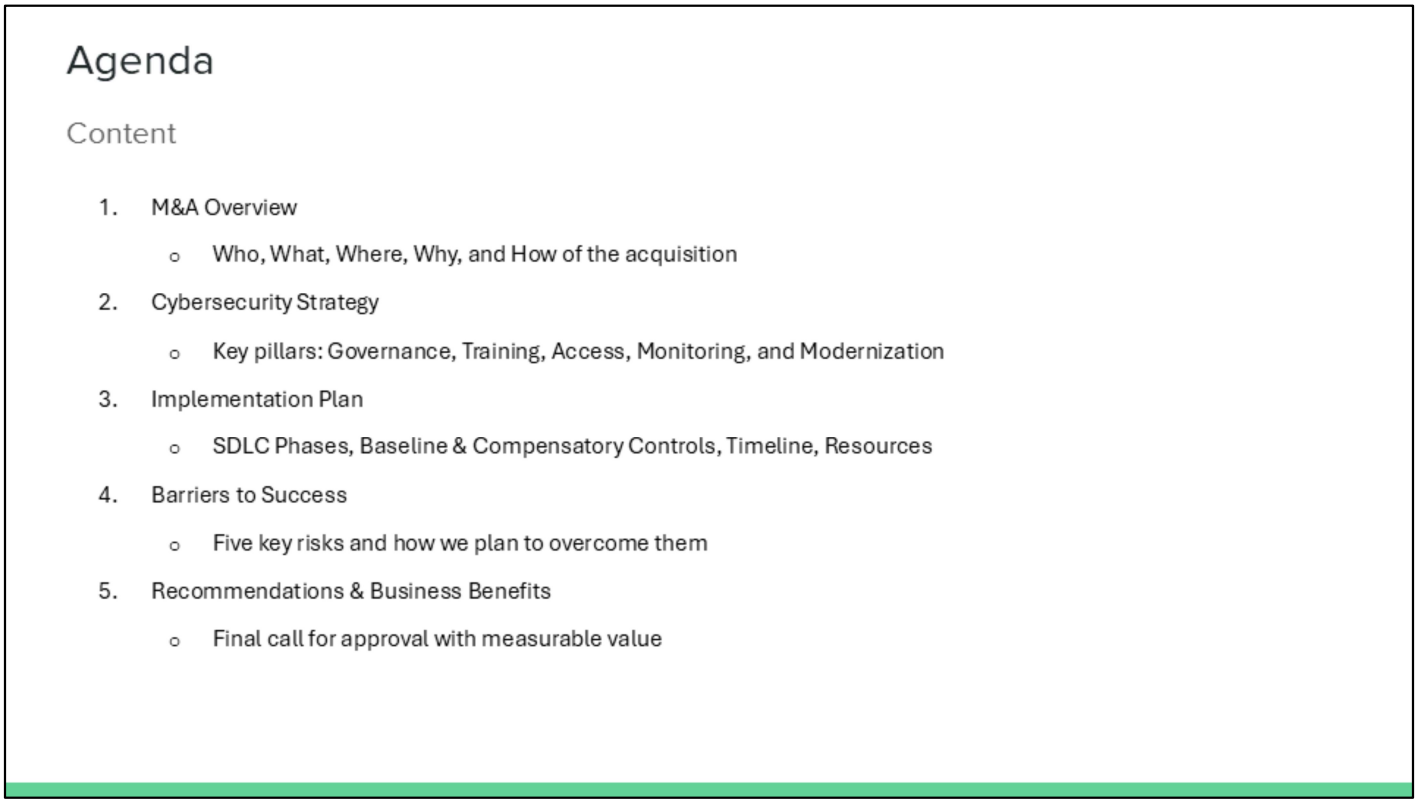
Padgett-Beale M&A Cybersecurity Strategy

Edison Maniwang
University of Maryland Global Campus
CSIA 485 Cyber Management and Policy Capstone
Professor Holly Ridgeway
May 4th, 2025

Good [morning/afternoon], members of the Board. My name is Edison Maniwang, and I'm pleased to present the cybersecurity strategy developed to support the acquisition of Island Banking Services. This strategy was created to ensure Padgett-Beale Financial Services can operate securely, meet regulatory expectations, and maintain the trust of customers and stakeholders. Today's presentation will walk you through the business context, our proposed cybersecurity framework, implementation steps, identified risks, and the strategic value this plan delivers. I look forward to your feedback and hope to gain your support for implementation.



In this presentation, we'll cover six key sections, starting with an overview of the merger and acquisition — answering who was involved, what assets were acquired, where operations will be held, why the acquisition took place, and how the new operations will unfold. Next, I'll walk you through our cybersecurity strategy, which is structured around five core pillars to address inherited and potential vulnerabilities. Then, we'll move into the implementation plan, which follows the System Development Life Cycle and includes detailed security controls, scheduling, and resource allocation. We'll identify the top five barriers that could threaten the success of this plan and present compensatory measures for each. Finally, I'll conclude with a summary recommendation supported by the business benefits we expect to achieve.

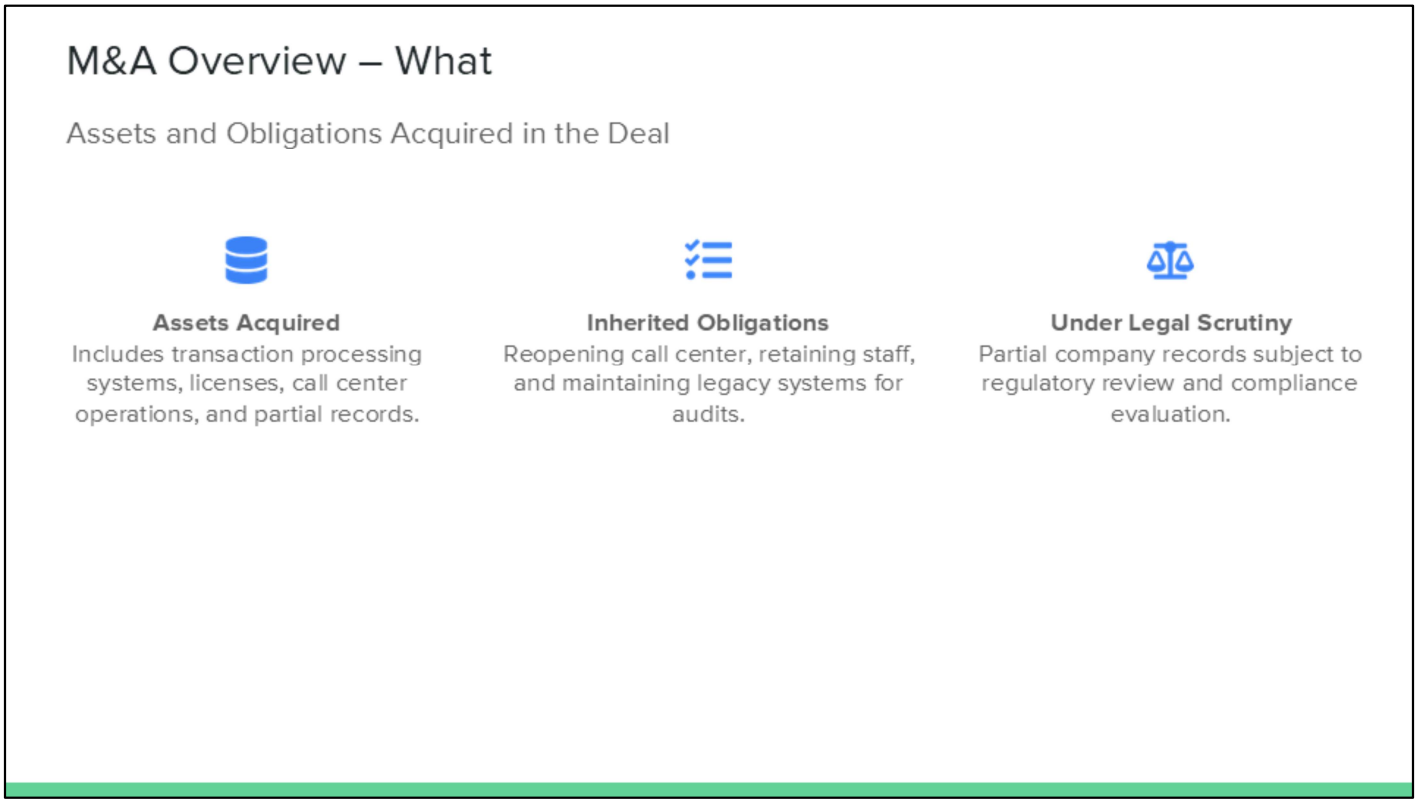
M&A Overview – Who

Identifying the Key Players in the Acquisition

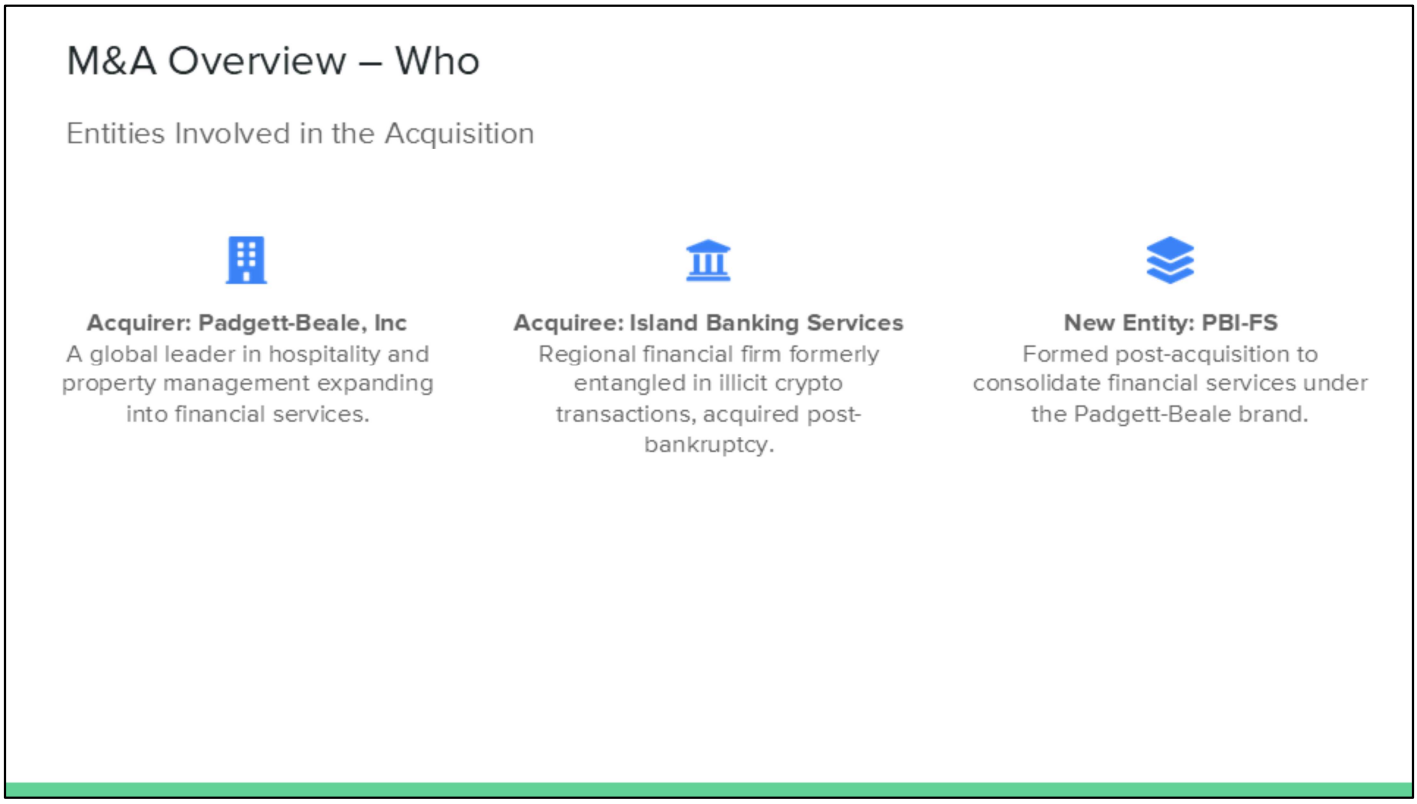
- **Acquirer: Padgett-Beale, Inc:** Global hospitality and property management enterprise expanding into fintech.
- **Acquiree: Island Banking Services:** Regional financial services firm with a checkered past in crypto compliance.
- **New Entity: Padgett-Beale Financial Services (PBI-FS):** Hybrid financial division combining hospitality expertise with digital finance.

Photo by Amy Hirschi on Unsplash

- At the heart of this acquisition lies a bold strategic maneuver. Padgett-Beale, known globally for its hospitality and real estate operations, steps into the fintech arena with the acquisition of Island Banking Services. This firm, while once mired in regulatory concerns over crypto transactions, brings valuable financial systems and infrastructure to the table.
- By forming Padgett-Beale Financial Services—or PBI-FS—the goal is clear: to merge Padgett-Beale's operational excellence with modern financial service capabilities. This blend aims not just at diversification but at transforming the very nature of customer engagement and business scope.
- Understanding who is involved gives us a lens into the strategy and intent behind this M&A. It's a calculated leap into a regulated, high-growth space, driven by legacy strength and a vision for innovation.



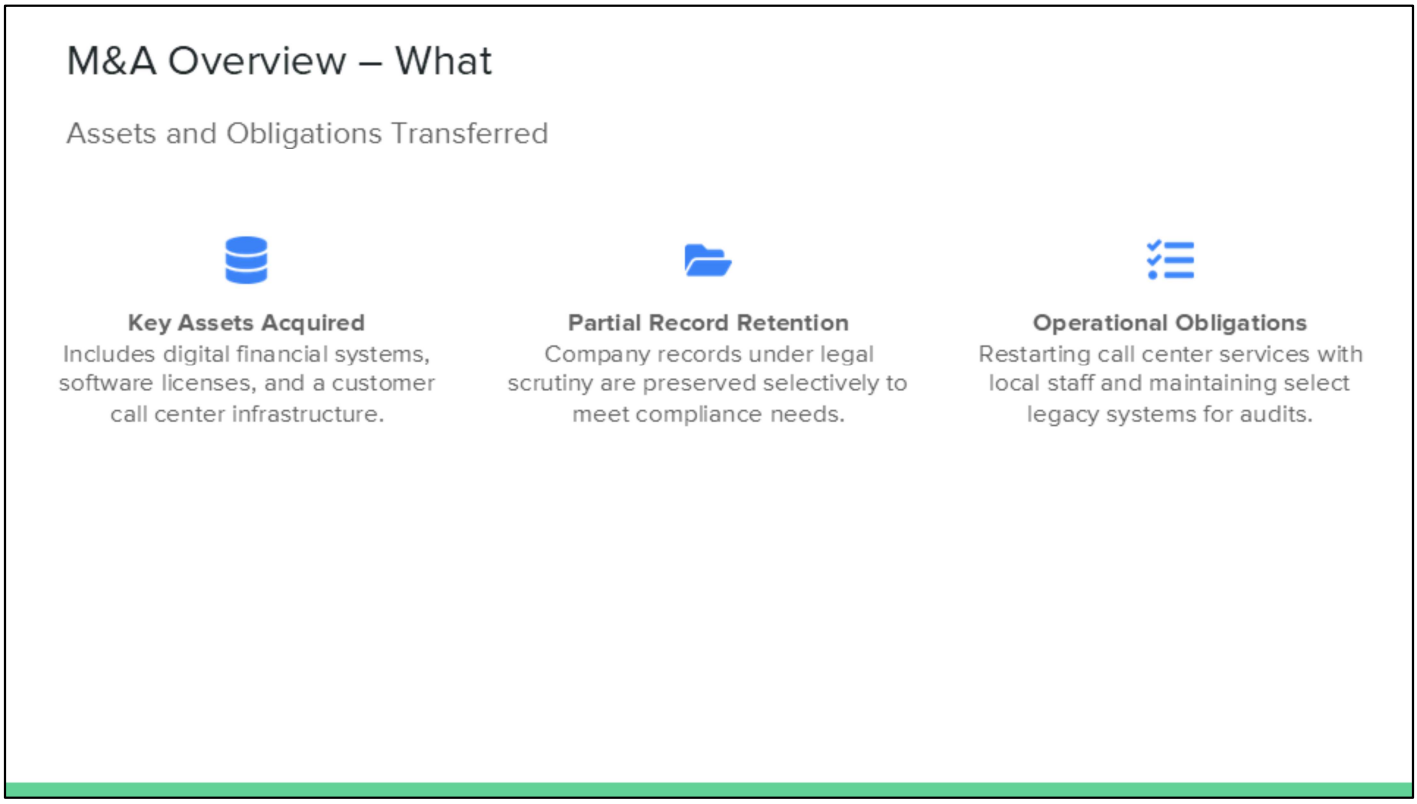
- The scope of the acquisition goes beyond traditional financial assets. Padgett-Beale has secured critical IT infrastructure, including financial transaction processing systems and operational licenses. These components lay the foundation for PBI-FS to rapidly re-enter the market.
- However, the deal also includes obligations that must be addressed proactively. These include reopening the call center on the island with retained staff and maintaining some legacy systems, not for function, but for audit and regulatory transparency.
- One of the more complex components involves partial company records that remain under legal review. This raises immediate governance and compliance challenges that will need to be addressed in the cybersecurity strategy. The acquired assets are valuable, but they come with baggage that must be responsibly managed.



- This slide outlines the principal entities involved in the strategic acquisition. Padgett-Beale, Inc., a global hospitality conglomerate, leads the acquisition as part of a diversification initiative. They are leveraging their operational sophistication to expand into the high-margin financial sector. The target of the acquisition, Island Banking Services, is a regional player with a history that includes compliance challenges, particularly in the realm of crypto-finance. Despite its troubled past, its core financial processing capabilities and localized customer base present an undervalued opportunity.

- Post-acquisition, the merged operations are being rebranded as Padgett-Beale Financial Services (PBI-FS). This new entity will integrate Padgett-Beale's risk-managed governance with Island Banking's operational assets to launch a compliant, tech-forward financial services platform.

- This move sets the stage for vertical expansion and operational synergy, reflecting Padgett-Beale's ambition to broaden its portfolio beyond traditional hospitality assets.



- In this section, we examine the tangible and intangible components of the acquisition. Padgett-Beale has acquired Island Banking's core assets, which include sophisticated financial transaction systems and critical software and hardware infrastructure. These systems form the digital backbone of the future Padgett-Beale Financial Services (PBI-FS) platform.

- Moreover, the call center operation—once dormant—is set to be reactivated, utilizing retained local staff. This decision supports community ties and mitigates onboarding costs. Importantly, some records that may have legal implications will be selectively maintained in accordance with U.S. compliance standards, ensuring transparency while minimizing legal risk.

- Padgett-Beale has also committed to maintaining minimal legacy systems exclusively for audit purposes. These systems, while not ideal from a security perspective, are necessary for demonstrating historical continuity and compliance to regulators.

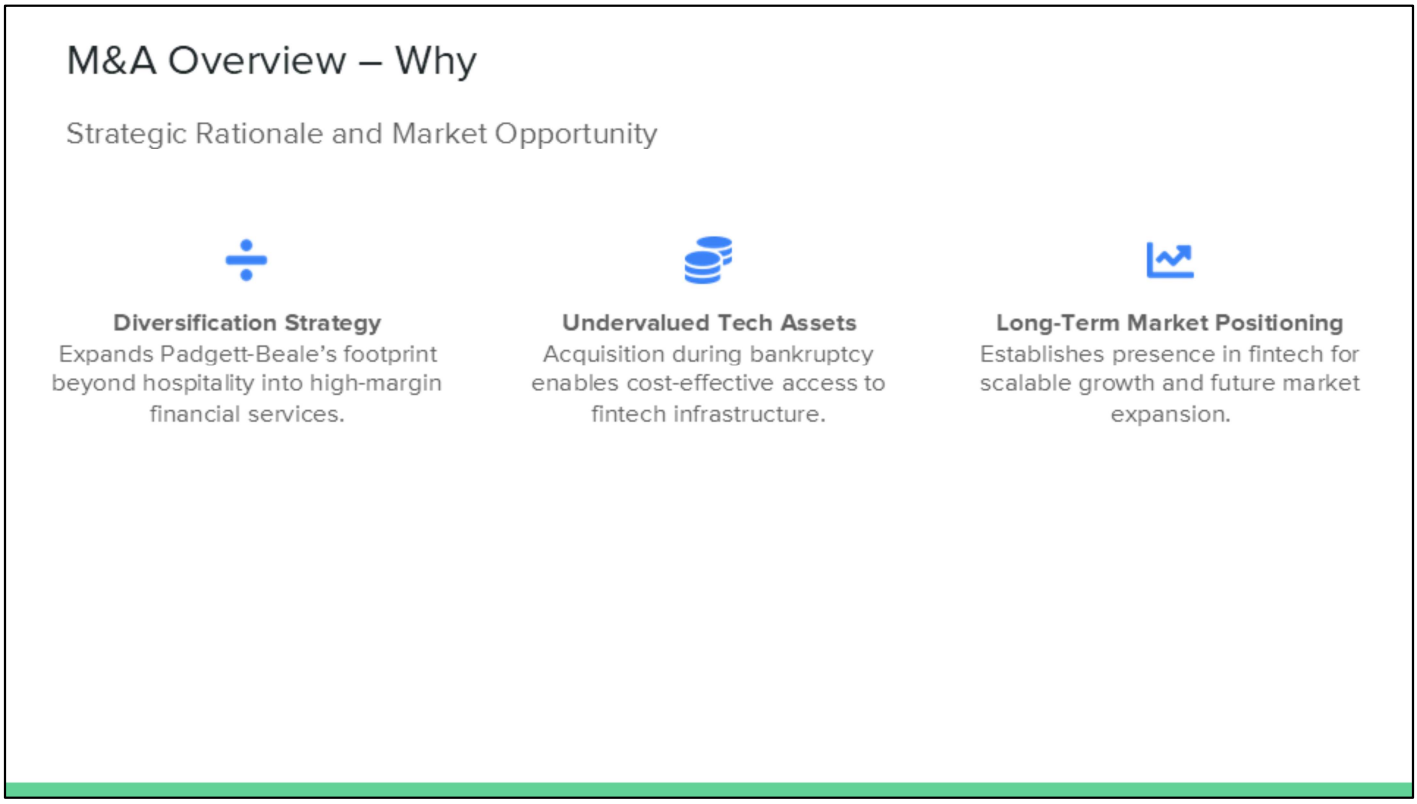
M&A Overview – Where

Operational Geography Post-Acquisition

- **Island-Based Call Center:** Physical operations for customer service will resume locally using existing infrastructure.
- **U.S.-Based IT & Security:** All data centers, IT functions, and cybersecurity operations will be housed within the United States.
- **Centralized Corporate Governance:** Executive oversight and compliance functions will remain at Padgett-Beale HQ in Delaware.

Photo by JM Photos on Unsplash

- The spatial distribution of operational responsibilities reflects both strategic intent and regulatory necessity. First, customer interaction remains local—Padgett-Beale will restore the Island Banking call center, offering continuity for regional clients and stabilizing the workforce. This decision also ensures culturally competent service and leverages existing facility investments.
- Conversely, all core IT functions—including data centers and security management—will relocate to the U.S. This shift is key for aligning operations with stricter U.S. data protection laws and centralizing cybersecurity oversight. Hosting these capabilities domestically reduces exposure to international data transfer risks and regulatory inconsistencies.
- Finally, executive governance and compliance oversight will be headquartered in Delaware, Padgett-Beale's corporate base. This centralization ensures that leadership has direct control over strategic direction, policy enforcement, and audit readiness—anchoring the new entity firmly within the U.S. legal and operational framework.



- Now let's turn to the strategic rationale behind the acquisition. Padgett-Beale, traditionally rooted in hospitality and real estate, is implementing a diversification strategy by entering the financial services domain. This move is designed not only to reduce dependency on its core sectors but also to tap into more stable and potentially higher-margin financial services.

- The timing of this acquisition is strategic. Island Banking Services was acquired post-bankruptcy, allowing Padgett-Beale to secure its technology stack and processing capabilities at a fraction of their original cost. These assets include both infrastructure and personnel that would be significantly more expensive under ordinary conditions.

- Moreover, this acquisition positions Padgett-Beale for scalable entry into the growing fintech space. By integrating legacy systems with modern cybersecurity controls, the firm can build a resilient and forward-looking financial platform that supports sustainable growth.

M&A Overview – How

Tactical Execution of Secure Integration

- **Secure Infrastructure Rebuild:** New architecture designed with zero-trust principles and compliance alignment.
- **U.S. Financial Law Compliance:** Adherence to GLBA, BSA, and SOX regulations from day one of operations.
- **CISO-Led Strategy:** Centralized cybersecurity governance under a newly appointed Chief Information Security Officer.

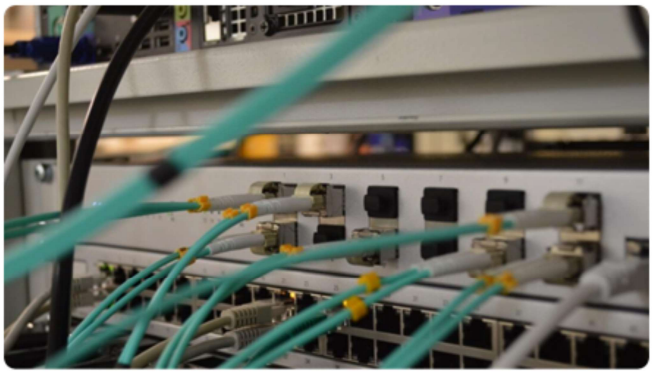


Photo by Thomas Jensen on Unsplash

- Executing this acquisition securely requires meticulous planning and compliance-driven architecture. First, Padgett-Beale will rebuild the technological infrastructure of Island Banking Services with a zero-trust design model. This includes strict access control, segmentation, and encryption protocols tailored to U.S. regulatory expectations.
- Second, the entire integration is shaped by legal frameworks such as the Gramm-Leach-Bliley Act (GLBA), the Bank Secrecy Act (BSA), and the Sarbanes-Oxley Act (SOX). These ensure that financial data handling, governance, and audit practices meet federal standards from the outset.
- Critically, this cybersecurity-driven transformation will be overseen by a newly appointed Chief Information Security Officer. This role consolidates strategic planning, risk oversight, and policy development under a single accountable executive, ensuring alignment with both business and compliance priorities.

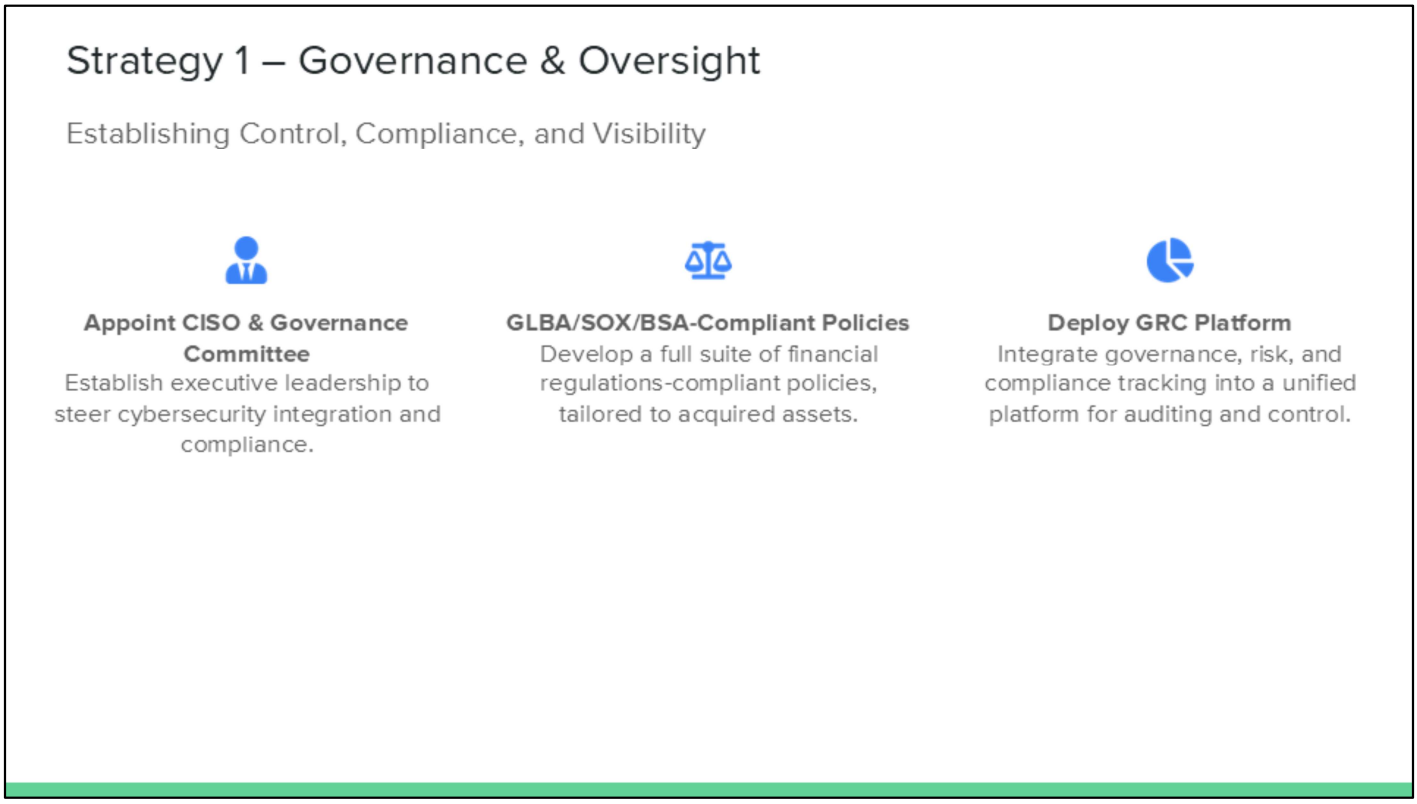
Cybersecurity Strategy Overview

Securing the Future of Padgett-Beale Financial Services

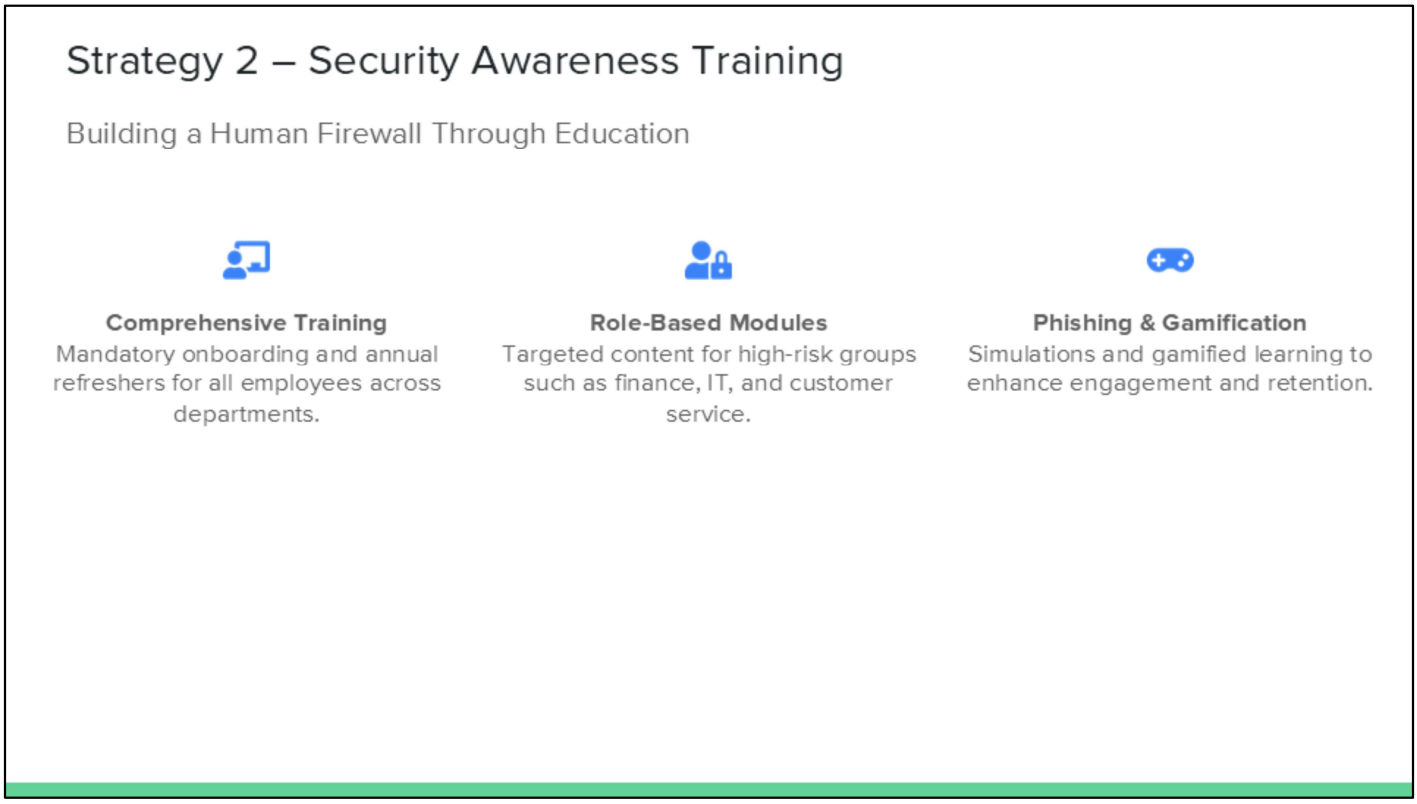
- **Cybersecurity Governance:** Centralized leadership, GRC integration, and policy enforcement across the organization.
- **Security Awareness & Training:** Company-wide annual training with role-specific modules and phishing simulations.
- **Access Control & Monitoring:** IAM solutions, centralized SOC, and real-time threat monitoring with SIEM/IDS.

Photo by Markus Spiske on Unsplash

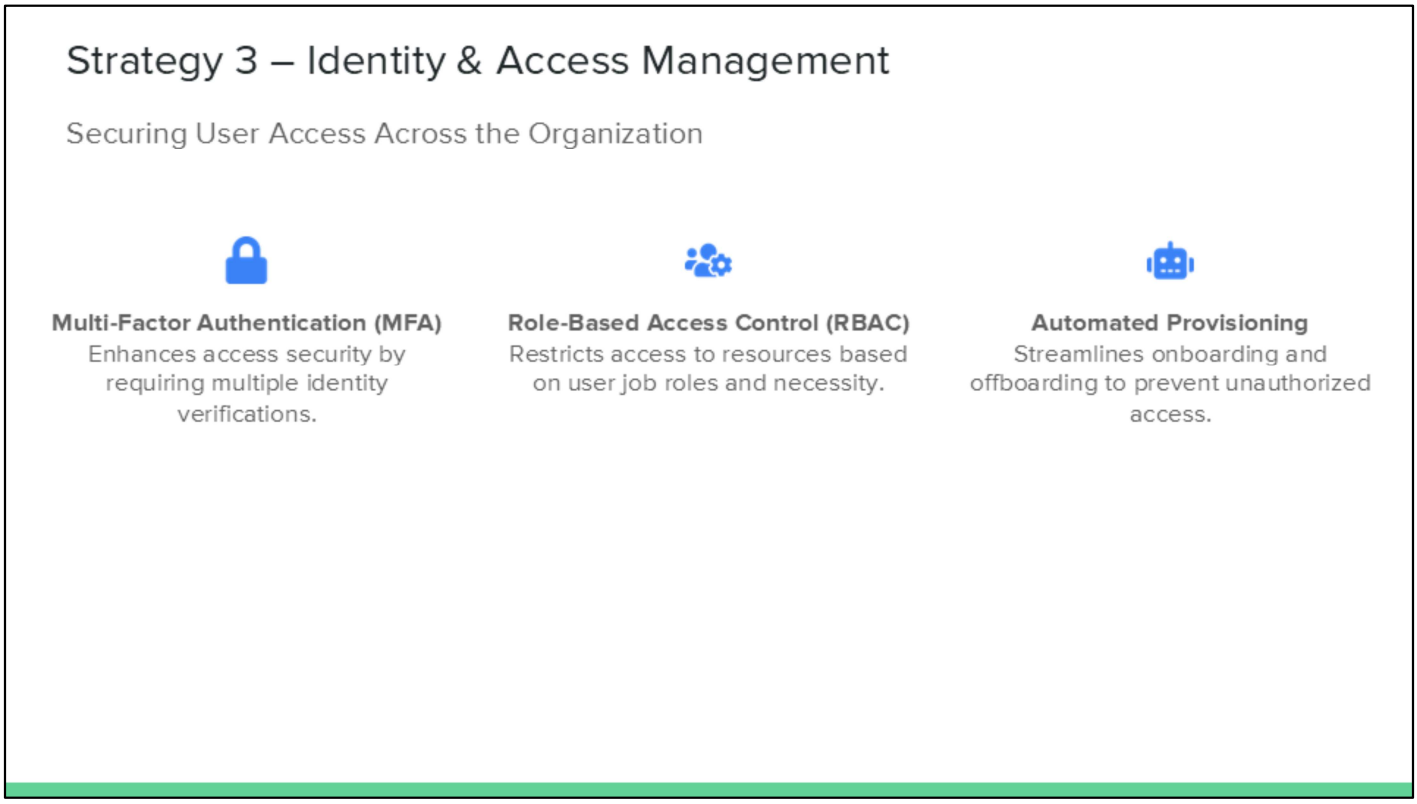
- The cornerstone of a secure integration for Padgett-Beale Financial Services is a layered, proactive cybersecurity strategy. This plan is not a bolt-on but a foundational component of the business model post-acquisition.
- First, governance is being redefined with the creation of centralized cybersecurity leadership and a Governance, Risk, and Compliance (GRC) platform. This ensures visibility across all risk domains, including financial and IT audits.
- Next, employee engagement through security awareness training is prioritized to reduce human error. This includes gamified simulations, phishing drills, and ongoing education—customized by role to reflect specific risk exposures.
- Finally, access is controlled through multi-factor authentication (MFA), role-based permissions, and constant network monitoring. The Security Operations Center (SOC) will employ both in-house analysts and potentially an MSSP for 24/7 incident readiness.
- This integrated model ensures regulatory alignment and operational resilience as the organization scales.



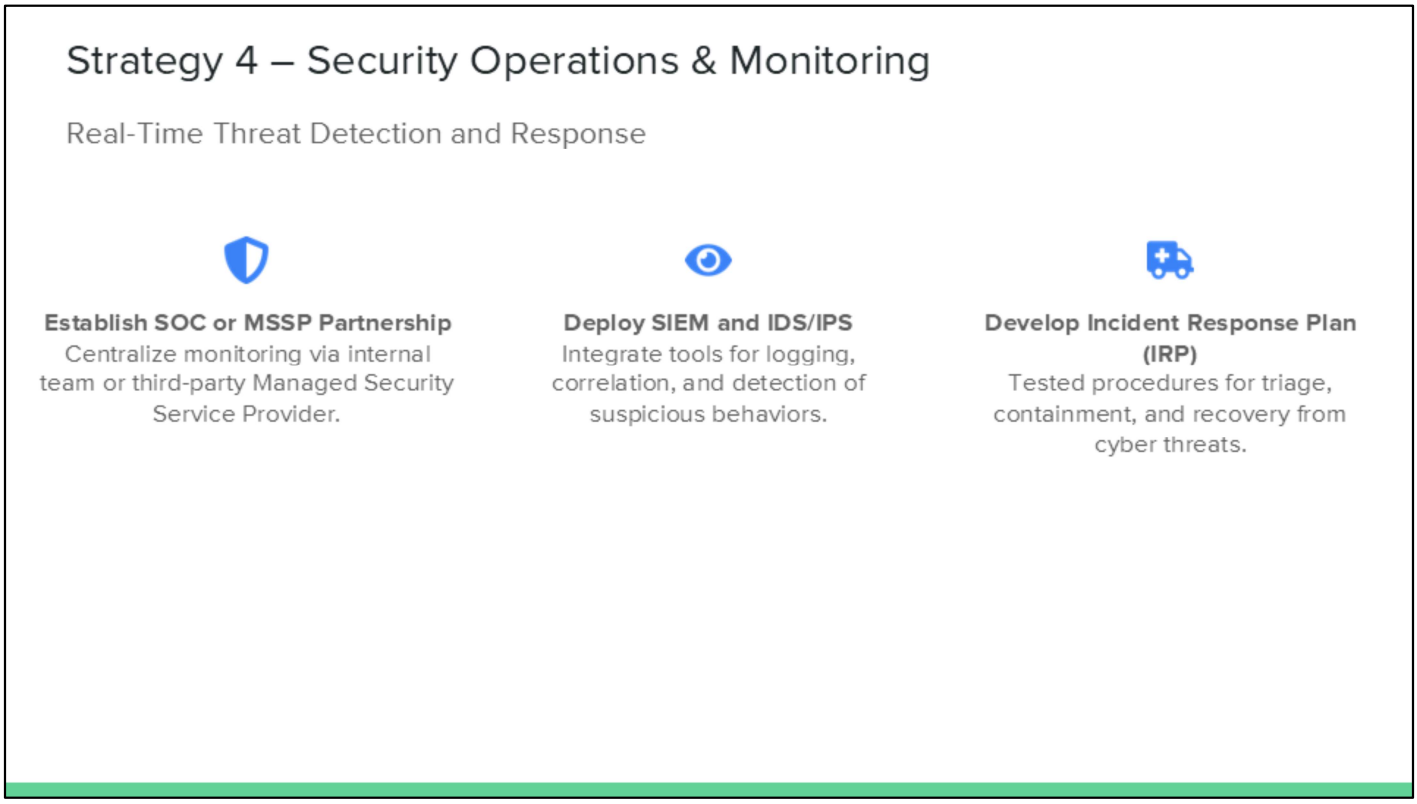
- The first strategic pillar—governance and oversight—builds the institutional control mechanisms necessary for secure operations. At the core is the appointment of a Chief Information Security Officer (CISO) and the formation of a Governance Committee. This leadership group ensures that cybersecurity priorities are aligned with both strategic and regulatory goals.
- One of their first tasks is to design and deploy security policies that comply with the Gramm-Leach-Bliley Act, Sarbanes-Oxley Act, and Bank Secrecy Act. These frameworks demand detailed documentation, risk assessments, and incident reporting structures to protect financial data.
- To streamline and enforce this compliance, Padgett-Beale will implement a GRC platform. This tool will centralize policy enforcement, track risk metrics, enable real-time control testing, and automate audit processes—giving leadership a continuous view of cyber risk posture and compliance status.



- One of the most important layers in any cybersecurity strategy is the human element. This strategy introduces a robust awareness training program, making cybersecurity part of the organizational culture from day one.
- First, all employees will receive onboarding training followed by mandatory annual updates. This ensures baseline awareness across departments regardless of role. The training content will be continuously updated to reflect evolving threats.
- Second, we'll deploy role-specific modules tailored to high-risk personnel—particularly those in finance, IT, and front-line customer support—who face elevated threat exposure. These modules focus on contextual risks and defensive behavior patterns.
- To increase participation and impact, phishing simulations and gamified learning will be implemented. These tactics have been proven to increase both engagement and long-term retention, making users not just aware but actively vigilant.



- Identity and Access Management (IAM) is central to securing the PBI-FS environment, ensuring the right people access only the information they need—and nothing more.
- First, Multi-Factor Authentication (MFA) is being mandated across all platforms, especially for remote access and high-privilege users. This reduces the risk of credential-based breaches, which account for a large percentage of modern attacks.
- Next, Role-Based Access Control (RBAC) ensures that employees can only access systems and data necessary for their responsibilities. This limits internal threat surfaces and simplifies compliance audits.
- Finally, automated provisioning tools will govern employee onboarding and offboarding, making sure that access permissions are swiftly updated with job changes. These IAM components are vital to preventing lateral movement and ensuring operational security during personnel transitions.



- Detecting and responding to threats in real time is critical to PBI-FS's cybersecurity maturity. The fourth strategic initiative centers on operational security.
- To begin, Padgett-Beale will either stand up an in-house Security Operations Center (SOC) or partner with a Managed Security Service Provider (MSSP) for 24/7 monitoring. Both approaches offer visibility across networks, systems, and endpoints.
- This setup will leverage SIEM (Security Information and Event Management) and IDS/IPS (Intrusion Detection and Prevention Systems) to aggregate logs, detect anomalies, and alert analysts. These technologies serve as the eyes and ears of the organization's security perimeter.
- Equally important is the formalization and testing of an Incident Response Plan (IRP). This document outlines containment and recovery procedures to ensure fast, coordinated action when an incident occurs—minimizing impact and accelerating return to operations.

Strategy 5 – Infrastructure Modernization

Rebuilding the Technical Foundation for Security

- **Legacy System Replacement:** Retire outdated or compromised infrastructure to reduce technical debt and attack surface.
- **Data Encryption Everywhere:** Utilize TLS for data in transit and AES-256 for data at rest.
- **Segmentation & Disaster Recovery:** Implement network segmentation by trust level and test DR protocols regularly.

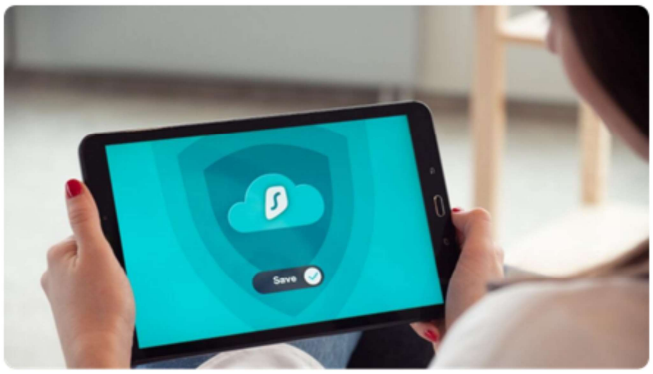
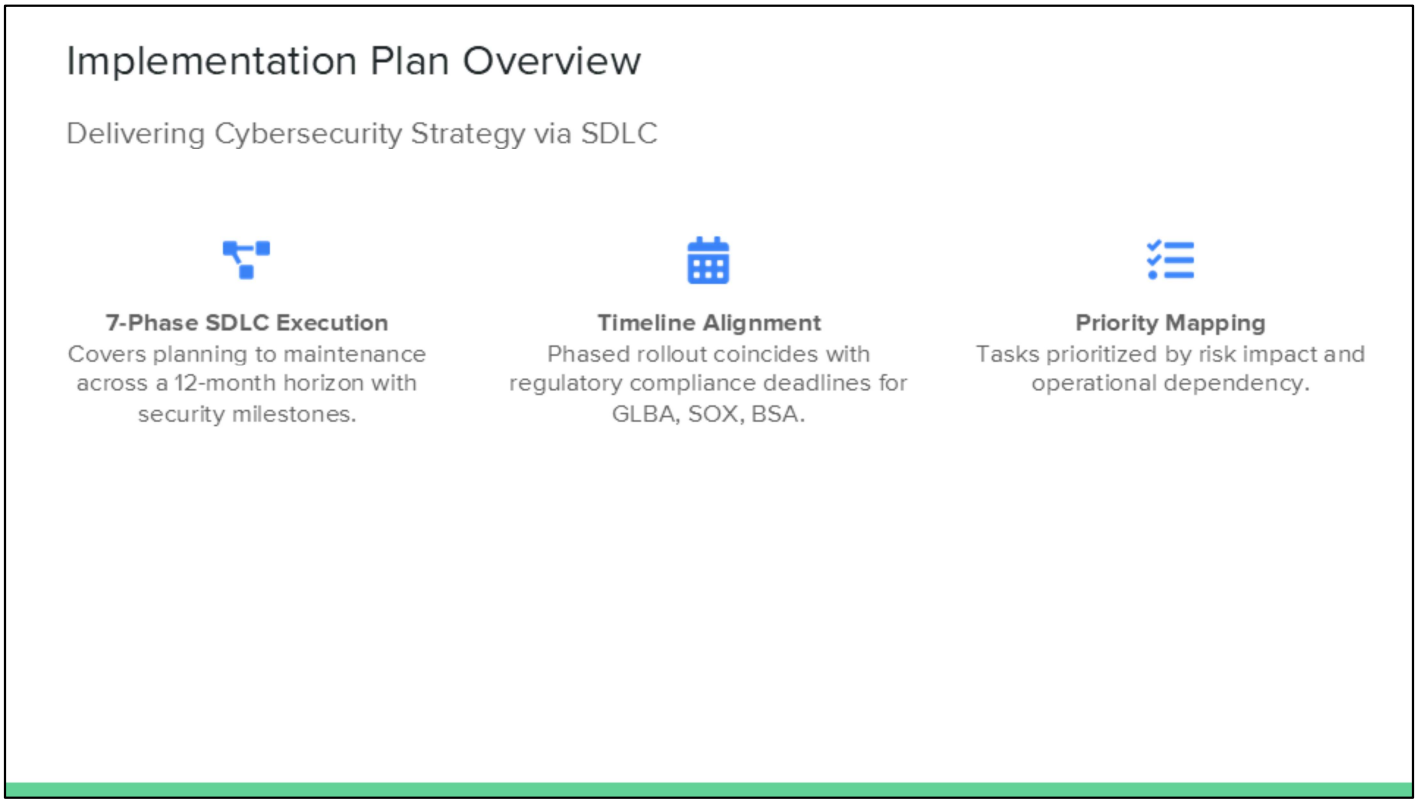


Photo by Dan Nelson on Unsplash

- The final strategy addresses infrastructure modernization—arguably the most technical yet essential component of the integration. Without a modern and secure foundation, no cybersecurity plan can endure.
- First, Padgett-Beale will retire all outdated or potentially compromised legacy infrastructure. These systems often contain unpatched vulnerabilities and outdated software, posing unacceptable risks. Their removal reduces the attack surface and prepares the way for secure modernization.
- Second, a robust encryption policy will be enforced. TLS (Transport Layer Security) will protect data in transit, while AES-256 encryption will be used for data at rest. These are industry best practices and align with federal financial regulations.
- Finally, the network will be segmented by department and trust level. This minimizes lateral movement in case of compromise. Disaster recovery capabilities will be tested rigorously, ensuring the organization can rapidly recover from system failures or attacks with minimal disruption.



- To transform strategic vision into operational reality, Padgett-Beale will use a 7-phase System Development Life Cycle (SDLC) model. This model structures the cybersecurity rollout from planning through to maintenance, ensuring methodical and trackable execution.
- The timeline is built around a 12-month window, deliberately aligned with compliance obligations under GLBA, SOX, and BSA. Each quarter introduces specific deliverables, from policy development to full system integration, allowing measurable progress and timely audit preparation.
- Tasks are further mapped to cybersecurity priority. High-risk or mission-critical items are addressed early, such as governance frameworks and access controls. Lower-priority tasks like modernization and fine-tuning are scheduled in subsequent quarters. This phased approach ensures business continuity while introducing new systems progressively and securely.

SDLC Phases Applied

Security-Integrated Software Lifecycle

- **Planning & Requirements:** Risk analysis, business alignment, and control definition based on compliance needs.
- **Design & Development:** Architect secure infrastructure and implement essential tools and platforms.
- **Testing to Maintenance:** Audit reviews, deployment execution, patching, and continuous monitoring.

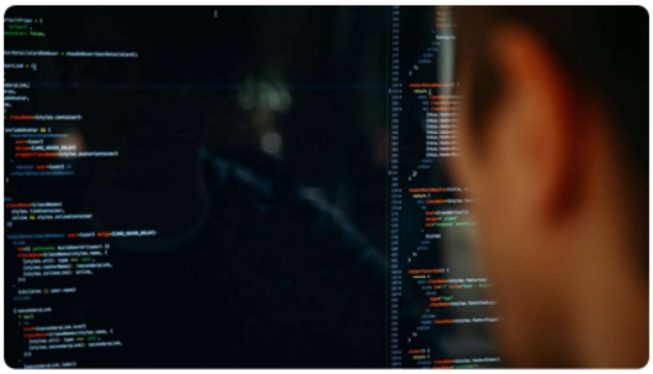
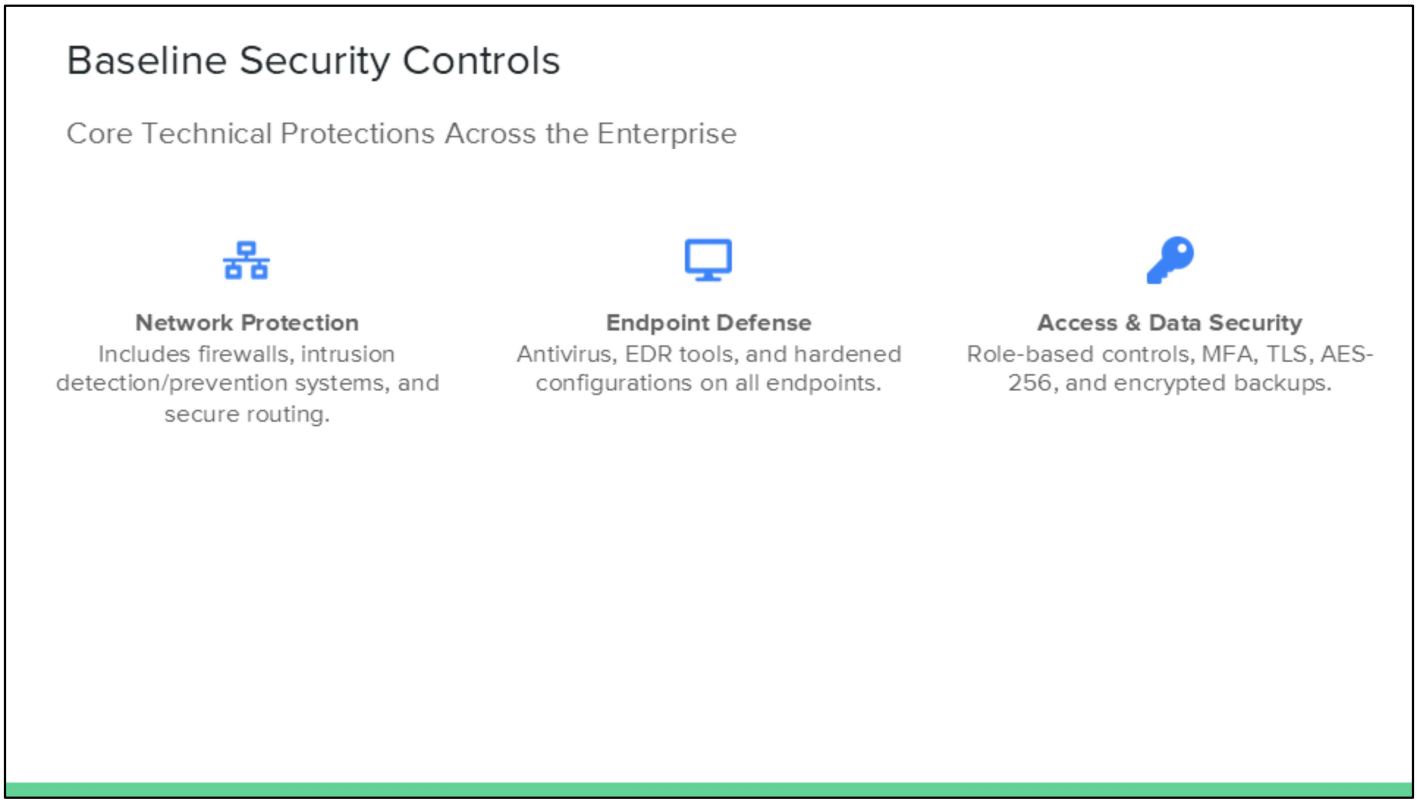


Photo by charlesdeluvio on Unsplash

- Let’s break down the applied SDLC phases that guide the implementation of the cybersecurity strategy. This model ensures structured and secure progress from initiation through full operational readiness.
- In the Planning and Requirements stages, the team performs a detailed risk analysis, maps controls to GLBA/BSA/SOX requirements, and ensures alignment with broader business objectives. These steps form the foundation of a defensible cybersecurity framework.
- During Design and Development, we create a secure system architecture and deploy foundational tools—such as SIEM, IAM, and encryption technologies. This is the operational core of the cybersecurity transformation.
- Finally, Testing, Deployment, and Maintenance ensure that systems function as intended. This phase includes simulations, audits, DR testing, and ongoing patching. Continuous monitoring is introduced during this phase to maintain a strong security posture as the business evolves.



- Baseline controls are foundational to any cyber defense posture. These are the must-have, non-negotiable technical protections that safeguard enterprise systems against the most common threats.
- On the network layer, Padgett-Beale Financial Services will deploy firewalls and IDS/IPS systems to filter and monitor incoming and outgoing traffic. Secure routers will establish segmented, policy-driven data flows, aligning with best practices under frameworks like NIST and CIS.
- For endpoints, all devices will receive hardened configurations, antivirus protections, and Endpoint Detection & Response (EDR) tools. These measures ensure that individual user devices do not become attack vectors into the broader environment.
- Access controls will be enforced through MFA and RBAC, while data integrity is protected using TLS encryption in transit and AES-256 at rest. All critical data will also be backed up securely and encrypted, reducing both breach and disaster recovery risks.

Compensatory Controls

Supplementing Gaps with Strategic Safeguards

- **Administrative Controls:** Policies, training, and nondisclosure agreements to guide and enforce secure behavior.
- **Operational Controls:** Physical access restrictions, change management protocols, and secure configurations.
- **Tactical Controls:** Advanced defenses like threat hunting, red teaming, and anomaly detection.

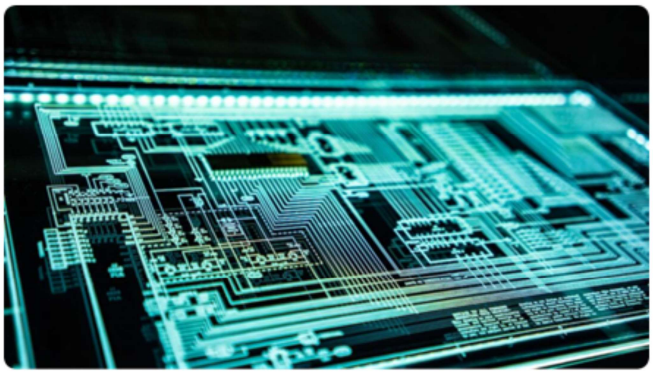


Photo by Adi Goldstein on Unsplash

- Compensatory controls are alternative safeguards deployed when baseline controls are insufficient or not feasible due to legacy constraints or operational risks. These controls are essential for adapting cybersecurity to real-world business conditions.
- Administrative controls form the first line, including detailed policies, employee security awareness programs, and legal instruments like nondisclosure agreements. These measures promote a culture of accountability and risk-conscious behavior.
- Operational controls manage the day-to-day realities of enterprise security. These include enforcing physical access restrictions to sensitive areas, controlling system changes via formal processes, and ensuring hardened system configurations are maintained across environments.
- Finally, tactical controls offer proactive, intelligence-driven defenses. This includes conducting regular threat hunts to detect stealthy adversaries, red teaming to test organizational readiness, and anomaly detection tools that surface deviations in network behavior. These layers collectively ensure that no single point of failure undermines the system.

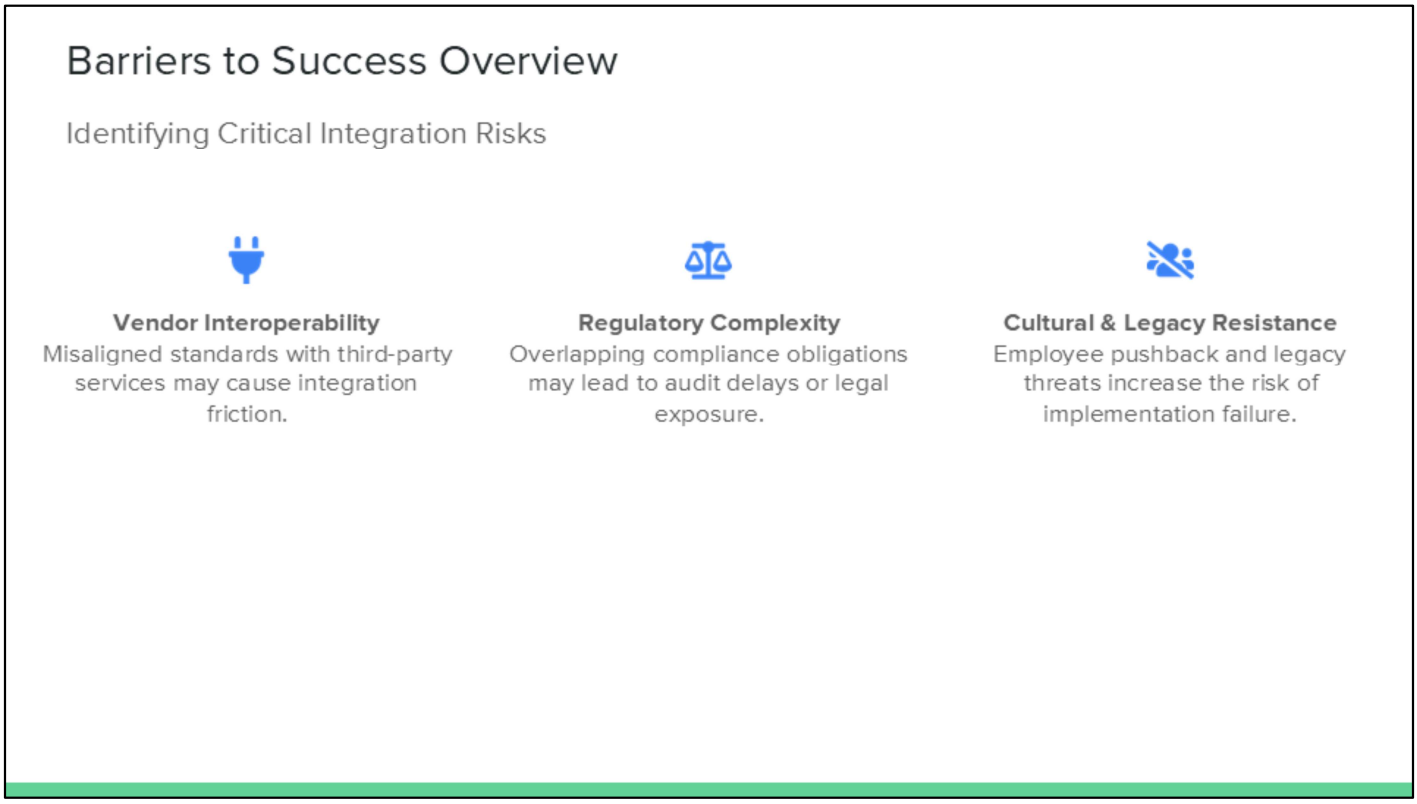
Timeline & Resource Estimates

Sequenced Execution and Budget Allocation

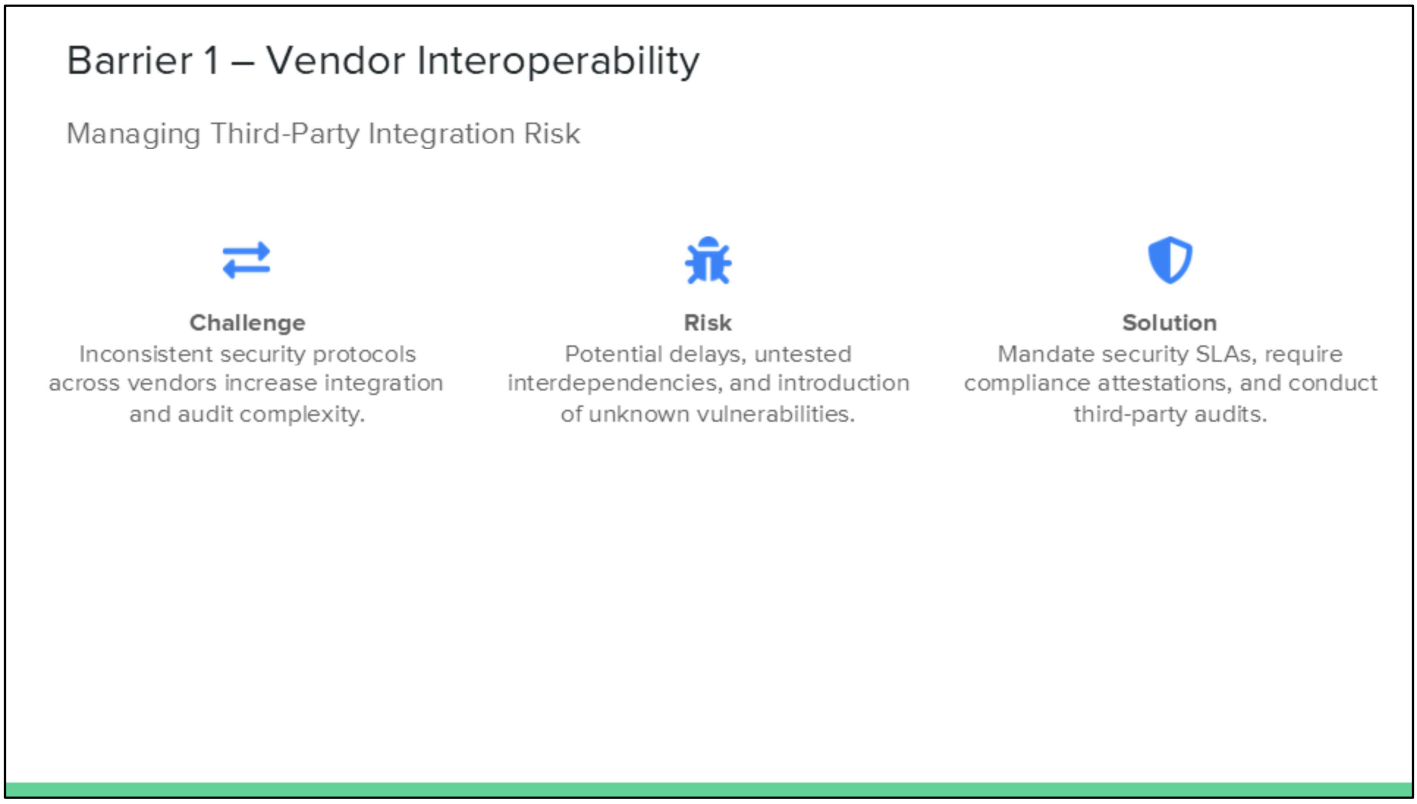
- **Quarterly Milestones:** Q1: Governance setup; Q2: Training/IAM; Q3: SOC/SIEM; Q4: Infra/DR testing.
- **Budget Forecasts:** Year 1: $1.09M total; Annual maintenance: $300K–$400K ongoing.
- **Personnel & Vendor Use:** Mix of internal staff and external MSSP/legal consultants ensures scalability.

Photo by Eric Rothermel on Unsplash

- An effective cybersecurity plan is only as strong as its execution—and that requires well-planned timelines and realistic budgeting. This slide outlines both the sequence and scale of the implementation effort.
- The timeline follows quarterly phases. Q1 will focus on governance and risk assessment; Q2 will deliver awareness training and IAM deployment; Q3 includes the SOC setup and SIEM rollout; and Q4 addresses infrastructure modernization and disaster recovery validation.
- In terms of budget, the Year 1 estimate stands at $1.09 million, covering capital expenses like hardware, software, consulting, and setup costs. Maintenance costs in future years are projected at $300K to $400K annually, covering updates, MSSP fees, and ongoing training.
- Execution will leverage both internal expertise and third-party support. This hybrid model maximizes institutional knowledge while scaling capacity via vendors for specialized services like GRC tools and SIEM operations.



- Even the most well-crafted cybersecurity strategy can falter if barriers to success aren't preemptively addressed. This slide presents the overarching risk categories likely to challenge the PBI-FS integration.
- First, third-party vendor interoperability poses significant hurdles. Legacy systems, especially those outside direct IT control, often operate under nonstandard protocols, making secure integration difficult. A lack of coordination can lead to delays and vulnerabilities.
- Second, the complexity of financial regulations—ranging from GLBA to SOX and BSA—can result in compliance fatigue. The burden of overlapping audit requirements increases the chance of nonconformance, fines, or reputational harm.
- Third, internal cultural resistance must be anticipated. Employees may resist new security controls such as MFA or policy-driven processes, while old infrastructure might harbor dormant threats. Change fatigue and misaligned incentives can derail otherwise strong policies.
- The following slides will explore each barrier in detail and propose mitigation strategies.



- Third-party vendors are both operational enablers and potential security liabilities. In this acquisition, Island Banking's legacy vendor ecosystem introduces a wide range of security and interoperability risks.
- The core challenge is inconsistency. Vendors may use outdated encryption protocols, insufficient authentication practices, or lack formal incident response standards. These misalignments can delay integration, complicate compliance audits, and leave exploitable gaps.
- The associated risks include delayed system rollouts, compatibility failures, and inadvertent exposure of sensitive data due to unaligned security baselines.
- To mitigate these issues, Padgett-Beale will enforce binding security SLAs for all vendors, require up-to-date compliance attestations (e.g., SOC 2, ISO 27001), and perform recurring security audits. These measures help establish a defensible and transparent third-party security posture.

- Operating within the U.S. financial regulatory framework requires constant attention to overlapping legal requirements. GLBA, SOX, and BSA all impose distinct yet intersecting mandates on data governance, audit trails, and financial reporting.
- This overlap can lead to duplicated efforts, documentation fatigue, and audit inconsistencies—especially during transitional periods like mergers. Each law has unique reporting thresholds and enforcement bodies, increasing the risk of inadvertent noncompliance.
- The business risks here include regulatory fines, loss of license, reputational damage, or prolonged audit disruption. These outcomes could delay product launches and erode stakeholder trust.
- Padgett-Beale will mitigate these risks through a dual approach: deploying a Governance, Risk, and Compliance (GRC) platform for automated policy management and control testing, and contracting legal compliance advisors to interpret regulatory nuances during integration.

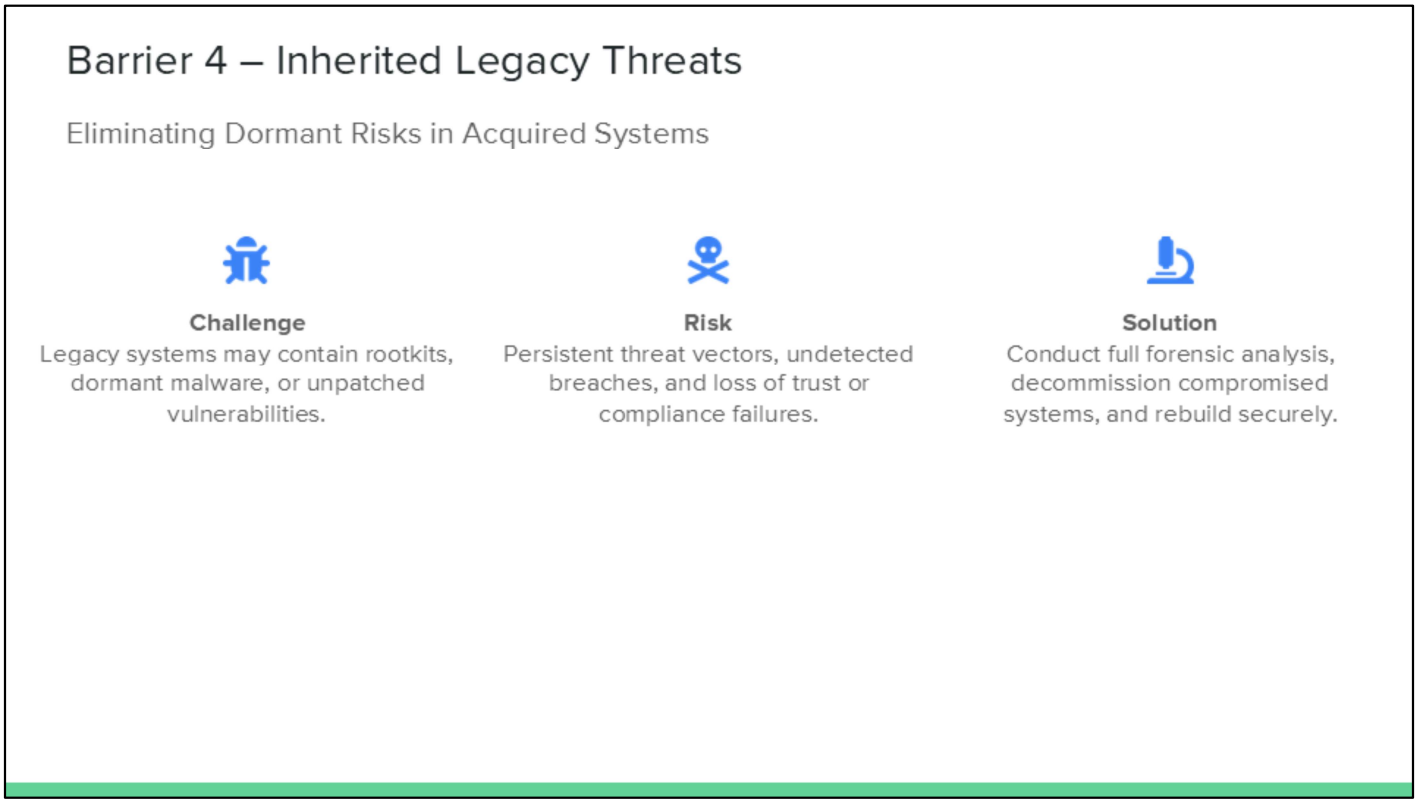
Barrier 3 – Resistance to Change

Overcoming Cultural and Behavioral Obstacles

- **Challenge:** Employee pushback against new MFA, training, and policy changes hampers adoption.
- **Risk:** Low engagement, poor security hygiene, and increased likelihood of social engineering breaches.
- **Solution:** Use gamified training, leadership support, and change champions to drive buy-in.

Photo by Markus Spiske on Unsplash

- Technology alone won't secure Padgett-Beale Financial Services—people play a critical role. Cultural resistance, particularly to MFA enforcement, frequent training, and new policies, is a common but often underestimated threat.
- Employees may view these changes as burdensome or unnecessary. This mindset leads to incomplete policy adherence, careless behavior, and greater susceptibility to phishing and insider threats.
- If not addressed, such resistance can nullify technical investments and increase the likelihood of a breach due to human error. The risk is not just technical—it's behavioral and strategic.
- To foster a security-first culture, Padgett-Beale will roll out gamified training that is both engaging and educational. Executive leadership will model desired behaviors, and internal "change champions" will serve as peer advocates. These measures are designed to embed security into daily routines and departmental KPIs.



- Legacy infrastructure is a double-edged sword in M&A scenarios. While it offers operational continuity, it also introduces unknown risks—especially when cybersecurity practices of the acquiree were outdated or deficient.
- These systems may harbor rootkits, trojans, or backdoors that have gone undetected. Their age and configuration complexity often make them incompatible with modern security tools, creating blind spots in monitoring and control.
- This represents a severe risk to Padgett-Beale's security posture, compliance standing, and operational integrity. A single undetected malware instance can serve as a persistent access point for adversaries.
- To address this, Padgett-Beale will perform full forensic audits on all legacy systems. Any asset that cannot meet security standards will be securely decommissioned. Where retention is necessary (e.g., for audit history), systems will be isolated, monitored, and restricted to read-only modes.

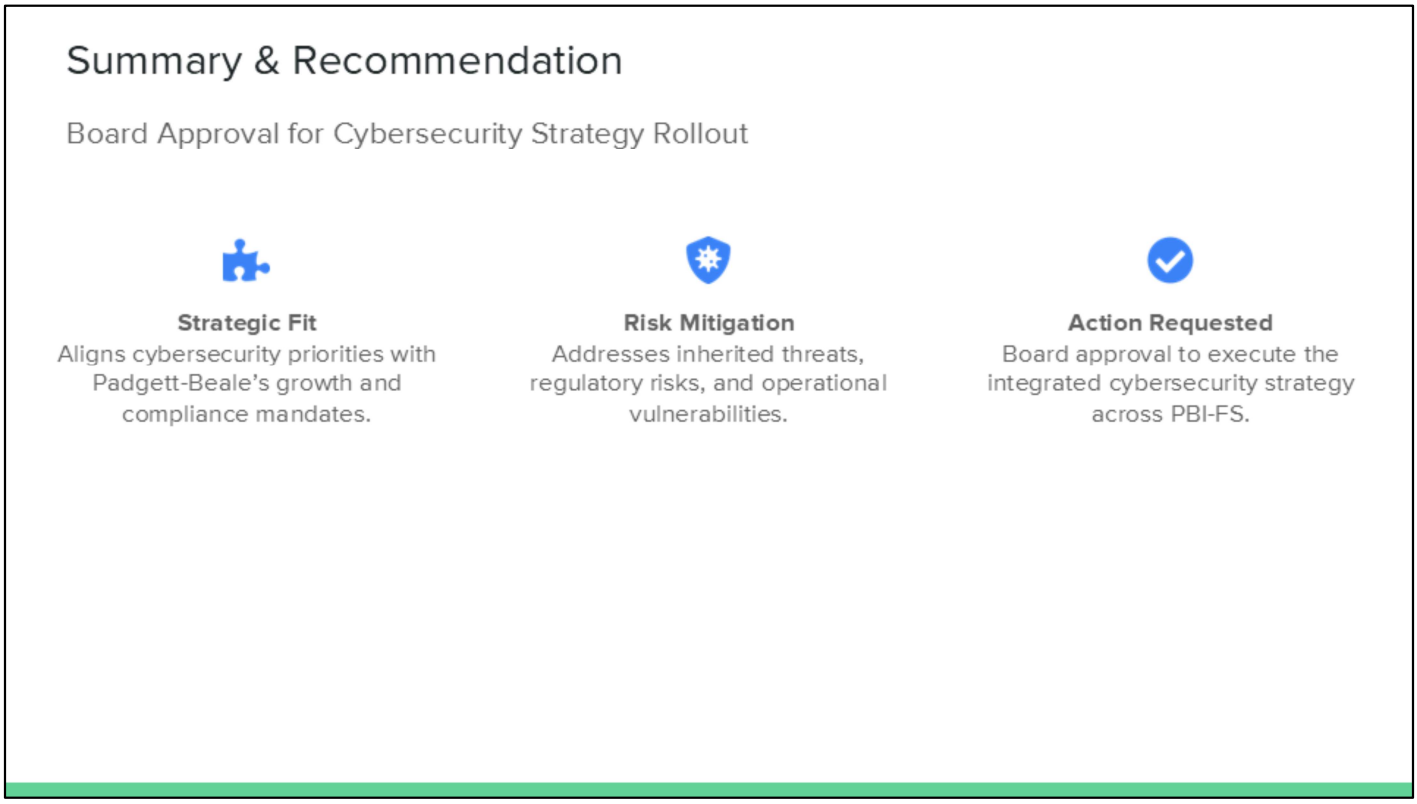
Barrier 5 – Environmental Disruption

Mitigating Natural, Geopolitical, and Cyber Threats

- **Challenge:** Natural disasters, geopolitical instability, and APTs threaten operational resilience.
- **Risk:** Downtime, data loss, reputational harm, and regulatory noncompliance.
- **Solution:** Deploy offsite backups, BCP testing, and MSSP-based incident response partnerships.

Photo by Justin Aikin on Unsplash

- The final barrier considers threats beyond traditional cybersecurity—natural disasters, geopolitical instability, and advanced persistent threats (APTs). These risks can disrupt operations, destroy data, and harm trust.
- Island-based infrastructure is especially vulnerable to hurricanes, earthquakes, and power instability. Meanwhile, geopolitical tensions and targeted cyber espionage (APTs) can undermine even the most well-designed networks.
- These risks threaten more than uptime—they can jeopardize regulatory compliance, result in costly downtime, and impact customer confidence.
- To prepare, Padgett-Beale will maintain encrypted offsite backups, conduct full-scale business continuity and disaster recovery tests, and leverage MSSP partnerships to ensure 24/7 incident response. This layered approach reinforces resiliency in the face of unpredictable global and environmental volatility.



- As we close, this summary consolidates the rationale, execution roadmap, and value proposition of Padgett-Beale's integrated cybersecurity strategy.
- The plan aligns with the broader corporate vision—securing a diversified financial services portfolio while ensuring regulatory compliance. Each strategy pillar—from governance and awareness to access control and modernization—has been crafted to address inherited and emergent risks.
- The strategy also provides scalable defenses against both known threats and long-term volatility. This includes physical disruptions, legacy system vulnerabilities, regulatory entanglements, and human behavior challenges.
- Today, the board is asked to formally approve the rollout of this cybersecurity strategy across the Padgett-Beale Financial Services unit. Doing so secures the firm's fintech ambitions, protects stakeholders, and lays a foundation for long-term operational resilience.

- The implementation of this cybersecurity strategy is more than a compliance exercise—it's a value multiplier across every dimension of business performance.
- First and foremost, it guarantees adherence to federal laws including GLBA, SOX, and BSA. This safeguards Padgett-Beale from financial penalties and legal exposure. But more than that, it embeds trust and reliability into the organizational fabric.
- The strategy strengthens operational resilience through SOC operations, disaster recovery planning, and continuous monitoring. These elements reduce the likelihood and impact of attacks while increasing uptime.
- For customers, the benefits are tangible: strong data protection builds confidence, improving client retention and acquisition. On the financial side, proactive security investments significantly reduce breach and litigation costs—often saving millions over time.
- Finally, by integrating security into the very structure of PBI-FS, Padgett-Beale ensures a robust foundation for scaling its financial services presence across future markets.

References

CanIPhish. (2025). Security awareness training price guide for 2025. https://caniphish.com/blog/how-much-does-security-awareness-training-cost

CrowdStrike. (2025). Endpoint, cloud & identity protection products. https://www.crowdstrike.com/en-us/products/

Federal Communications Commission. (2025). Interoperability. https://www.fcc.gov/general/interoperability

Fortinet. (2025). Network firewall price: Comparing security costs. https://www.fortinet.com/products/network-firewall-pricing

Glassdoor. (2025). Cybersecurity architect salary. https://www.glassdoor.com/Salaries/cyber-security-architect-salary-SRCH_KO0,24.htm

International Organization for Standardization. (2022). ISO/IEC 27001:2022 and ISO/IEC 27002:2022. ISO.

National Institute of Standards and Technology. (2018). Framework for improving critical infrastructure cybersecurity (Version 1.1). https://doi.org/10.6028/NIST.CSWP.04162018

References

National Institute of Standards and Technology. (2020). Security and privacy controls for information systems and organizations (NIST SP 800-53 Rev. 5). https://doi.org/10.6028/NIST.SP.800-53r5

SEBoK. (2023). Vee life cycle model. https://www.sebokwiki.org/wiki/Vee_Life_Cycle_Model

Tripwire. (2025). CIS Controls Version 8.1: What you need to know. https://www.tripwire.com/state-of-security/security-data-protection/cis-controls-version-8-1-what-you-need-to-know

UnderDefense. (2025). Managed SIEM pricing guide. https://underdefense.com/blog/managed-siem-pricing-guide/

University of Maryland Global Campus. (2020). CSIA 485 Padgett-Beale M&A Profile 2020.