UNIVERSITY OF DALLAS
Satish & Yasmin Gupta College of Business

Strategic Plan Part 2
Final Assignment

Alicia Draus and Isaiah Mosley

Strategic Cybersecurity Practicum – CYBS 8396
Dr. Branden Williams
Date of submission: July 22, 2025

Integrity Statement

By submitting this assignment, I (we) confirm that this assignment is my (our) own work, is not copied from the work (published or unpublished) of any other person, and has not previously been submitted for academic or professional purposes either at the University of Dallas or elsewhere. Any direct or indirect uses of material (e.g.: text, visuals, ideas …) from other sources have been fully acknowledged and cited according to American Psychological Association (APA) Style. I further confirm that I (we) will not share this assignment or my (our) response by any means, including online.

Table of Contents

Summary of Key Elements From Part 1

The first part of the strategic plan covered Square Inc.'s focus on aligning business and security practices. The introductory letter emphasized the commitment to secure financial transactions while maintaining compliance with GDPR and PCI DSS.

Square Inc.'s business mission, vision, and values highlight Square's dedication to empowering businesses with innovative and accessible payment solutions, while adhering to the IT philosophy, which explains how Square's technologies, policies, cloud strategies, and hybrid work models support this mission, guided by NIST standards.

Part one also covered the security organization chart, which lays out a detailed hierarchy of cybersecurity roles, from the CISO down to SOC analysts, showing a clear division of responsibilities to ensure 24/7 security coverage. The security justification was also discussed, supporting the need for this structure due to the company's size, sensitive data processing, and global operations. The plan reinforced that each role plays a vital part in defending against evolving cyber threats.

Security Mission and Vision Statements emphasized Square's goal to protect data while continuing with innovation and adhering to the core values of the CIA triad: confidentiality, integrity, and availability.

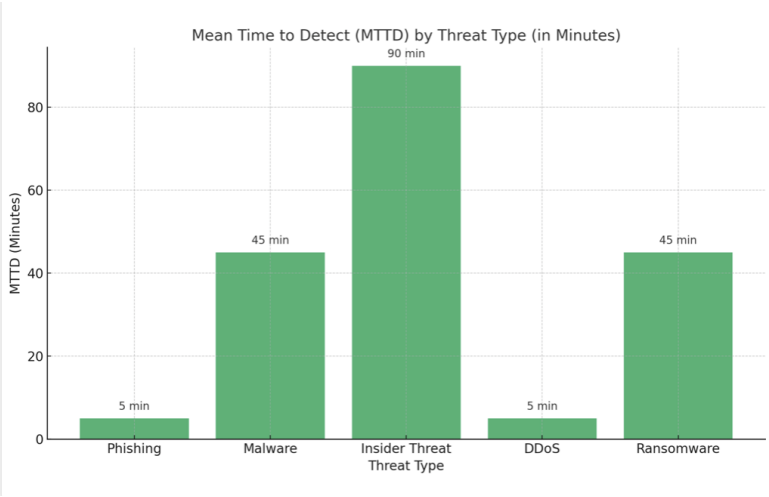
Lastly, the plan addressed security issues and challenges, identifying major concerns including compliance failures, mobile POS vulnerabilities, and phishing attacks. Citing investigations and incidents that call for urgent improvements in governance, compliance, and threat mitigation strategies.

Security Metrics

The four primary security metrics selected for collection include:

1. Mean Time to Detect (MTTD)

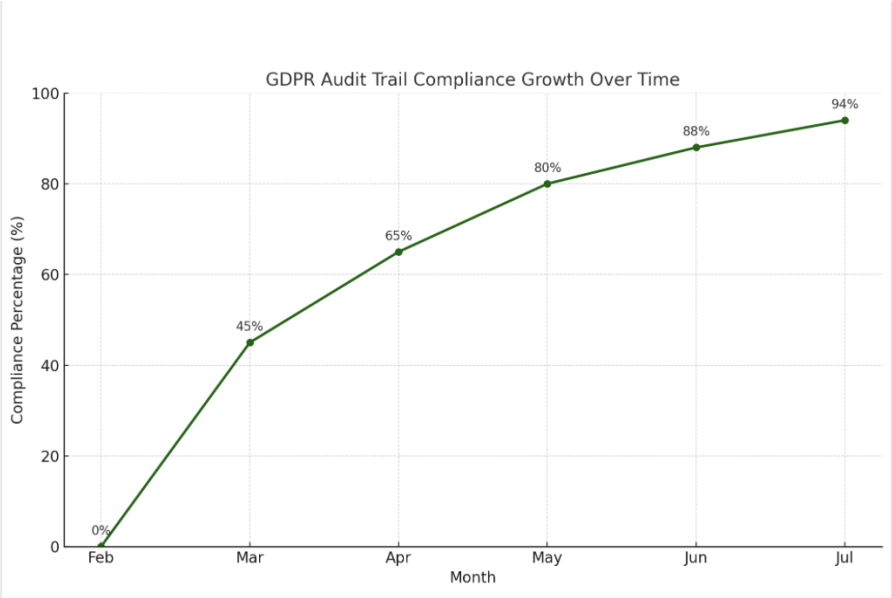
- Purpose of collection - This metric is collected to determine how long it takes the security team to detect a threat (SecurityScorecard, 2024).
- How is the data used- A lower MTTD indicates a faster threat detection capability, allowing for quicker containment and reducing the potential of security incidents. This metric is also used to refine detection strategies and optimize tool configurations (SecurityScorecard, 2024).
- Intended audience- The security team, incident response team, and IT team use this metric to enhance detection strategies.
- Frequency of collection - Data is collected on a weekly basis.
- Responsibility - The security team is responsible for collection, while the incident response team is responsible for analysis and reporting.



As shown above, the two threats that are detected the quickest for phishing and DDoS attacks.

2. Security Audit Compliance

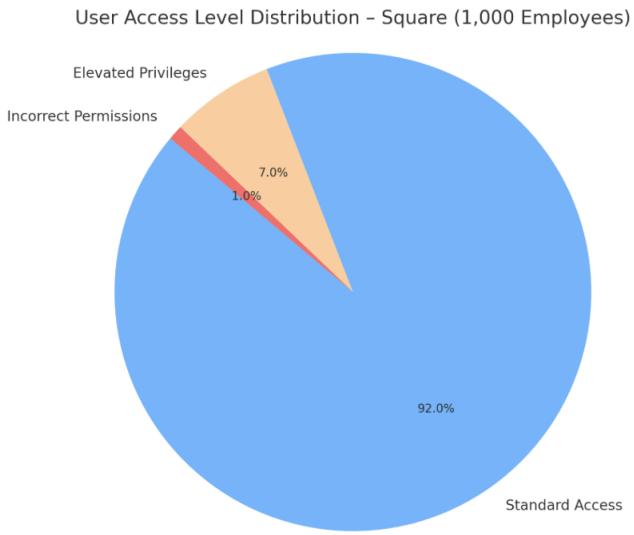
- Purpose of collection - This metric is collected to ensure that standards are being met across all systems and infrastructure. It verifies that data is properly recorded and retained in accordance with formal policy requirements (Atlassian, 2024).
- How is the data used - The data will be used to evaluate compliance with internal standards and regulatory requirements.
- Intended audience - The intended audience includes the security team, compliance team, and senior management.
- Frequency of collection - Security audit compliance is tracked and reviewed quarterly.
- Responsibility - The compliance team is responsible for collecting, analyzing, and reporting.



The graph above shows the rate of GDPR compliance. Due to the recent implementation of a formal GDPR compliance audit plan, compliance is showing 0% at the beginning of the year.

3. Identity and Access Management (IAM) Metrics

- Purpose of collection - This metric is collected to verify that users have appropriate permissions for their roles and that multi-factor authentication (MFA) is properly enforced (SOCRadar, 2024).
- How is the data used - The data will be used to ensure employees only have the minimum access necessary for their job functions and that no unauthorized elevation of privileges is occurring, in an effort to prevent insider threats. (SOCRadar, 2024).
- Intended audience - The security team and HR department use this metric.
- Frequency of collection - Data is collected on a monthly basis.
- Responsibility - The security team is responsible for collecting, analyzing, and reporting.



The pie chart above shows the access level percentage, where only 1% of employees used incorrect permissions.

4. Cybersecurity Awareness Training

- Purpose of collection - This metric is collected to assess employee cybersecurity knowledge and readiness to respond to threats (SOCRadar, 2024).

- How is the data used - The results will be used to identify individuals or departments that require additional cybersecurity training, helping to reduce overall organizational risk.
- Intended audience - The HR department, training team, and security team use this metric to identify employees who require additional training.
- Frequency of collection - Data is collected on a weekly basis.
- Responsibility - The security team is responsible for collecting, analyzing, and reporting.

The graph above shows a downward trend in the number of employees who clicked on simulated phishing emails over an 8-week period. This indicates that the cybersecurity awareness training demonstrates improved awareness and readiness across the organization.

Business Continuity Strategy

A business continuity plan is essential to ensure that critical business operations can continue in the event of a disruption or disaster (Whiteman & Seidl, 2019, p. 522). Square operates across multiple regions and relies heavily on continuous system uptime; therefore, having a continuity strategy is crucial in ensuring business operations continue uninterrupted.

Continuity Strategy

Square will implement a cloud backup strategy with a hot site. Square's services are "always-on," and this approach ensures real-time replication of data and infrastructure, allowing for instantaneous failover if primary systems are compromised. The hot site will be fully equipped and ready to take over operations with minimal downtime.

Plan Coverage

- Purpose: Provides a clear roadmap for relocating and restoring business functions following a disruption (Whiteman & Seidl, 2019, p. 552).
- Resource Requirements: Covers all essential components of IT infrastructure, including servers, hardware, cloud platforms, and business-critical applications.
- Roles and Responsibilities: Defines who is responsible for what during a continuity event (Whiteman & Seidl, 2019, p. 552).
- Exercise and Training Materials: Includes a schedule for continuity testing and training exercises, along with designated teams responsible for each phase.

Not Covered:

- Scope Limitations: Square's workforce spans multiple states and countries. This plan is designed as a flexible guideline and will not define detailed procedures for every geographic location (Whiteman & Seidl, 2019, p. 552).
- Extreme Disaster Scenarios: This business continuity plan does not address specific extreme disasters such as natural catastrophes or nation-state cyber warfare. Those events are covered under a separate Disaster Recovery Plan (Whiteman & Seidl, 2019, p. 552).

Key Organizational Players and Roles

- CEO – Provides executive oversight and final authority on plan execution.

- COO – Coordinates operational continuity and resource management.
- CISO – Oversees security risks and ensures continuity aligns with overall cybersecurity strategy.
- CTO – Manages continuity of technology infrastructure.
- Support Teams – Includes Network Security Analysts and the Incident Response Team, all of which play active roles during continuity events.

Testing the Plan

The plan will be tested after hours through a simulated disaster scenario involving failover to the hot site. The test will evaluate system recovery, internal and external connectivity, performance under load, and full system restoration (Swanson et al., 2010). Post test documentation will capture findings, identify gaps, and drive corrective actions. Regular testing cycles will be scheduled to ensure ongoing readiness and improvement.

Incident Response Procedure

Technologies Critical to Detect, Contain, and Remediate the Threat:

Detection – Determining whether an incident occurred (Whiteman & Seidl, 2019, p 522).

- SIEM (Security Information and Event Management): Enables data collection and correlation across multiple systems.
- EDR (Endpoint Detection and Response): Identifies unfamiliar files or suspicious activity on endpoints (Whiteman & Seidl, 2019, p. 522).
- NDR (Network Detection and Response): Monitors and detects malicious network traffic.

Containment – Preserving evidence, containing the incident, and beginning eradication (Whiteman & Seidl, 2019, p 522).

- SOAR (Security Orchestration, Automation, and Response): Automates the disabling of compromised user accounts.
- Firewall: Blocks malicious traffic at the perimeter (Whiteman & Seidl, 2019, p. 522).

Remediation/Recovery – Returning to normal operations (Whiteman & Seidl, 2019, p 522).

- Backups: Used to restore systems and data to a known-good state.
- Post-Incident Report: A follow-up report is created to document the event and lessons learned (Whiteman & Seidl, 2019, p. 522).

Key Organizational Players and Their Roles:

- CISO (Chief Information Security Officer): Oversees the incident response strategy and ensures executive alignment.
- CTO (Chief Technology Officer): Coordinates technical recovery and systems continuity.
- Infrastructure Security Manager & Network Security Analysts: Provide support in identifying vulnerabilities and managing network-level controls.
- SOC Manager, SOC Analysts, and Incident Response Team: Monitor, detect, analyze, and respond to threats in real time.
- Legal Support Team - Assist with fines, lawsuits, and remediation costs (Sterling, 2020).

How the Plan Will Be Tested

The plan will be tested after hours through a simulated ransomware attack. Participants will include:

- Two SOC analysts (handling detection and SOAR tools)
- Three members from the incident response team (responsible for modifying the response process)
- One network security analyst (working with the firewall and perimeter defense)
- In addition to live simulations, paper-based exercises will also be conducted to review various ransomware scenarios (BlueVoyant, n.d.).

Will Square Pay the Ransom?

No. A ransom will not be paid. According to the FBI, paying the ransom is strongly discouraged for several reasons:

1. There is no guarantee that the data will be recovered.
2. Paying incentivizes attackers to continue targeting more victims.
3. It supports and funds criminal activity (Federal Bureau of Investigation, n.d.).

When should Square contact law enforcement in the event of a ransomware attack?

Always. In accordance with CISA's recommendations, every ransomware incident will be reported to law enforcement. Reporting allows government agencies to share information about the attack, notify other organizations, and prevent further attacks (Cybersecurity and Infrastructure Security Agency, n.d.).

Security Staffing and Resource Strategy

Recruitment

Internal Recruitment: Human Resources will announce open job positions from within the work environment and post them on the company website. This strategy will offer clarity and equal opportunity, therefore inspiring employees to seek new job roles that match their interest or skills (S,H., 2025).

External Recruitment: Post job positions on highly recognized social media platforms, such as Indeed, or LinkedIn, to attract a diverse group of candidates with various experiences and skillsets. External recruitment is essential for hiring qualified candidates with exceptional skill sets and ideas outside the organization to fill employment openings (Techneeds, 2025).

Key Skills

Technical Skills: Candidates should have strong knowledge of various components of cybersecurity, including network security, threat intelligence, endpoint security, incident response, and security tools. Technical skills ensure cybersecurity professionals are equipped with the ability to comprehend, identify, and prevent a variety of cyber threats.

Communication Skills: Effective communication is essential to cybersecurity professions, as it provides clarification on security risks, modifications to customers, and their corresponding teams. Effective communication includes verbal and written communications, such as emails, report documentation, and other forms of communication, as it is vital for cybersecurity professionals to complete their tasks (Gaona, 2025).

Interviewing and On-boarding Process

Technical Interview: Technical interviews are critical in the hiring process as it allows candidates to showcase their problem solving skills, technical knowledge, and the capability for

critical thinking under extreme circumstances. Some scenarios may include quizzes, online coding assessments, and practical exercises to get the accurate results of candidates' skillset. (Tech Interview Handbook, 2025).

Comprehensive On-boarding: Providing a thorough on-boarding process is critical as it assists security professionals to adapt to the organizational culture and get familiar with their roles, staff members, operations, policies, and systems. A comprehensive onboarding process is important as it makes certain that employees feel comfortable, supported, and aligns with the organization's goals (SHRM, 2024).

Talent Acquisition

Competitive Compensation: Candidates will be offered a competitive salary that aligns with the industry standard or higher. Competitive compensation helps organizations attract and sustain top talent by proposing competitive salaries and benefits, as employees are typically seeking higher wages elsewhere.

Talent Development

Cybersecurity Awareness Training: Conducting annual cybersecurity training provides employees with insights to detect and prevent potential compromises using presentations, videos, quizzes, and realistic malware simulations (Luna, 2024).

Certification Programs: Designed for employees to get trained on current security solutions and software to identify, avoid, and address security issues. Employees are educated on various cybersecurity certifications such as Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH), and CompTIA Security + as they are standard certifications in the cybersecurity field (Liddle, 2025).

Retention Plan

Career Advancement: Offers best practices to prioritize career advancement, mental health assistance, a positive atmosphere, and adaptability as it is essential for retaining top talent. Career advancement opportunities include promotions, cross-training, and leadership programs to elevate cybersecurity professionals.

Acknowledgement and Rewards: Acknowledging and rewarding employees creates a culture of appreciation and motivates employees to continue executive performances that drive organizational success. Additionally, employees will remain loyal to the company, therefore retaining employees in the security department. Acknowledgement and rewards have many forms, such as public recognition, performance bonuses, and increased responsibility (Perkbox, n.d.).

Employee Departure

Exit interview: Conducting exit interviews gives the employee an opportunity to provide feedback on any issues within the company, as it will be beneficial to consider the reason(s) and make adjustments to improve employee retention.

Offboarding process: Robust security practices such as revoking access, device restoration and wiping, password reset, account activation, data transfer, and retention are important when former security employees exit the company, as it poses a significant threat to the organization's data and reputation (Haag, 2025). These practices are mandatory and should be the offboarding process of organizations.

Security Position Job Posting

Job Posting: Security Software Engineer

Company: Square Incorporated

Location: Oakland, California

Position: Full-time

About Square Inc.

Square Inc. is one of the leading financial technology companies that provides financial services and business solutions to customers globally. Square assists retailers in operating and expanding their businesses with its commerce options, such as software and banking services.

Job Description

As a Security Software Engineer, you will be responsible for developing highly effective systems that provide secure, flexible, and dependable authentication and authorization throughout the company, including Block's internal environment and addressing the requirements of all merchandise (Block Inc., 2025). You will work and report directly to the Information Security Manager, as they will provide guidance, support, and oversight.

Key Responsibilities:

- Conduct sophisticated initiatives pertaining to identification and access.
- Enhance and extend our fundamental systems within Square's framework settings while emphasizing reliability and security.
- Develop exceptional, thoroughly validated code in accordance with engineering standards.
- Prevent production delays caused by technological difficulties by promptly identifying and resolving them.
- Engage in design evaluations and offer constructive criticism to your fellow employees.
- Give informed technical choices while evaluating commercial implications and trade-offs.
- Cooperate with interdisciplinary teams to provide security measures (Block Inc., 2025).

Qualifications:

- Bachelor's degree in information technology, computer science, computer engineering, computer programming, software engineering, cybersecurity network technology, electrical engineering, math, or a similar field.
- 4+ years of experience in software engineering.
- Relevant certifications such as Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH), and CompTIA Security + are required.
- Eager to learn and expand your career in identity, security, and framework.
- Interested in learning that drives you to identify vulnerabilities in a complex system and undertake requisite measures to resolve them.
- The capability to withstand complicated circumstances, including various aspects such as size, unpredictability, and interrelation.
- Experience using AI platforms, security tools, or IT architectures to resolve security issues is a want but is not mandatory (Block Inc., 2025).

How to Apply:

Candidates should submit their resume and a cover letter to the company's careers website. Please make sure to include “Security Software Engineer” in the subject field. Qualified candidates will be invited to participate in a multiple interview process.

Benefits:

- Location-based salary
- Remote work
- Flexible schedules
- Paid Time Off

- Health Insurance
- 401(k) plan
- Career development and training programs.
- Positive work environment and dedicated teamwork (Block Inc., 2025).

Security Awareness and Education Plan

A security awareness and education program is essential in building an organization's first line of defense: its people. While firewalls and endpoint protection solutions are critical, they will not protect a human from clicking a phishing link. As cyber threats continue to evolve, especially in frequency, organizations must equip their workforce with the knowledge and vigilance necessary to protect digital assets and maintain compliance.

According to KnowBe4's 2022 research, consistent communication and education efforts increased employee cybersecurity awareness by 84% and significantly reduced the number of breaches. This highlights the importance of adopting a proactive, engaging, and data-driven approach to security training.

The elements of the awareness and education program include:

- Simulated Phishing Campaigns: KnowBe4's phishing simulations will be deployed weekly to assess real-world reactions and reinforce recognition of phishing attempts. KnowBe4 sends simulated phishing emails.
- Self-Paced Learning Modules: Employees will complete quarterly cybersecurity modules via the company's training portal.

- Monthly Security Tips: Advice and news delivered via email and internal channels that is focused on recent security issues and best practices.

The communication techniques include:

- Screensavers and System Messages: Short reminders on good security practices will appear on lock screens and login banners (National Institute of Standards and Technology, 2003).
- Web-Based Training Sessions: Interactive and engaging training will be deployed through KnowBe4.
- Organization-Wide Emails: Regular announcements from the CISO will highlight threats or policy changes (National Institute of Standards and Technology, 2003).
- Internal: A centralized resource center where employees can access policies, tips, and FAQs.

Key themes and topics:

- Phishing Awareness: How to spot suspicious emails, texts, and links (Talmi, 2024).
- Social Engineering Tactics: Understanding manipulation tactics, including baiting and tailgating. Emphasis on a “Never trust, always verify” approach (Talmi, 2024).
- Remote Work Security: Reinforcing VPN usage, endpoint protection, and safe Wi-Fi practices, especially when working in a public space (Talmi, 2024).
- Password and Authentication Best Practices: Promoting strong, unique passwords and the use of multifactor authentication (MFA), aligned with Square Inc.’s organizational policy (Talmi, 2024).

- Physical Security Protocols: Locking screens and securing mobile devices to avoid physical breaches (Talmi, 2024).

Schedule of the Communications and Training:

- Weekly: Simulated phishing emails targeting different departments, tailored to job function.
- Monthly: Security tips and updates via email and intranet.
- Quarterly: Formal training modules covering new threats, compliance requirements, and best practices.
- Annually: A full program review and update of training content.

Creators, distributors, and audience of the training:

- Creators- Executive Management, Security Team, and Systems Team will need to collaborate on budget, content, and implementation.
- Distributors- Deploying screensavers, login banners, and system messages by the Systems team. Launching KnowBe4 modules and phishing campaigns will be done by the Security team. The CISO will communicate organization-wide updates.
- Audience- No exceptions. All employees will partake in the training.

Measurement of Impact:

- Quiz Results: Each module ends with a knowledge assessment. Employees scoring below 80% must retake the module and will be flagged for further training or email simulations.
- Phishing Simulation Metrics: KnowBe4 will track click rates, report rates, and repeat offenders. Those who click on simulated phishing links will receive immediate feedback and follow-up training.

- Dashboard: Quarterly and annual reports, based on quiz results and simulations, will be shared with leadership to display training completion rates, trends, and areas of risk.

Security Newsletter

ISSUE
01
JULY
2025

Monthly Security Newsletter

Recent Security Risks and Tips

Did you know?

According to an assesment conducted by the Cybersecurity and Infrastructure Security Agency, 84% of employees clicked on a malicious link sent to their emails. Additionally, only 13% of employees reported phishing emails.

Tips to Remain Secure:

1. Check for suspicious sender information.
2. Check for typos in the email.
3. If you don't recognize the sender, report it.

Phishing Attacks

Phishing attempts are on the rise and Square is a target. These attacks start with an email that looks legitimate but contains a malicious link. Click that link, and you could unknowingly download malware that gives cybercriminals access to your device and our systems.

What to watch for:

- The email may look like it's from a coworker, vendor, or even leadership.
- It might urge you to click a link, download a file, or verify account details.
- If it slips past our email filter, it may land right in your inbox instead of Junk.

What to do:

- Don't click suspicious links or download unexpected attachments.
- If an email seems off, don't interact with it.
- Submit a ticket to the IT Support Desk and report the message as suspicious.

Our team will handle the rest with investigating, quarantining, and blocking future attempts. But your vigilance is our first line of defense.

Thanks for helping keep Square secure.

Square Inc

Budget

Category	Specific	Cost (per year)
Staff		
	CISO	$200,000
	SOC Manager	$120,000
	SOC Analysts x 10	$850,000
	Incident Response Team x 5	$400,000
	GRC Manager	$120,000
	Risk Assessment Specialist x 1	$75,000
	CTO	$200,000
	Application Security Manager	$120,000
	Infrastructure Security Manager	$120,000
	Network Security Analysts x8	$640,000
	Security Awareness Manager	$120,000
	Training Coordinator x 1	$65,000
Hardware		
	Network Security Appliances (including VPN)	$180,000
Software		
	EDR	$144,000
	NDR	$40,000
	SIEM	$75,000
	IDS	$15,000
	Training	15,000
Other		
	Auditing (Compliance or Penetration Testing)	80,000
Budget =		$3,579,000

Conclusion

A strong security plan is critical to protecting an organization. Square's cybersecurity strategic plans focus on aligning security initiatives with overall business needs by integrating security metrics, a business continuity plan, an incident response plan, and an education framework. These components build trust between stakeholders, maintain regulatory compliance, and reinforce customer confidence in Square's ability to safeguard their data and ensure

continuous service availability. The plans follow standards established by NIST, ensuring that Square's practices not only align with industry-specific regulations such as PCI DSS and GDPR, but also remain adaptable as threats evolve. Each initiative upholds the core principles of the CIA triad -confidentiality, integrity, and availability -by securing sensitive data, maintaining its accuracy, and ensuring reliable access to services.

Even with plans like these in place, companies continue to fall victim to cyberattacks. Often, these strategies are not properly implemented. Technology changes rapidly, and security plans must evolve just as quickly. Many organizations also overlook consistent employee training and fail to regularly test their systems, creating vulnerabilities. To successfully implement a strong security posture, support from the business is essential. Budgetary flexibility is necessary to deploy and maintain key elements, including the hot site continuity strategy, critical IT infrastructure, and security awareness campaigns. Executive support is also crucial for enforcing policies and ensuring alignment across all departments.

Everyone in the organization has a role to play in maintaining security, whether it's recognizing a phishing email, practicing good password standards, or adhering to access control protocols. Cybersecurity is not the sole responsibility of the IT or security departments; it must be a company-wide effort. With the right investment, executive leadership, cultural mindset, and strategic alignment, Square is positioned not just to defend against threats but to lead with security and trust.

References:

Atlassian. (n.d.). *Security measures*. Atlassian. Retrieved from https://www.atlassian.com/legal/security-measures#intro

Block Inc. (2025, July 1). Security Software Engineer, Identity Infrastructure. Retrieved from https://block.xyz/careers/jobs/4790781008?gh_src=84b43d668us

BlueVoyant. (n.d.). *Incident response process: The 6 steps and how to test they work*. BlueVoyant. Retrieved from https://www.bluevoyant.com/knowledge-center/incident-response-process-the-6-steps-and-how-to-test-they-work/

Cybersecurity and Infrastructure Security Agency. (n.d.). *Report ransomware*. CISA. Retrieved from https://www.cisa.gov/stopransomware/report-ransomware/

Federal Bureau of Investigation. (n.d.). Ransomware. FBI. Retrieved from https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/ransomware/

Gaona, J. G. (2024, April 30). *17 Essential Skills For Cybersecurity Success*. Marymount University. Retrieved from https://marymount.edu/blog/essential-skills-for-cybersecurity-success/

Haag, K. (2025, June 11). Security best practices when an employee leaves - Entre Technology Services. *Entre Technology Services*. Retrieved from https://www.entremt.com/security-best-practices-when-an-employee-leaves/

Indeed. (2025, March 26). How to Become a Security Software Engineer.

Retrieved from https://www.indeed.com/career-advice/finding-a-job/how-to-become-security-software-engineer#:~:text=They%20build%20software%20security%20systems,security%20breaches%20within%20the%20system

KnowBe4. (2022, June 20). KnowBe4 research finds increased frequency of security awareness training improves the prevention of security breaches [Press release]. KnowBe4. Retrieved from https://www.knowbe4.com/press/knowbe4-research-finds-increased-frequency-of-security-awareness-training-improves-prevention-of-security-breaches/

Liddle, A. (2025, July 2). *Your ultimate guide to cybersecurity certifications*. Cybersecurity Guide. Retrieved from https://cybersecurityguide.org/programs/cybersecurity-certifications/

Luna, C. D. (2024, November 5). *6 Best Cybersecurity training for employees in 2025*. eSecurity Planet. Retrieved from https://www.esecurityplanet.com/products/cybersecurity-training/

National Institute of Standards and Technology. (2003, October 1). Building an information technology security awareness and training program (NIST Special Publication 800-50). U.S. Department of Commerce. Retrieved from https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-50.pdf

Perkbox. (n.d.). *Why is Employee Recognition Important? | Perkbox*. Retrieved from

https://www.perkbox.com/au/guide/employee-recognition/benefits

S, H. (2025, June 18). *Internal recruitment: The smart HR strategy for retention, growth, and culture*. CultureMonkey.

Retrieved from

https://www.culturemonkey.io/employee-engagement/internal-recruitment/

SecurityScorecard. (2024, January 2). *20 cybersecurity metrics & KPIs to track in 2025*.

SecurityScorecard. Retrieved from

https://securityscorecard.com/blog/9-cybersecurity-metrics-kpis-to-track/

SHRM. (2024, May 15). *Complete employee Onboarding guide*. Retrieved from

https://www.shrm.org/topics-tools/topics/onboarding

SOCRadar. (2024, November 20). *Top 10 metrics every CISO track for better security*.

SOCRadar. Retrieved from

https://socradar.io/top-10-metrics-every-ciso-track-for-better-security/

Sterling, J. (2020, August 23). *Key players in your cyber incident response plan*. Usherwood.

Retrieved from

https://www.usherwood.com/blog/key-players-in-your-cyber-incident-response-plan

Swanson, M., Bowen, P., Phillips, A., Gallup, D., & Lynes, D. (2010). *Contingency planning guide for federal information systems* (NIST Special Publication 800-34 Rev. 1). National

Institute of Standards and Technology. Retrieved from

https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-34r1.pdf

Talmi, Y. (2024, March 18). 14 Cybersecurity awareness topics you need to cover. CybeReady. Retrieved from https://cybeready.com/cybersecurity-awareness-topics/

Tech Interview Handbook. (2025, July 10). *Software Engineer interviews: Everything you need to prepare*. Tech Interview Handbook. Retrieved from https://www.techinterviewhandbook.org/software-engineering-interview-guide/

Techneeds. (2025, January 12). *Best Practices for External Methods of Recruitment: Proven Strategies for Success*. Techneeds. Retrieved from https://www.techneeds.com/2025/01/12/best-practices-for-external-methods-of-recruitment-proven-strategies-for-success/

Whiteman, M., & Mattord, H. (2019). Chapter 10: Planning for Contingencies. In *Information Security:Management of Information Security* (6th ed.). Cengage Learning, INC.