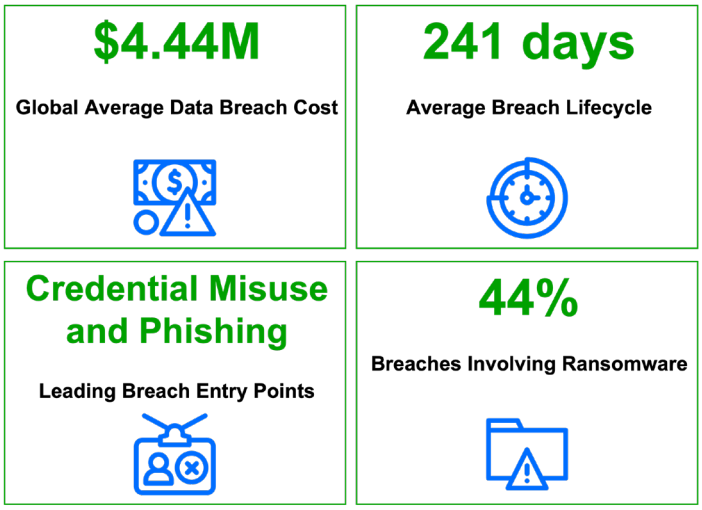
Five Ways CISOs Can Communicate Cyber Risk and Protect the Business

Cyber risk is no longer hypothetical. Every organization operates under continuous threat, and no industry is exempt. Recent breach research shows that attackers still operate inside environments for extended periods before detection, increasing operational disruption and business impact. According to the IBM Cost of a Data Breach Report 2025, the global average cost of a data breach is $4.44 million. While this reflects a decline from prior years due to faster detection and containment, the report also shows that organizations without strong identity controls and AI governance continue to experience higher costs and longer recovery cycles.



Sources:

IBM Cost of a Data Breach Report 2025
Verizon 2025 Data Breach Investigations Report

Figure 1.

Modern breaches are driven by identity misuse and unfold over months. Reducing impact depends on detecting risky behavior early,

The impact goes well beyond direct response costs. Loss of trust with customers, partners, and employees can persist long after systems are restored, affecting revenue, valuation, and growth.

Despite this reality, security is still often viewed as a cost center rather than a business enabler. Many executives understand the need for protection, but sustained engagement often follows a major incident.

Communicating risk clearly and credibly is a core responsibility of the CISO. Risk ownership does not sit with security alone. It is a shared, enterprise-wide concern that requires alignment across leadership. This guide outlines practical ways to communicate cyber risk in business terms and explains how Exabeam helps reduce exposure through behavior-driven security operations.

Figure 2.

Security operations starts from the expectation of compromise. Detection focuses on abnormal behavior, risk is scored continuously, and investigation begins before damage spreads.

How to Communicate Risk

1. Operate With An Assume-Breach Mindset

Industry analysts continue to reinforce that assuming compromise is the only sustainable security posture. Concepts such as zero trust and identity-centric security are necessary foundations, but they do not stop modern adversaries on their own.

Running security operations as if a breach has already occurred puts teams in a stronger position to detect and respond early. This approach prioritizes continuous monitoring, behavioral context, and investigation readiness. Detection focuses on indicators of compromise (IoCs) and attacker behavior rather than waiting for known signatures to trigger alerts. The goal is faster containment and reduced business impact.

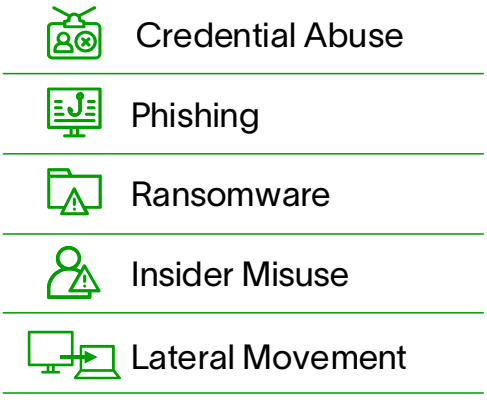


Figure 3.

The same attack patterns target both human and non-human identities, using credential abuse, social engineering, and lateral movement to gain and expand access.

2. Ground Risk in Industry-Relevant Threats

Executives do not need deep technical detail, but they do need a working understanding of the threats most likely to affect the business. Focus on realistic scenarios that map to your industry and operating model, including:

- **Compromised insiders:** Legitimate users whose credentials or devices are infected and then used as a foothold for further activity
- **Phishing and social engineering:** Deceptive campaigns that trick users into revealing credentials or executing malicious content
- **Ransomware and extortion:** Attacks that encrypt systems, disrupt operations, and often exfiltrate data to increase pressure
- **Malicious insider:** Employees or contractors who intentionally abuse authorized access to steal data or disrupt operations
- **Credential switching:** Attackers move between stolen accounts to avoid detection and expand access
- **Lateral movement:** Progressive movement through systems and identities to reach high-value assets
- **Unauthorized data exfiltration:** Sensitive data copied or transferred without approval by malware or trusted users

An assume-breach mindset helps leadership understand why these threats require detection strategies based on behavior, not static rules alone.

3. Build Executive Alignment Early and Often

Effective risk communication depends on ongoing executive collaboration. CISOs should engage peers across leadership functions individually, including finance, operations, legal, HR, IT, and revenue teams. These conversations should focus on shared responsibility and realistic outcomes, not fear-based scenarios.

Accurate reporting matters. Executives need a clear view of current exposure, detection gaps, and response readiness. When framed correctly, security becomes a business enabler that protects revenue, uptime, and brand trust rather than a sunk cost.

Figure 4.

A single security incident can disrupt operations, reduce revenue, damage customer trust, weaken reputation, and slow growth at the same time.

4. Translate Breach Impact Into Business Outcomes

Executives engage when risk is expressed in terms they own. Align breach scenarios to concrete business impacts:

- **Loss of continuity:** Disrupted systems and inaccessible data can halt core operations and delay recovery.
- Loss of revenue: Financial impact includes downtime, response costs, regulatory penalties, legal action, and restitution.
- **Loss of service:** Customers, partners, and employees depend on reliable access. Contractual penalties and churn often follow outages.
- **Loss of reputation:** Trust erosion can reduce market value and slow growth long after technical recovery.
- **Loss of opportunity:** Breach-related disruption often diverts investment, delays expansion, and increases customer acquisition costs.

Security operations exists to limit these outcomes by reducing dwell time and containing risk early.

Together, these impacts show why early detection and response change the outcome of a security incident. Reducing risk depends on understanding how identities behave over time, not just whether controls are in place.

Five Ways Exabeam Helps Reduce Risk Exposure

Legacy security tools that rely primarily on static rules and signatures struggle to keep pace with human and machine-driven attacks. Security operations teams need cloud-delivered platforms that consistently produce measurable outcomes through behavior-based detection and automation.

1. Establish Normal Behavior for Users, Assets, and Agents

Exabeam uses behavior intelligence to continuously analyze activity and establish baselines for users, assets, and non-human identities. This includes service accounts, APIs, and autonomous agents. Dynamic risk scoring highlights deviations from expected behavior, giving analysts immediate context for investigation.

2. Detect External Threats Using Multiple Signal Types

Exabeam combines behavioral analytics, rules, and IoCs to detect threats such as phishing, malware, and ransomware. This layered approach improves signal quality and reduces noise by correlating activity across identities, systems, and time.

Capabilities include:

- Behavior-driven and rules-based incident detection that prioritizes risk
- Automatically generated incident timelines that connect related activity across environments
- Dynamic peer grouping to compare behavior across similar users, devices, or agents
- Detection of lateral movement even when attackers rotate credentials, hosts, or IP addresses

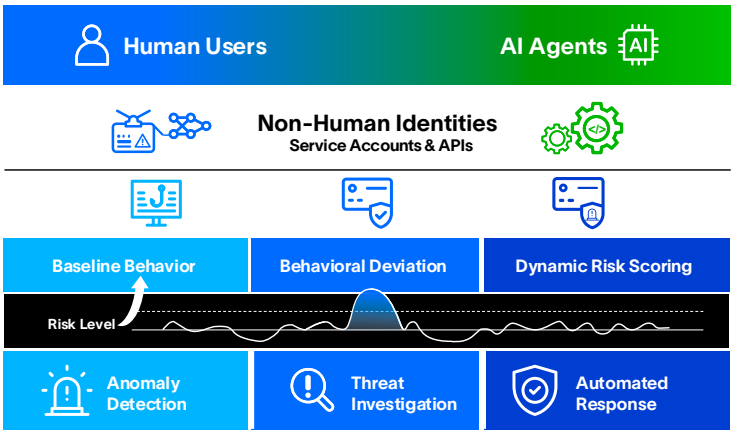


Figure 5.

Behavior Intelligence Coverage Model: Behavioral baselines deviation analysis, and dynamic risk scoring apply consistently across human users, non-human identities, and AI agents to surface risk early.

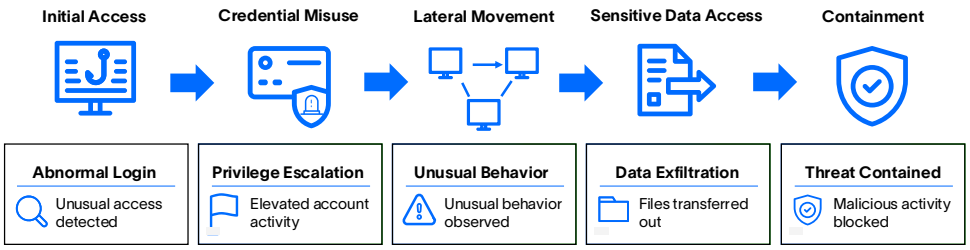


Figure 6.

Common attacks progress from initial access to internal movement and data exposure. Earlier detection and response reduce impact and limit how far an attacker can move.

3. Identify Insider Risk and Compromised Credentials Faster

Behavioral analytics makes it possible to detect insider threats and account compromise that evade traditional controls. By comparing activity against established behavior patterns, security operations teams can surface risky actions without relying on excessive alerts. End-to-end visibility into attacker progression supports faster, more confident response.

Security Challenge	Outcome Delivered
Alert Overload	Prioritized Risk
Credential Misuse	Early Detection
Manual Investigations	Faster Resolution
Insider Risk	Insider Risk Identified

Figure 7.

Behavior-driven detection and response turn common security challenges into measurable improvements for security operations teams.

4. Extend Security Operations in the Cloud

Cloud-delivered analytics and automation allow teams to move beyond traditional on-premises SIEM limitations. New-Scale Fusion supports modern security operations use cases while reducing infrastructure overhead and accelerating time to value.

5. Simplify Compliance and Audit Readiness

Manual compliance processes and disconnected tools increase audit risk. Exabeam provides prebuilt detection content and reporting aligned to common regulatory frameworks, helping teams demonstrate control effectiveness and reduce preparation effort.

Conclusion

Communicating cyber risk effectively means shifting the conversation from tools and alerts to behavior and business impact. When leaders understand how identity-driven activity leads to real operational and financial outcomes, security becomes a shared responsibility rather than a siloed function. A behavior-based approach gives CISOs a clearer way to explain risk, prioritize response, and align security operations with the goals of the business.

About Exabeam

Exabeam is the leader in behavior intelligence for the agentic enterprise. As organizations deploy digital workers and confront machine-speed adversaries, Exabeam delivers flexible, industry-proven solutions for insider threat coverage of humans and agents and faster, more accurate threat detection, investigation, and response (TDIR). Learn more at www.exabeam.com.

exabeam™

Learn more at
www.exabeam.com →