**PROJECT TEAM PERFORMANCE REPORT**

**GENERAL PROJECT INFORMATION**

|  |  |  |  |
| --- | --- | --- | --- |
| **PROJECT NAME** | | **PROJECT MANAGER** | **PROJECT SPONSOR** |
| **AWS CyberShift Initiative:  "Shifting Cybersecurity to the AWS Horizon"** | | Giuseppe Raciti | **OzCazual** |
| **EMAIL** | **PHONE** | **ORGANIZATIONAL UNIT** | |
| sales@securenet.com.au | (03) 97499 0528 | **SecureNET** | |

|  |  |  |
| --- | --- | --- |
|  | **System Version** | **Document Version** |
| **VERSION** | **1.0** | **1.0** |

**CONTENTS**

[**PROJECT COMPLETION REVIEW 2**](#_heading=h.n9u9l2fhm3i)

[PROJECT OBJECTIVES 2](#_heading=h.n4t745o2ok9f)

[PROJECT DELIVERABLES 2](#_heading=h.v85y4dgdfrs6)

[PROJECT SCHEDULE 3](#_heading=h.josjb8gwez8)

[PROJECT BUDGET 4](#_heading=h.iehbpg5epmuq)

[**TEAM PERFORMANCE 4**](#_heading=h.jibpkflct2pl)

[OVERALL PROJECT TEAM PERFORMANCE 4](#_heading=h.knaqbo410b6c)

[**KEY LESSONS LEARNT 6**](#_heading=h.gdvy16jet1i9)

[PROJECT SCOPE 6](#_heading=h.1pyzh0rggzym)

[PROJECT RESOURCES 6](#_heading=h.pcjz9ulgfw9x)

[PROJECT SCHEDULE 6](#_heading=h.9mmkjede451n)

[PROJECT BUDGET 6](#_heading=h.2wvrum9uy8rl)

[RISK MANAGEMENT 7](#_heading=h.h0y2smfigg5s)

[**PROJECT ARCHIVE 7**](#_heading=h.izve4x6dgzdr)

[RECORDS AND CORRESPONDENCE 7](#_heading=h.2u1y1by9vbfj)

|  |
| --- |
| PROJECT COMPLETION REVIEW |

|  |  |
| --- | --- |
| **PROJECT OBJECTIVES** |  |
| **PLANNED** | **EXECUTED** |
| * Design and implement a secure Amazon AWS cloud environment that can accommodate the increase in online sales and staff, which also has the scalability to manage future growth * The primary objective of the project is once the new AWS cloud infrastructure is implemented, SecureNET will do its best to implement robust security measures to protect the cloud system. This includes aspects such as access controls, encryption, authentication, and the authorization mechanisms to safeguard the system from cyber attacks * Implement strong authentication mechanisms, including Two-Factor Authentication (2FA), to enhance the security of user access to the cloud infrastructure * SecureNET will ensure smooth migration which will allow a seamless transition from the local infrastructure to the cloud environment, all while minimizing any downtime or disruption to normal business operations. * Ensure that the cloud infrastructure SecureNET has implemented adheres to the relevant compliance regulations, industry standards and best practices, to maintain the trust of the customers and stakeholders. * Enhance data confidentiality, integrity and availability * Implement an Incident Response Plan that proactively monitors, detects, and responds to security incidents effectively, to minimize the possible downtime and impact caused to OzCazual | * Achieved - This was built on cloud infrastructure not AWS. * Achieved - Various security measures were implemented to protect the cloud system. * Achieved - MFA was implemented on the infrastructure * Achieved - Implementation was completed without business disruption * Achieved - Implemented security measures were developed to best practice * Achieved - Implemented security controls have enhanced data CIA * Achieved - Testing and Red Team / Blue Team exercises demonstrated Incident response effectiveness. |
| **PROJECT DELIVERABLES** |  |
| The project has the following key outcomes:   * Produce a comprehensive report of the existing local infrastructure. * Produce documentation that outlines the cloud infrastructure security * Configure and secure the cloud environment * Produce documentation that details the implemented security controls and measures. * Safely and securely migrate the services from the existing infrastructure, to the cloud system * Test reports detailing red-blue team simulated exercises, testing the security of the cloud environment * Implement Incident Response Plans (runbooks) and monitoring systems * Produce detailed training materials on security awareness | * Completed - Produce a comprehensive report of the existing local infrastructure. * Completed - Produce documentation that outlines the cloud infrastructure security * Completed - Configure and secure the cloud environment * Completed - Produce documentation that details the implemented security controls and measures. * Completed - Safely and securely migrate the services from the existing infrastructure, to the cloud system * Completed - Test reports detailing red-blue team simulated exercises, testing the security of the cloud environment * Completed - Implement Incident Response Plans (runbooks) and monitoring systems * Completed - detailed the training materials on provided |
| **PROJECT SCHEDULE** |  |
| **High Level Timeline**: | |
| The project was planned to be delivered in three x 2 week sprints broken into:   * Planning sprint * Implementation sprint * Testing and documentation sprint   **Summary of performance against schedule:**  **Sprint One:**  Sprint one was achieved in two week and went exactly to plan with all documentation completed within the time period.  **Sprint Two:**  The project deviated from plan slightly in sprint two. Although a number of activities were completed earlier than plan, some sprint three activities were also brought forward. We also ran tasks concurrently from sprint two.  **Sprint Three:**  Sprint three was completed earlier as some documentation tasks were completed in parallel with the development. The presentation took longer than expected. A number of changes were required as more clarity was provided on scope. The Red/Blue team exercise was completed part way through Sprint three and the documentation was completed at the same time. | |
| Detailed of planned schedule: | Below is a snapshot of the completed project schedule: |
| **PROJECT BUDGET** |  |
| Overview of planned budget:  The total expected budget was mainly based on time and was $35,250 | Summary of executed budget:  The final cost for the project was $40,650, an overspend of $5,400. Sprint two was the main area of overspend and this exceeded the budget by $7,500.  The main reason for the over spend was the additional time taken to implement the Onedrive automated backup and recovery solution and the implementation of MFA. |

|  |
| --- |
| TEAM PERFORMANCE |

|  |  |
| --- | --- |
| OVERALL PROJECT TEAM PERFORMANCE | The team performed very well and was able to deliver the project on time and with additional scope items.  All project goals were achieved and successfully tested. The team was met with a number of complex implementations including  An additional challenge was with the capacity / storage of the test environments. A new environment was required to be established and the Project Manager led this work.  A very successful project where the team contributed to the overall solution.  One specific team member should be recognized for their achievements - The team's Project Manager Giuseppe Raciti, played a pivotal role within the team. Not only was he the project manager but lead the design and implemented some of the more complicated implementations. |
| **Project Manager:** Giuseppe Raciti (Pep) | Giuseppe displayed a leadership style that inspired his team members to perform to the best of their ability.  Taking the responsibility of creating the document templates required for the team to document the project from beginning to end, and reviewing each document upon its completion, ensure that all the requirements were met by each team member.  Giuseppe was essential in the construction of the red/blue team environment, allowing each team member to perform their designated attack. Each team member was able to simulate a real-world attack, utilizing the talent of the cyber team.  Giuseppe was able to efficiently communicate the expectations of the sponsor, and the requirements of the project, such as the project schedule, budget, mitigation, and migration to the cloud environment.  Giuseppe personally oversaw the acquisition of new technology and equipment required for the smooth and secure migration from the local and obsolete infrastructure to the cloud-based environment.  Giuseppe and his team were able to migrate the e-commerce system of OzCazual to the cloud environment, with no interruption to the customers and clients of OzCazual. |
| **Cyber Security Specialist:** Shaun Heywood | Shaun provided a supporting hand to his fellow team members within the project wherever required.  Shaun also took ownership of the implementation of the antivirus / malware EDR. Sophos Endpoint Security and Control was successfully implemented into the Windows and Linux systems, configured, tested, and formed part of the red / blue team functional exercise.  Shaun provided documentation, reporting and presentation development.  Shaun also led the red team exercise for the antivirus / malware simulation, utilising a phishing attack from a threat actor containing a malicious payload. |
| **Cloud Architect / Engineer:** Mark Byrne | Mark provided a supporting hand to Pep within the project management duties and assisted with scheduling, WBS creation and budgeting.  Mark also took ownership of the implementation of the traffic monitors (Wireshark) for Linux and Windows and the IDS (Snort) for Windows.  Mark also supported performance reporting and presentation development.  Mark also led the red team exercise for the Brute Force attack. |
| **Server Administrator:** Mauricio Guerra | Mauricio G. Guerra has demonstrated support in server administration. He was able to implement Sophos XG Firewall and Splunk enterprise, enhanced network security and data monitoring capabilities.  Mauricio led the Red Team exercise for Dos Attack to Linux Web Server |

|  |
| --- |
| KEY LESSONS LEARNT |

|  |  |
| --- | --- |
| PROJECT SCOPE | The importance of research and knowledge acquisition was highlighted throughout the project. The team realized that in-depth research into cloud infrastructure best practices, security measures, and compliance regulations is essential for making informed decisions. This knowledge serves as a foundation for implementing robust security controls and ensuring compliance with relevant standards. Investing time in thorough research and staying up to date with the latest industry trends can significantly enhance project outcomes.  The project also highlighted the significance of adaptability and flexibility in project management. The ability to respond to changing requirements and unforeseen challenges is crucial. Agile project management methodologies proved effective in managing changes and ensuring project success. Regularly evaluating project performance, identifying lessons learned, and implementing improvements are also vital for ongoing growth and success. Reflecting on the project's successes and challenges provides valuable insights for continuous improvement and organizational growth |
| PROJECT RESOURCES | Three types of resources were used throughout the project.   1. People 2. Process 3. Systems   The team performed exceptionally well and worked consistently and collaborated well. This was supported by WhatsApp messaging apps and Google Drive for documentation collaboration  Once a week the team held check-in meetings and this helped gain shared understanding of areas of risk and timeline slippage.  The Azure Lab was one area that failed the team as the resources allocated to this were below the required resources of the project. This was identified early and the team pivoted to a VM box environment hosted by Giuseppe Raciti. |
| PROJECT SCHEDULE | The schedule was broken into three sprints and this was appropriate for the phases of the project.  The team had to work consistently for each sprint and some team members were required to work some very long hours to achieve the work.  Despite being able to achieve the project in three sprints, the key lesson would be to include an additional sprint for supporting systems such as MFA and Backups. This would have provided more reasonable allocation of tasks and reduced the stress on team members to deliver additional scope within a capacity constrained time frame. |
| PROJECT BUDGET | There was a significant overspend on the budget. As many of the solutions had not been implemented before, it was unclear during planning how much time and the level of complexity that was involved in implementing them.  These included MFA, Onedrive backup and Sophos. We also didn’t anticipate the Azure lab to run out of storage and the need to shift from this environment to Pep’s VM environments also took time and hence budget.  Key lessons would be to include additional contingency for untested systems or complete an initial design spike before starting the project to assess the size of the tasks. |
| RISK MANAGEMENT | The following are the important risk management lessons learned during the project:  **Thorough Risk Assessment**: It was critical to conduct a thorough risk assessment in order to identify potential threats and vulnerabilities. The assessment formed the basis for designing a risk management strategy and enabled preventative measures to be implemented.  **Clear Project Planning and Communication**: It was critical to develop a complete project plan with defined objectives, timelines, and resource allocation. Establishing regular communication channels with key stakeholders ensured that everyone was kept up to date on the project's development and allowed for conversations about risk mitigation strategies.  **Robust architecture Design and Testing**: Because the initial system architecture was inadequate, it was critical to redesign the network infrastructure to be robust and scalable. Implementing redundancy and failover measures, as well as thorough testing and validation prior to the migration, helped assure the new infrastructure's effectiveness and flexibility.  **Multi-Layer Security Controls**: It was critical to implement a multi-layered approach to security. Deploying industry-standard security controls including firewalls, intrusion detection/prevention systems, and multifactor authentication with Active Directory (AD) provides critical protection against a variety of threats and vulnerabilities.  **Continuous Risk Monitoring and Assessment**: To discover and respond to security problems quickly, ongoing risk monitoring, including logging and monitoring techniques, was essential. Regular security audits and assessments also ensured that the security measures in place remain effective.  **Simulation Exercises**: Conducting red team/blue team exercises to replicate real-world attacks proved to be a valuable exercise in evaluating the efficiency of the implemented security measures and incident response capabilities. The lessons learned from these exercises informed us of any changes or enhancements that need to be made to the security infrastructure.  **Comprehensive Documentation**: Preparing and maintaining detailed technical documentation is critical for future reference, maintenance, and troubleshooting. All network architecture information, security controls, and configurations were provided in this documentation.  By applying these key lessons, OzCasual can enhance their risk management practices and effectively mitigate potential risks, ensuring the security and integrity of their systems and data |

|  |
| --- |
| PROJECT ARCHIVE |

|  |
| --- |
| **RECORDS AND CORRESPONDENCE** |
| All key documentation has been archived in the SecureNET Project Management Office (PMO) project archive folders and also provided to OzCasual Project Management Office and stored on OneDrive. To access these please contact the OzCasual PMO office |

|  |  |  |
| --- | --- | --- |
| PREPARED BY | TITLE | DATE |
| Giuseppe Raciti | Project Manager | 13/07/2023 |