Qualicart

Team XYZ

By: Hector, Steven, Tristan, Eric, Jay, Cassandra

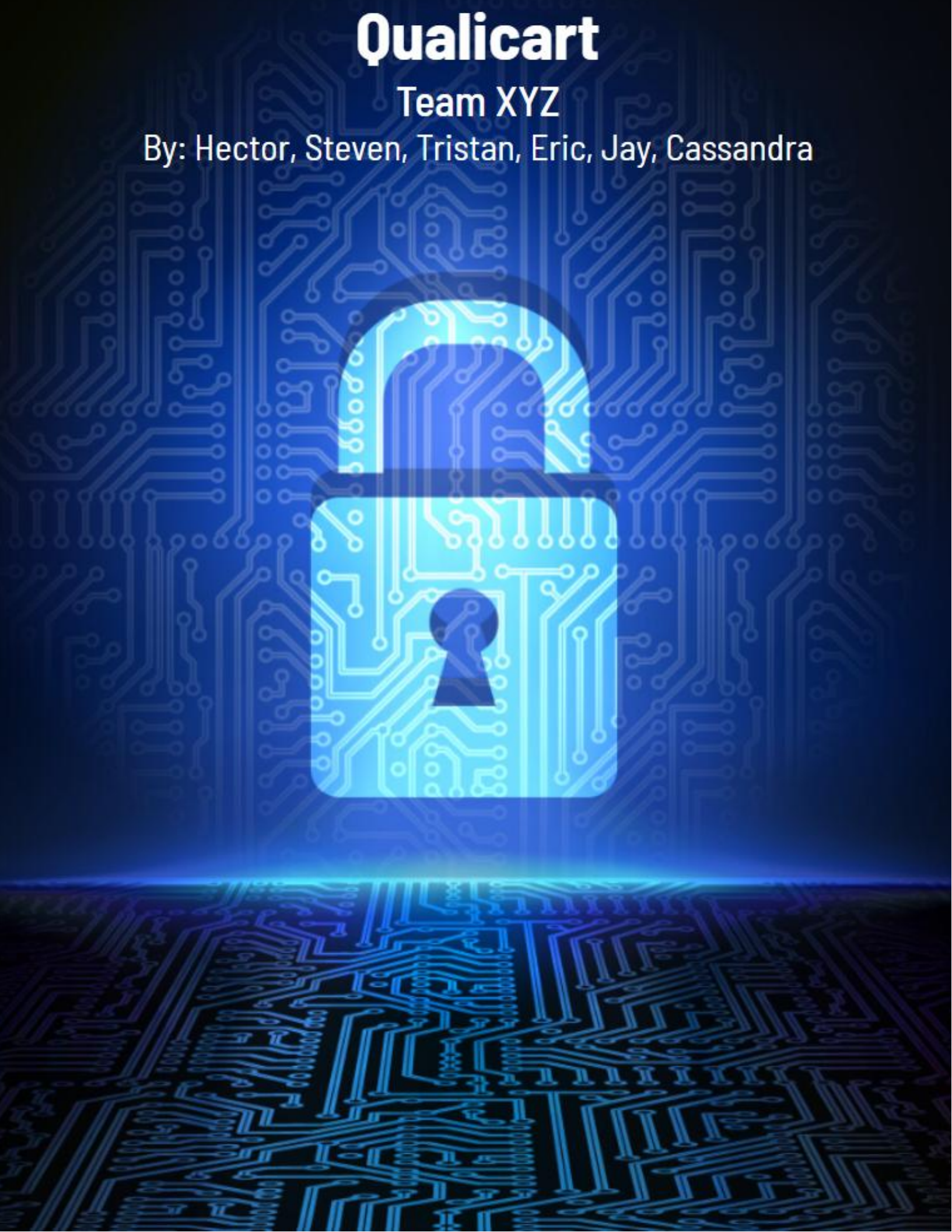


Table of Contents

1. Executive Summary

1.1 Purpose:

Qualicart Corporation, an emerging leader in global e-commerce and supply chain solutions, is preparing for the launch of its Qualicart app. This launch introduces significant cybersecurity challenges that require a risk assessment and a strategic cybersecurity roadmap to ensure the protection of digital assets, customer data, and business operations. By implementing this structured cybersecurity plan, Qualicart can enhance trust, protect critical assets, and ensure the secure operation of its digital ecosystem.

The purpose of this Cybersecurity Incident Response Plan (CIRP) is to outline and establish a set of procedures for identifying, responding to, and recovering from any cybersecurity incidents in a timely and efficient manner. It outlines who direct contacts to go to and offers an attentive team with someone available at all times. Although a cybersecurity plan with many security features is crucial for cybersecurity, cyber threats and incidents remain a consistent risk that always has to be monitored. This Incident Response Plan is incredibly important for Qualicart Corporation to ensure minimal damage, protected sensitive information, and restored normal operations as soon as possible. These are key and imperative parts to the success of any corporation's cybersecurity.

1.2 Framework Scope:

This plan applies to all employees, contractors, and third-party vendors who interact with the organization's IT infrastructure, including hardware, software, and data. Each party has a responsibility to keep private and confidential data secure and should report any scams or evidence of cyber threats and incidents.

1.3 Objective:

Qualicart must make cybersecurity be of utmost importance. Qualicart needs to focus on many cybersecurity challenges including application security, encryption, up-to-date software, access controls, threat monitoring, and risks from third parties. They must also ensure a proper incident response plan in the case of cyber threats and incidents. There are constant cyber threats that Qualicart may face. Some include phishing and social engineering attacks, ransomware attacks, supply chain attacks, data breaches, and distributed denial of service attacks. These threats put both Qualicart and Qualicart's stakeholders at risk; therefore, they

must be carefully and strategically monitored for and prevented. If these are not properly addressed, businesses will be vulnerable to threats, which can lead to financial loss, damage to reputation, and legal consequences.

Team XYZ promises to detect any security incidents early and rapidly inform Qualicart and any additional stakeholders. A quick response will be administered with techniques to contain the incident, preventing additional damage. Team XYZ will work with Qualicart to minimize the impact of the incident on business operations and on sensitive data, recover the systems that have been affected, and strengthen the area of the breach. Formal documentation will be created as an incident report and to record the way the incident was addressed and lessons that were learned to better adapt to new challenges in the future while still suiting Qualicart's app infrastructure.

1.4 Risk Assessment:

If risks and vulnerabilities are not addressed, they can cost Qualicart upwards to $10,600,000.00 or more. It is important to address them on the timeline that Team XYZ has created for Qualicart to prevent risks taking place and damaging the company, its reputation, its finances, or its stakeholders.

1.5 Business Impact:

Working with Team XYZ, Qualicart will benefit from one-of-a-kind security efforts and protection. Team XYZ offers a solution that will enhance Qualicart's security position through proactive efforts, continuous monitoring, and constant improvement to encapsulate the increasing demands of cybersecurity. This focus on cybersecurity will reduce any damage to Qualicart at the company and stakeholder level. Team XYZ has created a strong response plan for immediate reactions to risks with the least amount of damage possible. Team XYZ will diligently make sure to offer these solutions within regulation compliance and the highest standard of work. This security leverage will allow Qualicart to continue to focus on other core aspects of its business.

1.6 Conclusion:

Cybersecurity is a huge part of the success of a business. Team XYZ urges Qualicart to address any cybersecurity risks that Team XYZ has identified and to work with them to implement a comprehensive solution that ensures the security of Qualicart.

2. Incident Response Team (IRT)

2.1 Roles and Responsibilities:

- **Incident Response Manager (IRM):** Hector Mayolet
  - Coordinates overall response efforts.
  - Communicates with senior management.
  - Ensures legal and regulatory compliance.

- **Technical Response Team (TRT**): Jay Goodman, Steven Luu
  - Identifies and assesses the technical nature of the incident.
  - Provides support in containment, eradication, and recovery.
  - Works closely with the IRM and forensic experts.

- **Forensics and Analysis Team:** Jay Goodman, Eric Huang
  - Investigates and analyzes the root cause and scope of the incident.
  - Preserves evidence for possible legal actions.

- **Communication Officer:** Cassandra Krute
  - Handles internal and external communications.
  - Notifies affected parties and regulatory authorities if needed.

- **Legal and Compliance Team:** Tristan Hellijas, Steven Luu
  - Reviews incidents for legal or regulatory impact.
  - Ensures incident reporting complies with applicable laws.

3. Incident Classification and Severity Levels

To effectively defend Qualicart's expanding digital ecosystem, including the groundbreaking QualiCart app, our team at xyzIT believe it is essential to categorize and prioritize security incidents with precision. Proper classification is proven to allow for faster and smarter responses and helps ensure that the most critical issues receive immediate attention.

3.1 Incident Types

Given that Qualicart is tech-driven and operates globally, our team recommends focusing on six major categories of security incidents:

- **Malware Infection**
    - Includes viruses, worms, trojans, and particularly ransomware, which can encrypt vital company data and hold it hostage.
    - These threats often enter through email attachments, unsecured downloads, or compromised vendor systems.
    - With Qualicart's international app deployment, malware could exploit varying regional security standards.
- **Data Breach or Leak**
    - Unauthorized access or exposure of sensitive business data, including client trade details, user credentials, and proprietary supply chain analytics.
    - Especially dangerous in Qualicart's context, as it risks exposing strategic sourcing data and regulatory documents.
- **Denial of Service (DoS) / Distributed DoS (DDoS)**
    - Deliberate attempts to overwhelm servers and disrupt the QualiCart app's availability.
    - A single attack could stall operations for hundreds of SMEs, leading to massive reputational damage.
- **Phishing and Social Engineering**
    - Deceptive schemes that trick employees into revealing passwords or granting access to systems.

  - These threats target human vulnerability and are often overlooked despite being one of the most successful attack vectors.

- **Insider Threats**
  - Can be malicious or accidental but always damaging.
  - With Qualicart's distributed team and contractors across regions, insider threats pose a real challenge in monitoring and control.
- **Advanced Persistent Threats (APT)**
  - Long-term, highly targeted attacks usually backed by sophisticated criminal organizations or nation-states.
  - These are particularly relevant as Qualicart rises in global prominence and becomes a geopolitical alternative to China-based platforms.

3.2 Severity Levels

To empower Qualicart's IT and leadership teams to prioritize effectively, we recommend adopting a four-tier severity model:

- **Low Severity**
  - Minor disruptions with no threat to core systems or sensitive data.
  - Example: an employee mistakenly downloads a harmless file flagged by antivirus software.
- **Medium Severity**
  - Localized impacts that do not threaten critical infrastructure.
  - Example: unauthorized access to a non-sensitive internal system, or an isolated malware detection.
- **High Severity**
  - Substantial risks to operations or data integrity, possibly affecting the app, its APIs, or payment systems.
  - Example: a phishing attempt successfully harvesting credentials from a supply chain partner.
- **Critical Severity**

- Incidents that jeopardize core services or legal standing, such as system-wide breach or compromise of user financial data.
- In this scenario, response times are measured in minutes not hours, and involve executive decision-making.

By applying these classifications, Qualicart will not only be better equipped to respond in real-time but will also be able to communicate incident status and urgency across departments with clarity and consistency.

4. Incident Identification and Reporting

Timely identification and reporting of security incidents are foundational to Qualicart's cybersecurity posture. In a global, digital-first company, where milliseconds can impact supply chains, a delay in detecting an attack can snowball into business disruption, financial loss, or regulatory non-compliance.

4.1 Detection Mechanisms

To detect potential threats early and accurately, we propose a hybrid approach that combines technology and human vigilance:

- **Automated Security Monitoring**
  - Implement AI-driven threat detection tools that monitor server logs, user behavior, and network activity in real time.
  - These systems can flag anomalies such as unusual login attempts, traffic surges, or data exfiltration patterns.
- **Security Information and Event Management (SIEM)**
  - Deploy a centralized SIEM platform to collect and correlate security data across systems and subsidiaries (QualiTech, QualiLogistics, etc.).
  - This will enhance visibility across the ecosystem and reduce detection time from days to minutes.
- **Employee Vigilance Programs**
  - Train all employees—from software developers to customer service reps—to recognize suspicious emails, phishing attempts, and social engineering.
  - Regular simulations and security drills will reinforce this awareness and improve response rates.
- **Threat Intelligence Integration**
  - Connect detection tools to external threat feeds so Qualicart can stay ahead of emerging threats in real-time, especially those targeting supply chain platforms and e-commerce businesses.

4.2 Reporting Procedures

Speed and clarity in reporting are critical. A clearly defined reporting pipeline ensures that incidents are escalated quickly and accurately:

- **Incident Reporting Channels**
    - Employees should report any suspected security incident immediately via pre-established channels:
        - Dedicated cybersecurity hotline.
        - Internal helpdesk ticketing system.
        - Emergency reporting email (*security@qualicart.us*).
- **Incident Report Checklist**
  To streamline triage and ensure no critical detail is missed, every report should include:
    - **Timestamp** – When the incident was first noticed.
    - **Incident Description** – What was observed (unexpected behavior, error messages).
    - **Affected Systems or Services** – Whether it impacted the QualiCart app, data systems, or customer accounts.
    - **Initial Response Actions** – Any immediate steps the reporter took (disconnecting from Wi-Fi, notifying IT).
- **Non-Retaliation Policy**
    - Employees must feel safe reporting issues. A clear policy of non-retaliation will foster transparency and a culture of accountability.

By investing in a strong detection and reporting framework now, Qualicart will set the foundation for operational resilience as it scales. Incidents are inevitable, but how swiftly and effectively they are reported can be the difference between a minor disruption and a multimillion-dollar crisis.

5. Analysis of Qualicart's Cybersecurity Maturity

The National Institute of Standards and Technology (NIST) Cybersecurity Framework provides a structured model for managing and reducing cybersecurity risk. Qualicart's assessment revealed critical gaps and improvement opportunities across the five NIST functions: **Identify**, **Protect**, **Detect**, **Respond**, and **Recover**. Each function contains multiple subcategories, with varying maturity levels and priority ratings based on their potential impact on the organization.

5.1. Identify Function

This function focuses on understanding business context, resources, and risk to inform cybersecurity decisions.

- **Asset Management (ID.AM)**: Multiple subcategories under this theme are rated at "Low" maturity. This includes tracking physical devices and software assets. The low maturity here means Qualicart may not have a complete or updated inventory of its IT environment, increasing the risk of shadow IT and vulnerability exposure. Investing in automated asset discovery tools (estimated costs of $150,000) is far cheaper than upwards of $500,000 in potential damages.
- **Business Environment (ID.BE)**: Subcategories like understanding the organization's role in the supply chain and defining critical services are crucial, especially given Qualicart's global operations. These areas are mostly at "Low" maturity and marked "High" priority. Training staff in business continuity is critical and would reduce service disruptions during incidents.
- **Governance (ID.GV)** and **Risk Assessment (ID.RA)**: These subcategories assess policies and legal/regulatory requirements. Most are at "Medium" maturity but need enhancement to "High" to ensure consistent enforcement of security policies and compliance. Strengthening governance can prevent fines and regulatory penalties that often exceed mitigation costs.

5.2. Protect Function

This function implements safeguards to ensure delivery of critical services.

- **Identity Management (PR.AC)**: These subcategories—like controlling access to assets—are rated "Medium" but are targeted for "High" maturity. Strong identity management thwarts unauthorized access, a common vector in breaches.

- **Awareness and Training (PR.AT)**: Currently at "Low" maturity, these subcategories include ensuring all staff are trained on their security roles. The cost of comprehensive training (~$60,000) is negligible compared to reputational damage and losses from a phishing breach due to human error.
- **Data Security (PR.DS)**: Includes protecting information through encryption, backups, and integrity checks. Weaknesses here can lead to data leakage. Improving this area is a "Medium" priority, but essential, especially as Qualicart deals with consumer data.
- **Information Protection Processes (PR.IP)**: This area is about maintaining policies and procedures. Several subcategories are "Medium" maturity but should be elevated to "High." Formalizing patch management, for instance, reduces the risk of known exploits being used in attacks.

5.3. Detect Function

This function ensures timely discovery of cybersecurity events.

- **Anomalies and Events (DE.AE)**: Subcategories such as establishing a baseline of network operations and monitoring for anomalies are mostly "Medium" maturity. Targeting "High" maturity here will enable faster identification of suspicious activity, cutting down the window of attacker presence in the system.
- **Security Continuous Monitoring (DE.CM)**: This includes real-time monitoring of assets and networks. Investment in SIEM (Security Information and Event Management) systems, while costly, is invaluable. A proactive detection system helps stop breaches before significant damage is done.

5.4. Respond Function

Responding effectively to detected incidents is key to damage control.

- **Response Planning (RS.RP)** and **Communications (RS.CO)**: Several of these are "Low" or "Medium" maturity. A coordinated incident response plan reduces downtime and chaos during a breach. The cost of developing and regularly testing response plans is minimal when compared to the millions potentially lost during an uncoordinated response to ransomware or data exfiltration.

- **Mitigation (RS.MI)**: This includes containing the impact of incidents. Raising this to "High" maturity ensures that Qualicart can limit operational disruptions, maintain customer confidence, and restore services faster.

5.5. Recover Function

This function focuses on restoring services and minimizing impact post-incident.

- **Recovery Planning (RC.RP)** and **Improvements (RC.IM)**: These subcategories are mostly at "Medium" maturity. Structured recovery planning helps bring systems back online efficiently. After-incident reviews ensure lessons are captured and acted on.

5.6. Financial Perspective: Why Maturity Pays Off

A recurring theme throughout this assessment is the financial upside of maturity. For many subcategories, the **estimated cost of mitigation (typically $50,000–$150,000)** is dwarfed by **potential breach-related damages (ranging from $300,000–$500,000 or more)**. This is a classic risk vs. reward equation: an ounce of prevention is worth a pound of cure.

Examples:

- **Training and Access Control**: ~$60,000 vs. breach cost of $500,000+
- **Asset Inventory Systems**: ~$150,000 vs. breach cost of $500,000
- **Incident Response Planning**: ~$100,000 vs. recovery and reputation costs in the millions

Beyond the numbers, there's also **intangible value**: protecting brand reputation, maintaining customer trust, ensuring up time, and meeting regulatory requirements. None of which can be easily recouped once lost.

6. Current Assessment of Qualicart's Cybersecurity Maturity

Understanding where Qualicart currently stands in terms of cybersecurity maturity is essential to charting a clear path forward. To that end, we conducted a comprehensive evaluation of our cybersecurity practices using the NIST Cybersecurity Framework (NIST CSF), a globally recognized standard that helps organizations manage and reduce cybersecurity risk.

This assessment looked at three key elements for each NIST subcategory:

1. **Our current maturity level**
2. **The priority level for improving it**
3. **The target maturity level we aim to reach**

6.1. Where Qualicart Stands Today

Across all the assessed subcategories, we found that:

- **30 subcategories are currently at a "Medium" maturity level** – meaning we have processes in place, but they may be inconsistently applied or lack full integration across departments.
- **25 subcategories are still at a "Low" maturity level** – where minimal or ad hoc processes exist, exposing us to higher cyber risk.
- Only **1 subcategory currently reaches a "High" maturity level**, where practices are well-established, consistently implemented, and measurable.

This distribution indicates that while we've laid a foundational framework, there are still substantial gaps, especially in areas currently assessed as "Low."

6.2. Our Ambition: Where We Want Qualicart to Be

Our goal is ambitious but necessary. We're targeting:

- **37 subcategories to reach "High" maturity**, ensuring that our cybersecurity practices are robust, standardized, and continuously improved.
- **19 subcategories to reach at least "Medium" maturity**, focusing on solidifying foundational controls and processes.

This aspirational shift is key to aligning cybersecurity practices with our business growth, customer trust, and compliance needs.

6.3. Priorities: Where to Focus First

To help focus resources and drive impact, each subcategory was also assigned a **priority level**:

- **41 subcategories were marked as "Medium" priority** – these are important but not immediate red flags.
- **13 subcategories were labeled "High" priority** – these are urgent and present the highest risk or opportunity. They typically correspond to areas where we're currently "Low" but need to be "High."
- **2 subcategories were considered "Low" priority**, usually because they are already being handled reasonably well or have lower risk exposure.
-

6.4. What This Means for Qualicart

This assessment tells a clear story: while Qualicart is on the right path, there still is work to do to bring Qualicart's cybersecurity capabilities in line with best practices.

High-priority areas, such as business continuity training, asset inventory management, and unauthorized access control are especially critical. These directly relate to past incidents in the industry and, if left unaddressed, could expose Qualicart to similar threats.

Investing in these areas is not just about compliance**,** it's about protecting our customers, our operations, and our brand.

Each recommended improvement also includes a tailored mitigation strategy and cost estimate, helping leadership weigh decisions in both business and technical terms. For example:

- Enhancing asset discovery tools is estimated at **$150,000.00** but could prevent damages of **$500,000 or more**.
- Training staff in incident response and business continuity may cost **$150,000**, but it's crucial to maintaining service during a breach.

By systematically improving our maturity in these key areas, we position Qualicart not only to defend against threats, but to lead with confidence in a digitally connected marketplace.

7. Incident Identification and Reporting

7.1 Detection:

Team XYZ will implement our top-of-the-line automated monitoring tools and security software. With around-the-clock supervision, our team works vigilantly to detect potential cybersecurity incidents. Any potential incident picked up by our monitoring tools and security software will be further analyzed. Constant spot checks will also act as a way to detect any abnormalities among secure data. With these monitoring methods, advanced detection will ensure a timely response.

7.2 Reporting Procedures:

If a cybersecurity threat is identified by anyone, whether a member of Team XYZ, an employee of Qualicart Corporation, or any stakeholders, a report of the suspected incident must be immediately filed. This report will go to a designated channel for Team XYZ to monitor more closely and decide if further action is necessary. This report will require essential information, including: name of reporter and team, date and time of occurrence, description of incident, system(s) impacted, and any immediate actions taken. This report will be a vital step in determining the cause of the incident, what information and systems were affected, and what the best course of action is to minimize the harm caused by the attack. Subsequent information will be added by Team XYZ based on the response to the report and actions taken against the threat and for Qualicart recovery. This information is imperative to have in the continuous strengthening of Qualicart's security posture.

8. Incident Response Procedures

8.1 Initial Assessment:

The preliminary evaluation is an essential starting point in Qualicart's incident response strategy, corresponding with the NIST CSF subcategory RS.AN (Analysis). When a possible incident is identified, Team XYZ, in collaboration with Qualicart's Technical Response Team (TRT), will promptly confirm its authenticity. This process involves examining alerts generated by automated systems, analyzing log files, and verifying irregularities reported by personnel or detection tools (RS.AN-1). After confirmation, the team will assess

8.2 Containment:

- Short-Term Containment:

Immediate containment refers to the prompt actions taken to halt the progression of a cybersecurity incident once it has been confirmed. By the NIST CSF subcategory RS.MI-1, Qualicart will swiftly isolate compromised systems from the network to mitigate further harm. This process may include disabling user accounts, quarantining infected devices, disconnecting affected systems, and stopping data transfers. These rapid measures are essential to restrict the impact of the incident, safeguard sensitive data, and maintain forensic evidence. Team

- Long-Term Containment:

Once the immediate danger is addressed, attention turns to long-term containment, which guarantees system stability and uninterrupted business operations while preparing for comprehensive remediation. This stage involves applying system updates, modifying access controls, implementing new security settings, and introducing compensating measures to protect the environment while keeping operations ongoing. Long-term containment corresponds with RS.MI-2 and RS.MI-3, stresses the importance of implementing corrections, documenting newly discovered vulnerabilities, and carrying out incident-specific response plans. These approaches are customized according to the nature and severity of the incident and are crucial for preventing further exploitation of vulnerabilities until the issue is fully eradicated. By stabilizing the impacted systems in this phase, Qualicart can maintain essential business activities confidently as recovery planning commences.

8.3 Eradication:

Once the threat has been managed, the subsequent step is to eliminate it from Qualicart's environment. This requires identifying and deleting harmful files, closing exploited vulnerabilities, disabling compromised accounts, and removing unauthorized access points (RS.MI-2). The objective is to ensure that no traces of the attack linger in the environment. A forensic analysis is conducted as part of this process to verify that all signs of the attacker have been removed and to gain insights into how the breach occurred. Following PR.IP-12 from the Protect function of the NIST CSF, Qualicart will also assess contingency plans and implement secure configuration practices throughout the affected systems to avert re-entry and strengthen security measures.

8.4 Recovery:

After the environment has been cleared, Qualicart will initiate the recovery phase, in line with the NIST CSF subcategories under the Recover (RC) function. Systems and services will be brought back online using verified, clean backups, following the organization's disaster recovery protocols (RC.RP-1). The restored systems will then undergo testing to ensure their operational status and to confirm that there is no lingering malware or configuration issues (RC.IM-1). Ongoing monitoring will be put in place to identify any indications of reinfection or recurring problems (RC.CO-2). Both internal and external stakeholders, including customers and vendors, will be kept updated on the recovery efforts through established communication procedures to foster transparency and trust (RC.CO-1 to RC.CO-4). These communication measures ensure that all parties are aware of the actions taken and what they can anticipate moving forward.

8.5 Scenarios:

To make certain that Qualicart is ready for various cyber incidents, Team XYZ will perform testing based on scenarios and tabletop exercises that replicate real-world threats. These scenarios will cover phishing and social engineering attacks, ransomware events, distributed denial-of-service (DDoS) attacks, insider threats, and breaches involving third-party vendors. Each scenario will adhere to customized playbooks that align with the company's existing risk landscape and operational dependencies. This initiative supports RS.IM-1, emphasizes the ongoing enhancement of the incident response process. Insights gained from these exercises will be utilized to improve policies, procedures, and technical defenses. These anticipatory actions guarantee that Qualicart can not only react efficiently when an incident occurs but also continually adapt its defense strategies in response to an ever-changing threat landscape.

9. Communication Plan

9.1 Mean of Communication:

- Provide communication channels for easy updates or notification (Email, Social Media, Phone Number)

- Work with PR teams for methods of public transparency on statements and press releases.

9.2 Spokesperson:

- Designate a spokesperson from leadership to represent the company.

- Ensure the spokesperson is trained to align with company values and goals.

9.3 Internal Communication:

- Notify senior management, the board, and affected departments.

- Keep employees updated on the status and any actions they need to take (e.g., password resets, system downtimes).

9.4 External Communication:

- Inform customers, partners, and third-party vendors if their data or services were affected.

- Work with legal and compliance teams to notify regulators if required.

- Provide clear instructions and steps for affected parties (e.g., reset passwords, update security practices).

9.5 Handling of Feedback:

- Collect the questions and concerns of the stakeholders.

- Analysis/review of the feedback & respond accordingly.

10. Post-Incident Review

10.1 Incident Documentation:

- Identify which incidents require post-incident review.

- Record detailed information about the incident, actions taken, and timelines.

- Collect logs, forensic evidence, and reports from relevant teams.

- Assign/Reassign roles and responsibilities based on the outcomes of the incident.

- Review response strategies to ensure they can account for all outcomes including unexpected events.

10.2 Root Cause Analysis:

- List out potential root causes that could have led to the issue.

- Explore each route and confirm the root cause of the issue.

- Document the root cause and the factors that led up to it. (5 Whys technique, Ishikawa Diagrams, etc.)

Ensure that the root cause is identified and any similar areas of vulnerability.

10.3 Lessons Learned:

- Conduct a debriefing session with the Incident Response Team and other relevant stakeholders.

- Identify improvements to current security measures, policies, and response procedures.

- Update the Cybersecurity Response Plan based on findings.

10.4 Reporting:

- Produce a final incident report summarizing the timeline, impact, and response.

- Distribute the report to management, regulators (if required), and affected parties.

- Ensure the proper precautions are taken to prevent this issue from occuring again.

10.5 Retesting:

- Ensure everyone has undergone proper training.

- Allow for a reasonable amount of time to pass before testing again.

- Simulate a real-world situation and monitor/record how people react.

11. Preventative Measures and Training

11.1 Metrics and Continuous Improvement:

A proactive approach to cybersecurity is essential for reducing vulnerabilities and strengthening Qualicart's overall security posture. This section outlines the key strategies and programs implemented to prevent incidents and ensure continuous improvement.

- **Employee Training**

Regular cybersecurity awareness training is provided to all employees to build a strong human firewall. Topics include phishing recognition, password hygiene, proper data handling, and secure use of devices and systems. By educating staff, we reduce the likelihood of successful social engineering and insider threats.

A perfect example of employee training is for lifeguard training. Clearly defined roles are crucial, yet they are often overlooked. For example, during my time at the YMCA, we had training sessions in Rochester for Wilderness First Aid and CPR. One of the biggest challenges, especially for lifeguards, was the lack of set procedures and defined roles. In emergency situations, such as a drowning, multiple lifeguards knew how to respond, but they often hesitated because no one was sure who should take the lead. As a result, it could take up to 30 seconds for a lifeguard to initiate a rescue and perform the first rescue breath.

To prevent these delays, we implemented a detailed plan that assigned specific responsibilities to each lifeguard, regardless of their location. For example, one lifeguard would focus on removing the victim from the water, another would be in charge of CPR, and another would call an ambulance. This system significantly improved response time and, ultimately, the survival rate of victims. Similarly, implementing a structured system like this in a business such as Qualicart would be crucial, as it ensures that employees have clearly defined roles and objectives.

- **System Updates and Patching**

All Qualicart systems follow a strict patch management schedule. Operating systems, applications, and firmware are routinely updated to address known vulnerabilities. Vulnerability scanning tools are used to identify weaknesses, which are then prioritized and patched accordingly.

Drawing from past industry incidents, such as the Target breach, where internal threat detection tools successfully identified anomalies but failed to prompt timely action. Qualicart should take additional steps to not only detect but also respond decisively. Our systems are configured to

flag any unusual activity, and more importantly, our response framework that every alert triggers a clear, predefined escalation path.

To prevent the kind of breakdown that occurred in the Target case, Qualicart needs to maintain a comprehensive incident response plan with assigned roles and responsibilities for every possible threat scenario. This structure ensures swift, coordinated action and minimizes downtime or damage in the event of a breach, reinforcing our commitment to operational continuity and customer trust.

- **Backup and Recovery**

Routine backups of critical systems and sensitive customer data are conducted daily, with secure storage maintained both on-site and off-site. These backups are encrypted and tested regularly to ensure quick and reliable recovery in the event of data loss, ransomware attacks, or system failures.

At Qualicart, protecting user data is not just a technical priority, but critical for the business at hand. The loss or mishandling of consumer information can have enormous impacts, especially for emerging companies that lack the financial capital to pay in the case of lawsuits or penalties. For Qualicart, which is still building its brand and market presence, even a single mistake in data protection could severely damage customer trust. What distinguishes an effective response plan is not just the ability to detect a threat, but the ability to recover quickly and minimize impact. In this regard, our team is trained and tested on restoration procedures, ensuring that we are prepared for anything and protecting what is most important, which is our customer's data.

11.2 Pen Testing:

Regular penetration tests are conducted by Team XYZ to uncover potential vulnerabilities before they can be exploited. These assessments cover web applications, network infrastructure, and cloud environments. Findings from pen tests are documented, prioritized, and remediated based on risk level. Which could adjust the potential 3 Year Roadmap implementation on the NIST CSF Framework based on its risk level.

Another method to strengthen our defenses, Qualicart employs a combination of Red Team (offensive), Blue Team (defensive), and Purple Team (collaborative) testing. This comprehensive approach simulates real-world attacks, evaluates detection and response effectiveness, and identifies gaps in both technology and process.

- Red Team: Simulates threats to the Qualicart System.

- Blue Team: Is supposed to simulate the defenses of Qualicart including their response plan.

- Purple Team: Facilitates collaboration between Red and Blue teams to share insights, improve detection strategies, and improve overall security posture.

11.3 Metrics and Continuous Improvement

Cybersecurity is not a one-time initiative, it is a continuous process of measurement, feedback, and evolution. At Qualicart, we use key performance indicators (KPIs) to evaluate the effectiveness of our security controls and identify areas for improvement.

Core cybersecurity metrics tracked include:

- **Phishing Test Click Rates**
  Measures user susceptibility to simulated phishing attempts and informs future employee training.
- **Patch Deployment Timelines**
  Tracks the speed at which critical vulnerabilities are addressed across systems.
- **Mean Time to Detect** and **Mean Time to Respond**
  Indicates how quickly threats are identified and mitigated after detection.
- **Compliance Audit Results**
  The following of internal policies, industry standards, and regulatory requirements.

These metrics are reviewed monthly by the security team and executive leadership. Insights gathered are used to adjust training content, refine detection systems, and strengthen policies.

11.4 Scenario-Based Testing and Preparedness

At Qualicart, regular testing is integral to our cybersecurity readiness strategy. These simulations provide a controlled environment to test our response capabilities, improve decision-making, and ensure that all departments understand their roles during an actual threat.

Our scenarios reflect the most relevant and high-risk threats to e-commerce platforms, including:

- **Ransomware Attacks**
  Simulating the encryption of systems and data to assess response time, communication protocols, and recovery procedures.
- **Insider Threats**
  Testing detection and mitigation strategies for malicious or negligent activity originating from within the organization.
- **Distributed Denial-of-Service (DDoS) Attacks**
  Evaluating the resilience and failover capabilities of our web infrastructure during high-traffic disruptions.
- **Social Engineering**
  Practicing containment, privilege revocation, and impact analysis in the event that high-level access credentials are breached.

These exercises are not only technical, they involve leadership, legal, communications, and customer support teams to make sure its whole response including each department at Qualicart. Post-incident reviews are conducted after each drill to identify gaps, communication, or technology, and to refine incident response plan.

12. Three-Year Cybersecurity Roadmap

This three year road map outlines a robust, strategic, and actionable three-year cybersecurity roadmap for Qualicart Corporation. Designed in alignment with the NIST Cybersecurity Framework, it includes a quarterly maturation approach integrating essential NIST subcategories. The roadmap has been developed with a deep understanding of Qualicart's evolving digital ecosystem, including its app development and supply chain innovations. By aligning subcategory implementation with business risk, impact, and readiness, this plan enhances resilience and provides sustainable cybersecurity growth.

12.1. Year 1: Foundation and Visibility

Q1-Q2: Establish Governance and Asset Awareness

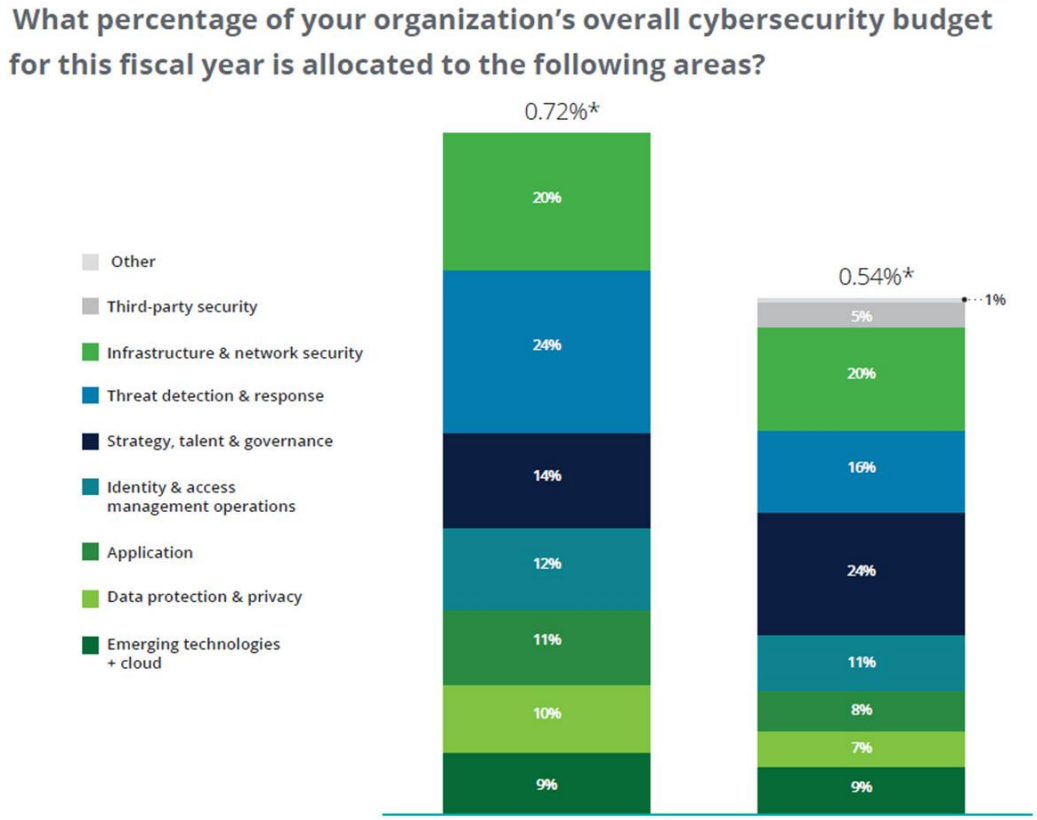
- **ID.AM-1 to ID.AM-6 (Asset Management):** Qualicart's success hinges on a diverse and international IT infrastructure supporting its portal and mobile applications. Mapping physical and digital assets (ID.AM-1, ID.AM-2) ensures visibility across devices, applications, and systems. Given its reliance on smart warehousing and global logistics (QualiLogistics), the identification and cataloging of these platforms and applications (ID.AM-3, ID.AM-4) is foundational. Prioritizing resources (ID.AM-5) ensures focus on those enabling core business operations. Defining roles (ID.AM-6) clarifies responsibility amid rapid organizational scaling.
- **ID.BE-1 to ID.BE-5 (Business Environment):** Qualicart’s mission to provide a secure, scalable, and non-China-centric e-commerce and logistics solution makes it imperative to link cybersecurity to its core operational dependencies. Mapping its critical delivery functions and supplier networks (ID.BE-3) ensures the cyber strategy reinforces its competitive edge.
- **ID.GV-1 to ID.GV-4 (Governance):** Rooted in its post-breach founding narrative (inspired by incidents like Yahoo and Equifax), cybersecurity governance must evolve from foundational policy reviews (ID.GV-1) to embedding risk into governance structures (ID.GV-4). This early emphasis on policy and regulatory compliance aligns with QualiTrade's role in navigating international trade laws.

Q3-Q4: Risk Insight and Supply Chain Strategy

- **ID.RA-1 to ID.RA-6 (Risk Assessment):** With Qualicart’s launch pending, understanding vulnerabilities within its ecosystem—from mobile interfaces to API integrations with

international logistics systems—is critical. Threats must be contextualized within both the tech stack and geopolitical landscape (ID.RA-3, ID.RA-4).

- **ID.RM-1 to ID.RM-3 (Risk Management Strategy):** By end of Year 1, establishing risk tolerance (ID.RM-2) provides the strategic lens for decision-making on protective measures and investments in Year 2.
- **ID.SC-1 to ID.SC-5 (Supply Chain Risk Management):** Given Qualicart's reliance on diverse regional suppliers (Latin America, Southeast Asia), it must embed security into supply chain contracts and vendor evaluations (ID.SC-2, ID.SC-4). The organization's differentiation depends on securing these dynamic and often less-regulated ecosystems.



12.2. Year 2: Safeguards and Detection

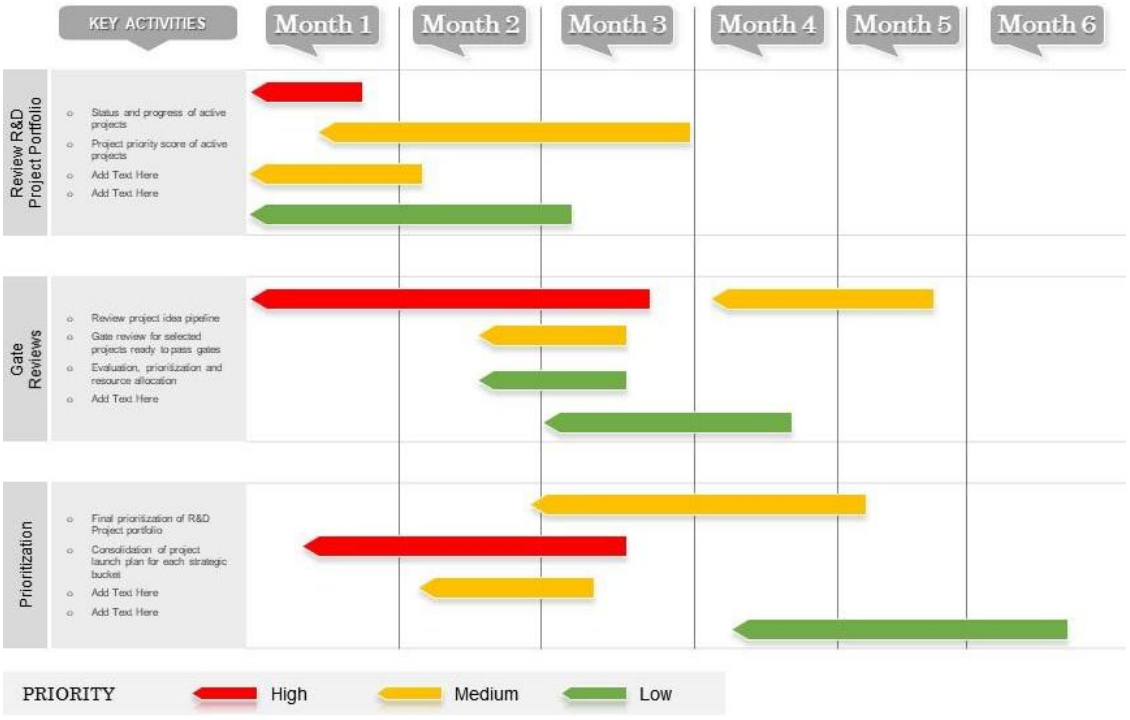
Q1-Q2: Protective Measures and Access Controls

- **PR.AA-1 to PR.AA-5 (Identity Management, Authentication and Access Control):** Qualicart's distributed workforce and third-party integration demands stringent access controls. Applying RBAC and implementing MFA are critical in light of threats to B2B platforms (e.g., credential stuffing).

- **PR.AT-1 to PR.AT-5 (Awareness and Training):** Tailored training for logistics operators, developers (QualiTech), and compliance teams (QualiTrade) ensures contextual security behaviors. Creating this culture of awareness is central to maintaining operational continuity and defending against social engineering.
- **PR.DS-1 to PR.DS-6 (Data Security):** With QualiCart processing SME trade transactions and sensitive customer data, securing data-at-rest and in-transit (PR.DS-2, PR.DS-4) is mandatory. The company's use of blockchain (QualiTech) amplifies the importance of protecting transaction integrity.

Q3-Q4: Platform Integrity and Infrastructure Resilience

- **PR.PT-1 to PR.PT-5 (Protective Technology):** The high-tech nature of Qualicart's innovations—AI for demand forecasting and smart contracts—demands hardened platforms. Integrating endpoint detection and continuous system integrity monitoring supports NIST best practices.
- **PR.IR-1 to PR.IR-4 (Infrastructure Resilience):** Given Qualicart's logistics focus, even short outages can have major ripple effects. Developing error problem solving systems and secure failovers supports their sustainability and customer trust.
- **DE.CM-1 to DE.CM-7 (Security Continuous Monitoring):** With digital interactions occurring 24/7 across global time zones, real-time SIEM and anomaly detection is crucial for minimizing dwell time and preventing reputational damage.



12.3. Year 3: Response, Recovery, and Optimization

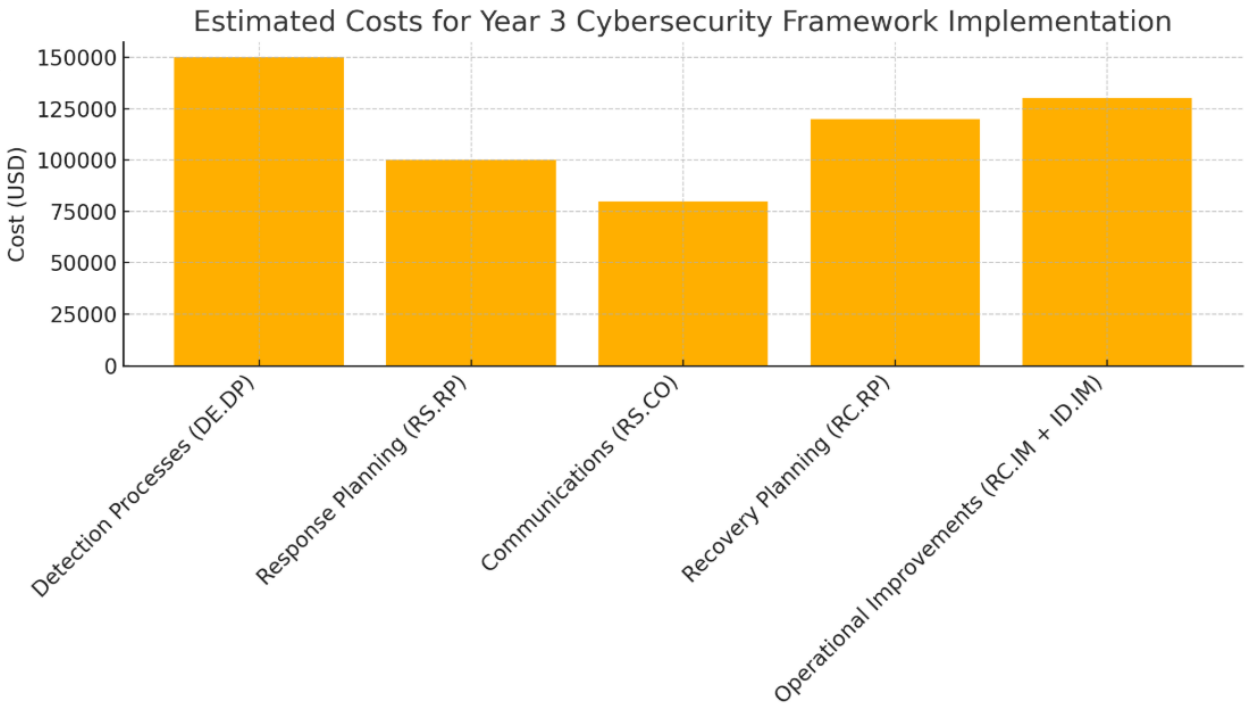
Q1-Q2: Incident Preparedness and Responsive Capabilities

- **DE.DP-1 to DE.DP-5 (Detection Processes):** Having matured its monitoring capabilities, Year 3 formalizes detection playbooks and ensures correlation with Qualicart's risk scenarios. These processes reduce response latency and optimize alert fatigue management.
- **RS.RP-1 to RS.RP-5 (Response Planning):** A hallmark of resilience is swift and coherent response. Developing detailed response procedures, informed by Year 1's risk assessment, ensures readiness across subsidiaries like QualiTrade and QualiLogistics.
- **RS.CO-1 to RS.CO-5 (Communications):** Given Qualicart's ambition to become a global e-commerce leader, transparent stakeholder communication post-breach is not optional. Establishing media, customer, and regulatory response frameworks mitigates fallout.

Q3-Q4: Recovery and Maturity Elevation

- **RC.RP-1 to RC.RP-3 (Recovery Planning):** Robust DR capabilities are vital for Qualicart's digital logistics network. Recovery of data and platform continuity tests should encompass mobile app and warehouse automation systems.
- **RC.IM-1 to RC.IM-3 (Improvements):** A dynamic threat landscape and ongoing platform updates (e.g., blockchain ledger modifications) necessitate feedback loops from incidents and testing into operational security improvements.
- **ID.IM-1 to ID.IM-4 (Improvements under Identify):** Conducting maturity reviews ensures that the roadmap evolves with business direction—be it entering new markets, adopting AI innovations, or facing novel threat actors.

In short, cybersecurity is insurance against existential risk. Delaying investment doesn't save money instead it shifts costs to crisis response and reputational repair. By implementing the measures in this report, Qualicart not only safeguards its infrastructure but also secures its future in a competitive, high-risk digital market. With an intentional focus on foundational visibility, mid-term control hardening, and late-stage resilience, this three-year road map plan serves as both a strategic directive and a practical guide. The inclusion of every relevant NIST subcategory ensures full NIST compliance coverage and alignment with industry best practices, creating a durable and adaptable cybersecurity system for years to come.


Estimated Costs for Year 3 Cybersecurity Framework Implementation
Cost (USD)
150000
125000
100000
75000
50000
25000
0
Detection Processes (DE.DP)
Response Planning (RS.RP)
Communications (RS.CO)
Recovery Planning (RC.RP)
Operational Improvements (RC.IM + ID.IM)

13. Costs and Comparisons

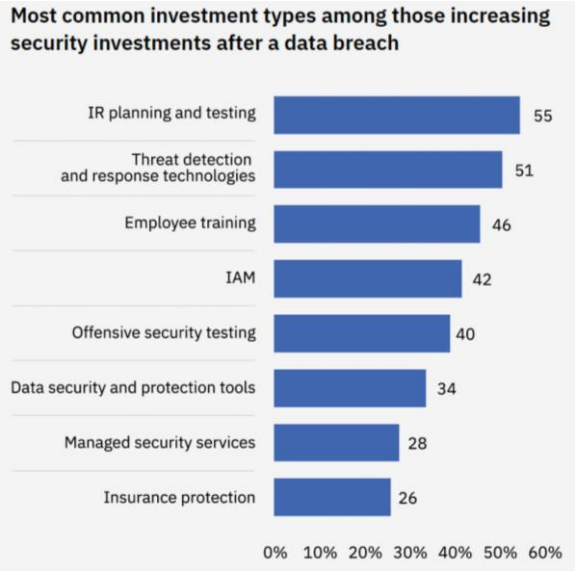
Investing in cybersecurity is not just a technical requirement, it is a business imperative. For Qualicart, proactive implementation of NIST Cybersecurity Framework measures represents a strategic defense against catastrophic financial loss.

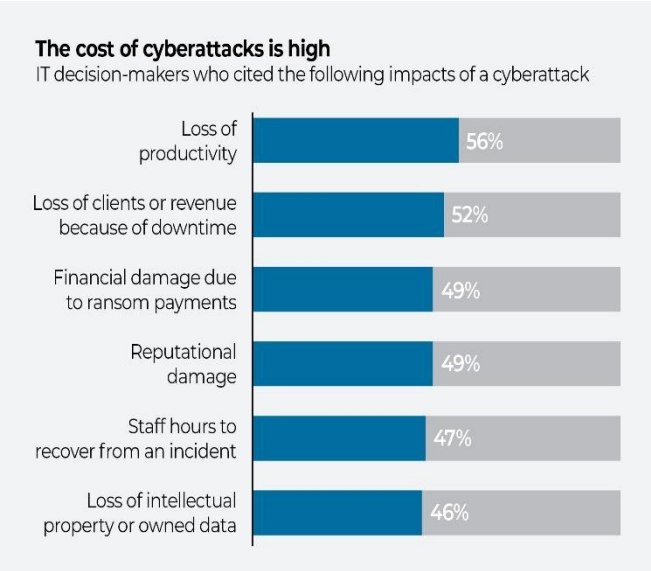
13.1. Financial Perspectives Rationale

The estimated cost to implement priority cybersecurity controls is approximately **$7.2 million**. This includes tools like automated asset discovery, data encryption, multi-factor authentication, and employee training. This investment may seem high but in comparison to the real-world costs of data breaches experienced by other major companies, you will see it is significantly more cost effective.

Consider these examples:

- **Target (2013):** Over **$300 million** in losses due to a third-party vendor compromise.
- **Yahoo:** A breach affecting 3 billion accounts ultimately led to a **$350 million** reduction in its sale price.
- **Uber:** Paid **$148 million** in fines after covering up a breach that exposed data of 57 million users.
- **Home Depot:** Spent **$179 million** recovering from a breach caused by stolen credentials.





These incidents show that a single vulnerability, whether from poor access control, weak training, or inadequate monitoring, can erase years of profit and irreparably damage customer trust.

For example, Qualicart's planned $150,000 investment in asset visibility could prevent up to **$500,000** in losses from unmanaged systems. A $100,000 training initiative could avert phishing attacks that often-cost millions. Implementing endpoint detection and access controls, although costly, could stop attacks like those that crippled companies like JP Morgan and LinkedIn.

14. Conclusion and Recommendations

Qualicart's should aim to have success and long-term sustainability. As the company prepares to launch its app and scale its operations, having a solid and flexible Cybersecurity Incident Response Plan is essential to protect customer trust, business continuity, and internal operations.

This plan outlines an approach to identifying, responding to, and recovering from cyber threats. It includes clear roles and responsibilities, proactive detection methods, scenario-based testing, and detailed communication strategies. These elements ensure that Qualicart is not only prepared for potential incidents but can respond quickly and effectively when they occur.

Looking ahead, we recommend the following actions:

• Review and update the Cybersecurity Incident Response Plan quarterly or after any major incident to stay aligned with emerging threats and evolving business needs.

• Conduct regular simulation exercises and penetration tests to make sure all departments are prepared and fully understand their roles during a threat.

• Use KPI's, such as detection and response times, phishing test results etc, to continuously refine training, policies, and response procedures.

• Prioritize employee training and system preparedness. Making sure that each person knows their role in a specific threat. This can make the difference between a contained threat and a widespread disruption.

• Maintain strong data protection through consistent backups and tested recovery procedures. This helps reduce the risk of permanent data loss and reinforces customer confidence.

As Qualicart continues to grow, smart investment in cybersecurity will be essential. Allocating funds toward better detection tools, training programs, and secure infrastructure will help safeguard the business from costly breaches and operational downtime.

Team XYZ is ready to support Qualicart in building a strong, adaptable security foundation. Together, we can make sure that Qualicart stays resilient and secure while continuing to innovate and expand.

"At Team XYZ your safety is our number one concern"

15. Contact Information

- **Incident Response Manager (IRM):**
  - **Hector Mayolet** ham4731@teamXYZ.rr.com

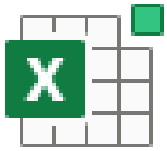
- **Technical Response Team (TRT):**
  - **Jay Goodman** jkg9629@teamXYZ.rr.com
  - **Steven Luu** sl4028@legalXYZ.rr.com

- **Forensics and Analysis Team:**
  - **Jay Goodman** jkg9629@teamXYZ.rr.com
  - **Eric Huang** eh3874@teamXYZ.rr.com

- **Communication Officer:**
  - **Cassandra Krute** cpk7247@teamXYZ.rr.com

- **Legal and Compliance Team:**
  - **Tristan Hellijas** tch6483@teamXYZ.rr.com
  - **Steven Luu** sl4028@teamXYZ.rr.com

16. Appendix



Qualicart CSF Analysis & Costs

Related Historical Breaches Analysis

17. Works Cited

Webpages & Reports

ABC News. Bizarre NSA-Linked Hacking Saga: Exploits Prove Real. 18 Aug. 2016, https://abcnews.go.com/International/bizarre-nsa-linked-hacking-saga-exploits-prove-real/story?id=41484443.

BreachSense. Home Depot Data Breach. https://www.breachsense.com/blog/home-depot-data-breach/.

CNN Business. CrowdStrike Outage: We Finally Know What Caused It - and How Much It Cost. https://www.cnn.com.

Columbia University School of International and Public Affairs. Sony - Written Case. Nov. 2022, https://www.sipa.columbia.edu/sites/default/files/2022-11/Sony%20-%20Written%20Case.pdf.

Columbia University School of International and Public Affairs. Target Final Report. Nov. 2022, https://www.sipa.columbia.edu/sites/default/files/2022-11/Target%20Final.pdf.

Daniel, Lars. "Facebook Data Breach Fallout—Millions May Receive Compensation." Forbes, 18 November 2024, https://www.forbes.com/sites/larsdaniel/2024/11/18/facebook-data-breach-fallout-millions-may-receive-compensation/#. Accessed 7 February 2025.

Dark Reading. Deconstructing the 2016 Yahoo Security Breach. https://www.darkreading.com/cyberattacks-data-breaches/deconstructing-the-2016-yahoo-security-breach.

Forbes. "From Home to HQ: The Battleground of the Hybrid Workplace." 24 Jan. 2025, https://www.forbes.com/sites/sap/2025/01/24/from-home-to-hq-the-battleground-of-the-hybrid-workplace/.

Gnaratna, Shanika. "LinkedIn: 2012 data breach much worse than we thought." CBS News, 19 May 2016, https://www.cbsnews.com/news/linkedin-2012-data-breach-hack-much-worse-than-we-thought-passwords-emails/. Accessed 7 February 2025.

Home Depot. Home Depot Provides Update on Data Breach Investigation. 6 Nov. 2014, https://ir.homedepot.com/news-releases/2014/11-06-2014-014517315.

J.P. Morgan Data Breach Lawsuit Says Info of 451K People Stolen by Cybercriminals. https://www.cnn.com.

McHaney, Roger, et al. "Teaching Case: Cybersecurity Breach at Target." Journal of Information Systems Education, vol. 29, no. 1, 2018, pp. 11–20, https://jise.org/Volume29/n1/JISEv29n1p11.pdf.

Mosyan, David. "How exactly hackers got into LinkedIn and Dropbox." Medium, 31 July 2023, https://medium.com/@dmosyan/how-exactly-hackers-got-into-linkedin-and-dropbox-f153e96f6abc. Accessed 7 February 2025.

National Institute of Standards and Technology (NIST). Cybersecurity Framework 1.1 Archive. 16 Apr. 2018, https://www.nist.gov/cyberframework/csf-11-archive.

Nature Editorial Staff. "AI and Cybersecurity: The Ongoing Battle." Nature, 2025, https://www.nature.com/articles/d41586-025-00118-y.

Perlroth, Nicole. "Shadow Brokers Leak Raises Alarming Question: Was the NSA Hacked?" The New York Times, 16 Aug. 2016, https://www.nytimes.com/2016/08/17/us/shadow-brokers-leak-raises-alarming-question-was-the-nsa-hacked.html.

Perlroth, Nicole. "Yahoo Says Hackers Stole Data on 500 Million Users in 2014." The New York Times, 22 Sept. 2016, https://www.nytimes.com/2016/09/23/technology/yahoo-hackers.html.

Savage, James. Top-Secret NSA Report Details Russian Hacking Effort Days Before 2016 Election. Brown University, 5 June 2017, https://cs.brown.edu/people/jsavage/VotingProject/2017_06_05_Interecept_Top-SecretNSAReportDetailsRussianHackingEffortDaysBefore2016Election.pdf.

Trend Micro. Uber Breach Exposes the Data of 57 Million Drivers and Users. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/uber-breach-exposes-the-data-of-57-million-drivers-and-users.

U.S. Department of Justice. Former Chief Security Officer of Uber Convicted on Federal Charges for Covering Up Data Breach. https://www.justice.gov/usao-ndca/pr/former-chief-security-officer-uber-convicted-federal-charges-covering-data-breach.

Wired. Uber Paid Off Hackers to Hide a 57 Million User Data Breach. https://www.wired.com/story/uber-paid-off-hackers-to-hide-a-57-million-user-data-breach/.

YouTube Videos

ABC News. How the Shadow Brokers Leak Exposed the NSA. YouTube, 17 Aug. 2016, https://www.youtube.com/watch?v=fGQhdzc571w.

CNBC. J.P. Morgan Hack: How It Happened. YouTube, 20 Nov. 2014, https://www.youtube.com/watch?v=butCn023nwM.

CNN. NSA Leaker Reveals Details of Hack. YouTube, 2 Aug. 2016, https://www.youtube.com/watch?v=hskXUMNzRlQ.

The Verge. Yahoo's Data Breach Explained. YouTube, 23 Sept. 2016, https://www.youtube.com/watch?v=v5rAW9oqTD8.

Wired. Inside the Uber Data Breach Cover-Up. YouTube, 21 Nov. 2017, https://www.youtube.com/watch?v=niCk6Qnmcrw.