are the operational heartbeat of the university. **Workday** manages payroll and HR, ensuring faculty and staff compensation remains uninterrupted. **Moodle** is the primary learning management platform, delivering course materials, assessments, and grades. **SAP** handles financial transactions, procurement, and budget control. Disruption to any of these for more than two hours directly halts core operations—faculty payments would be delayed, course access for students blocked, and essential procurement paused. RTO is set to **2 hours**, RPO to **15 minutes**, ensuring near-real-time data protection.

Tier 2 - High-Priority Systems

This tier includes **ServiceNow**, which supports IT service management and incident tracking, and **Monday.com**, which manages cross-departmental projects. While downtime here doesn't stop teaching or payroll, it impacts response times, project delivery, and operational coordination. These systems have an RTO of **8 hours** and an RPO of **1 hour**, allowing for controlled recovery without long-term operational damage.

Tier 3 – Supporting Systems

This includes internal communication tools (e.g., staff intranets, bulletin boards) and non-critical applications used for student engagement and event coordination. While useful, these can be unavailable for up to **24 hours** without significantly affecting academic delivery or core operations. RPO is set at **4 hours**, balancing cost and necessity for backup frequency.

Tier	**Systems**	**Function**	**RTO**	**RPO**	**Impact if Unavailable**
Tier 1	Workday, Moodle, SAP	Payroll, HR, Learning Management, Finance	2 hours	15 mins	Halts payroll, course delivery, and financial processing

Tier 2	ServiceNow, Monday.com	IT Service Management, Project Coordination	8 hours	1 hour	Slower response to IT issues, delays in project timelines
Tier 3	Internal Communication Tools, Event Apps	Staff comms, student engagement	24 hours	4 hours	Reduced communication efficiency, minor inconvenience

This structure ensures that in the event of another ransomware attack, Jurassic University can focus its recovery efforts on systems that have the highest operational and reputational stakes, while still having a plan for secondary and tertiary systems. By integrating this tier-based approach into the Disaster Recovery Plan (DRP), the university can protect its academic continuity, avoid costly delays, and maintain trust with students, staff, and stakeholders.

Gap Analysis & Root Cause

The ransomware attack exposed several weaknesses in Jurassic University's IT security posture, highlighting the gap between the institution's existing safeguards and the resilience needed to withstand modern cyber threats. One of the most notable gaps was the **lack of comprehensive network segmentation** - critical systems such as Moodle, Workday, and SAP were all connected on the same network layer, meaning that once the attackers gained entry, they could move laterally with minimal resistance.

Another weakness was in **backup management**. While backups existed, they were stored in a location connected to the main network, making them vulnerable to encryption by the same ransomware. There was also no clear process for regularly testing backup restoration, so recovery readiness was more assumed than proven.

Access control policies also played a role in the gap. Several user accounts had more privileges than required for their daily tasks, increasing the potential damage if those credentials were stolen. In addition, **multi-factor authentication (MFA)** was not consistently enforced for all high-privilege accounts, leaving a door open for attackers who obtained stolen usernames and passwords.

The **root cause** of the incident appears to be a phishing email that bypassed existing email filtering rules. An unsuspecting staff member clicked on a malicious attachment, unknowingly installing the ransomware payload. From there, the malware exploited unpatched software vulnerabilities to escalate privileges and spread through the network.

From a lesson-learned perspective, the attack showed that **technical defenses alone are not enough**. Without strong security awareness training, employees remain the first and weakest line of defense. It also proved that security measures need to be layered – segmentation, strict access

controls, offline backups, and consistent patching all must work together to prevent or contain such breaches.

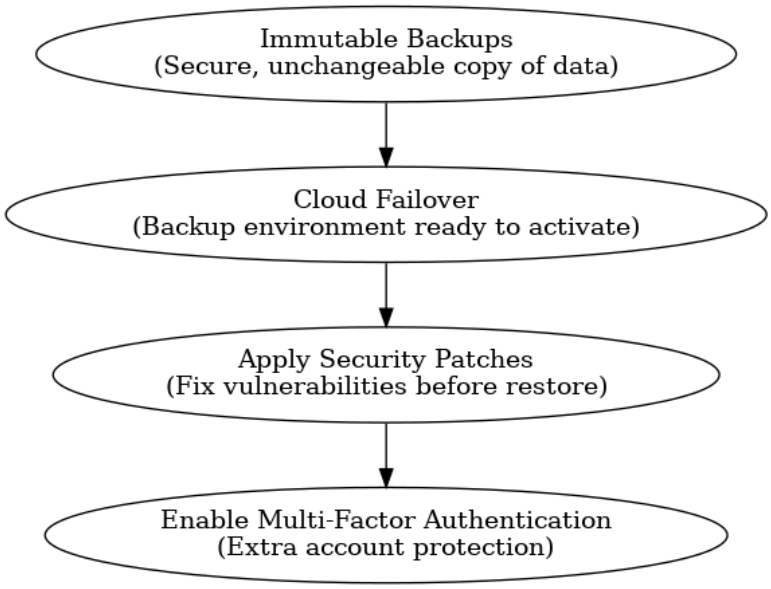
Disaster Recovery Strategy & Roadmap

We approach the recovery of the most important systems to the university community first and then the less essential systems, with the intention of minimizing disruption to education and operations. We begin with Moodle, as it's the lifeline for 18,000 students—every hour offline means missed lectures, late assignments, and anxious students. We next restore Workday, so the staff and faculty are paid on time and HR functions smoothly again. Third is SAP; it handles finance functions like billing and reimbursements—still important, but less essential than keeping classes and payroll in balance. Finally, we take back ServiceNow (for support services) and Monday.com (for project management)—convenient for internal workflow but not essential to the act of teaching. This prioritization ensures that we take back learning first and employee well-being second. For instance, in the case of Munster Technological University, when ransomware attacked, shutting down campuses for a week, it was best to prioritize critical systems so the university could reopen and continue classes within days instead of weeks.

To recover safely, we will rely on proven technical methods that act as safety nets in a crisis. Immutable backups ensure that we always have a "locked" copy of information that can't be tampered with or erased by ransomware, and thus if the main system is compromised, we can recover safely from a new, trusted source. Cloud failover has a secure copy of our systems in the cloud ready to take over if our data center is down. Multi-Factor Authentication (MFA) adds an additional step of logging in—such as entering a phone code—to critical accounts, locking out attackers even if they have a password. We will apply all security patches before reconnecting any system, closing vulnerabilities such as repairing a broken lock before opening a door. That is what real-life success stories look like, like a hospital backing out of a ransomware lockdown within hours using immutable backups, avoiding paying ransoms and downtime altogether. That is the kind of resilience we aim to have at Jurassic University.

Technical Recovery Measures

Flowchart



This diagram shows the step-by-step technical actions Jurassic University will take to ensure a secure and reliable recovery after a ransomware attack. The process begins with creating **immutable backups** that cannot be altered or deleted, ensuring a safe copy of all critical data. Next, a **cloud failover** environment is prepared to take over if the primary data center is unavailable. Before any systems are brought back online, all **security patches** are applied to close known vulnerabilities. Finally, **multi-factor authentication (MFA)** is enabled on all administrator accounts to prevent unauthorized access during and after recovery. This flow ensures that recovery is both fast and secure, reducing the risk of reinfection.

Our recovery process is segregated into three well-delineated phases that lead us step by step and avoid confusion. Phase 1 (0–24 hours) is all about rapid containment and targeted recovery: we get impacted systems isolated right away to prevent spread, activate our disaster recovery setup, and restore Moodle and Workday from clean backups—quickly testing for login functionality and payroll processing to ensure rudimentary operation resumes, following best practice guidance for rapid containment and critical service restoration. In Phase 2 (1–7 days), we restore secondary systems like SAP, ServiceNow, and Monday.com using checksum validation to ensure data integrity and performing checks to ensure that everything from financial transactions to help desk tickets is accurate and working perfectly. Phase 3 (1–4 weeks) is long-term hardening: we deploy security patches, enable MFA, and stand up Endpoint Detection & Response (EDR); then we conduct a thorough review to document lessons learned, update our disaster recovery plan, and rehearse recovery steps through a drill so we're ready next time. This methodical, expert-led

process makes sure systems aren't just recovered—but returned healthier and more secure than ever.".

Recovery Timeline:

Phase	Timeframe	Main Action	Systems Restored
Phase 1 – Immediate Response	0–24 hours	Stop attack, switch to backups, basic recovery	Moodle, Workday
Phase 2 – Full Recovery	1–7 days	Restore remaining systems, verify data integrity	SAP, ServiceNow, Monday.com
Phase 3 – Hardening & Review	1–4 weeks	Apply security, review results, update recovery plan	All systems secured and operational

Here is a real-life example we can utilize in the report. In November 2019, WED2B, a leading UK bridal wear retailer with a headquarters in Milton Keynes and some 60 UK and European stores, was hit by a serious ransomware attack late on a Friday night. The first signs of trouble were when antivirus warnings began to fail, shortly followed by a wave of file encryption sweeping through their network. Within a brief period, around 5 terabytes of NAS-stored data had been encrypted, as well as valuable third-party backups hosted in Microsoft Azure.

Management in IT acted swiftly to contain the incident. One of the first steps they took was to isolate store sites from the central network in order for retail operations to continue in a restricted manner while recovery efforts commenced. Knowing that time was of the essence, the team prioritized the restoration of essential infrastructure from immutable backups—secure data copies that are immune to ransomware's deletions or modifications. It was a lifesaving decision: Active Directory was restored in under 30 minutes, returning critical authentication and access functionality. Soon thereafter, more than 1 terabyte of SQL databases—key business and transactional data—was restored in about an hour.

By early Saturday afternoon, less than 24 hours from initial detection, all of WED2B's essential systems were back online. There was no ransom payment and no data loss, according to the company. The difference in system recovery time for those with immutable backup protection and those without was stark. Those that were protected with immutability were fully recovered within a day, while the NAS space not covered by this precaution took weeks to recover. This incident fully demonstrated the important role that immutable backups must play in ransomware recovery—enabling fast restoration, ensuring operational continuity, and avoiding costly downtime and ransom payment.[1]

Execution Plan

When responding to a ransomware incident, speed, coordination, and clarity are essential. This execution plan outlines exactly who does what, how decisions are made, and how information flows internally and externally during the recovery process. The goal is to get critical systems restored quickly, minimize downtime, and reassure all stakeholders that the situation is under control.

Roles & Responsibilities of Each IT Department

- Enterprise Architecture, Compliance & Governance (EACG) – Ensures that recovery actions comply with internal policies and external regulations (e.g., GDPR, FERPA). They also update governance documents after the incident to reflect lessons learned.
- Project Management Office (PMO) – Coordinates the overall recovery effort, assigns tasks, monitors progress, and makes sure all teams meet their RTO (Recovery Time Objective) and RPO (Recovery Point Objective) targets.
- Infrastructure & Operations (IAO) – Restores physical and virtual infrastructure, activates cloud failover systems, and ensures that network connectivity is secure and stable before systems go live.
- Cybersecurity (CS) – Acts as the "first responder" team, containing the ransomware, isolating infected systems, performing forensic investigations, and applying necessary patches. They also enforce Multi-Factor Authentication (MFA) on all critical accounts.
- Service Management Office (SMO) – Provides front-line support to faculty, staff, and students during the recovery. They maintain the incident log and share updates on which services are available.
- Application Development / DevOps (DO) – Restores core applications such as Moodle, Workday, and SAP, and tests them to ensure they function correctly and integrate smoothly with other systems.

Escalation & Decision-Making Process

1. **Detection** – The Cybersecurity (CS) team confirms the ransomware attack and isolates affected systems immediately.
2. **Activation** – The CIO activates the Disaster Recovery Plan (DRP) and alerts the Executive Steering Committee (ESC).
3. **Prioritization** – Recovery priorities are set according to the Business Impact Analysis: Tier 1 (Moodle, Workday), followed by Tier 2 (SAP), then Tier 3 (ServiceNow, Monday.com).
4. **Delegation** – The PMO assigns specific recovery tasks to the relevant IT departments.

5. **Verification** – Before restored systems are reconnected to the network, they are reviewed and approved by the CIO and ESC.
6. **Post-Recovery Review** – The ESC leads a lessons-learned meeting to update the DRP, address gaps, and strengthen future readiness.

Communication Plan

When an incident happens, the main way to communicate inside the university will be through Microsoft Teams for secure chat and video calls. If this is not working, encrypted email or satellite phones will be used. Updates will be sent every two hours while the issue is active, and then twice a day until everything is fixed. These updates will go to IT teams, department heads, and the Emergency Steering Committee (ESC).

For people outside the response team, students and staff will get updates through SMS, university-wide emails, and a live status webpage. Any news for the media or public will come only from the Communications Office. Vendors and partners will be contacted directly by phone or secure email to share information about system availability.

The messages will follow three stages. In the containment stage, the team will confirm the problem and say which systems are affected. In the recovery stage, updates will include timelines for when systems will be restored and how to access them. In the completion stage, the team will confirm that all systems are working and explain any new security steps that have been added.

Budget & Resource Allocation

Recovering from ransomware requires more than just technical fixes — it demands the right mix of tools, skilled professionals, and preventive measures to avoid future incidents. The table below outlines the budget required for Jurassic University's recovery and resilience program.

Category	Cost (USD)	Justification
System Restoration	$200,000	Cloud failover activation and restoration of Tier 1 & 2 systems from immutable backups
Security Upgrades	$150,000	MFA licensing, Endpoint Detection & Response (EDR) tools, firewall upgrades, and patch management
External Consultants	$80,000	Forensic specialists and compliance advisors to ensure secure, efficient recovery
Staff Training	$50,000	Cybersecurity awareness workshops and quarterly disaster recovery drills

Communication Tools	$10,000	Enhancements to the SMS alert system and outage status webpage
Contingency Reserve	$10,000	Funds for unexpected technical or operational expenses

Estimated Total Budget: $500,000

Budget Rationale

System restoration focuses on bringing critical systems like Moodle and Workday back online within hours instead of days, so teaching and operations can continue with minimal disruption. Security upgrades are applied at the same time to close any vulnerabilities and prevent the same issue from happening again. External consultants may be brought in to provide expert guidance and speed up problem-solving during the crisis. Staff training is an important part of the process, helping people recognize phishing attempts and avoid accidental mistakes that could lead to breaches. Clear communication tools keep students, staff, and partners updated throughout the recovery, reducing confusion and frustration. Contingency funds give the university the flexibility to cover unexpected costs, ensuring the recovery can move forward smoothly even when challenges arise.

Long-Term Continuity & Prevention Measures

The most effective way to guarantee the resistance of ransomware and other threats online on a long-term basis is to make Jurassic University develop a forward-looking strategy that will incorporate prevention, ongoing improvement, and the ability to recover in a short period. The major strategies to ensure the continuation of the operation of the university include the following:

DRaaS Migration for Tier 1 & 2 Systems

It is important to migrate Tier 1 and Tier 2 systems (Moodle, Workday and SAP) to a Disaster Recovery as a Service (DRaaS) platform that can help minimize recovery time and better protect the information. Using DRaaS, real-time backups are geographically dispersed to provide high security to these critical systems and allow fast restoration in the event of a ransomware attack. Immutable cloud backups will ensure the university possesses the secure copy of all important data, which cannot be changed or lost under the action of ransomware. The failover feature of the cloud will ensure business activities do not come to a stop even when the data centre is exposed.

1. **Quarterly Disaster Recovery Drills**
   While technical systems and solutions are essential, the human element plays a significant role in ensuring the success of any disaster recovery plan. Quarterly disaster

recovery drills will be conducted to familiarize IT staff and key departments with recovery procedures and help identify any gaps in the current plan. These drills should be designed to simulate real-world ransomware attacks, including system restoration, data integrity checks, and communication processes. The drills will also provide an opportunity to refine the escalation process and ensure that decision-makers understand their role in a crisis. By practicing recovery regularly, Jurassic University can improve response times and minimize the risk of oversight during a real disaster.

2. **Centralized Backup Management**
   Even though technical systems and solutions are critical, human factors cannot be overlooked when any disaster recovery plan is being developed. Disaster recovery drills will be carried out on a quarterly basis in order to familiarize the IT staff and key departments with the recovery procedures and assist in highlighting any potential gaps in the current plan. Such drills are to be conducted to emulate true-to-life ransomware attacks, and system restore, data integrity verification, and the communication processes should be considered. The drills would also help trim down the escalation process and make decision-makers aware of their role during a crisis. Recovery practice will allow Jurassic University to advance on their response rates and reduce the chance of overlooking the actual disaster.

3. **Annual Review and Updates to DRP**
   An update on the Disaster Recovery Plan (DRP) must take place on an annual basis. Since the DRP will also need to be updated with the latest technologies and threats, the current plan should undergo configuration to accommodate recent trends in cybersecurity and disaster management. That is, the integration of new recovery technologies, changes in recovery time objectives (RTO) and recovery point objectives (RPO) were necessary and making sure that the plan reflects any changes to the operational structure the university may undergo. Frequent revisions will keep the plan relevant and useful so that the institution will cope with changing threats.

Policy and Infrastructure Changes for Long-Term Resilience

1. **Security Policy Overhaul**
   The review and restructuring of the security policies in the university is necessary. The new policies are also expected to center on integrating security practices throughout the departments, enforcing firm patching schedules, and instituting well-defined procedures of responding to security problems. In particular, they should be the policies that focus on the need to implement Multi-Factor Authentication (MFA) on all the important systems as well as on administrative accounts to avoid unauthorized access.

2. **Increased Investment in Cybersecurity Training**
   To develop cybersecurity culture, the ESC must ratify a strategy in which all the

university faculty and staff take compulsory cybersecurity courses. Indoctrination ought to include issues like phishing, secure computing online and actions to undertake in case of security breach. Additional risk mitigation will be achieved by increasing the awareness of all levels of the organization which are likely to face successful ransomware attacks.

3. **Expansion of IT Infrastructure for Scalability and Redundancy**
   The ESC will be sanctioned to enlarge the IT infrastructure setting in the university having concentration on redundancy and scalability. These would be installing geographically diverse data centers, improving the strength of a failover system and improving the network security infrastructure of the university to support cloud-based Disaster Recovery and system recovery in a shorter span of time.

4. **Annual Review and Update of the DRP**
   It is imperative to ensure that the ESC will require that an annual review and update of the Disaster Recovery Plan (DRP) is conducted. Such a review ought to include the lessons learned to that point based on the quarterly drills, real-life events, and changing threat environment. The DRP must also be stagnated to make it relevant and functional based on the shift in the technology stack and needs of the university.

By authorizing the abovementioned actions, implementing the required changes to the policies and infrastructure, Jurassic University should be in a better position to resist a ransomware attack, recover faster, and ensure coherent functioning of its main processes. Not only will these help mitigate the financial and reputational risks of cyber threats but will also create a proactive security-oriented culture at the institution.

Such preventive steps will increase the resilience of the university greatly against the effects of ransomware attacks and other interference. Through investment in sound disaster recovery technologies, continuous testing, and continual upgrades, the Jurassic University will be able to improve its overall security profile and further protect its jeopardized processes.

RTO/RPO Table:

System	RTO (Max downtime)	RPO (Max data loss)	Reason for Priority
Moodle	4 hours	15 minutes	Students need classes to continue
Workday	8 hours	1 hour	Payroll & HR functions

SAP	12 hours	1 hour	Finance & billing
ServiceNow	24 hours	4 hours	Internal help desk
Monday.com	24 hours	4 hours	Project coordination

RTO/RPO Table Explanation:

RTO (Recovery Time Objective) - The maximum amount of time that a system can be down before it impacts the organization. For example, **Moodle** and **Workday** must be restored within 2 hours to minimize disruption to academic and payroll operations.

- **RPO** (Recovery Point Objective) The acceptable amount of data loss. A **30-minute RPO** for critical systems like Moodle and Workday ensures that recent data is not lost, and systems can be restored with minimal disruption.

Full Attack Timeline

Phase	Time	Main Actions	Systems Impacted	Recovery Actions
Phase 1 – Initial Containment	0–24 hours	Identification of the attack, quarantine of the system, limitation of propagation increase. Bring into effect DR plan and restore important systems.	All Tier 1 and Tier 2 systems were impacted.	Isolate infected systems, start restoring the Moodle and Workday in immutable backups, minimal testing of functionality of the systems.
Phase 2 – Full Recovery	1–7 days	In order to carry out testing, restore the non-critical systems, test the data integrity.	SAP, ServiceNow, Monday.com	Restoration of the SAP, ServiceNow, and Monday.com in a full manner. Integrity of data and validation of business processes.

Phase 3 – Hardening & Post-Incident Review	1–4 weeks	Implement security patches, turn on multi-factor authentication (MFA), post-mortem analysis and recovery drill.	All systems operational.	Apply security patches, apply an EDR, apply MFA and perform a complete recovery exercise. Lessons learned should be incorporated in order to review and update DR plan.

This time schedule presents major steps towards the recovery and restoration process of the system of the university with each stage accentuating various elements of the recovery plan, such as the containment, and the long-term hardening. The **RTO/RPO** table establishes that the sequences of recovery priorities are combined with criticality of the systems to make the operation run smoothly and effectively as far as a recovery process is concerned in case an attack occurs.

References / Works Cited

1. Rubrik. (n.d.). *WED2B ransomware recovery: 100% recovery within 24 hours with zero data loss and zero ransom paid* [Case study]. In *Becoming Unstoppable Against Ransomware: Customer Success Stories* (pp. 7–10). Rubrik. Retrieved August 10, 2025, from https://www.rubrik.com/content/dam/rubrik/en/resources/case-study/ransomware-customer-ebook.pdf