SIXTH WALL

The Executive Case for Enterprise Security

Translate security operations into business outcomes your C-suite and board will act on.

CISO EXECUTIVE COMMUNICATIONS | SECURITY CULTURE STRATEGY | EXECUTIVE TRAINING

INTRODUCTION

From Cost Center to Strategic Enabler

Your security team operates continuously across threat intelligence, awareness, insider threat, identity management, incident response, vulnerability management, and governance. Each of these functions protects the enterprise's ability to operate, grow, and maintain trust. Collectively, they represent one of the most significant investments your organization makes in resilience.

The challenge is that this value is largely invisible to the people who fund it. When the CFO reviews the security budget, when business unit leaders engage with security policies, when the board asks about cybersecurity posture - those moments determine whether security is positioned as a strategic enabler or treated as operational overhead.

The difference between those two outcomes is rarely technical. It's narrative. The CISOs who earn sustained executive buy-in are the ones who consistently frame security in the language of business outcomes - not technical activities.

This guide provides a structured framework for doing exactly that. It maps every major security function to the business value it delivers and provides ready-to-use language for board presentations, budget discussions, and every conversation where security's contribution to the enterprise needs to be clearly articulated. The difference ultimately comes down to three disciplines, which this guide is designed to help you build.

THE STRATEGIC VIEW

What Security Delivers to the Business

The table below is the foundation of your executive narrative. Each row connects a security function to the specific business outcomes it enables - not as a report on what happened last quarter, but as a strategic map of how security protects revenue, reputation, regulatory standing, and operational continuity across the enterprise.

Function	What It Protects	Business Outcome
Cyber Threat Intelligence	Early warning on threats before they reach the enterprise	Avoided incidents, informed investment decisions, competitive awareness
Training & Awareness	Employee behavior at the point of attack	Reduced breach likelihood, lower insurance premiums, regulatory compliance
Insider Threat	IP, customer data, and sensitive systems from internal risk	Protected trade secrets, avoided regulatory fines, maintained customer trust
Identity & Access Management	Who has access to what, and whether that access is appropriate	Prevented unauthorized access, audit readiness, zero-trust foundation
Incident Response & SOC	Business continuity when attacks occur	Minimized downtime, controlled recovery costs, protected reputation
Vulnerability Management	The attack surface adversaries exploit	Reduced exploitable risk, vendor accountability, patch compliance
Governance, Risk & Compliance	Regulatory standing and enterprise risk posture	Avoided fines, maintained certifications, board-level risk visibility

Reframing the Conversation

When business leaders ask what security does, the most effective answer isn't a list of tools, headcount, or blocked attacks. It's a clear articulation of what the team enables:

> *"Our team protects the company's ability to operate, grow, and maintain trust. We do that across every threat vector - from external adversaries to insider risk to regulatory compliance. The work spans seven core functions, each mapped to a specific business outcome. Each one contributes to the goals this leadership team cares about most."*

The following sections provide the detailed messaging behind each function - including the specific language shifts that transform technical reporting into strategic business communication.

SECTION 01

Cyber Threat Intelligence

Your CTI team operates as the early warning system for the enterprise. They continuously monitor the global threat landscape - scanning dark web forums, tracking threat actor campaigns, analyzing malware variants, and correlating signals from intelligence feeds with your specific environment. When a new vulnerability is disclosed or a threat actor targets your industry, CTI identifies the risk before it becomes an incident.

What Business Leaders Don't See

- Proactive threat monitoring that prevents incidents from ever reaching the enterprise
- Intelligence briefings that inform strategic decisions about technology investments and risk posture
- Industry-specific threat analysis that keeps the organization ahead of adversaries targeting their sector
- Coordination with law enforcement, ISACs, and peer organizations to share and receive actionable intelligence
- Vulnerability prioritization that ensures limited resources address the most critical risks first

Translating to Business Language

Technical framing	Business framing
"We monitor threat feeds and IOCs"	**"We identified 3 active campaigns targeting our industry this quarter and took action before they reached us"**
"We track APT groups"	**"We monitor the specific threat actors targeting our sector and share intelligence with industry peers - so we see attacks coming before they arrive"**
"We analyze vulnerabilities"	**"We prioritize which risks to address first so the business can make informed decisions about where to invest limited resources"**

SECTION 02

Security Training & Awareness

Your training and awareness team is the front line of your human defense strategy. They design and deploy awareness campaigns, administer training programs, create targeted content for high-value targets (executives, finance, HR), run simulated phishing exercises, and maintain a continuous drumbeat of security-conscious messaging across Slack, intranet, email, and in-person channels. In an era of AI-powered phishing and deepfake social engineering, this team's work has never been more critical.

What Business Leaders Don't See

- Ongoing campaign design that keeps security top-of-mind without creating fatigue
- Targeted programs for high-risk groups - executives, finance teams, employees with privileged access
- Real-time adaptation to emerging threats: when a new phishing technique appears, awareness content deploys within days
- Simulated phishing and social engineering exercises that measurably reduce click rates over time
- Deepfake awareness training that prepares employees for threats most organizations aren't ready for
- Metrics and reporting that demonstrate behavior change, not just completion rates

Translating to Business Language

Technical framing	Business framing
"We run phishing simulations"	**"Our phishing click rate dropped from 18% to 4% this year - that represents [X] fewer potential breach entry points per quarter"**
"We do security awareness training"	**"We run a continuous behavior-change program that reduces the likelihood of our employees being the entry point for an attack - the same entry point responsible for 60% of breaches industry-wide"**
"We send out security reminders"	**"We maintain a targeted communications program that keeps [X,000] employees current on threats like AI-generated phishing and deepfake voice scams - threats that have increased 1,500% since 2023"**

SECTION 03

Insider Threat

Your insider threat program monitors for risks that come from within the enterprise - whether from malicious insiders intentionally exfiltrating data, negligent employees who mishandle sensitive information, or compromised credentials being used by external actors who have gained access to legitimate accounts. This team also watches for fraudulent workers, contractor risks, and the growing threat of AI-enabled identity fraud in hiring processes.

What Business Leaders Don't See

- Continuous behavioral monitoring that detects anomalous data access patterns before they become breaches
- Investigation and response capabilities that handle sensitive cases with discretion and legal compliance
- Collaboration with HR, Legal, and business units to manage risk without disrupting operations
- Vetting processes that identify fraudulent worker risks - an emerging threat as AI-generated identities become more sophisticated
- Protection of intellectual property, trade secrets, and sensitive business data from both intentional and accidental exposure

Translating to Business Language

Technical framing	Business framing
"We monitor user behavior analytics"	**"We protect the company's most sensitive data from internal threats - the kind that cost an average of $4.9M per incident and take the longest to detect"**
"We investigate insider incidents"	**"We identified and contained [X] potential data exposure incidents this year before they became reportable breaches - avoiding regulatory, legal, and reputational costs"**
"We do DLP monitoring"	**"We safeguard the intellectual property and customer data that underpins our competitive position and regulatory standing"**

SECTION 04

Identity & Access Management

Your IAM team controls who has access to what across the enterprise - and ensures that access remains appropriate as people change roles, join, or leave the organization. They manage authentication, authorization, privileged access, and the zero-trust architecture that underpins modern security posture. In an era where attackers increasingly 'log in' rather than 'break in,' IAM is the function that determines whether stolen credentials become a breach.

What Business Leaders Don't See

- Lifecycle management of user identities across onboarding, role changes, and offboarding
- Privileged access controls that limit the blast radius of compromised credentials
- Multi-factor authentication and adaptive access policies that balance security with user experience
- Zero-trust architecture that verifies every access request regardless of network location
- Access certification and review processes that maintain compliance and reduce standing privileges

Translating to Business Language

Technical framing	Business framing
"We manage IAM and PAM"	**"We ensure that every employee has exactly the access they need - no more, no less - and that former employees and contractors lose access immediately upon departure"**
"We enforce MFA"	**"We add a layer of verification that prevents stolen passwords from becoming breaches - the single most cost-effective control in our security program"**
"We do access reviews"	**"We continuously verify that access privileges match current roles - closing the gaps that auditors flag and attackers exploit"**

SECTION 05

Incident Response & SOC Operations

Your Security Operations Center and incident response team are the always-on heartbeat of enterprise defense. They triage alerts around the clock, investigate potential compromises, contain active threats, and run tabletop exercises so the organization is ready for the worst-case scenario. When a breach does occur, this team determines the difference between a contained incident and a headline.

What Business Leaders Don't See

- Monitoring and triage of thousands of alerts per day, with escalation protocols that prioritize business-critical systems
- Incident containment that minimizes operational disruption, data loss, and recovery costs
- Tabletop exercises and scenario planning that prepare leadership for coordinated crisis response
- Post-incident analysis that continuously improves defenses and closes gaps before they're exploited again
- Coordination with legal, communications, and regulatory teams during incidents to protect reputation and compliance standing

Translating to Business Language

Technical framing	Business framing
"We responded to X incidents"	**"We contained X potential business disruptions this year, with an average response time of [X hours] - well below the industry average of 241 days to identify and contain a breach"**
"We run tabletop exercises"	**"We prepare the executive team for coordinated crisis response so that if an incident occurs, we minimize operational downtime, customer impact, and regulatory exposure"**
"We monitor the SOC"	**"Our team evaluates over [X,000] security events daily, filtering them to the [X] that require action - so the business operates uninterrupted while we handle the threats"**

SECTION 06

Vulnerability Management & Risk

Your vulnerability management team continuously scans the enterprise for weaknesses - across applications, infrastructure, cloud environments, and third-party integrations. They prioritize remediation based on exploitability and business impact, coordinate patching with IT and development teams, and manage the risk register that informs strategic security investments.

What Business Leaders Don't See

- Continuous discovery and prioritization of vulnerabilities across an attack surface that grows with every new application and vendor
- Risk-based remediation that protects business-critical systems first, not just what's easiest to patch
- Third-party and supply chain risk assessment that protects the enterprise from vendor compromises
- Metrics that translate technical vulnerability counts into business risk exposure the board can act on
- Coordination across IT, DevOps, and business units to close gaps without disrupting operations

Translating to Business Language

Technical framing	Business framing
"We patched X vulnerabilities"	**"We reduced our exploitable attack surface by X% this quarter, focusing on systems that support revenue-generating operations and customer data"**
"We do vulnerability scanning"	**"We continuously assess our environment against the same vulnerabilities that adversaries are actively exploiting - and we close them before they can be used against us"**
"We manage third-party risk"	**"We evaluate every vendor that touches our data or systems - because 30% of breaches last year involved third-party compromise"**

SECTION 07

Governance, Risk & Compliance

Your GRC function is the connective tissue between security operations and the enterprise's regulatory, legal, and fiduciary obligations. This team maintains the risk register, manages audit relationships, ensures compliance with frameworks like SOC 2, HIPAA, PCI DSS, and emerging SEC disclosure requirements, and translates the work of every other security function into the governance language the board and regulators require.

What Business Leaders Don't See

- Risk quantification and reporting that gives the board actionable visibility into the enterprise's security posture
- Regulatory compliance management across multiple overlapping frameworks and jurisdictions
- Audit coordination that demonstrates control effectiveness and avoids findings
- Policy development and governance that balances security requirements with business agility
- SEC cybersecurity disclosure readiness and board reporting frameworks

Translating to Business Language

Technical framing	Business framing
"We maintain compliance"	**"We ensure the organization meets every regulatory obligation - protecting the company from fines, litigation, and the reputational damage of a compliance failure"**
"We manage the risk register"	**"We give the board a clear, quantified view of cyber risk alongside every other enterprise risk - so security investment decisions are informed by the same rigor applied to financial and operational risk"**
"We prepare for audits"	**"We maintain continuous audit readiness - so when regulators or customers ask to see our controls, the answer is always ready, not reactive"**

PUTTING IT INTO PRACTICE

From Framework to Action

The CISOs and security leaders who consistently earn executive buy-in share three disciplines that set them apart from their peers:

1. They communicate in outcomes, not activities. Every metric, every update, every board slide answers the question: 'What did this protect, prevent, or enable for the business?' Technical detail serves the narrative; it never replaces it.

2. They build a narrative, not a report. The board doesn't need a dashboard. They need to understand the strategic picture: what is the threat landscape, how is the organization positioned, what is the team doing about it, and what investment is required to maintain that position.

3. They make security visible on their terms. The most effective security leaders establish credibility through consistent, strategic communications that build executive understanding and trust well before they're needed most.

Ready to build this capability at your organization?

Sixth Wall partners with CISOs and security leaders to develop the executive communications strategy, board narrative, and organizational culture that position security as a strategic business enabler. Our founder led the organization behind a U.S. patent in AI-driven security behavior change and brings Fortune 3 executive communications experience to the work that matters most: earning the executive buy-in your program depends on.

CISO Executive Communications | Security Culture Strategy | Executive Training

info@sixthwallsecurity.com | sixthwallsecurity.com