Secureworks®

EXECUTIVE SERIES

Reporting to the Board

A Toolkit for CISOs

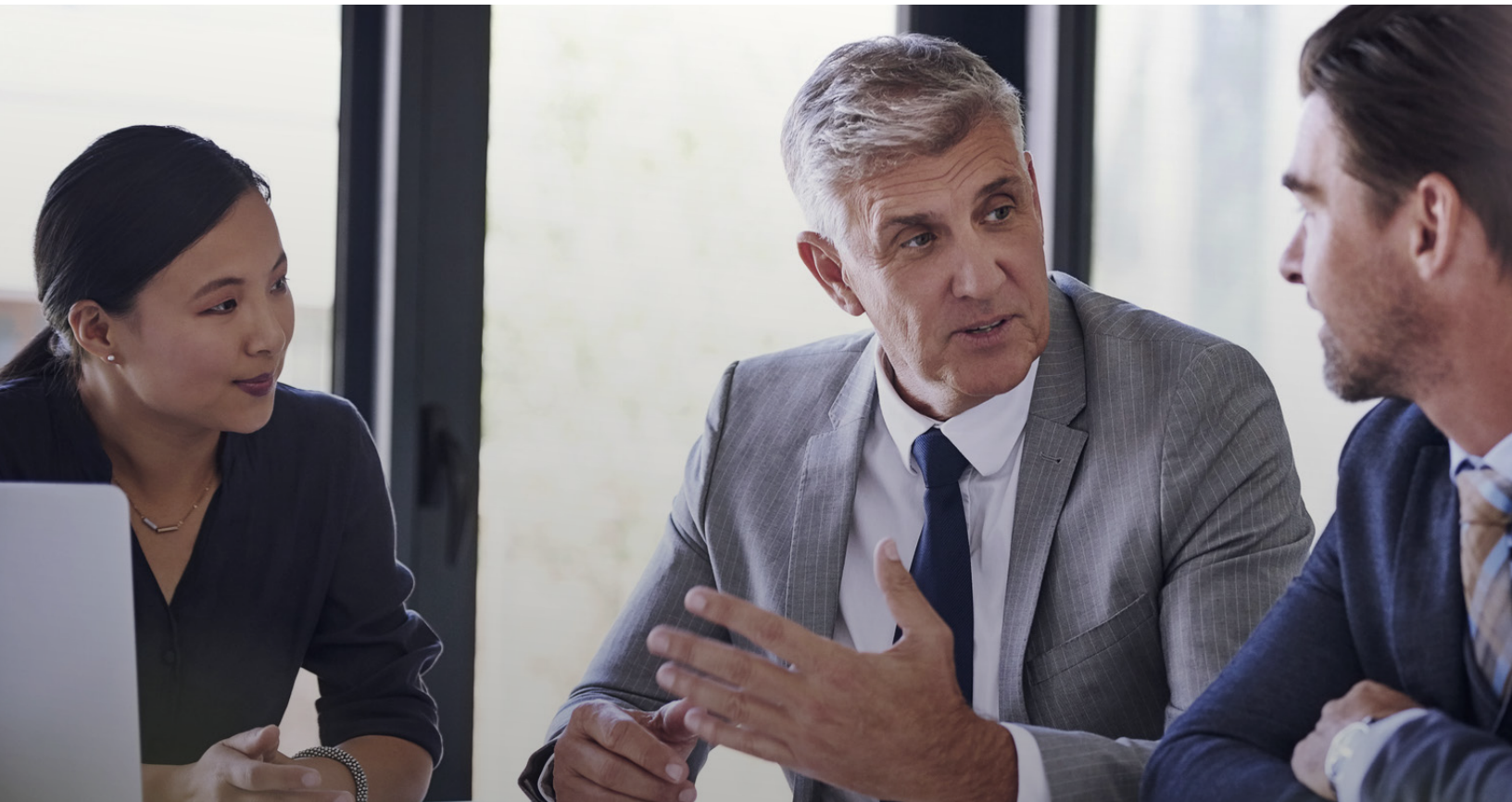


Table of Contents

Secureworks®

Introduction

Now more than ever, cybersecurity is a front and center priority for boards of directors. As businesses become more digitally empowered due to the shift to remote work and cloud migration, cyber threats are finding more ways to breach defenses, increasing the risk to business operations and bottom line. From loss of revenue and intellectual property to legal liability and reputational damage, plus the cost to resolve, boards of directors bear the responsibility for appropriate oversight of the risks associated with a breach. To execute their due diligence, they rely on their organization's cybersecurity leader to help them understand two things: What are the risks to the business, and how well is the company managing those risks?

In this toolkit, you'll find steps for building a foundational relationship with your board, techniques for implementing a successful reporting process, and tips for creating a board presentation agenda that will help you establish your role as a trusted and credible leader.

Informed by customer input, as well as observations across more than 4,000 customer organizations globally, this guide is comprised of leading practices from Chief Information Security Officers (CISOs) from all types of industries. These CISOs have established strong C-suite and board reporting relationships. Secureworks® believes these practices will better position CISOs to not just survive a crisis, but lead through a breach, should one occur.

Boards are Increasingly Concerned About Cybersecurity

Boards have a responsibility to protect shareholder value. And now the assets on which corporate value depends are largely digital and intangible, putting them at risk from cyber threats.

88% of boards of directors view cybesecurity as a business risk.

In 2016, that number was **58%.**

Source: 2022 Gartner Board of Directors Survey

Seven Objectives for Your Board Reporting Relationship

1. Provide practical knowledge of the threat environment.
2. Identify your company's top risks.
3. Demonstrate that your security strategy is aligned with your company's risks, tolerance, and goals.
4. Adopt a company-wide cybersecurity risk management framework.
5. Establish benchmarks based on the results of testing and assessments.
6. Develop a dashboard to monitor cybersecurity risk over time and against relevant benchmarks.
7. Establish and agree on a roadmap to demonstrate progress.

You'll know you've met your cybersecurity reporting goals when your board:

- Understands risk in the context of your unique business and its objectives.
- Can confidently say that risk is managed effectively and there is a process in place to continually test those assumptions.
- Can confidently say the security investment is appropriate to both known and anticipated risk.
- Has a high degree of confidence that your organization is crisis-ready.

Embrace the Opportunity

As the Chief Information Security Officer (CISO) role continues to evolve from security expert to business leader, more security leaders are answering the call to provide their board of directors with a better understanding of how, and how well, the organization is managing the business risks inherent in a cybersecurity breach.

This is not a simple task. Even CISOs with a well-established board reporting relationship must adapt their tactics as board members grapple with new and unfamiliar risk issues, such as global data protection regulations or digital transformation.

It's difficult for board members, too. The linkages between cybersecurity risk and business risk aren't always intuitive to business leaders who don't have an IT or security background. Your boardroom audience has very little insight into the complexity of your operations or the persistence of your cyber adversaries. It's up to you to share enough information to ensure they are confident the risks are well-managed, without overloading them with details. Legal, risk, and security advisors encourage board members to focus on the big picture issues, such as those shown in Figure 1.

To avoid making conversations with your board feel more like an inquisition than a briefing, be proactive in your approach and pre-align your primary talking points with the board's priorities. Board members are conditioned to test assumptions. The key to understanding the board's expectations - before you walk into the room - is careful preparation.

As challenging as it can be to establish the right reporting framework with your board, there are rewards. When you present to the board and executive team, you have an opportunity to educate, align priorities, and ask for leadership support in the areas where you need it most, such as holding other functional areas accountable or gaining a seat at the table in strategic initiatives.

Figure 1: Eight Areas of Board Oversight for Cybersecurity Risk (Source: Board Cyber Risk Oversight Framework, Secureworks)

Lay the Right Foundation to Improve Receptivity

Board meeting agendas are tightly packed, and directors can be quick to deprioritize what they are hearing if they don't relate to the content. To significantly improve receptivity, be proactive about two things: fostering one-on-one interaction with board members outside of the formal setting and laying an educational foundation about the cyber threat environment, including threat actors and their motives.

Do Your Research

Understanding perspectives and motivations in the boardroom is a good way to establish trust and gain confidence. Research the backgrounds of your board members to determine what they bring to the table. Are they former CEOs or CFOs? Have they led corporate mergers or digital transformations previously? Each one brings a unique leadership perspective to the table that may predispose them to interpret your reports and proposals differently than you expect. What's more, directors often serve on more than one board, particularly in public companies, and may bring expectations about cybersecurity shaped by their experience with those other businesses. A little homework will tell you if one of your board members has been through the trial of a public breach.

Make It Personal

No matter how much research you do, meeting directors for the first time in a formal presentation is not ideal. It's helpful to have a few well-placed advocates for cybersecurity before wading in. Forming individual relationships with select members of the board and executive leadership team ahead of time is even better. Start by identifying those with the strongest interest in the subject matter. Discuss the organization's strategic initiatives and gain an understanding of what keeps them up at night.

Some CISOs have found it useful to find a sponsor among the executive team, often the CFO or General Counsel, who is willing to share information about the company's strategic goals and facilitate an introduction to board members.

If possible, engage with the chair of the board committee with primary responsibility for cybersecurity risk, whether that be the Audit or Risk committee, or a special committee dedicated to IT, information security, or data protection. Discuss the top potential business impacts and risks that can win consensus with the broader board as the focus for your agenda. Ask them what they want to hear more about. Remember: from their perspective, cybersecurity is a means to a business outcome.

High Visibility from CISOs

90% of CISOs said they present directly to their company's board and/or audit committee, three-quarters of them on a quarterly basis.

Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2021

Take Every Opportunity to Educate

Many CISOs tout the value of coming to the boardroom prepared to discuss breaches making headline news. When a major news story breaks, board members will likely reach out and ask for assurances. Instead of succumbing to a cycle of reactionary fire-drills, use that opportunity to educate proactively. One leading practice is to offer up a simple, informative "anatomy of a breach" story.

Most board members like to improve their knowledge of cybersecurity risk by learning how a breach happened, including the result of forensic investigations, threat actor motivations, and a layman's overview of the techniques, tools, and procedures used. Effective storytelling will enable you to successfully demonstrate how the breached company became vulnerable to the threat and what your organization does differently — or could do differently — to avoid becoming a victim.

Your anatomy of a breach story should be simple. Describe the event in terms of business vulnerabilities and business impact, including reputational damage and loss of revenue, market share, or business continuity. Then discuss the potential impact of a similar breach on your own organization and how you may or may not be managing that same risk.

You have limited time to convey ideas in the boardroom. Acronyms and complex cyber speak will erode the board's receptivity to your ideas.

The more you educate your board about cybersecurity risks, the better positioned you will be to dispel myths such as, "we can't be breached" or "cybercriminals don't want anything we have." Instead, board members will begin to understand that security is a process of continuous improvement, not a one-and-done program that simply needs ongoing maintenance.

Establish a Common Language (Hint: The Language of Business)

As part of their risk oversight responsibility to stakeholders, corporate directors must quickly identify risk and progress trends. Establishing a common language with your board—defined as using the same specific terms and definitions for cybersecurity metrics every time you meet—makes the board's job much easier, and will help you win the board's confidence and trust.

Dialect is also important. The language of business is numbers, including revenue and margins. The language of cybersecurity operations—e.g., signatures, cryptography, and exploits—has no place in board reporting. You may have success pulling in a few select operational terms, but only if they are defined well and reinforced quarter after quarter. You want them to become part of your common language with the board.

In the boardroom, time is limited, so eliminate acronyms from your vocabulary. Acronyms, without definition, will erode the board's receptivity to your ideas. And pausing to define a term like IPS will rob you of time that might be more wisely spent on making a case for your budget or establishing your credibility.

Reporting Tip

FUD is Not Your Friend

Ensure that the tenor of your security discussions is balanced between pessimism and positivity.

The threat environment is justifiably scary. Rather than sowing fear, uncertainty, and doubt (FUD), use your seat at the table to build confidence in your strategy to protect critical assets and accelerate revenue opportunities in the face of threats.

Join Peer Exchanges to Share Best Practices

Secureworks customers consistently cite three types of knowledge essential to doing their job:

- Insights gained through their own experiences and security tools
- Insights their vendors bring from working across thousands of customers
- Insights gained from other security leaders who share their lessons learned and best practices

Consider joining a peer networking group to discuss board challenges and learn what has and hasn't worked for other security leaders. And ask your vendors for support in developing better metrics and risk assessment conversations.

Once you've laid foundational relationships with directors and established common language, you can build confidence and trust with practical reporting.

The Dos and Don'ts of Board Reporting

What Not to Report	Consider This Instead
Acronyms	Full names and descriptions
Technical and security jargon	Business terms and a common language for every meeting
Tactical plans that tell how security works	Strategic plans that demonstrate why security is a means to a business outcome
A problem with no solution	A realistic roadmap for improvement
Metrics without measurement	Replicable metrics that track trends
Data without business relevance	Financial, operational, reputational, and regulatory concerns that align with board oversight responsibilities
Too much data	Confidence-building stories about proactive plans

Align Your Message with the Business

Too often, CISOs find that their first board presentation devolves into a contentious discussion about a single metric that the board doesn't understand. You may be tempted to pad your report with extra data in an attempt to highlight the risk, but that won't address the root cause of the disconnect. To increase board receptivity and build confidence that the risk is being managed effectively, offer enough context to make the data relevant to likely business risks and strategic goals.

Avoid the Tactical Components of Your Program

Useful board reports address business risk, not cybersecurity risk. Your message should be practical and not overly-dependent on all the details of your day-to-day battle against the adversaries. Boards expect that the organization's security program has put the appropriate IT support, controls, and processes in place to prevent what it can, detect what it can't prevent, and respond quickly to mitigate risk. They don't need to know how cybersecurity works, nor do they need to learn your whole security dashboard. What they do need to know - to exercise their fiduciary duties with confidence - is that the risk is being managed. That means they care deeply about the impact a breach could have on innovation, productivity, revenue, reputation, and shareholder value.

Use a Revenue and Margin Lens

For cybersecurity, proving a return on investment (ROI) can be a mythical goal. While some security initiatives will improve efficiencies and squeeze more value out of existing investments, it is difficult to measure a return on risk prevention. This underscores the importance of delivering your cybersecurity risk report in terms of business outcomes that impact current or future revenue and margin.

Lead with Anticipated Business Impact

Clearly articulating the alignment between cybersecurity practices and business outcomes will help manage budget expectations and avoid misaligned priorities.

Breaches have an obvious link to business impact, causing many board members to focus only on crisis readiness and response plans. When tackling the difficult task of demonstrating how the rest of your program is connected to business outcomes, it may be helpful to highlight cybersecurity's role in organizational resilience. For example:

- **What IT systems will have the most impact on business availability if they experience an outage due to cybersecurity breach or remediation?** By addressing the risk of losing business availability, you have an opportunity to discuss where to prioritize resources and enforce security policies.

- **Of all the products we deploy, which would have the most impact on revenue or reputation if it put consumer safety at risk and had to be pulled?** Help boards imagine how threat actors could use the company's unique vulnerabilities to harm customers, partners, or consumers, and then describe what protections are necessary to mitigate those risks.

- **Where is the workflow of mission-critical intellectual property that could weaken our competitive position if it were stolen or made public?** Is that system behind a firewall or in the cloud? Who has access to the information and on what devices? Discussing the flow and storage of digital assets will lead to a conversation about administrative access controls and authentication initiatives.

These questions will help directors think about the consequences of not taking security actions, and also lead to a discussion about how to prioritize and apply limited resources in a way that has the greatest impact on risk mitigation. To ensure early alignment with the company's strategic initiatives, you'll also want to emphasize positive business outcomes. Link security dollars spent to outcomes such as risk reduction, productivity achievements, and new strategic undertakings.

Put a Different Twist on Risk Tolerance and Investment

CISOs seem to universally agree on one thing: the biggest driver behind a company's level of tolerance for cybersecurity risk is whether or not they've been breached before. Low-tolerance strategies can cost more. To help board members understand the options and trade-offs:

- Start with a snapshot of the current state of risk, end to end
- Review the desired outcomes
- Present several investment options at varying levels (use a threat effectiveness lens to highlight how hard it would be for a threat to succeed and the price point to stop it)
- Articulate the tradeoffs at each level (what you will gain and what will need to be deprioritized)

In addition to assembling the data, consider interviewing C-suite leaders in advance and including their perspectives on what risks they're willing to accept. While it requires some rigor, this exercise may help you land on an agreed tolerance more quickly.

Explain the Limitations of Industry

Boards naturally want to benchmark cyber risk and investment against industry baselines and standards. Industry context—including threat trends for the type of data you handle—is an essential component of your risk assessment. It also informs regulator expectations of your company's level of cybersecurity rigor. Your challenge is, however, to expand the lens through which your board assesses risk to include the uniqueness of your company's threat landscape, including poorly-enforced policies and processes, insufficient resources for patching, poorly-architected IT infrastructure, and lack of third party oversight.

Reporting Tip

Boards should understand that if you're breached because your environment presents the path of least resistance for an adversary, it will be of little consolation that you had the same controls and investment level as your industry peer group.

Room for Improvement

Only **33%** of corporate directors say their board of directors understand cybersecurity vulnerabilities very well.

Source: PwC's 2021 Annual Corporate Directors Survey

Prepare Your Presentation with the Right Agenda and Dashboard

Security is a fairly new discipline in the boardroom, creating an undefined playing field for CISOs. Board members want CISOs to explain the organization's cybersecurity approach in terms that are easy to understand. One way to do this is to describe what problems exist and the approach to solving them. Support your statement with high-level facts whenever possible, including performance and results indicators.

Universal cybersecurity risk management frameworks, such as the NIST Framework for Improving Critical Infrastructure Cybersecurity, are essential for guiding that conversation.

Practical board reporting also demonstrates that the security program is consistently delivering on projections and promises. Your agenda, and any dashboards you present, should include adequate evidence to give the board confidence that you know the current level of risk, what vulnerabilities are a priority, and what progress is being made to address them.

Questions Boards Are Asking (or Should Be)

- Is cybersecurity being managed appropriately and effectively across our organization?
- Have we tested those assumptions with independent third parties?
- Have we established an appropriate cyber risk escalation framework that includes our risk appetite and KPI/KRI reporting thresholds?
- Do we have adequate data governance policies and controls to protect critical assets?
- How do we manage risk from our third parties and suppliers, including Cloud and critical business suppliers?
- Are we able to rapidly contain damages and mobilize response resources when a cyber incident occurs?
- Do we have a tested incident response plan for the whole business?
- How are we staying current on the threat landscape?
- Do we have adequate organizational talent to govern, own, and execute the cybersecurity agenda?
- How does our program align with industry standards, those of our peers, and regulatory requirements?
- Is our organization cyber-focused and culturally cyber-conscious?
- Are we focused on, and investing in, the right things from a people, process, and technology perspective?

Tips For Agenda Planning: Three Board Meeting Scenarios

Chances are that your next board presentation will fall into one of the following three categories. Here are some tips shared by Secureworks customers for leading a productive conversation in each scenario:

01

First-time Appearance, Onboarding New Board Members

If you've done your foundational ground work, then you have a good idea of what's important to your audience. Address their needs first, then swiftly move to your concerns about the top risks and threats and how they relate to business operations and objectives.

Plan for interruptions and discussion
A two-way dialog will help you identify what's most useful to the board.

Link your program to the organization's top business risks

- What data and IP are mission critical?
- Where is that data and how is it accessed?
- What are the top threats that may go after them?
- What are the top cybersecurity risks to the business and how likely is each one?
- Which risks are most important to avoid?
- Can any risks be mitigating or transferred through insurance?
- What is the plan for the remaining risk?

Consider including a third-party risk assessment
Third-party assessments establish an un-biased baseline of risks and exposures. They can lend credibility to your security roadmap and may help reinforce your concerns about strategic initiatives that are increasing security risk.

Establish cornerstone issues
Use an introductory meeting or annual update to suggest a couple of issues that relate to the long-term value of the enterprise and should stay on the board's radar. Over time, the board will become your advocate for change on these issues by setting a tone-at-the-top expectation for the whole company.

Reporting Tip

Board Members Suffer from Slide Fatigue

Slideware is rarely your friend in the boardroom. Keep your live presentation materials to no more than five slides (sometimes 1-3 will do), and focus on the quality of your narrative. Always have quantifiable information available as backup, or in the board book, but don't rely on the slides do the talking for you.

Reporting Tip

A Picture is Worth a Thousand Words

Sharing a high-level view of the organization's IT infrastructure configuration and where the crown jewels are located can be an effective risk management discussion tool.

02

Quarterly Reporting with Dashboard Review

To help board members fulfill their risk oversight responsibility, establish a reliable and consistent set of metrics that acts as a gauge against your baseline. The numbers you report should be replicable and communicate trends over time.

- Less is more on your dashboard. The business relevance and quality of your metrics are more important than volume. Rather than presenting the number of unpatched systems, for example, provide a month-over-month update on patch latency, specifically for mission-critical systems.
- Help the board revisit known risks to ensure that controls are in place and assess their effectiveness.
- Explain the timeline to resolve specific exposures and describe the mitigating controls you've put in place.
- Demonstrate your readiness for "the big incident" by highlighting established protocols.
- Show that steady progress is being made against the roadmap.
- Use insights from the metrics to highlight how security is supporting the organization's key strategic initiatives.
- Finally, plant the seeds for future investment in response to changes in the threat landscape.

03

Annual Report

This is your chance to roll up the year's prior presentations to demonstrate the strategic value of the investments made to date—and present future concerns that may warrant budget adjustments. Aligning progress with the agreed-upon roadmap will help make the case for renewed support from the board.

- Always start with your "ask." What do you want from the board or what do you want them to agree to?
- Provide a narrative about progress against desired outcomes: business execution, security controls, and risk position. Keep it high level.
- Leverage a rollup of your quarterly metrics to provide risk and vulnerability trends, as well as the current state of risk exposure.
- For public companies, this may also be a time to prepare annual business risk disclosures. Be prepared to review incident and breach impact metrics.
- Illustrate how improved security has reduced business risks or helped achieve goals such as digital transformation.
- Paint a picture for what's next given emerging known threats.
- Clarify your action plan and reiterate your asks for resources or support.

Reporting Tip

Dashboard Components to Consider

- Emerging threat trends
- Incident or breach trends
- Time to respond
- Time to detect
- Vulnerability management
- Compliance and control
- Data loss prevention, integrity, and availability
- Third party vendor risk
- Employee awareness
- Status of key initiatives
- Assessment results

Dashboards Are a Supporting Prop, Not the Presentation

A useful board report tells a story about how well risk is being managed at the business level. Within that report, your dashboard plays a supporting role, while the narrative you use to explain the risk is essential.

Within the dashboard, key metrics should be replicable—appearing consistently in each report over time—to help board members assess risk trends over time.

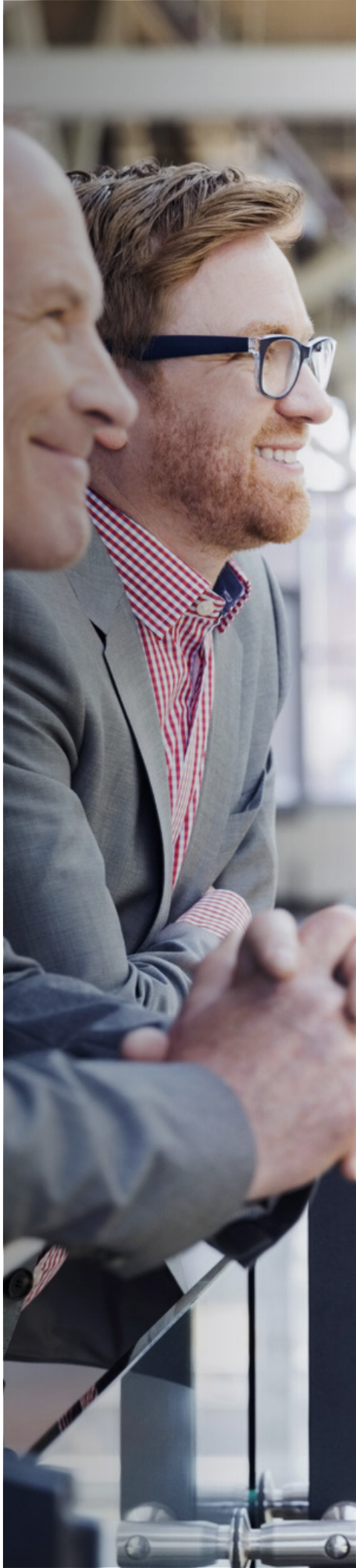
Secureworks®

Conclusion

As CISOs take a business leadership position, it is important to do so with thought and purpose. Building relationships with your executive team and members of the board is critical to earning the support that will help you lead confidently through a breach should one occur.

Consistency in board reporting will pay off as you establish metrics and narratives the board comes to rely on for assessing the organization's response to cybersecurity risk. To maintain that confidence, stay focused on business outcomes. A lapse into tactics that describe "how the security program works" will distract attention from the more valuable "why security is important" story, pulling the discussion off track and threatening to erode the board's perception of your leadership role.

Finally, continue to test the effectiveness of your security program and help the board benchmark better management of the risk over time. Together, these factors will support a reporting framework that helps you answer your board's most burning question: "How secure are we?"



About Secureworks

Secureworks® (NASDAQ: SCWX) is a global cybersecurity leader that protects customer progress with Secureworks Taegis™, a cloud-native security analytics platform built on 20+ years of real-world threat intelligence and research, improving customers' ability to detect advanced threats, streamline and collaborate on investigations, and automate the right actions.

Corporate Headquarters

United States

1 Concourse Pkwy NE #500
Atlanta, GA 30328
www.secureworks.com

Asia Pacific

Australia

Building 3, 14 Aquatic Drive Frenchs Forest, Sydney NSW Australia 2086

Japan

Otemachi One Tower 17F, 2-1,
Otemachi 1-chome, Chiyoda-ku,
Tokyo 100-8159,
Japan
www.secureworks.jp

Europe & Middle East

France

8 avenue du Stade de France 93218
Saint Denis Cedex

Germany

Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany

United Kingdom

One Creechurch Place,
1 Creechurch Ln
London EC3A 5AY
United Kingdom

1 Tanfield
Edinburgh EH3 5DA
United Kingdom

United Arab Emirates

Building 15, Dubai Internet City Dubai,
UAE PO Box 500111