Executive Summary

Monarch Capital is currently facing serious cybersecurity challenges that threaten both company operations and client relationships. The company's threat detection time averages 72 hours, which is significantly slower than the industry standard of four hours. In addition, many of the company's security procedures reference outdated systems, and the security team is operating at 140% capacity. These weaknesses have caused client concerns, delayed contracts, and financial losses totaling approximately 2.1 million per year. Because of increased industry concerns and new insurance requirements, Monarch Capital must implement security improvements within the next 120 days.

To address these issues, this project proposes upgrading Monarch Capital's cybersecurity infrastructure by implementing a Security Mesh Architecture System and improving our security team. This modern security approach protects individual assets and access points. The solution will include AI-powered threat detection tools, a next-generation firewall, improved access control platforms, and automated monitoring systems. A company-wide security training program and external cybersecurity audit will help improve procedures and ensure compliance with industry standards.

The project requires an estimated 2.71 million investment in new security infrastructure and training resources. These resources include advanced security monitoring systems, threat detection tools, and personnel responsible for implementing employee training programs. The implementation timeline will span approximately 90 days, including system upgrades and employee training sessions. An additional 30 days will be used for documentation and verification for the insurance provider.

Problem Statement

Cybersecurity Infrastructure

Our company, Monarch Capital, has outdated data centers, insufficient incident response proficiency, incomplete security documentation, and an understaffed security team, which has created a high-risk cybersecurity posture that may threaten client data confidentiality, regulatory compliance, and insurance eligibility. Immediate action and remediation are required within at least 120 days to meet insurer requirements and to reduce possible exposure to cyber threats and other possible drawbacks. The IT and security teams have an average response time of 72 hours, which exceeds the industry standard of at least 4 hours. Due to this delay, our company, Monarch Capital, is exposed to longer threats with time, which increases the likelihood of data breaches and disruptions for operations.

Incomplete Documentation

In addition to certain weaknesses in our technology, internal security processes are insufficient. 50% of our security documentation is inaccurate and outdated, which doesn't reflect current procedures and compliance. Due to the lack of updated documentation, this will create an inconsistent response procedure, weaken survey readiness, and increase contractual and regulatory risks. We must have accurate and precise documentation to ensure that it's essential for guiding our staff in the right direction with proper maintenance, implementation, and course of action to protect our systems and data. With outdated and missing documents, it's easier for our team to fall into inconsistent processes, and increasing the chances of running into errors. Therefore, updating and making sure our documents are accurate is huge for our company, Monarch Capital, to perform security procedures properly and precisely.

Understaffed Security Team

In addition, our security department is operating at 140% capacity, indicating strains on severe resources. This causes major complications that may limit the team's ability to implement new strategies, increasing errors and mistakes within the department, and may create sustainability concerns that can be related to burnout. This situation that is happening within our company is further instructed by an external directive from the company's insurance provider, which issued a 120-day deadline to complete required security improvements. Failure to meet these requirements can result in a loss of coverage, significantly increasing financial exposure. Our organization must modernize our infrastructure, strengthen our incident responses, stay up to date with government documentation, and balance our resource capacity to reduce risks and continue operations and financial protection.

Proposed Solution

As one of the primary concerns is private client data, we propose recreating the security team from the ground up. With the security team operating at 140% capacity, their effectiveness in monitoring, incident response, and system maintenance has declined. The current server infrastructure is outdated and may cause operating issues, while the procedures and training for security and hardware do not meet modern industry standards.

To address both the protection of the client data, the changes and additions of the internal security team, and the upgrades to the server architecture, we would need to increase security personnel while off-boarding some current employees, update and procure new hardware for data storage, and update security procedures.

Implementaiton

To implement the proposed solution for the security team, the first step will be to rebuild

and restructure the department. Rebuilding the security department will begin with the replacement of 10 personnel. The replacement personnel who are hired will be required to have the CompTIA Server+ certificate. The remaining staff members will receive additional training through TrainingCamp to obtain the CompTIA Server+ certification. This training will take approximately one month to complete. An additional two people will be hired for server management.

The implementation of the hardware changes will be more efficient and straightforward. Once the new server machines are installed, the IT team, along with the security team, will back up the current servers and transfer data over to the new servers. This will allow for improved performance, stronger and modern security measures, and better scalability for further data and company growth.

Security procedures and documentation will be implemented after the new infrastructure is installed and secured. The updated procedures will begin by explaining the new hardware, while also explaining access control, incident responses, security of the system, and regular security tests. These procedures and policies will allow us to meet industry response time and standards.

Technical Requirements

To introduce new hardware for storing confidential client and internal data, we proposed in-house server upgrades. These upgrades will be at half the cost of cloud upgrades, saving money over time while also being able to maintain the degradation of hardware for years to come. We estimate that the cost of this new hardware will be 2.7 million dollars. Below are the technical specifications and cost for the new server hardware:

- 100 Gb/s network infrastructure:

    - Estimated cost: $200,000 per year.
    - This upgrade will significantly increase data transfer speeds within the data center to allow for faster processing.
- Firewall management system:
    - Estimated Cost: $700,000
    - A new firewall system will allow the security team to manage what packet information can be sent and received from the servers. This will cut down the response time.
- Server storage system:
    - Estimated Cost: $1.8 million.
    - RAID configuration.
    - NIST full data encryption requirements.
    - Role-based access control and multi-factor authentication with Cisco DUO.
    - 2.1+PB of storage, 2x AMD EPYC 9005 CPUs, 486 GB DDR4 RAM
    - Regular 24-hour interval backups.

Success Metrics

With the proposed solutions in place, the effectiveness will be measured using several metrics. The primary goal is to make sure that data is secure while also reducing incident response time from 72 hours to under 4 hours, meeting and exceeding industry standards. One metric that will be tracked using the security dashboard is the number of attacks that have been blocked. We'd like to see at least a 95% unauthorized access block rate, compared to our current unauthorized rate of 76%. We'd also like to measure the time to resolution (TTR) for any tickets that may be submitted regarding data that may be inaccessible to certain employees. This TTR

should be under 4 hours; resolution times may vary depending on the variety of issues. We were also given a timeline of 4 months (120 days) to verify to the insurance company that insures the company that we have measures in place to secure client data. We will be able to meet this requirement within 3 months.

Resource Requirements

In order to address the vulnerabilities that have been identified in Monarch Capital's internal data center, an investment is required in the infrastructure, personnel, and security operations. The estimated cost of the security overhaul is going to be approximately $2,750,000. This amount will include all capital expenditure and operational improvements needed. The majority of the budget will be allocated to hardware and infrastructure upgrades. For the hardware and networking equipment, the estimated range of the price is $2,700,000. All other funds of the budget will be utilized to support security software licenses and monitoring and compliance tools to maintain enterprise-level cybersecurity standards.

Staffing Needs

The current security team is operating at 140% capacity, which is the reason why there is a 72-hour incident response time. In order to meet the standard 4-hour response procedure, additional personnel must be hired in order to spread the workload evenly and ensure proper coverage is available across monitoring systems. 10 current associate-level and mid-management level employees will be replaced within the cybersecurity department whose skills and training are no longer up to date with current industry standards. Many of these positions are also significantly overpaid relative to their qualifications, and retraining them is not the best financial option because it would be more costly than hiring new personnel with up-to-date certifications and knowledge. The new hires will consist of fresh college graduates and early career

professionals who possess current industry training and are better prepared for the role. This transition will reduce overall payroll expenses by roughly half, because the current approximate average salary for the 10 employees being replaced is $193,000, while the average salary for the recruits will be roughly $95,000. Overall, the replacement of the team will allow us to respond faster to security incidents and support the upgraded systems much more efficiently.

The positions being replaced are as follows:

- 2 Cybersecurity Analysts
- 1 Cybersecurity Operations Lead Analyst
- 1 Cybersecurity Operations Manager
- 1 Data Integrity & Security Specialist
- 1 Governance, Risk, and Compliance Specialist
- 1 Network Infrastructure Engineer
- 2 Server Warehouse Technicians
- 1 Server Warehouse Lead Technician

Technology Requirements

The technology upgrade will focus on improving the security performance and the operational reliability of the systems. To modernize Monarch Capital's data center and improve cybersecurity, the company will implement a 100 Gbps network, upgrade enterprise servers, and deploy advanced security monitoring tools. It will also update firewall systems, strengthen data encryption and secure storage, and introduce automated incident response software.

Timeline With Milestones

- Weeks 1-4: Infrastructure procurement and staff recruitment
- Weeks 5-9: Hardware installation and network upgrades
- Weeks 10-16: Implementation of monitoring systems
- Weeks 16-18: Security testing and compliance verification

Risk Mitigation

Monarch Capital's current upgrade process for its security systems has some possible challenges that are linked to the risks we identified earlier, namely employee adaptation and technology disruption, though with some mitigants, they are not insurmountable hurdles. Our current environment has a 10Gbps network backbone, on-premise servers with RAID 10 storage that distributes and duplicates data across multiple drives for fast access and redundancy should one drive fail, and partial disk encryption that, though not meeting the full-disk standards of the NIST, at least scrambles data even on stolen hardware.

Potential Challenges

Employee adaptation has 40% chances of initial policy compliance issues, 35% chances of shadow IT occurrence within the 90-day transition period to meet the 120-day insurance requirements, and security fatigue due to overwhelm. On the other hand, technology disruption can be caused by 100Gbps infrastructure upgrades, with vendor delays exposing unencrypted client data like SSNs and tax returns, affecting trust with our HNW clients

Contingency plans

For employee issues, our strategy is to utilize a customized training strategy, HR and CISO-led training sessions (30 minutes, weekly for the first 4 weeks), departmental security champions (one champion per department to report adoption metrics and identify shadow IT),

easy SSO authentication, and a 30-day grace period for minor infractions. If non-compliance is more than 15%, we add 1:1 refreshers. For technology disruptions, our strategy is to conduct staged rollouts in non-production environments (weeks 1-2), vendor audits by day 15, off-peak deployments (2-6 AM, weekends), and external expert audits, penetration testing, and vulnerability scans by day 30. All these strategies help us achieve our goal of a 70% reduction in overall incident costs.

Alternative Approaches

If hardware delays extend beyond day 45, we'll pivot to a cloud-hybrid solution, utilizing NIST-encrypted cloud storage for new uploads, incurring 20% additional short-term costs, allowing us to quickly scale our threat detection capabilities. For training overload, we'll double our training groups to 50 people, utilizing online LMS tools, and shorten our training to 12 weeks, still achieving 95% training completion.

Success Factors

Executive buy-in and visibility of support through regular bi-weekly review sessions are key, where metrics like zero-day threat detection within 5 minutes, along with keeping our 80-person HNW-focused workforce resilient, are monitored.

Monitoring methods

KPIs like threat response within 4 hours, 99.99% compliance through SSO logs and champion reports, 95% reduction of unauthorized access through CASB tools, and sub-minute activations are monitored through real-time dashboards, with executive meetings every two weeks that adjust according to requirements like shadow IT increases, and quarterly audits that confirm ROI on infrastructure investments of $2.3M through 70% lower costs on incidents, which can be directly linked to early testing and compliance initiatives.

Collaboration Record

Jordan Fagundes

For this proposal, I contributed to the project's **Proposed Solution**. Utilizing the RPG game to understand how the company operates and what issues it is currently having. We gathered information into a document that can allow us to split ideas on how to improve the said issues. I began by creating a shared folder where each person would have access to the information and proposal documentation. I also helped with the overall content of the proposal, such as making sure everyone was on the right page when it came to facts like the budget. Made sure that the formatting adhered to APA standards and that there were no mistakes in the basic structure of the document.

I also helped guide the team by encouraging discussion, sharing ideas, and making sure everyone agreed with the proposed ideas so that each member had a voice in the project. We communicated outside of class through our group chat to keep everyone aligned and progressing. To make sure that everyone got what they wanted to do, we didn't assign roles; rather had everyone choose what they wanted to, making sure no one was forced to do something.

Jacob Soriano

For this team project proposal, I contributed to the team's **Problem Statement**. During the process of creating this proposal, my main task was to figure out the main points that Monarch Capital was facing and how those issues may affect our company. With that in mind, I was able to gather my information from our RPG scenarios that were played in class, which were *Forming the Guild* and *The Process Problem.* It was a smooth process to find the information I needed through the notes we took during these games we played. To ensure that our report was

accurate and retained the right information, I communicated with my team members, exchanged information, and we worked as a team to do our best on this proposal. And with the help of our Team Captain, Jordan Fagundes, I was able to ask him for help, and he helped guide the team and me to success on this proposal.

Pedro Basulto

For the Team Project Proposal, I worked on the Executive Summary. I used the notes from the RPG activity to make the Executive Summary. In the Executive Summary, I briefly explained our company's problem and proposed solution. I also include key details of the project proposal. I collaborated with my team when developing the proposed solution and contributed by sharing ideas.

Anmol Gill

For the project proposal, I handled writing the Resource Requirements section. This section includes the budget, staffing needs, technology requirements, and timeline of the project. I estimated the overall cost of implementing the new cybersecurity proposal to be $2,750,000. The majority of the budget is allocated to upgrading the company's hardware and networking equipment. I also included details on the tools and software needed, as well as the monitoring systems required to maintain enterprise-level standards. In the staffing needs section, I analyzed the issue of the team operating at 140% capacity, in which we required replacing outdated associates and mid-level managers with new and more qualified personnel. In addition, I explained how hiring early-career professionals would save about 50% of our salary compensation, which contributes to improved operational efficiency and reduced payroll expense. Finally, in the technology requirements and deadline section, I identified key upgrades

needed for the upgrade, consisting of new servers, improved firewall systems, stronger encryption protocols, and more. The timeline is a structured list that outlines the phases of procurement and recruiting, installation, implementation, and testing. Through the project, I collaborated with my groupmates to maintain consistency, accuracy, and precision throughout the writing of this document.

Jerad Britton

My name is Jerad Britton, and for this team project proposal, I helped with the Potential Challenges, Contingency Plans, and Monitoring Methods sections. I reviewed the original draft based on team feedback and critique. I used RPG scenario notes on Monarch Capital's operations and risks to understand areas such as vague information in contingency plans and unclear technical terms (RAID, NIST encryption). I contributed by adding more information such as current environment baseline, step-by-step information on triggers/owners/timelines for contingency plans, and clear explanations for technical specifications. I also connected this information with results such as 70 percent cost reduction for incidents and 99.99 percent compliance. I collaborated by using a group chat for input on drafts. I also used APA style for consistency. I included everyone's ideas to ensure consistency on facts such as a $2.3 million budget and 90-day insurance. Jordan, being the team captain, helped me refine the tone for this team project proposal. I helped ensure that this team project proposal is more detailed but still accessible for non-technical team members.