SECURING AZUMER WATER’S DISASTER RELIEF OPERATIONS – FINAL REPORT

Quinton G. Green – IT Capstone Task 3 – Final Report

Date of Submission: May 12, 2025

Securing Azumer Water’s Disaster Relief Operations: A Comprehensive, Multi-Layered Cybersecurity Implementation and IT Infrastructure Enhancement Plan for Resilience Against Social Engineering, Data Loss, and Network Intrusion

Quinton G. Green

Western Governors University

**Table of Contents**

[Proposal Overview 3](#_Toc174618293)

[Problem Summary 3](#_Toc174618294)

[IT Solution 4](#_Toc174618295)

[Implementation Plan 5](#_Toc174618296)

[Review of Other Work 9](#_Toc174618297)

[Summary of Four Works 9](#_Toc174618298)

[Relation of Works to Proposal Design 9](#_Toc174618299)

[Project Rationale 11](#_Toc174618300)

[Current Project Environment 12](#_Toc174618301)

[Methodology 13](#_Toc174618302)

[Project Goals, Objectives, and Deliverables 14](#_Toc174618303)

[Goals, Objectives, and Deliverables Descriptions 14](#_Toc174618304)

[Goals, Objectives, and Deliverables Table 16](#_Toc174618305)

[Project Timeline with Milestones 17](#_Toc174618306)

[Outcome 18](#_Toc174618307)

[References 21](#_Toc174618308)

**Proposal Overview**

**Problem Summary- A.1**

Azumer Water, a FEMA-partnered nonprofit focused on disaster relief, relies on a centralized database of 1,073 volunteers to coordinate the delivery of bottled water to crisis-affected communities. Recently, the organization suffered a cybersecurity incident after a spear-phishing campaign exploited a lack of staff and volunteer security awareness. The attack resulted in unauthorized access and theft of the volunteer database, which contained sensitive personal and background information, including partial Social Security numbers. The incident highlighted serious deficiencies in Azumer’s IT infrastructure: there was no reliable data backup. The database resided solely on an unprotected local machine with ad hoc USB copies; the organization’s wireless network still used deprecated WEP encryption; and the firewall remained improperly configured.

Furthermore, staff and volunteers have not been trained in recognizing phishing or social engineering attempts. Collectively, these issues present a high risk of data loss and confidentiality, network intrusion, and operational disruption. The project will address these critical gaps by implementing a multi-layered cybersecurity strategy that enhances IT infrastructure, strengthens user awareness, and establishes resilient, standard-aligned security policies and procedures to protect Azumer Water’s mission-critical operations.

**IT Solution- A.2**

The proposed solution is a multi-layered cybersecurity enhancement integrating technology, policy, and training. It will introduce a Comprehensive Cybersecurity Program that includes (1) stronger technical controls (properly configured firewall, secure Wi-Fi, encryption, intrusion detection, backup systems), (2) updated policies and procedures (password policies, access controls, incident response plan, continuous monitoring), and (3) security awareness training (phishing simulations, annual training for staff and volunteers). This approach aligns with industry’s best practices such as the NIST Cybersecurity Framework, which emphasizes continuous risk management and protection of confidentiality, integrity, and availability (CIA) for any sized organization.

By combining preventative controls (firewall, password multifactor authentication, software patching), detective measures (monitoring, Intrusion detection system logs), and corrective plans (disaster recovery, incident response plan), the solution directly addresses the identified risks. For example, security awareness training will mitigate social engineering (phishing) attacks, encrypted offsite backups will prevent total data loss, and network hardening will combat intrusions from attackers. The solution prepares the organization to respond to future threats.

**Implementation Plan- A.3**

**Phase 1: Policy Development & Training Prep**

**Goal:** Develop foundational policies and prepare staff awareness program.

|  |  |
| --- | --- |
| **Action** | **Responsible Party** |
| Draft new policies (password, acceptable use, incident response, access control) | **Cybersecurity Manager** |
| Review and approve policies | **Executive Director**, **Legal Advisor** |
| Develop training content and phishing templates | **Cybersecurity Manager** & **Training Coordinator** |
| Translate training materials into plain language for volunteers | **Communications Director** |
| Schedule initial training sessions | **HR Manager** & **Volunteer Coordinator** |

**Phase 2: Infrastructure Implementation**

**Goal:** Deploy technical defenses and security architecture upgrades.

|  |  |
| --- | --- |
| **Action** | **Responsible Party** |
| Replace WEP with WPA3 and segment networks (guest, admin, volunteer) | **Network Engineer** |
| Reconfigure enterprise firewall with deny-by-default rules and logging | **Systems Administrator** |
| Deploy backup solution (Ex., cloud + local + offsite drive) | **Database Administrator** & **IT Support Specialist** |
| Enable and enforce MFA for admin and remote access accounts | **Systems Administrator** |
| Document all configurations for audit and handoff | **Cybersecurity Manager** |

**Phase 3: Training, Testing, and Simulation**

**Goal:** Validate system integrity, raise awareness, and measure preparedness.

|  |  |
| --- | --- |
| **Action** | **Responsible Party** |
| Launch phishing simulation campaign and track click-throughs | **Cybersecurity Manager** |
| Conduct volunteer and staff training sessions | **Training Coordinator** |
| Perform backup restoration drills | **Database Administrator** |
| Test firewall configurations with vulnerability scanner | **Cybersecurity Analyst** |
| Simulate incident response tabletop exercise | **IT Team**, **Executive Director**, **Communications Director**, **HR**, **Volunteer Coordinator** |

**Phase 4: Handoff, Monitoring, and Continuous Improvement**

**Goal:** Institutionalize improvements and prepare for long-term sustainability.

|  |  |
| --- | --- |
| **Action** | **Responsible Party** |
| Finalize and distribute updated IT Security Manual | **Cybersecurity Manager** |
| Establish routine log monitoring and reporting (SIEM or centralized logging) | **Systems Administrator** |
| Schedule quarterly phishing and DR drills | **Cybersecurity Manager** & **Training Coordinator** |
| Conduct project closeout meeting with stakeholders | **Executive Director**, **IT Team**, **Cybersecurity Manager** |

**Implementation Plan continued- A.3a.**

The implementation plan is appropriate for the proposed IT solution because it applies a comprehensive, phased, and risk-based approach that directly addresses Azumer Water's critical vulnerabilities while aligning with its organizational structure, mission-critical needs, and limited technical resources as a small nonprofit. (Ferry, 2024)

The plan is organized into distinct phases that mirror industry-standard methodologies. The risk assessment has already been completed where vulnerabilities like phishing, insecure network protocols like deprecated WEP encryption, ensure firewall configurations, and lack of data backups were identified. The phases move through design, implementation, testing, and evaluation to protect critical IT systems and PII data. The phases are structured, evaluated, and integrated to ensure critical business functions are not disrupted, allowing disaster relief functions to continue with no interruption.

The most critical vulnerabilities are addressed first to mitigate immediate threats of data loss and social engineering by aligning the organization to essential frameworks (NIST SP 800-53, the NIST Cybersecurity Framework, and the FISMA requirements) (NIST, 2010) and principles like the 3-2-1 backup rule (Hooper, 2022). The plan emphasizes the transition from WEP to WPA3, regular backup protocols, and a structured incident response strategy that incorporates phishing simulations and automated alerting.

These measures are tailored to Azumer Water’s current threat landscape, ensuring that both technical and human vulnerabilities are addressed. The plan not only upgrades hardware and software infrastructure but also integrates targeted security awareness training for both staff and volunteers. By simulating phishing attacks and social engineering scenarios, the plan builds a culture of vigilance, ensuring that employees and volunteers can actively recognize and report suspicious activities to address the human component in cyber-attacks. By assigning tasks responsibility to different key roles, the plan enforces accountability, governance, and infrastructure management efficiently and effectively.

This implementation plan is designed for a continuous process of enforcing policy updates, comprehensive documentation records, regular testing and evaluation, continuous monitoring, and ongoing risk mitigation. This develops resiliency within Azumer’s IT infrastructure and enforces meeting regulatory compliance standards for continuous improvement and asset protection. (NIST, 2020)

**Review of Other Work**

**Summary of Four Works – B.**

**1.Nonprofit Cybersecurity Best Practices:** *Nonprofit Cybersecurity: Protect Volunteer Data.”* Galaxy Digital Annelise Ferry (2024) emphasizes that “nonprofits are particularly vulnerable to cybercriminals” and often lack readiness for breaches ([galaxydigital.com](https://www.galaxydigital.com/blog/nonprofit-cybersecurity#:~:text=Nonprofits%20are%20particularly%20vulnerable%20to,deal%20with%20breaches%20in%20cybersecurity)). Her work outlines steps like enabling multifactor authentication and conducting phishing training, noting 93% of incidents result from phishing and 60% of nonprofits lack training ([galaxydigital.com](https://www.galaxydigital.com/blog/nonprofit-cybersecurity#:~:text=3,Has%20Received%20Phishing%20Prevention%20Training)).

**2. Backup and Recovery Guidelines:** Hooper, A. *“Data Backup Best Practices for Nonprofits.* TechSoup (2022) recommends the 3-2-1 backup rule (three copies, two media, one offsite) as an industry standard ([blog.techsoup.org](https://blog.techsoup.org/posts/data-backup-best-practices-for-nonprofits#:~:text=Creating%20backups%20is%20a%20strategic,a%20good%20measure%20to%20take)). It stresses frequent backups, as many organizations “find that their most recent backup was weeks or even months ago” when an attack strikes ([blog.techsoup.org](https://blog.techsoup.org/posts/data-backup-best-practices-for-nonprofits#:~:text=One%20of%20the%20most%20important,ability%20to%20serve%20your%20community)).

*3.***Title*:* “Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) – NIST SP 800-122**” This work details best practices for safeguarding PII, offering recommendations that are integral to our backup and data protection strategies for sensitive volunteer information (NIST, 2010)

*4.***Title:** **National Institute of Standards and Technology. (2020). *Security and Privacy Controls for Federal Information Systems and Organizations (NIST SP 800-53 Rev. 5)*. U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-53r5**

This publication provides a comprehensive set of security controls that are critical for ensuring the confidentiality, integrity, and availability (CIA) of IT systems. Its guidelines directly inform the security hardening and regulatory compliance aspects of this project (NIST, 2020)

**Relation of Works to Proposal Design- B.1**

**1.Nonprofit Cybersecurity Best Practices: “*Nonprofit Cybersecurity: Protect Volunteer Data.”*** Galaxy Digital Annelise Ferry (2024) - This supports the need for Azumer’s staff training and MFA solution being a critical design component in this project.

**2. Backup and Recovery Guidelines: Hooper, A. *“Data Backup Best Practices for Nonprofits.* TechSoup (2022)**)- This reinforces our plan for robust, frequent backups and geographically separated storage as a design component in this project.

3. **“Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) – NIST SP 800-122 -** This work details best practices for safeguarding PII, offering recommendations that are integral to our backup and data protection strategies for sensitive volunteer information

*4.* **“NIST SP 800-53: Security and Privacy Controls for Federal Information Systems and Organizations -** Its guidelines directly inform the security hardening and regulatory compliance aspects of this project.

**Project Rationale- C.**

Azumer Water’s current IT environment is insecure. Critical assets (email, web, volunteer database) run on open-source servers in the main office, with an improperly configured firewall. The wireless network uses obsolete WEP encryption, exposing all traffic to eavesdropping. Employees casually copy data to USB drives, risking data leakage. Passwords are never forced to expire, and no formal security incidents have yet prompted action. The staff has no security training and little formal policy enforcement which poses a significant risk to its disaster relief operations and volunteer data. This context (limited budget NGO, reliance on volunteers, mission-driven urgency) means the solution must be cost-effective and easy to adopt.

Nevertheless, the environment’s vulnerabilities are severe: a single phishing click already enabled an attacker to steal the entire database. The project must therefore establish a secure baseline environment quickly (better network configuration, backup system, policy enforcement) while acknowledging that Azumer’s mission requires high availability and trust in relief efforts. Given the increased targeting of nonprofit organizations by cyber attackers and hacktivist groups, it is imperative to establish a proactive cybersecurity strategy. Implementing a layered security framework not only protects sensitive information but also ensures the continued operational integrity of the organization**.**

**Current Project Environment- D.**

Azumer Water operates within a complex environment characterized by:

* **Outdated IT Infrastructure**: The organization’s web, email, and database servers run on open-source platforms with deferred security configurations.
* **Insecure Network Practices**: Use of the WEP wireless protocol and poorly configured firewalls increase vulnerability.
* **Limited Security Awareness**: Both full-time employees and volunteers lack formal training in identifying phishing and social engineering attacks.
* **Inadequate Data Protection**: The absence of scheduled backups and reliance on insecure USB transfers exposes critical volunteer data to theft and loss.

These environmental factors create an urgent need for enhanced IT security measures to safeguard ongoing disaster relief operations.

**Methodology -E.**

The project will follow a risk-based, Systems- Development Life Cycle (SDLC) methodology. Initially, a risk assessment (informed by NIST and nonprofit guides) will prioritize threats (phishing, ransomware, data theft) and asset criticality (volunteer database, communications). We will use an iterative approach: implement high-priority controls first (ex: firewall configuration, backups, MFA) to mitigate urgent risks, then proceed to secondary measures (Ex: full vulnerability assessment, continuous monitoring tools). The methodology is semi-waterfall with defined phases, but each phase includes feedback loops: after implementing controls, we will test their effectiveness (Ex: simulate phishing, test restore from backups) and refine the plan. And finally, in the maintenance phase setting up ongoing review processes and remediation procedures to ensure sustained security posture. Project management best practices will guide scope management, stakeholder communication (coordination with Azumer’s CEO and FEMA), The methodology will ensure that each phase is documented, measured, and aligned with industry’s best practices and regulatory standards.

**Project Goals, Objectives, and Deliverables- F.**

**Goals, Objectives, and Deliverables Descriptions**

The proposed cybersecurity implementation project for Azumer Water is structured around four key goals, each with specific objectives and tangible deliverables.

**Goal 1: Strengthen Security Awareness Among Staff and Volunteers**

* **Objective 1.1:** Develop and deliver cybersecurity training focused on phishing, password hygiene, and data protection.
  + **Deliverables:** Training presentation, instructional videos, training attendance logs.
* **Objective 1.2:** Conduct routine phishing simulation campaigns to evaluate awareness.
  + **Deliverables:** Phishing test reports, user performance metrics, follow-up training materials.

**Goal 2: Protect the Confidentiality and Availability of Volunteer Data**

* **Objective 2.1:** Implement 3-2-1 backup strategy with encryption and offsite/cloud storage.
  + **Deliverables:** Configured backup software, documented backup schedule, restoration test logs.
* **Objective 2.2:** Encrypt the volunteer database and all communication channels.
  + **Deliverables:** Encryption configuration reports, policy for encryption management.

**Goal 3: Fortify Network Infrastructure**

* **Objective 3.1:** Configure the enterprise firewall with deny-by-default rules and real-time monitoring.
  + **Deliverables:** Firewall rule set documentation, system logs, access control policy.
* **Objective 3.2:** Upgrade the wireless network from WEP to WPA3 and segment traffic into guest, admin, and volunteer VLANs.
  + **Deliverables:** Network configuration documentation, segmentation diagram, WPA3 deployment report.

**Goal 4: Establish Incident Response and Continuous Monitoring Framework**

* **Objective 4.1:** Develop and test an Incident Response Plan (IRP) through simulations.
  + **Deliverables:** Final IRP document, tabletop exercise report.
* **Objective 4.2:** Implement SIEM or centralized logging for continuous monitoring.
  + **Deliverables:** Monitoring tool configuration logs, quarterly audit schedule, log retention policy.

Together, these goals form a comprehensive and realistic roadmap that addresses the most pressing cybersecurity risks identified in the Azumer Water case study, ensuring both short-term mitigation and long-term resilience.

**Goals, Objectives, and Deliverables Table**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Goal** | **Supporting Objectives** | **Deliverables Enabling the Project Objectives** |
| 1 | Strengthen Security Awareness | 1.1 Develop and conduct security training for staff/volunteers. | 1.1. Training curriculum and materials |
| 1.2 Perform routine phishing simulations. | 1.2. phishing simulation results and reports; |
| 1.2. updated security policy enforcing training |
| 2 | Protect Data Confidentiality and Availability | 2.1 Implement 3-2-1 backup strategy with offsite encrypted copies. | 2.1. Deployed backup solution (e.g., automated cloud backups, external drives) |
| 2.1. backup schedule and restoration test results |
| 2.2 Encrypt database and communications | 2.2. encryption policy and configuration documentation. |
| 3 | Fortify Network Infrastructure | 3.1 Configure and enable the enterprise firewall | 3.1. Firewall configuration logs and ruleset; system log set up |
| 3.2 Upgrade wireless (WEP→WPA3) and segment networks. | 3.2. new wireless AP setup with WPA3 |
| 3.2. network segmentation diagram |
| 3.3 Deploy IDS/monitoring |  |
| 3.3. IDS/monitoring system set-up documentation. |
| 4 | Establish Incident Response and Continuous Monitoring | 4.1 Develop and test an Incident Response Plan | 4.1. Incident Response Plan document  4.1.2. IR tabletop report with test results and participant feedback; |
|  |  | 4.2 Implement continuous security monitoring (SIEM/logging) | 4.2. SIEM setup logs, monitoring schedule, audit checklist |

**Project Timeline with Milestones- G.**

|  |  |  |  |
| --- | --- | --- | --- |
| **Milestone** | **Duration**  **(hours or days)** | **Projected Start Date** | **Anticipated End Date** |
| Approved security policies; finalized implementation timeline and task assignments | 3 weeks | June 2, 2025 | June 20, 2025 |
| Security training curriculum and phishing simulation scenarios completed | 4 weeks | June 23, 2025 | July 18, 2025 |
| Firewall configured; WPA3 deployed; segmented wireless implemented; backup system operational | 6 weeks | July 21, 2025 | August 29, 2025 |
| Staff/volunteer training completed; first phishing simulation conducted and documented | 3 weeks | September 2, 2025 | September 20, 2025 |
| Incident Response Plan tested; monitoring/logging tools deployed and reviewed | 3 weeks | September 23, 2025 | October 11, 2025 |
| Final project documentation delivered; stakeholder presentation completed | 4 weeks | October 14, 2025 | November 8, 2025 |

**Outcome- H.**

The successful implementation of this project will result in a significantly improved cybersecurity posture for Azumer Water, characterized by a fortified IT infrastructure, robust incident response and disaster recovery capabilities, enhanced organizational preparedness through targeted security awareness training, and demonstrable regulatory compliance. Specifically, upon completion:

* **Fortified IT Infrastructure:**
  + The volunteer database will be secured using encryption, regular automated backups, and strict access controls.
  + The network will be hardened with improved wireless security (transition from WEP to WPA3) and properly configured firewall settings, deterring unauthorized access and intrusions.
* **Incident Response and Disaster Recovery:**
  + The organization will have an established, tested incident response plan and continuous monitoring capability that enables rapid containment of cyberattacks.
  + Real-time threat detection and automated alerting will close the “reactive” gap currently present.
* **Enhanced Security Awareness and Preparedness:**
  + Employees and volunteers will participate in tailored security awareness training, including phishing simulations, which will improve their ability to recognize and report social engineering attempts.
  + The introduction of multi-factor authentication (MFA) and updated password policies will further reduce the risk of unauthorized access.
* **Regulatory Compliance and Justified Investment:**
  + All implemented controls will align with FISMA, NIST SP 800-53, and NIST SP 800-122 standards, ensuring regulatory compliance.
  + The project will produce a detailed IT proposal, including a cost–benefit analysis, which justifies the investment in a modernized, resilient IT architecture tailored for disaster relief operations.

**Criteria for Success**

Success will be measured using the following criteria:

* **Infrastructure Security Metrics:**
  + Reduction in the number of vulnerabilities identified in periodic network scans.
  + Demonstrable improvements in backup integrity, with regular, successful backup logs in alignment with the 3-2-1 backup rule.
* **Incident Response Efficacy:**
  + Reduced incident response and recovery times, validated through simulated cyberattack drills.
  + Successful execution of real-time monitoring and automated alerting, with incident logs demonstrating immediate detection and containment.
* **Training and Awareness Outcomes:**
  + Increased staff and volunteer proficiency, measured by pre- and post-training assessments and simulation reports (e.g., a reduction in successful phishing attempts during simulations).
  + Positive user feedback collected through surveys on training effectiveness.
* **Compliance Verification:**
  + Achievement of audit results that confirm adherence to FISMA, NIST SP 800-53, and NIST SP 800-122 requirements.
  + Documented evidence of security policy enforcement and procedural improvements.
* **Overall Program Management:**
  + Adherence to the project timeline and milestones.
  + Achievement of predefined deliverables outlined in the IT proposal, ensuring that technical solutions are fully implemented without disrupting Azumer Water’s disaster-relief operations.

**Data Collection Methods**

Data necessary to evaluate these outcomes will be collected through:

* **Automated Monitoring Tools:**
  + Logs from network monitoring systems, intrusion detection systems (IDS), and backup systems will provide quantitative data on vulnerabilities, incident response times, and system uptime.
* **Simulation and Drill Testing:**
  + Periodic phishing simulations, incident response drills, and vulnerability assessments will generate performance data for analysis.
* **Employee and Volunteer Surveys:**
  + Pre- and post-training surveys and feedback forms will assess improvements in security awareness and the effectiveness of training modules.
* **Audit Reports and Compliance Checks:**
  + Regular internal and external audits will verify documentation of compliance with FISMA and NIST guidelines, providing both qualitative and quantitative measures of regulatory adherence.
* **Project Management Tools:**
  + Tracking tools (such as Gantt charts and milestone reports) will be used to monitor adherence to the project timeline and deliverable completion.

**Data Measurement**

Data will be measured using clearly defined quantitative and qualitative metrics:

* **Quantitative Metrics:**
  + Percentage reduction in identified vulnerabilities (as seen in vulnerability scan reports).
  + Average incident response times and recovery durations (measured during simulated drills).
  + Backup success rate (measured via backup logs and recovery tests).
  + Percentage of staff and volunteers passing security training assessments.
  + Compliance scores resulting from audit checks expressed as a percentage adherence to defined standards.
* **Qualitative Metrics:**
  + User satisfaction ratings from training surveys.
  + Auditor observations and feedback regarding the efficacy of newly implemented policies and infrastructure changes.
  + Stakeholder feedback on the improvement in operational resilience and the quality of documentation within the IT proposal.

Through these data collection and measurement techniques, the project’s success will be reliably monitored and evaluated, ensuring that Azumer Water’s IT infrastructure is not only secured against current threats but remains resilient and compliant in the long term.

**References**

* National Institute of Standards and Technology. (2020). *Security and Privacy Controls for Federal Information Systems and Organizations (NIST SP 800-53 Rev. 5)*. U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-53r5
* National Institute of Standards and Technology. (2010). *Guide to Protecting the Confidentiality of Personally Identifiable Information (NIST SP 800-122)*. U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-122
* Ferry, A. *“Nonprofit Cybersecurity: Protect Volunteer Data.”* Galaxy Digital (2024) [galaxydigital.com](https://www.galaxydigital.com/blog/nonprofit-cybersecurity#:~:text=3,Has%20Received%20Phishing%20Prevention%20Training)[galaxydigital.com](https://www.galaxydigital.com/blog/nonprofit-cybersecurity#:~:text=Nonprofits%20are%20particularly%20vulnerable%20to,deal%20with%20breaches%20in%20cybersecurity).
* Hooper, A. *“Data Backup Best Practices for Nonprofits.”* TechSoup (2022) [blog.techsoup.org](https://blog.techsoup.org/posts/data-backup-best-practices-for-nonprofits#:~:text=Creating%20backups%20is%20a%20strategic,a%20good%20measure%20to%20take)[blog.techsoup.org](https://blog.techsoup.org/posts/data-backup-best-practices-for-nonprofits#:~:text=One%20of%20the%20most%20important,ability%20to%20serve%20your%20community)