Diligent | Security Scorecard

Messaging Guide for CISOs: **How to Translate Cybersecurity KPIs Into Business Metrics**

When presenting to the board of directors, it's important to speak the board's language. CISOs often have limited time allotted to their presentations at board meetings, so it is crucial to explain cybersecurity matters in terms of their business impact.

This guide will help you demonstrate to the board the effectiveness of your cybersecurity solutions by highlighting critical KPIs, business risks and mitigation strategies in management terms – so you can ensure all parties are aligned.

Diligent | Security Scorecard

PREPARING FOR THE MOST PRESSING QUESTIONS ON THE BOARD'S MIND

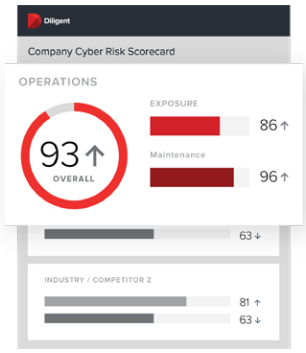
What is the organization's cyber risk level?	To convey the overall risk level, you should highlight your organization's risk appetite and tolerance levels. Risk appetite is a predefined level of risk that is deemed acceptable by an organization. Risk tolerance is the measure of how much risk an organization can handle before becoming unsustainable. Using these measurements allows you to represent your organization's overall cyber risk regarding cybersecurity performance.
What are the organization's top risks?	When determining your organization's top risks, you need to evaluate the historical impact individual cyber threats have had on your company's bottom line. By looking at the financial impact of successful attacks, you can create a qualitative risk analysis and display top risks side by side. This will help you explain where risk is concentrated and which risks require additional attention.
What compliance requirements must the organization meet?	With complex geopolitical situations and a host of new cybersecurity concerns, regulatory bodies are taking action, and your organization must be prepared. One key piece of legislation is the U.S. Securities and Exchange Commission's recent proposal on cybersecurity risk management, calling for a written cybersecurity program and notification of cybersecurity incidents, among other requirements. Other requirements such as the German Supply Chain Act and the European Union's Supply Chain Directive signal increased focus on compliance and security worldwide. Amidst evolving legislation, your organization needs to stay ahead of requirements to help protect critical systems and maintain compliance.
How is the organization's risk posture trending?	To see how your risk posture is trending, you should compare your cybersecurity performance to the organization's risk appetite statements. Evaluating how well your cybersecurity solutions uphold your risk appetite will give your board an idea of whether the risk is increasing or decreasing. Leveraging IT compliance technology can help you visualize risk posture, identify opportunities for improvement and effectively report on program maturity to the board.
Is the organization's level of cybersecurity spending appropriate?	Determining whether you are spending enough money on cybersecurity can be difficult as there is no way to quantify the financial loss from a cyberattack until after it has occurred. That said, using data to show the ROI on cybersecurity investments illustrates how effectively money is being spent and how your technology is helping automate processes and save on operating costs. Demonstrating the return on investment will influence your board's cybersecurity budget allocation and ensure that spending is done in a way that sustains your security capabilities. You'll want to emphasize that investing in appropriate automation and reporting capabilities can help drive new revenue in the business. IT compliance can also equip businesses to enter new markets and obtain new certifications by leveraging streamlined common controls frameworks.
What is the cyber risk associated with a new business prospect?	New business prospects provide an opportunity for growth but can also introduce additional cyber risks. Showing the board that you are doing your due diligence to identify potential business opportunities is crucial, as is having a thorough vetting process in place for partners. Demonstrate that your compliance team is well-funded, credible and defensible by highlighting your full visibility screening and onboarding processes for third parties.
How does the organization compare to its peers?	Annually, boards of directors review their position within their market. Security rating platforms enhance their ability to gain insight into how well they compare with their peers, which impacts their annual financial planning. Security rating platforms collect publicly available information, which means that you can use the ratings to share your performance in a business-level language. If your security rating is lower than a peer's, you can drill down into the risk factors associated with the ratings — both your own and those of your competitors. If one risk factor is causing the difference, you can more easily report to your board how to improve the score and the budget they need to allocate to meet the market-level standard. On the positive side, if your security ratings are stronger than your peers, you can explain to your board that you manage cybersecurity risks more effectively than your competitors do. Drilling down to the individual factors across your industry allows you to show your team's expertise and gives the Board confidence in your abilities as a CISO. Additionally, you can use these scores as metrics to prove your ability to generate revenue opportunities, automate workflows and stay compliant as the board looks toward new business objectives.

Diligent | Security Scorecard

EXPLAINING KEY CYBERSECURITY KPIs TO THE BOARD

How to explain intrusion attempts	The word to focus on here is "attempt." Malicious actors will always attempt to gain entrance to data; the question is where cybercriminals focus their attacks and your ability to thwart them. For example, if you're continuously monitoring organizational IP addresses and know the types of information associated with those addresses, you can gain visibility into the key business risks. As part of your monitoring, assume that you find that malicious actors focus on IP addresses associated with your corporate website. You know that no customer portal exists on the site, and internal users accessing the backend must use unique logins and passwords. Since the organization doesn't store non-public information (NPI) on that address and the likelihood of credential theft providing access to systems, networks, and software storing NPI is low, you can tell the board that the financial risk is low while the reputation risk is medium.
How to explain Mean Time to Detect (MTTD)	Ultimately, the primary information you need to give your board about this metric is: The time was short. The faster you can detect a risk, the more rapidly you can mitigate the threat. If your dashboard shows that you continuously monitor and maintain a consistent security rating, you can explain the link between the two. Your board can understand that you maintain a robust security posture if you can say, "we were able to detect security threats within hours, meaning that we were able to mitigate them rapidly to prevent additional risk to the organization."
How to explain Mean Time to Respond (MTTR) and Mean Time to Contain (MTCC)	Unfortunately, malicious actors will more likely than not find a way to infiltrate your organization's security defenses despite the best detection methods. Response time, then, becomes the next most important metric for your dashboard. The 2022 IBM Cost of a Data Breach report noted that the average cost of breaches when security AI and automation are fully deployed was, on average, $3.05M lower than organizations with no security automation and AI. With an AI platform, you can have real-time visibility into the threat vector associated with the security incident, meaning that you can respond more rapidly to the threat. If your security rating platform provides visibility into the risk factor associated with the security incident, you can prove how rapidly your team responded. For example, suppose the cybercriminals gained access to your systems using a cross-site scripting attack and your platform reviews for web application security as a risk factor. In that case, you can easily see the lowered score to respond directly to that issue. Then, you can monitor the risk factor and provide the increased score post-response as a metric for proving rapid response time. Additionally, the improved score gives a metric that provides the Board confidence over your ability to contain the threat. If the enhanced post-incident risk factor score stays stable, you can show that the threat has been successfully contained.
How to explain patching cadence	Proving that all systems are continuously updated according to best practices can be challenging. The 2017 Equifax data breach arose from a single unpatched server. With a security rating platform that monitors patching cadence across all endpoints, you can gain insight into how well your organization maintains its patching cadence. A high score for that risk factor indicates that you appropriately update all devices, systems, networks, and software to mitigate risk. With this metric, you can tell the board that your ability to view all these locations and effectively update them lowers their financial and reputation risks.
How to explain risk management effectiveness	Your security rating platform enables you to review all your vendors in the same way you manage your security. Often, organizations lack visibility into their supply chain risk. The 2022 IBM Cost of a Data Breach Report also noted that breaches caused by third parties cost even more than other types of breaches, at an average of 4.33 million USD. If you're continuously monitoring your supply stream with a security rating platform, you can give your give your Board confidence over technology decisions. In the same way you use these metrics to prove your cybersecurity posture, you can prove governance over your vendors. Not only can you show the board that your supply stream is secure, but you can also give data surrounding your monitoring, including your communications with them and their response times.

Present a Comprehensive Cyber Health Snapshot in an Intuitive Dashboard



Cyber Risk Scorecard, powered by SecurityScorecard, enables your board to have visibility into your organization's cyber ecosystem and keep a pulse on your cyber posture in real time. This facilitates an ongoing dialogue between the board and the CISO on critical issues and strategic decisions well beyond the boardroom.

Cyber Risk Scorecard is available to all Diligent Boards customers, with an optional Data & Intelligence add-on to enable organizations to dive deeper into cyber risks.

About Diligent Corporation

Diligent is the leading governance, risk and compliance (GRC) SaaS provider, serving more than one 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.

About SecurityScorecard

SecurityScorecard is the global leader in cybersecurity ratings and the only service with over two million companies continuously rated. SecurityScorecard's patented rating technology is used by over 1,000 organizations for self-monitoring, third-party risk management, board reporting, and cyber insurance underwriting; making all organizations more resilient by allowing them to easily find and fix cybersecurity risks across their externally facing digital footprint. SecurityScorecard is the only provider of instant risk ratings that automatically map to vendor cybersecurity questionnaire responses – providing a true 360-degree view of risk.

For more information:

Email: info@diligent.com | Visit: diligent.com