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

In a recent Diligent survey, we asked directors to name the issue that gives 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?

“[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 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.

1. **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.”

2. **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?

3. **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.

4. **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.”

5. **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.
Come equipped with a dashboard view
“In many board meetings, we get 10 minutes of fame if we’re lucky, sometime 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

Board-CISO communications are an ongoing journey, and both parties need to prepare for a long and winding road ahead. “I had a board member ask me very early in my career, ‘When would we be done?’ And I said, ‘We will never be done,’” Soto related in the Diligent webinar. “This is an evolving topic and you will always be hearing new things about this topic.”

The good news is that technology solutions are available to make this journey smoother, both for identifying and communicating risk and for creating effective presentations that give leadership enhanced visibility into the organization’s risk posture.

IT Risk Management by Diligent enables organizations to identify, assess, and remediate internal risk via a single, comprehensive, collaborative platform.

The solution integrates with threat and vulnerability feeds and streamlines and strengthens IT risk and compliance through:

- Automated workflows and processes with pre-configured content
- Advanced risk modeling for multiple use cases or stakeholders
- Real-time visibility via ready-to-use visualizations and executive dashboards
- Best-in-class support from industry practitioners

Third-Party Risk Management by Diligent enables organizations to bring third-party data together across departments and systems, then leverage this information for data-driven decisions.

The solution is equipped with pre-built, industry-standardized questionnaires, such as SIG Lite and CAIQ Lite, and ready-to-use storyboard visualizations. It integrates with third-party security and financial intelligence providers and enables:

- Establishing a centralized inventory of third-party data
- End-to-end management of third-party assessments
- Risk-based control assessments
- Third-party KPI and KRI reporting
- SLA performance monitoring
- Contract management

“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

Contact Diligent today to learn more
# Appendix:

## Security Program Overview Dashboard

<table>
<thead>
<tr>
<th>Business Risk Profile</th>
<th>Sources</th>
<th>Risk Drives</th>
<th>Cybersecurity Program Highlights</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inherent Risk Level:</td>
<td>- Lorem ipsum dolor sit amet</td>
<td>- Lorem ipsum dolor sit amet</td>
<td>- Lorem ipsum dolor sit amet</td>
</tr>
<tr>
<td>Moderate</td>
<td>- Lorem ipsum dolor sit amet</td>
<td>- Lorem ipsum dolor sit amet</td>
<td>- Lorem ipsum dolor sit amet</td>
</tr>
</tbody>
</table>

### Program Maturity Level (Based on NIST CSF 2019-2022)

### NIST Cybersecurity Framework Maturity Level Comparison

## Cybersecurity Program 20xx Plan

<table>
<thead>
<tr>
<th>NIST Cybersecurity Framework Key Functions</th>
<th>NIST Maturity Level (As of date)</th>
<th>20XX Objectives</th>
<th>Targeted Maturity Levels by date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity (Identity management, governance, risk assessment, policy oversight)</td>
<td>Tier x (Preparation)</td>
<td>1. Lorem ipsum dolor sit amet, consectetur adipiscing elit 2. Lorem ipsum dolor sit amet, consectetur adipiscing elit 3. Lorem ipsum dolor sit amet, consectetur adipiscing elit</td>
<td>Tier x</td>
</tr>
<tr>
<td>Protect (Identify, manage, and assess control, data security, controls, awareness and training)</td>
<td>Tier x (Preparation)</td>
<td>1. Lorem ipsum dolor sit amet, consectetur adipiscing elit 2. Lorem ipsum dolor sit amet, consectetur adipiscing elit 3. Lorem ipsum dolor sit amet, consectetur adipiscing elit</td>
<td>Tier x</td>
</tr>
<tr>
<td>Detect (Detect and respond to incidents, contain and recovery)</td>
<td>Tier x (Preparation)</td>
<td>1. Lorem ipsum dolor sit amet, consectetur adipiscing elit 2. Lorem ipsum dolor sit amet, consectetur adipiscing elit 3. Lorem ipsum dolor sit amet, consectetur adipiscing elit</td>
<td>Tier x</td>
</tr>
<tr>
<td>Respond (Respond to incidents, communicate, analyze, protect)</td>
<td>Tier x (Preparation)</td>
<td>1. Lorem ipsum dolor sit amet, consectetur adipiscing elit 2. Lorem ipsum dolor sit amet, consectetur adipiscing elit 3. Lorem ipsum dolor sit amet, consectetur adipiscing elit</td>
<td>Tier x</td>
</tr>
<tr>
<td>Recover (Recover planning, communications)</td>
<td>Tier x (Preparation)</td>
<td>1. Lorem ipsum dolor sit amet, consectetur adipiscing elit 2. Lorem ipsum dolor sit amet, consectetur adipiscing elit 3. Lorem ipsum dolor sit amet, consectetur adipiscing elit</td>
<td>Tier x</td>
</tr>
</tbody>
</table>

## Cyber Risk Scorecard

![Cyber Risk Scorecard](image1)

![Cyber Risk Scorecard](image2)
About Diligent Corporation

Diligent is the leading governance, risk and compliance (GRC) SaaS provider, serving more than 1 million users from over 25,000 organizations around the globe. Our modern GRC platform ensures boards, executives and other leaders have a holistic, integrated view of audit, risk, information security, ethics and compliance across the organization. Diligent brings technology, insights and confidence to leaders so they can build more effective, equitable and successful organizations.