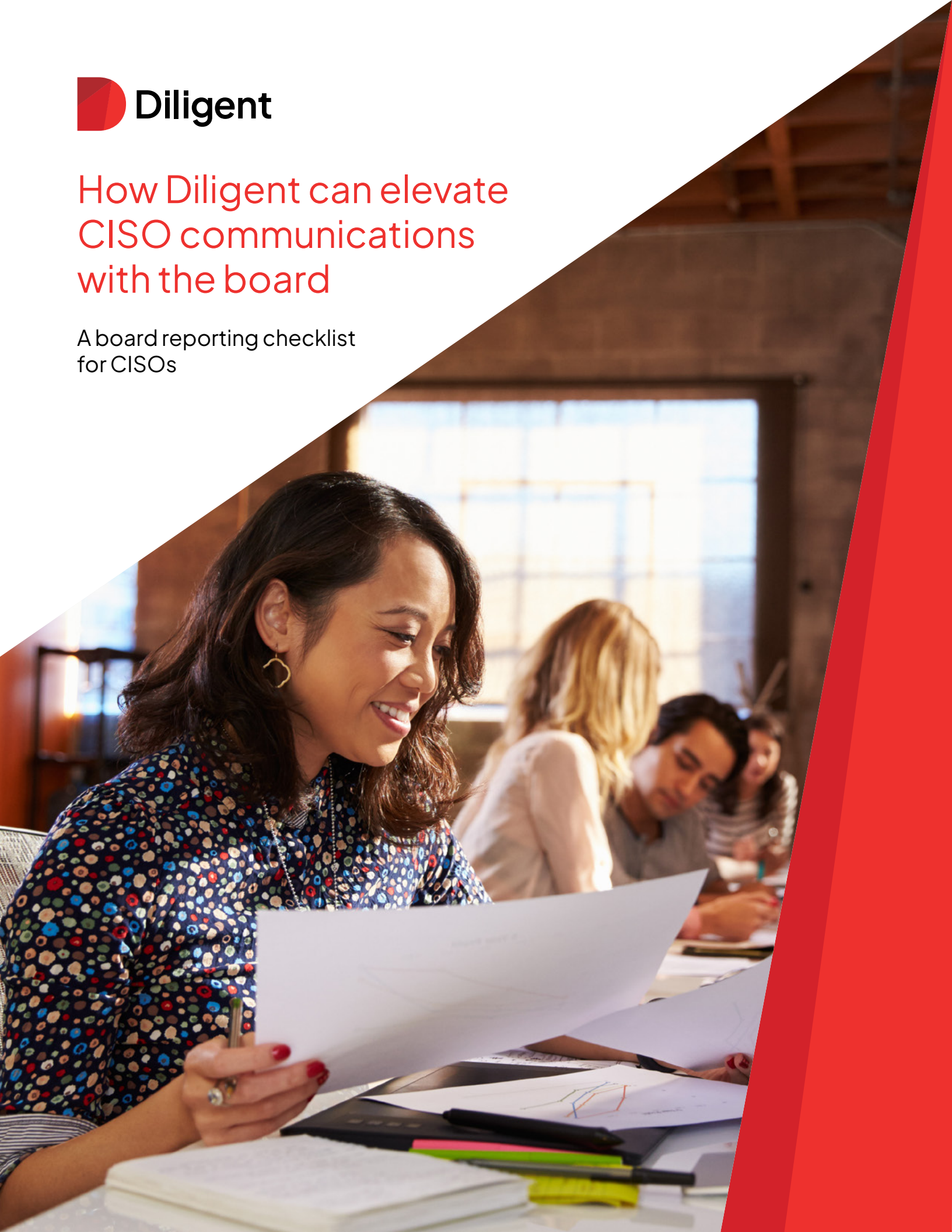
Diligent

How Diligent can elevate CISO communications with the board

A board reporting checklist for CISOs



As a CISO, you have crucial info to convey about cyber risk, and your board wants to hear it.

In a Diligent survey, we asked directors to name the issue that would give them the most concern if they were to confront it in a crisis. Cybersecurity topped the list by a huge majority, at 75%, with supply chain disruption coming in a distant second at 46%.

Yet 41% of our respondents also told us that cybersecurity is the most challenging issue to oversee — even above other complex issues such as talent, culture, leadership succession and transition, diversity and inclusion, and climate risk.

Corporate leaders must be prepared with sound cybersecurity practices, which are critical for a company's bottom line. How can you as a CISO make sure that nothing important gets lost in translation in your communications with these leaders while building strong relationships for the future?

When it comes to communications between the CISO and the board, having tools that facilitate effective collaboration is essential.

The good news is that Diligent not only offers a solution to help you identify and communicate risk, but also enables you to create effective presentations that give leadership enhanced visibility into the organization's risk posture.

> "[Board members are] very concerned about their ability to effectively oversee cyber risk, and they're really looking for good support and good information coming from within the senior management team."

Dottie Schindlinger
Executive Director
Diligent Institute

Tips for successful presentations to the board

Tips follow from a recent panel discussion about building an effective dialogue on cyber risk, featuring Dr. John Zangardi, CEO of Redhorse Corporation; Myrna Soto, CEO and founder of Apogee Executive Advisors; and Henry Jiang, CISO, Diligent.

01 Use accessible, user-friendly language

The panelists' first word of advice: Leave the technical jargon behind. Cybersecurity is rife with acronyms and specialized terminology that can confuse and intimidate even the most accomplished executive who lacks this background.

Zangardi is a former military aviator who served as Department of Homeland Security CIO, Acting Department of Defense CIO and Navy CIO. In the defense world, he explained, executive leaders often share a common language with those doing the briefing, like the terminology of aviation. In the corporate world, by contrast, "Most boards don't have people who understand the language of cybersecurity nor did they come out of the profession of IT. They mainly come out of finance or sales or are the CEO… English is the right language to use [in this environment], not technical jargon."

As a current corporate CISO, Jiang advised how to bridge this language gap: "Use meaningful and impactful vocabulary, so that board members can easily absorb what the root cause really is and the issues related to cyber risk areas."

02 Convey the impact

Soto echoed this guidance. As the former global CISO for Comcast Corporation, current member of four publicly traded boards and advisor to a number of privately held companies, she declared: "One of the most critical things that any CISO needs to do is to be able to translate the risks associated with cybersecurity."

"Give board members a very business-level view," she advised. For example, how could a cyber vulnerability put your brand at risk? What steps will your company need to take to recover from an incident, and is your company prepared?

03 Highlight the "so what?" factor

Importantly, link cyber risk to the top priorities on your board's agenda, such as regulatory compliance and what's going on in your company's industry.

"Everybody is reading the newspaper. They're reading the headlines on the latest breach," Jiang noted. "Be prepared to explain how your company may be similar, how it may be different and what we've learned from this critical event," he advised. This kind of information resonates and builds a relationship of transparency between CISOs and board members.

04 Share your clear perspective

Throughout, be proactive and forthright. "Your board members are not looking for a weather forecast that shows sunny and bright all day," Soto said. "What they're really looking for is your perspective of what is concerning to you, why, and what you need from a support perspective."

05 Tell your board how they can help

Board members can play an important role in cybersecurity efforts: communicating with stakeholders, asking questions of management and setting the tone from the top. But many may be unaware of this role — which makes ongoing communications and strong relationships with the CISO even more vital.

Your cybersecurity board presentation checklist

☐ Come equipped with a dashboard view

"In many board meetings, we get 10 minutes of fame if we're lucky, sometimes that might be even further reduced depending on the agenda," Jiang said. "So, I always have a dashboard view. Consider this your most important slide," Jiang added.

☐ Be ready to share your risk profile

During Zangardi's time flying and commanding military squadrons, "Before every flight, the pilot would literally sit down and go, 'These are the risk factors that I see with this flight.'" Whether these are technical issues, team members undergoing personal stress, or the latest cyberattacks in your industry, "the idea is to present how you're going to handle a bad thing if it happens," he said.

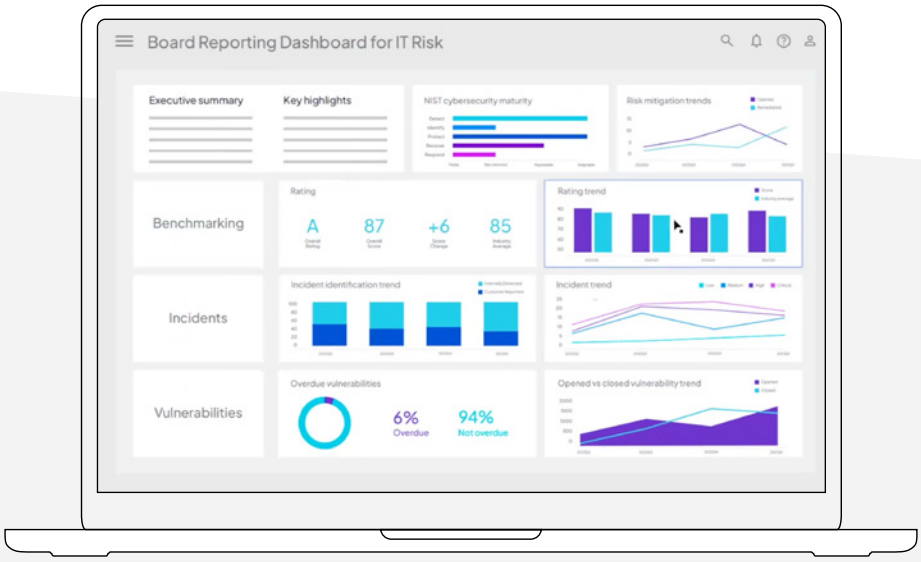
☐ Know your company's top risks

Jiang typically works with his security operations team to draw up a list of top five risks based on real data. Are processes missing in a pivotal area? Could new regulations lead to legal issues?

Use examples and straightforward language to tell the story. And don't overlook third-party risks: potential threats related to partners, customers and suppliers of products or services who have some amount of access to your systems and network.

☐ Explain "inherent" and "residual" risks

"Risk is a subjective term," Jiang said. Start with the inherent risk: your company's risk level if you don't do certain things to protect your information and technology assets. Then outline your "residual risk" — the risks that



remain after you account for all cybersecurity practices, processes, training, systems and precautions.

☐ **Detail a risk's potential consequences — without drama**

Soto advised against "entering the boardroom and creating a huge amount of fear or creating a doomsday scenario. But you do need to be very transparent."

☐ **Provide a risk framework and mitigation plan**

Board members are familiar with enterprise risk frameworks, Soto noted, so CISOs should use them to their advantage to show trends, connect the dots and explain probability and impact.

Frameworks focused on particular controls and outcomes are especially helpful for presenting to the audit committee, she elaborated. "Audit committees are looking for that specificity because their responsibility is to sign off on the efficacy and the effectiveness of the remediation plans."

☐ **Benchmark and validate as you go**

Regular macro updates to the full board are a powerful way for CISOs to educate board members on their organization's cybersecurity practice, Soto declared. "Whenever possible, bring third-party validation that you may have executed on, whether it be an external penetration test or an assessment by a third party. That goes a long way."

See examples of a security plan dashboard, a cybersecurity plan and a cybersecurity scorecard in the attached appendix.

How Diligent can help

IT Risk Board Reporting Dashboards by Diligent enable organizations to aggregate their high-volume IT risk data and organize it into a consumable format for the board. Take control of your IT risk story with a solution that lets you:

- Deliver curated data in user-friendly reports using templatized, repeatable dashboards
- Consolidate and manage your IT risk data through one secure platform
- Benchmark your organization's performance against competitors across your industry
- Surface the right data quickly and easily, so you have more time to focus on elevating the board's understanding of cybersecurity and IT risk

"In the 21st century, there is not a single major business decision that does not include cybersecurity considerations. Cybersecurity needs to be woven into the entire process, from R&D through manufacturing through public relations. That's the message about cybersecurity: We're all in this together."

Larry Clinton
President
Internet Security Alliance

Diligent

About Diligent

Diligent is the global leader in modern governance, providing SaaS solutions across governance, risk, compliance, audit and ESG. Empowering more than 1 million users and 700,000 board members and leaders with a holistic view of their organization's GRC practices so they can make better decisions, faster. No matter the challenge.

For more information or to request a demo:

info@diligent.com | diligent.com

1138731560