exabeam

White Paper

A CISO’s Guide to Communicating Risk

The Business Value of Cybersecurity

An investigation confirms it: your organization has been breached.

You know that on average, it takes 212 days before a breach is detected[1]. So you have to wonder: How long have we been compromised? What will it take to recover? And above all, how badly will it damage our reputation?

You consider what breach reparation and remediation entail. Confirming and containing the breach will be expensive, and you’ll need to answer on the cost. Your experts could spend hundreds of hours over many months — maybe years — solving this crisis, diverting their efforts away from driving the business. Considering that the average data breach costs $18.5 million,[2] your organization will likely face a massive bill. And cleaning up the attack may be the smallest portion of that total. Fines and penalties are more expensive than incident response, and the worst fallout by far is reputational.[3] Losing the trust of your customers and the public has consequences that reach further and last longer than the single cybersecurity threat that started it all.

Thankfully, this is just a hypothetical situation — but it’s neither a rarity nor a worst-case scenario.

Organizations today are targeted constantly, and the threats increasingly come from trusted identities and credentials; of the breaches reported in 2021, 89% were associated with legitimate users or devices[4]. And for those companies that haven’t implemented fundamental cybersecurity defenses and incident response processes, the bad luck of encountering a dedicated adversary could ruin their business.

This paper details key angles of risk communication for CISOs:

- What executives need to understand about the threat landscape
- How to educate leaders on the business consequences of breaches
- Essential elements of an executive incident response
- Why collaboration is key in a crisis
- How CISOs can introduce the “assume-breach” mindset to their C-suite peers

Considering that a breach could occur in January, and you might not find out until November, it’s clear that the only sensible approach to cybersecurity is to assume you’ve been breached. By running your security operations center (SOC) proactively, as if a breach has already occurred, you put yourself in a much better position to both detect and protect against attacks.

[1] IBM Security, Cost of a Data Breach Report 2021, p. 22

[2] Cyber crime and FS: blocking the path of least resistance, Financier Worldwide

[3] Ibid. p. 58

[4] 2021 Data Breach Investigations Report, p. 18

Embracing a "we've been breached" mentality

One of the major challenges facing CISOs is the view, common among their executive peers, that cybersecurity is entirely a cost center. Not everyone sees that it enables business or creates value. And even though many leaders nominally understand the need for robust security, it often takes an actual breach to get their attention — and by then, it's already too late.

One of a CISO's key roles is to help embed an "assume-breach" mindset within the C-suite and the board, because security — or lack thereof — has critical ramifications. If a new CFO joins an organization and makes a request, it's almost certain to be adopted; so how can CISOs establish similar credibility to get the executive leadership team on board with a more proactive approach to risk, threats, and opportunities?

> The worst time to make an introduction is in a crisis."
>
> **Steve Moore, Vice President and Chief Security Strategist, Exabeam**

Moreover, what can be done to show that the CISO isn't just the bearer of bad news, but rather a recognized leader who drives business value? Now more than ever, the CISO is critical to revenue, operations, employee engagement, recruitment and retention, and business development — and it's time to change the narrative to reflect this new reality.

Contending with today's threat landscape

CISOs know intimately that cybersecurity threats continue to increase in their severity and sophistication. Since 2018, the percentage of breaches caused by human error has hovered around 20% (17% in 2021).[5] And given all of the employee training and security awareness investment companies continue to make, this number is noteworthy. The C-suite relies on the CISO's expertise for awareness of today's most challenging threats:

Compromised insiders — users with authorized access to an organization's data, whose credentials and assets have been infected with malware and now serve unknowingly as a home base for criminal activity

Phishing — one of the most common methods for transferring malware onto a victim's machine, this type of attack usually takes the form of fraudulent communications that appear to be legitimate

Ransomware — the malware encrypts any files and systems it infects, rendering them unusable — and exfiltrating the data — until the organization pays the ransom to decrypt them

Malicious insiders — employees or contractors with trusted access credentials who set out to disrupt operations or steal data, often in order to enrich themselves or intentionally harm their company

Credential switching — a combination-type attack used by threat actors wherein they hijack different accounts to target different hosts, or hopscotch from stolen account to stolen account in an attempt to infiltrate

Lateral movement — the ability for attackers to move progressively and incrementally through a network, eluding commodity security controls that are designed to be context aware

Data exfiltration — this occurs when data is copied, transferred, removed, or retrieved without permission, either by malware or by a malicious actor who may or may not have authorized access

The "we've been breached" mindset is essential for anticipating and preempting these threats — as well as the new types of attack that will emerge in the future.

The workplace and the workforce will continue to evolve too, changing and expanding the attack surface. We have already witnessed the shift to distributed work and

[5] Verizon, 2021 Data Breach Investigations Report, p. 16

the transition to cloud environments. Employees can now sign into their workspaces from anywhere, on any device. And companies are facilitating this by moving more of their operations — and data — to the cloud. CISOs and SOCs must be vigilant of every person, device, and cloud; each is a potential point of attack.[6]

The business impacts of a breach

It's part of a CISO's job to be aware of the risks and costs associated with a data breach — but what about the rest of the senior leadership team? In some cases, it's difficult for executives to comprehend both the short-term and long-term ramifications. Given CISOs' expertise, they have an opportunity to step in to educate key stakeholders and protect the business. It's important to ensure that the entire C-suite realizes what they could lose in a serious security event.

Loss of continuity

A bad breach could hold business-critical data and systems hostage, disrupt them, or destroy them, making basic operations impossible. The publicized ransomware attacks of 2021, and the distributed denial-of-service attack on Microsoft illustrate the complexity and fallout of serious attacks.

Loss of revenue

Leaders need to be aware of the massive financial impacts that result from a breach. It's not just the costs of retrieving data, or investing hours to rectify the situation, or losing profits as vital systems remain offline. It could include paying reparations to victims and fines to regulators.

Loss of service

There's an entire ecosystem of internal and external stakeholders that depend on the products and services an organization provides — and that includes employees, partners, contractors, and customers. A cyberattack will impact all of these groups; executives need to know what their contractual obligations are and how they'll be penalized for failing to meet them.

Loss of reputation

A breach will impact an organization's revenue and profitability even when it is contained, operations resume, and service is restored. The deficit of public trust that results from a breach represents a significant long-term risk.

Loss of opportunity

In a breach, 38% of an organization's financial losses[7] are lost business opportunities, and they come in a variety of forms. Customer turnover can increase. Lost revenue can limit investment potential — or damaged value and reputation can drive up the investment it takes to attract and acquire opportunities.

While it may seem negative to raise awareness of these risks, it's essential to remember that the role and contributions of the CISO are fundamentally positive, proactive, and forward-looking. An assume-breach mindset is not about existing in a heightened state of anxiety or panic; it's about maintaining focus on business productivity, profitability, and long-term value. And one of the top benefits a CISO brings to the table is a sense of confidence; preparedness is fundamental to peace of mind.

> The million-dollar question that every single board member will ask a CISO at some point in their career is 'how secure are we?' And so how do you actually measure that to be able to tell that story?"
>
> **Tyler Farrar, Chief Information Security Officer, Exabeam**

Of course, that confidence only comes with buy-in across the executive level. Leaders must take action, not only to invest in the best possible security systems, processes, and response strategy, but also to adopt and implement them across the organization.

A coordinated executive is an effective defense

One of the most powerful ways of both mitigating risks pre-breach and minimizing damage post-breach is to implement an executive incident response plan. This means that multiple positions and portfolios across the senior leadership team need to recognize the indispensable role they play in preventing and managing crises. Moreover, they must be accountable to the board, investors, and customers in meeting these responsibilities.

[6] The State of DevOps Report, p. 1

[7] IBM Security, Cost of a Data Breach Report 2021, p. 16

To establish these expectations and responsibilities, CISOs need to proactively connect with executives one-on-one, demonstrating how to work collaboratively to manage risk.

Most importantly, CISOs must accurately report the state of the organization's security, but they can also help the C-suite see how security is a business enabler.

> Collaboration starts with the CISO calling their shots and saying, 'Look, this is who I am; this is the value I'm going to bring, and this is what I need from you. This is how I expect to operate. And this is what a world-class organization looks like.'"
>
> **Steve Moore, Vice President and Chief Security Strategist, Exabeam**

CEO

Around 68% of business executives don't allow security measures that slow down a company's progress[8]. Yet, the CEO's prioritization of cybersecurity sets the tone for the executive team.

When they invite the CISO to the table to share cybersecurity expertise, it sets the stage for strategic collaboration on preventing and containing cyberattacks.

Honesty and transparency are assets in communications with a CEO. They may want reassurance that the business has been breach-proofed, but they need to hear the truth:

- No business system can be optimized without the right resources; the CISO should articulate what's absent, and what might happen without it
- While the SOC is building, or has built, the best possible defense, it's up to the CISO to contextualize its importance to other business units — and then the organization's leaders must drive adoption

Security touches every part of the organization, which is why emphasizing an ethic of shared responsibility across the C-suite helps establish a coordinated executive approach.

> I think that a leader's real role in a company is to be someone who breaks down barriers to execution."
>
> **Tyler Farrar, Chief Information Security Officer, Exabeam**

CFO

Working with a CFO, a CISO can help uncover cost-saving opportunities in the short, middle, and long term. CFOs face massive budgetary considerations related to digital transformation, and the CISO can contextualize the value of immediate infrastructure investments in minimizing future losses, both through a reduction in the incidence of breaches and a more efficient incident response when they do occur. The average cost of data breaches at organizations with robust incident response planning and testing was $3.25 million in 2021, compared to $5.71 million for organizations that lacked these capabilities. That's a difference of $2.46 million, or 54.9% — and those savings depend on a CISO's expertise[9].

CIO

There can be a sense of conflict between CIOs and CISOs because it's not always clear where one portfolio ends and the other begins. But in truth, these areas of overlap are opportunities for partnership and collaboration. Leaders should apply shared expertise toward patching infrastructure, onboarding cloud apps, and establishing detailed topologies of the technology stack in the event an incident does occur.

[8] 5 Reasons DevOps And Security Need To Work Together, Forbes

[9] IBM Security, Cost of a Data Breach Report 2021, p. 25

A significant portion of IT involves security, but the CISO needs to frame this function as fundamentally business-first — something that supports operational efficiency and customer experience. There's also an opportunity for conversations with the CIO about building and adopting the strongest modern security processes when implementing cloud infrastructure.

CRO

Sales and revenue leaders may not always realize it, but they have a vested interest in powerful cybersecurity. A breach has a major impact on the value of a company, with implications for customer retention, lead generation, customer privacy, and closing sales.

The CISO needs to help revenue-focused peers see how data security impacts sales activity. What security concerns are sales teams hearing from leads and prospects in the field — and are those concerns affecting the pipeline? A CRO that understands the overall value of industry-leading cyber defenses becomes a powerful supporter for future threat prevention initiatives.

CMO

Along with supporting growth, the CMO is invested in the reputation and value of the brand, making cybersecurity threats a major concern in their role. Since breaches have a tremendous reputational impact, the public relations apparatus of any organization must be deeply involved in incident response strategy. This is essential to protecting both the brand and the investments in it, since reputational damage can confound the market and decimate the return on an organization's working spend. However, the close relationship between security and PR presents an opportunity for CISOs and their CMO peers to mutually benefit by championing security modernization.

CHRO

The decision makers in charge of human resources are important stakeholders in an executive incident response strategy. They strive to measure, monitor, and maintain positive employee and contractor sentiment, in addition to providing context on employees when necessary. These become much more difficult after a data breach.

An insecure workplace erodes trust, lowers morale, and diminishes a culture of excellence. And a lackluster culture is ineffective, accompanied by loss in the form of wasted hours and low productivity. That means building powerful defense capabilities will tangibly assist CHROs in their mission to recruit and retain top talent and build a thriving culture.

In addition, a robust and intelligent security apparatus can supply the insights HR teams need to support internal investigations. Demonstrate how powerful threat mitigation empowers HR, and the CHRO becomes another executive ally.

CTO/CPO/CIO

Technology leaders prioritize the procurement, development, and deployment of new solutions; this means security should be top of mind for these decision makers, and they have a proactive role to play in an executive incident response program.

The CISO can help to ensure they consider all angles on the security of new solutions by emphasizing the need for DevSecOps: embedding security at every stage of the development lifecycle, architecture, and Cloud and on-premises infrastructures.

Through the CISO's expertise, the CTO/CPO/CIO gains a deeper understanding of the best-in-class systems and processes in cybersecurity, and how those will best position the organization. Investing in security by implementing automation, adding 2 factor authentication, developing or procuring apps, and expanding IT management can make a massive impact. In 2021, organizations with intelligent security solutions, powered by AI or machine learning, saw an average cost of $2.90 million for a data breach, compared to $6.71 million for those that hadn't, representing a difference of 80%.[10]

General Counsel/Risk Officer

Privacy and security regulations are complex, and compliance is non-negotiable. Costly audits, penalties, and litigation can follow from a serious security incident, and research has found that compliance failure was the top factor amplifying the total cost of a breach.

An organization's head counsel is on the hook to prove that appropriate action was taken to protect stakeholders' data before, during, and after the breach. They play a key role in establishing attorney-client privilege for response communications, as well as when engaging outside help, and should review internal and external statements.

[9] IBM Security, Cost of a Data Breach Report 2021, p. 25

By working with these executives, showing them which security systems are in place, and flagging opportunities to introduce additional measures, CISOs can enlist them as advocates for further cybersecurity training, process, and investment.

> It's that constant engagement and tying it to their objectives, and how they align to the overall business objectives, that should be shared amongst every single C-level executive."
>
> **Steve Moore, Vice President and Chief Security Strategist, Exabeam**

True leadership in times of crisis

Eventually, a serious security incident or breach will happen, which is precisely why the CISO has to build connections and relationships across the C-suite. A coordinated executive strategy not only includes having explicit responsibilities and expectations for each senior role, but an effective, comprehensive, and repeatable process that can immediately be launched along with the right communications and messaging.

An assume-breach mindset keeps your organization prepared to mobilize in a practical and methodical way, without confusion and panic. As a CISO, you can model this by practicing self-awareness, servant leadership, and candor. Be transparent about what's happening, and be a willing collaborator. Above all, have empathy for your colleagues and employees.

The assume-breach mindset is also one of action

If there's been a security incident, it's incumbent upon the CISO's team to find the compromise in your systems. But first, and hopefully long before a breach takes place, you must find the compromise with your executive peers. That opens the door to collaborate on an effective threat mitigation strategy. It will reduce costs for the organization, increase happiness and job satisfaction for employees, build trust within your partner ecosystem and customer community, and differentiate you from the competition.

An assume-breach mindset is essential, considering undetected data breaches happen every day, but CISOs need to take it a step further — and act. By raising awareness, proactively planning, and introducing intelligent security technologies, they make powerful contributions to the wider success and long-term resiliency of the entire organization.

[10] IBM Security, Cost of a Data Breach Report 2021, p. 7

About Exabeam

As the leading Next-gen SIEM and XDR, the Exabeam Fusion SOC Platform is a modern, modular, and cloud-delivered solution for SIEM and XDR. Exabeam delivers advanced security analytics, automated threat detection and incident response (TDIR) with a use case-based approach focused on delivering outcomes.

For more information, visit exabeam.com.

Exabeam provides the following benefits:

Industry-leading behavioral analytics and automation to detect and respond to threats overlooked by other tools

- 51% reduction in the time it takes to detect, triage, investigate, and respond to threats
- 83% of analysts report triaging twice as many alerts than with their legacy SIEM
- 92% of customers report value in week one
- Advanced SOC capabilities with threat-centric, use-case packages

Want to learn more about Exabeam? Get a demo today.

exabeam