The GOAT Guide for Reporting to the Board

A CISO's Playbook for Communicating Cyber Risk Effectively

By

Gary Grit

Head of Cybersecurity
at Grazing, Inc.

Author

Aviv Cohen

CMO, Pentera

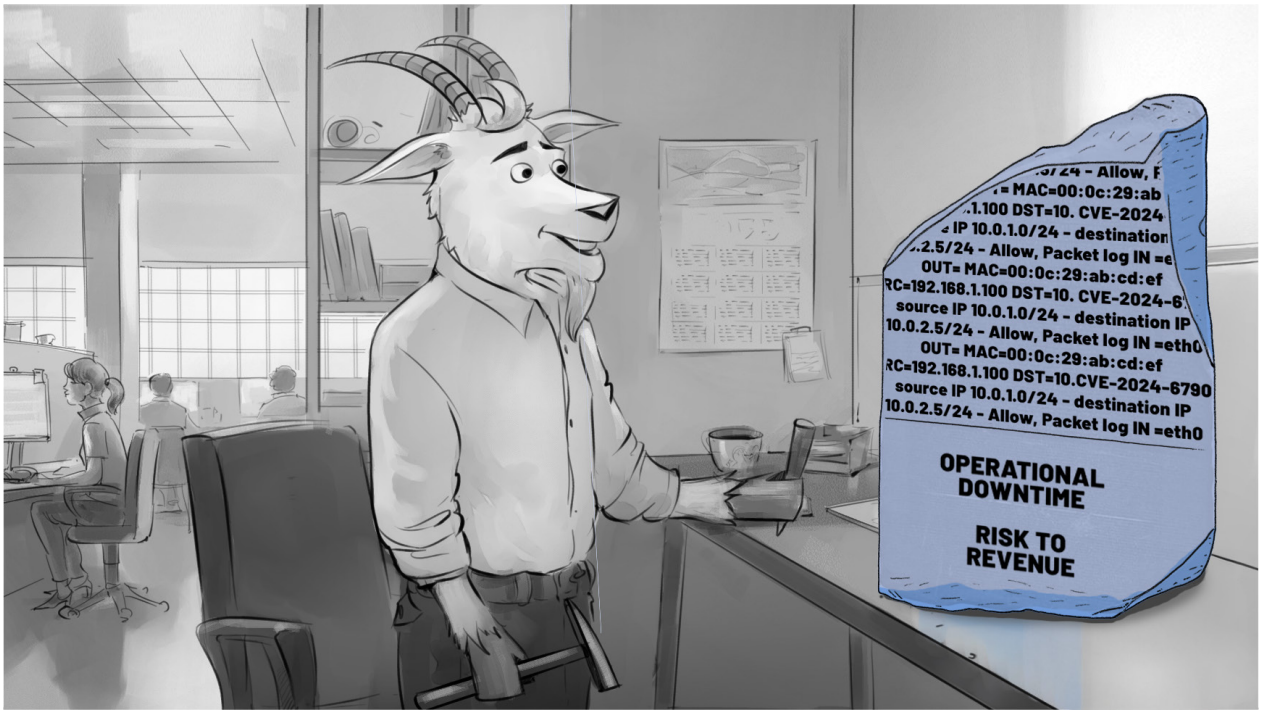
PENTERA

Foreword

This guide brings together the insights and experience of CISOs and CIOs from around the world into a practical playbook for security leaders. It's grounded in their real-world experience of reporting cyber risk to the board - navigating regulatory demands, presenting complex data clearly, and earning trust where it matters most.

Narrated by the fictional Gary Grit, a cyber GOAT, it walks readers through the nuances of risk reporting, regulatory accountability, business alignment, and how to become the board's trusted advisor. From managing incident fallout to communicating security posture across business initiatives, this guide brings clarity and, practical tips to one of the most high-stakes aspects of a CISO's role.

One-Introduction
Your Rosetta Stone to Board Literacy



Hey there, my cyber fellows.

Several months ago, I trotted into my new role as CISO at Grazing, Inc., and it's been a wild ride! We've tightened up our defenses, rolled out the framework for Continuous Threat Exposure Management, aka CTEM, and dug ourselves out of the post-breach hole.

But now comes a different kind of challenge - my first board of directors meeting.

I'm no novice at this, I've led board-level meeting discussions before - just never with this herd. So I turned to my notes from previous board meetings to refresh my memory and get myself into the right mindset. I also reached out to my network of fellow CISOs, who include a few wise old rams who've weathered more boardroom storms than I have. I asked them what worked, what flopped, and how they earned the board's trust without boring them with firewall logs or vulnerability charts.

Their advice was clear: Understand what's top of mind for your board and present the relevant facts, not more, not less.

Every board is different. Some are hyper-focused on financial risk, others on operational uptime, brand reputation, or compliance. Before you can speak their language, you've got to learn what keeps them up at night.

It took me a while to realize that communicating cyber risk isn't about dumbing things down. It's about reframing. Turning technical truths into business insights. Showing the board how cyber threats connect to things they care about most.

This guide aims to be a Rosetta Stone - helping you turn exposure data into compelling, business-relevant narratives that your board can understand and act on.

Inside, you'll find practical tools, proven frameworks, and real-world stories that show how other CISOs turned those board meetings into meaningful moments of influence. Trust me, learning the language of the board is key to your success, as you become the board's trusted advisor for all things related to cyber risk.

So let's get to it. These are the items we'll be addressing:

- Why Cyber Reporting is More Critical Than Ever
- The Business Issues That Drive Board Concern (Grab the cheat sheet included!)
- The Board Report: Where to Start
- Where Reporting Typically Fails: Tips on What to Avoid
- Share a Story, Not a Status Update (The celebrity threat briefing template)
- Keeping the Focus: Using Outcome-Driven Metrics (The 9 ODM starter pack)
- Demonstrating Progress: Using Protection-Level Agreements
- Map Risk to Strategic Business Initiatives (Get the M&A reporting template)
- Presentation Template for the Next Board Meeting

This is the guide that I wish my peers shared with me back in the day, and hopefully, your roadmap to becoming the G.O.A.T. of cyber risk communication.

> ***I start with what I want them to come away with and structure the conversation around it.***
>
> 3-time manufacturing company CISO
> and board member at 2 tech companies

Two

Why Cyber Reporting is More Critical Than Ever

Whew! The board meeting's coming up fast and I know it's not going to be a walk in the pasture. The stakes feel higher than usual because having already met some of the members, I know they're a sharp and strategic group of thinkers. It's clear cybersecurity isn't buried in the IT appendix anymore, it's inching closer to center stage. And honestly, it's about time. As to why cyber is getting more board attention recently, I think there are a few reasons why…

1. Regulatory Pressure is Real!
From the U.S. SEC's new cyber disclosure rules to Europe's NIS2 directive and the UK's Cyber Governance Code of Practice, one message rings loud and clear: boardrooms are now in the breach blast radius. Directors are being held personally accountable for cybersecurity oversight, and failure to show defensibility isn't just embarrassing - it's potentially career-ending.

This is not just about ticking boxes anymore. It's about proving, with clear documentation, that my organization is aware of its risks and is actively reducing them. Regulators are no longer asking, "Did you get breached?" They're asking, "Did you see it coming, and what did you do about it?" As Grazing's CISO, it's on me to arm my board members with the understanding and the proof that we've done everything within our power to protect our most valuable assets and data.

2. Cyber is Being Seen as a Business Risk
According to Gartner[1], 88% of boards now categorize cybersecurity as a business risk. That means they don't want to hear about buffer overflows or port scans, they want to understand exposure and their defensibility. They want to know:

- Are we more secure than we were last quarter?
- How do we stack up against recent headline breaches?
- What's our risk relative to others in our vertical?

I view this as an opportunity to switch the narrative. Go from being the bearer of bad news to the strategist helping my board members sleep at night.

3. Defensibility Is the New ROI
Let's face it, "return on security investment" has always been a murky metric. But today, the ROI is clearer than ever: **don't just protect your systems - show it in the numbers.** Strong cyber reporting helps me demonstrate that I have the right insights, I'm making informed decisions, and I've taken action. That's my legal shield. That's my business case.

Lead the Herd

Here's the kicker: too many CISOs still aren't fluent in boardroom speak. That's a shame because this is our chance to lead, not just in tech stacks and compliance strategies, but in conversations that truly matter. I step into the room and show my board I've got the roadmap, the metrics, and the mindset to steer the ship, not just avoid icebergs.

Next, I hope to spend more time with the team fine-tuning our security objectives to make sure they're aligned with business initiatives. Then we'll be able to determine what tactics we'll deploy to achieve them.

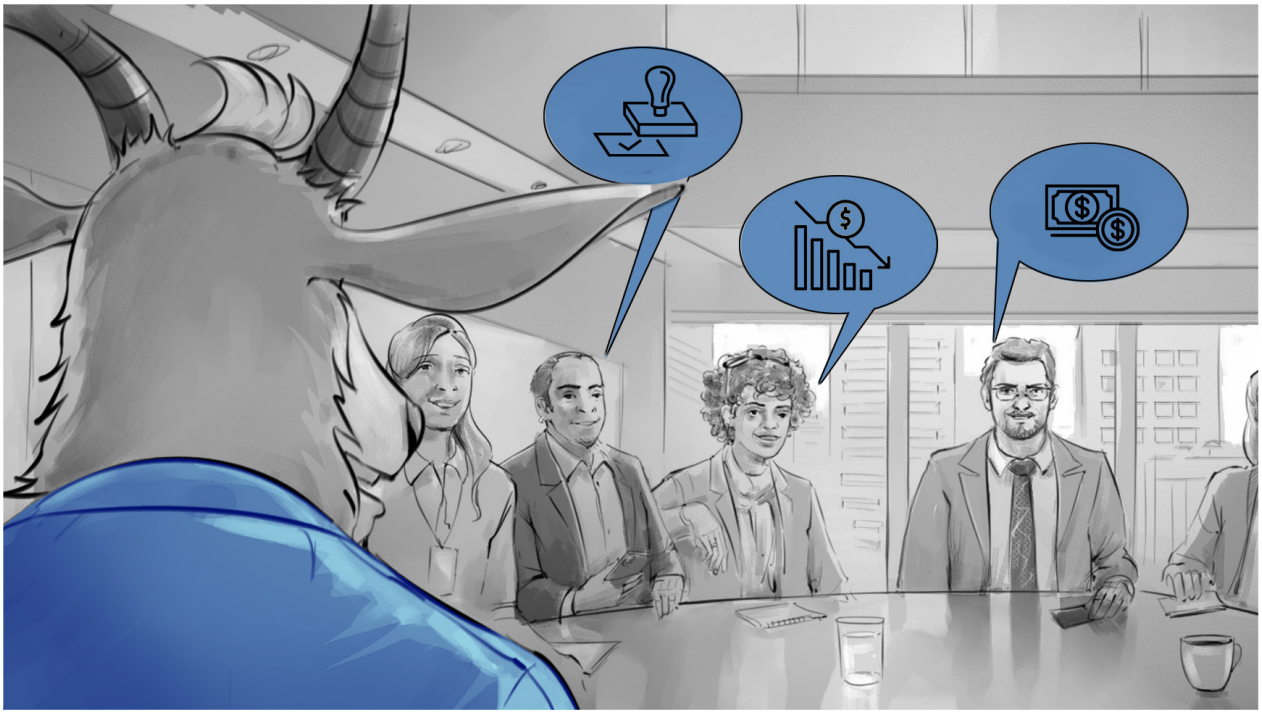
Also, I promised my kids a picnic at the goat park on Sunday if I survive another round of revision requests. Hooves crossed.

> ***If you show up to the board meeting asking for a budget, you've already failed. Those conversations should happen before and add a full-stop at the end.***
>
> 5-time tech company CISO

[1] Gartner, 2024 Growth Agenda: Align Cybersecurity Investments with Business Grown, 11 June 2024

Three

The Business Issues That Drive Board Concern



It took me a long time to realize this, but it's a truth everywhere I've worked - the board doesn't care how many vulnerabilities we patch, they care about how cybersecurity is helping to move the business forward.

This means shifting gears. Less talk about CVEs, more about how we're enabling growth, protecting customer trust, and minimizing possible disruption. I'm not chasing perfect security - I'm building smart, risk-informed defenses that keep the business agile and safe.

If security is too tight, we frustrate users. Too loose, and we end up on the wrong side of the news, or worse, a regulator. So, I told the team, "We're done reporting posture for posture's sake. It's time to show how security supports business outcomes."

To help with that, I created a quick guide that aligns cybersecurity with the issues boards actually care about. Whether it's regulatory pressure, operational resilience, or shareholder trust, this is how we frame the conversation.

Use this cheat sheet to frame the conversation when speaking to the board:

Board Concern	Translation to Board Speak
Data Protection	• Are the organization's most critical assets - its "crown jewels" and core servers - adequately protected? • Which systems, if compromised, would expose the company to the greatest risk?
Business Operations	• What is the potential impact of a cyber incident on operational continuity? • How much downtime could key systems endure before disrupting service delivery, revenue, or customer experience?
Regulatory and Compliance Exposure	• What level of cyber risk is considered acceptable by regulators? • Are current controls aligned with mandated standards such as SEC disclosure requirements, NIST, GDPR, or industry-specific mandates?
Legal Liability	• In the event of a breach, would the organization's chosen level of protection be considered defensible? • Would the chosen risk level meet legal thresholds of duty of care?
Partner Ecosystem Risk	• How would accepted cybersecurity standards affect existing and potential partnerships? • Will third parties view protection levels as sufficient to warrant trust and continued collaboration?
Brand Reputation and Shareholder Trust	• Are the current risk levels justifiable to customers and investors? • If a breach were to occur, would leadership be able to demonstrate that reasonable defensive measures were taken?
Cyber Insurance Viability	• Do our protection levels meet or exceed insurer requirements? • Could higher protection benchmarks reduce premiums or broaden coverage terms?
Benchmarking Against Peers	• How does our cybersecurity posture compare to industry standards? • Are we meeting, exceeding, or falling behind the security maturity levels of similar organizations?

Next, I'll show you how to start formulating the board report, now that we've identified the board's priorities. But tonight I'm heading to a goat yoga class. Really looking forward to it, nothing relieves stress like cradling a baby goat!

> ***You need to speak the board's language as much as possible, in order for them to have any chance of understanding the implications of what's involved for any risk.***
>
> Global CISO, IT Executive (CISSP/CRISC), ORBIE Winner

F o u r
The Board Report: Where to Start?

I'm rolling up my sleeves, putting on my reporting gloves (yes, they're needed), and getting to work preparing our next board update. Consider yourself warned, this isn't something you can pull together the night before. I want to give the board something meaningful, not just a data dump, so I've got to build our story step by step.

Here's how I approach it and how I recommend every security leader get started:

Step 1: What → So What → Now What

First things first: Crystalize the message. I structure my report in a way that ensures the key messages get across loud and clear.

- **What happened?**
  We ran a safe version of the Conti ransomware strain. Found it could jump from DevOps to Finance in three hops. Conti has been linked to high-profile attacks across healthcare, finance, and manufacturing. It boasts a trail of destruction that's made it a top-tier threat.

- **So what?**
  That means our finance data was one phishing click away from encryption - where all that data would have become inaccessible. As far as regulators are concerned, that's a material risk.

- **Now what?**
  We've isolated the relevant pathways that gave way to the attack, mitigated the vulnerabilities, and we're retesting every two weeks to confirm.

Step 2: Get the Right Data

I don't just throw every metric at the wall to see what sticks. I start by asking: Which assets are most valuable for Grazing? Which exposures could truly disrupt our operations?

Using Pentera, my team and I prioritize risks that impact our crown jewels: customer systems, production environments, and anything that could lead to regulatory or reputational fallout. This risk-based lens is what frames the entire conversation. If it doesn't affect business outcomes, it doesn't make the cut.

Step 3: Deliver the Evidence

Once I have our high-impact exposures locked in, it's time to validate and show how the gaps are being managed.

We use ServiceNow GRC for compliance reporting and showing risk alignment with regulatory requirements. And Pentera helps us map out attack paths, validate whether controls are actually working, and confirm if key exposures are being closed. That evidence becomes the heart of our report: "Here's the issue. Here's what we fixed. Here's what still needs attention." This level of validation isn't optional - it's table stakes. Think NIST, ISO 27001, SEC disclosures. They all expect verifiable risk mitigation.

Step 4: See the Trend

Last, but definitely not least, I'm establishing trendlines. Cyber reporting isn't static, it's about progress (or lack thereof).

By tracking risk metrics over time, especially for those same high-priority assets, I can show the board how our posture is evolving. Where we've improved, where we've regressed, and what changes (like a new cloud rollout) had ripple effects.

Pentera's continuous validation makes this easy. Anytime our environment changes, we get an updated snapshot. That means no surprises, and no excuse for flying blind.

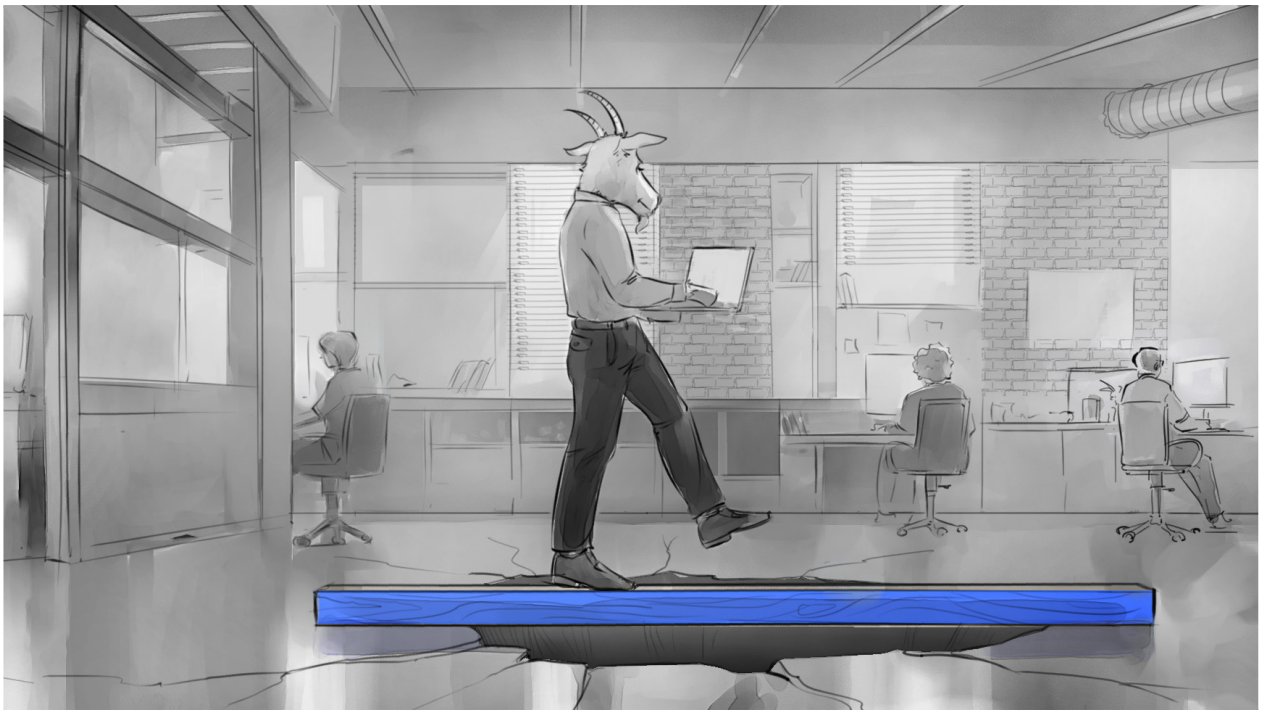
Tomorrow, I'll be packaging this up into a presentation for the board. But for now, I'm celebrating small wins: a clear narrative, backed by real data, that shows we're building not just a secure org, but a resilient one.

Also, this weekend? No dashboards, no detection rules. Just me, a hammock, and a new book titled "Zero Trust for Goats." Sounds like a classic.

> ***Don't present technical debt as failure. Present it as a conscious tradeoff the business made - and show the plan to address it.***
>
> 3-time manufacturing company CISO and
> board member at 2 tech companies

Five

Where reporting typically fails: Tips on what to avoid



An old board report draft from before my time fell into my hands recently. Let's just say… it reads like a firewall config file met a compliance checklist in a dark alley. No narrative. No context. Just numbers. The last thing I want is for my board members to glaze over and tune out, so here are the five most important things I avoid when building my report:

Pitfall #1: The Tech Swamp

Too many reports drown in jargon - firewalls, SIEM logs, CVSS scores, TLS versions. The board doesn't need a lesson in protocols. They need clarity on risk so you need to provide the context: what's exposed, what that means for the business, and what's being done about it?

Tip | Translate tech into business impact. Instead of "unpatched RDP endpoint," try "a vulnerability that allows lateral movement to our financial systems."

Pitfall #2: The Data Dump

Throwing every metric onto a slide doesn't show progress - it shows panic. Dishing up tons of data with no direction or context just runs the risk of confusing your audience. For example, don't just take the latest pentest with all those numbers of ports left open and misconfigurations left exposed.

Tip

Pick 5-7 metrics that matter. Focus on exposure to critical assets, remediation timelines vs. operational constraints, and trends. Tell a story: where you were, where you are, and where you're headed.

Pitfall #3: The One-Way Brief

Reporting without a call to action is like presenting a menu with no intention of preparing the meal. What does the board need to do?

Tip

Be clear. Do you need funding? Policy support? Executive alignment? End with a recommended course of action, not a hypothesis.

The Golden Rule: Be Honest

It's not your job to provide air-gapped-level protection, but it is your job to provide transparency. If there's exposure, say it. Then show the plan to fix it and the cadence to track it.

My team and I do just that. We show how exposure to a database has been reduced by 80% over two months, while mapping out the remaining 20% - what's blocked, what's in progress, and what needs executive support.

> ***Don't try to make everything perfect.***
> ***Come humbly and let the board understand your trade-offs.***
>
> 3-time manufacturing company CISO and
> board member at 2 tech companies

S i x
Share a Story, Not a Status Update

When I work on my board presentation, I never start with numbers. I start with a story.

Here's the trick: if you open with "patch rates are up 13%," you've already lost them. The board isn't there for a status update; you need to lead with a narrative that leads to smart decisions.

So I follow this tested-and-proven narrative arc:

Use Metaphors to Make It Stick

Boardrooms are full of smart folks, but they're not living in the SIEM. To help your message land, wrap it in something familiar. Metaphors go a long way to communicate technical risk into business-relevant messages that have clarity and support recall.

Instead of:

> *"We identified a subset of internal endpoints, primarily remote laptops and contractor workstations, that are still accessible without enforced MFA. These exposed endpoints lead to key services like internal databases, the AD, and shared mounted file systems."*

Try:

> *"It's like lowering the drawbridge to the castle. Sure, the castle walls are there, but anyone can come in if they just walk across the drawbridge."*

Or for a more modern-day twist:

> *"Think of our cloud posture like a cargo ship, one loose container can cause a spill, even if the rest of the ship is tight."*

Metaphors give your report color, make your insights memorable, and help the board retell your story when you're not in the room.

> ***Make it a suspense story.***
> ***What changed? What's next? Show you're climbing the mountain.***
> 5-time CIO at multiple tech companies

Keep It Structured

I really try to apply the age-old saying of *"Keep it simple, stupid."* Each element is concise and to the point. I don't assume they remember a strategy that I presented a while ago. Instead, I open with the big story, not a stack of charts, and repeat the narrative at every meeting. Board members are busy people, they forget. That's okay. Repetition is reinforcement.

This structure isn't just good communication, it's a key quality of leadership.

Anticipate the "Celebrity Threats"

Don't wait for someone to ask, *"Could Volt Typhoon get to us?"* Be ready. In cases like that, I open with:

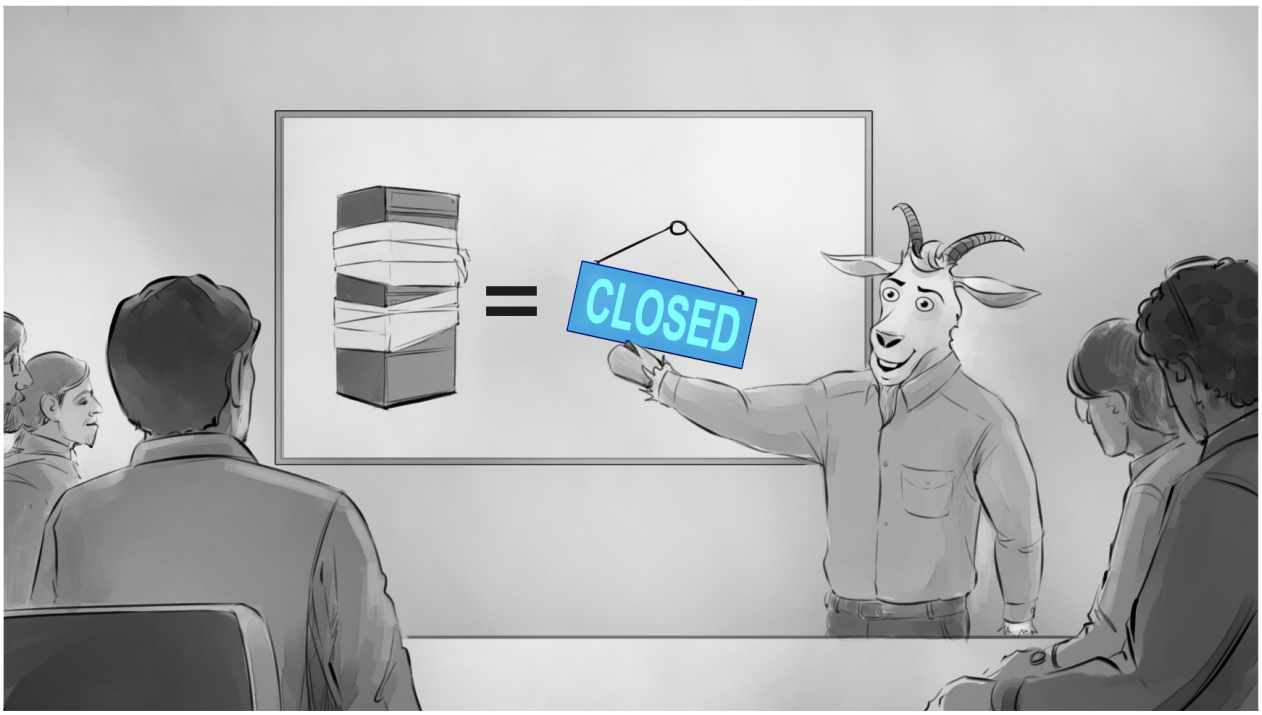
> *"You've probably seen headlines about MGM and Volt Typhoon. We ran emulations. Here's what we found… Here's what we fixed…"*

To do this, I validate the threat, confirm its impact, and map the defenses. Typically, after showing this, the board's trust in our program shoots up like a goat on a rocket.

Check out this template I prepared for briefing the board on a celebrity threat. No matter how you use it, always remember: tell the story, lead the narrative, and never let your airtime go to waste.

> ***Your stakeholders are bombarded with information from internal and external entities. Your goal must be to become their trusted advisor in Cybersecurity.***
> 30 year veteran CIO at leading tech companies

S e v e n
Keeping the Focus - Use Outcome-Driven Metrics (ODMs)



Back when I was a young buck, I used to walk into board meetings armed with charts on "critical vulnerabilities" like it was golden hay. Turns out, nobody cared. But when I said, *"Here's the risk of customer downtime if this goes unpatched,"* every eye in the room locked in.

That's the power of **Outcome-Driven Metrics**, or ODMs.

Let me explain how I picked these, because I didn't just throw darts at a buzzword board. I wanted metrics that actually mean something - to me, to my team, and most importantly, to the board.

These were my criteria:

1. **Risk Comes First:** Every ODM I chose ties to a real threat, phishing, malware, third-party vulnerabilities. If it can cause a breach, it needs a metric.

2. **Bottom Line is Impact:** I always ask, *"What could knock out operations or damage trust?"* That's why I'm tracking things like DLP rules and disaster recovery, because they matter when things go sideways.

3. **Visibility Into Control Effectiveness:** It's not enough to say we have tools. I need to know if they're working. Are malware detections trending up? Are our crown jewel systems patched fast enough? I need to answer that.

4. **Relevance to Business Strategy:** Whether we're launching a new product or vetting a company for acquisition, I need to ensure all the new practices are aligned with our standards.

So ODMs aren't just about creating new acronyms for cyber (we all know there's more than enough!) It's how I turn cyber performance into boardroom fluency. None of them require a decoder ring, but are all clearly understandable in five seconds flat. This was one CISO's nine-point ODM model - and it's a beaut. (In fact, I've adapted my own scorecard based on this model)

Attack Vectors	Defensive Posture	Enterprise Risk
1. % of employees failing phishing tests	**4.** % of internet-facing assets patched within SLA	**7.** Third-party risk score for critical vendors
2. Malware detections (trending up or down?)	**5.** Crown jewel systems patched within xx days	**8.** EDR coverage on servers and endpoints
3. DLP rules triggered (especially for customer data)	**6.** % of internal servers lacking any compensating controls	**9.** Disaster recovery testing success and recovery time

The metrics that I developed for our environment keep me focused on business outcomes, not pin-point issues like firewall logs.

Real Talk: How ODMs Change the Conversation

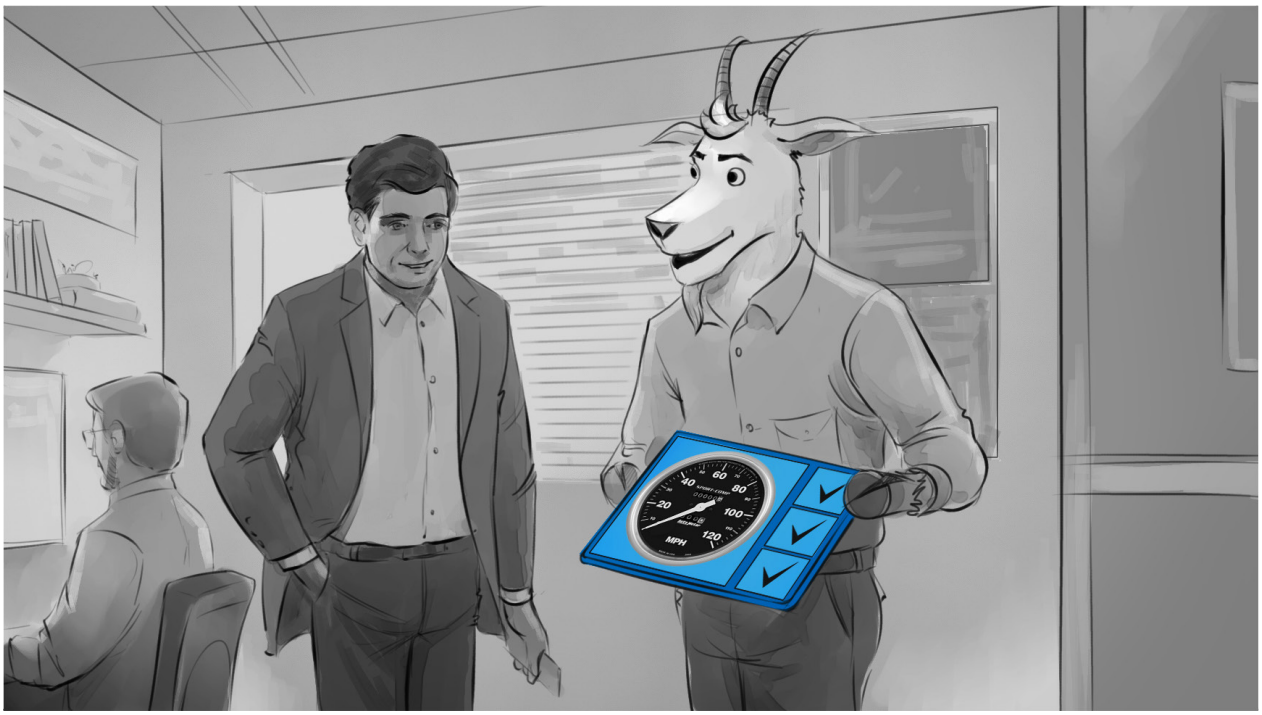
In the past, I've used ODMs to frame our patching cadence. We committed to patching all crown jewel systems within 15 days. The board saw and approved. Why? Because it's measurable, consistent, and defensible. But always ask: Does this metric move the business?

Insights from Splunk and Microsoft Sentinel make it easy, we can aggregate security telemetry into measurable, board-facing KPIs and then use CyberSaint for mapping metrics to business outcomes.

Next, I'll share how I apply KPIs to each of my metrics. But tonight, my wife and I are planning to watch, "The Men Who Stare at Goats" with George Clooney, as he tries to take down goats with his mind. As if that's even possible!

> ***You don't need ROI. You need to show defensibility and materiality. That's what the board cares about.***
>
> Global CISO, IT Executive (CISSP/CRISC), ORBIE Winner

E i g h t
Demonstrating Progress: Using Protection-Level Agreements (PLAs)



We've done it and I'm so glad we're on the other side of it! We formalized our **Protection-Level Agreements**, aka PLAs. Think of them as SLAs, but for cyber risk. They make the invisible visible and the vague verifiable.

How do PLAs fit in with ODM? The ODM is the barometer that you report on, the PLA is gauging the level to which you've been able to meet it.

A PLA becomes a mutual commitment between security and leadership. It says:

- *Here's how much protection is required*
- *Here's the level that we've protected it to*
- *Here's the variance to which we've met it*

For example, our endpoint PLA states: All endpoint protection coverage on critical systems need to be validated every month. Simple and clear, it totally cuts out the guesswork.

ODM	PLA	Last Conducted	Variance
Validate endpoint protection coverage on critical systems	Monthly	28 days	2
Validate endpoint protection coverage on other systems	Bi-monthly	74	-14

PLAs make metrics manageable. If we meet the benchmark, great, we're aligned and defensible. If we miss it? That's not failure - it's a signal. It tells us that we either need more budget, better tools, or a segmentation strategy to reduce the exposure.

We didn't pull numbers out of the haystack. We use a history of assessment results and benchmark ourselves against similar companies via SecurityScorecard. So we have an idea of whether we are leading, lagging, or just holding the fence up with duct tape.

This measurement technique arms the board with confidence that our expectations aren't just arbitrary, but pragmatic to the needs of the organization and are industry-aware.

Grounded in Reality

I can't claim defensibility without clarity. PLAs are my proof. They show that I acted within a defined risk posture, and they highlight where I need to evolve.

See this example of how I will add PLAs to my regular cyber threat report:

Our Current PLA for Mitigated High Severity Vulnerabilities

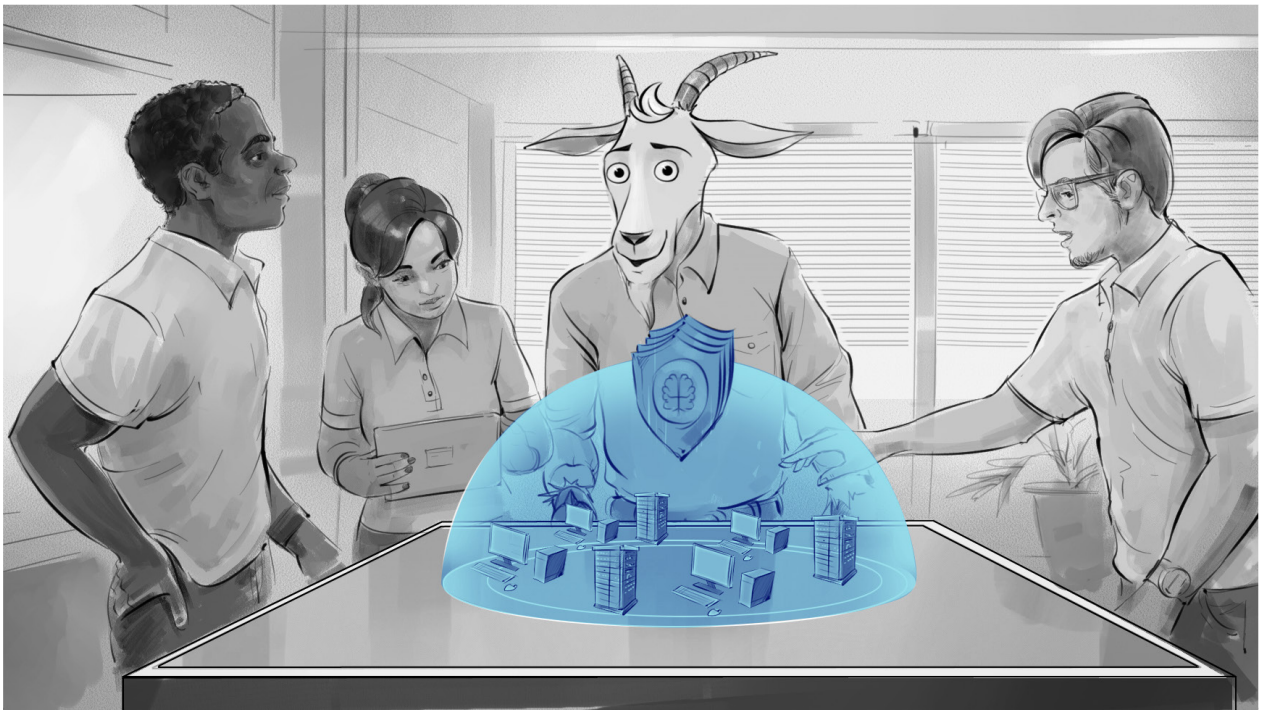
- **Detection Time:** 85% of high-severity vulnerabilities detected
- **Remediation Time Frame:** 92% of exposed paths were remediated within 72 hours
- **Isolation Readiness:** Confirmed automated isolation of compromised endpoints (response time under 10 minutes)
- **Residual Risk:** <10% of assets currently require further hardening

Next, I'm mapping PLAs to each critical business unit. Meanwhile, I've promised my wife a PLA of my own: "Zero emails after 6pm unless it's an emergency."

Spoiler alert: I've already violated it. Twice.

> ***It's not about patching everything. It's about showing that our critical assets are covered and that our controls are consistent, reasonable, and effective.***
>
> Director, Cybersecurity & BISO for multinational organizations

Nine
Map Risk to Strategic Business Initiatives



Recently, it feels like I have been trying to herd cats, but instead of cats, they're business initiatives running off in every direction. M&A talks, cloud migrations, new product launches. Everywhere I look, another flag goes up saying, "Cybersecurity, we need you!" It's both exhilarating and exhausting at the same time. But this is exactly where CISOs belong - not just in the SOC, but in the strategy room.

Tying Protection Levels to Business Moves

Whether we're launching a new product or absorbing another company, I ask four questions:

1. What new risks does this introduce?
2. What's already protected?
3. What still needs fixing?
4. How will we track this through execution?

We use our ODMs and PLAs as a starting point. When checking companies Grazing is considering for acquisition, their systems have to meet our baseline before anything else happens. No exceptions. I tell the executives, "We don't want their security surprises becoming our security emergencies."

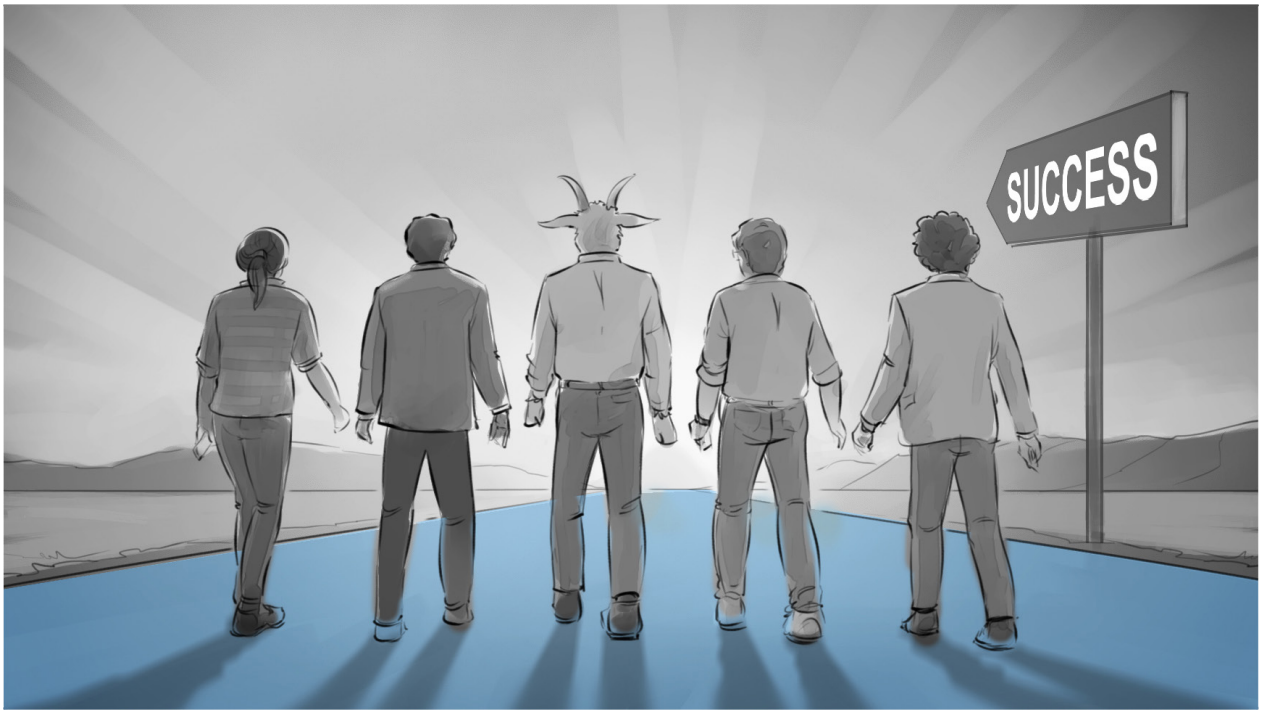
As I was briefing my team on a recent M&A project, I pulled the Marriott/Starwood story out of my hay feeder. "Remember this?" I said. "A missed vulnerability in one environment became a $100 million lesson for the purchasing company." No one wants to repeat that, so everyone is on board. By the project's end, I created this M&A project cybersecurity report template that you can use and adapt to your environment and requirements.

Automated tools are key, as they show the gaps fast. In fact, we use CATO Networks to provide secure scalable and policy-enforced connectivity to help us monitor the remote environment. Then, we use Pentera to replicate attack paths remotely. Turns out, one misconfigured access policy exposed a database node. We flagged it, fixed it, and reran the test within 48 hours. Meeting delivery timelines - that's how I've built trust with business teams.

Next, I'm scheduling one-on-one time with each business unit leader to get ahead of their security initiatives. But tonight, I'm treating myself to a cheese platter and catching up on "Goats of Anarchy" videos. Honestly, those goats have a better business continuity plan than some organizations I've seen.

> ***Security is not a 'no' word, it's an 'empower' word.***
> ***Let's empower the business to thrive, safely.***
>
> 3-time CISO at public companies & cybersecurity visionary

Ten
Closing Note



The board meeting's finally behind me. After weeks of prep, thinking through the narratives, crunching the numbers, and a near-burnout of my laptop battery, it feels really good to be on the other side of it.

It's been one heck of a journey through the trenches of cybersecurity communication, but these lessons have helped transform me from a tech translator to a boardroom rockstar (if you don't mind me tooting my own horn about it).

The journey from jargon jungles and blank stares to executive savvy, can take a while and oftentimes be a bumpy road. But I've gotten to a point now where I'm equipped to make board presentations clear and aligned, not technical. I present confidently and with proof, I show rather than tell, and I own the narrative by aligning it to the strategy.

So here's my final tip: Don't chase perfection. Chase progress. How do you do this? Validate your posture, speak the board's language, and use every project as a chance to show that security enables business.

Signing off now, with a plan and a fair amount of grit,

Gary Grit, CISO
Grazing, Inc.

Gary Grit CO

Appendix

CISO Board Report Template
Download

Celebrity Threat Report Template
Download

M&A Reporting Template
Download

Tested Security is Trusted Security

Pentera is the market leader in Automated Security Validation, empowering companies to proactively test all their cybersecurity controls against the latest cyberattacks. Pentera identifies true risk across the entire attack surface, prioritizing and guiding remediation to effectively reduce exposure. Pentera's security validation platform is essential for Continuous Threat Exposure Management (CTEM) operations.

Key aspects of Pentera's exposure management approach include:

- **Automated Attacks:** Conduct continuous penetration testing across the entire attack surface, mimicking attacker techniques to identify exploitable vulnerabilities and misconfigurations in your security defenses.
- **Prioritize based on real risk:** Score the vulnerabilities based on their exploitability and potential business impact, so you can focus resources on the most critical exposures. Provide relevant teams with clear recommendations for effective mitigation.
- **Comprehensive attack surface mapping:** Get full visibility of external and internal assets to uncover blind spots across your networks, endpoints, and cloud environments.
- **Integration with security ecosystem:** Seamlessly integrate Pentera with your existing security tools to streamline workflows, enhance remediation efforts, and automate vulnerability management processes.

Pentera's approach ensures organizations can proactively manage their exposure, minimize risks, and strengthen their defenses against active cyber threats. For more information: Pentera.io

Trademark Disclaimer

Copyright ©2025 Pentera. All rights reserved.