Diligent

A CISO's Guide to **Conducting Productive Cybersecurity Conversations with the Board**

Chief information security officers (CISOs) have hundreds of cybersecurity metrics to manage, but only a fraction of those will be relevant to the board and C-suite. A good CISO must distill data into an easy-to-understand dashboard and communicate risk to a board that doesn't want complex technical details.

With data coming from many directions, and leadership expecting the CISO to make sense of it all, choosing metrics that are aligned with organizational goals is essential.

When presenting to the board, CISOs should speak to cybersecurity risk as a strategic business opportunity, instead of focusing exclusively on operational risk. Similarly, any metrics the CISO presents should be actionable and aligned with the organization's objectives.

This guide provides practical solutions for CISOs looking to thrive as strategic partners to the board.

Diligent

How to Better Articulate Your Cybersecurity Posture to the Board

To increase your cybersecurity budget or extend your team's capacity, you need to articulate your current cybersecurity posture to the board/executives. By demonstrating ongoing value, CISOs will hopefully see an increase in resources, not just risks.

Here are some ways to better articulate your cybersecurity posture to the board and create a sustainable risk management program.

Focus on the Right Metrics

Metrics aren't merely numbers: They're a chance to tell a story about an organization's past, present and future. CISOs must make that story an interesting and valuable one for the board audience. Some tips:

- Organize metrics by departments (e.g., governance, security ops)
- Select the metrics that influence behavior
- Establish a baseline of risk priorities based on your policies and risk appetite
- Focus on the speed of incident closure, not only the incident count

Make Sure You Have the Right Technology

Can you merge data from different tools — not just security and governance, risk and compliance (GRC) tools, but enterprise resource planning (ERP) systems too? It's essential that your tech solution can process data through an analytics engine, put it on a schedule and create storyboards for easy data sharing.

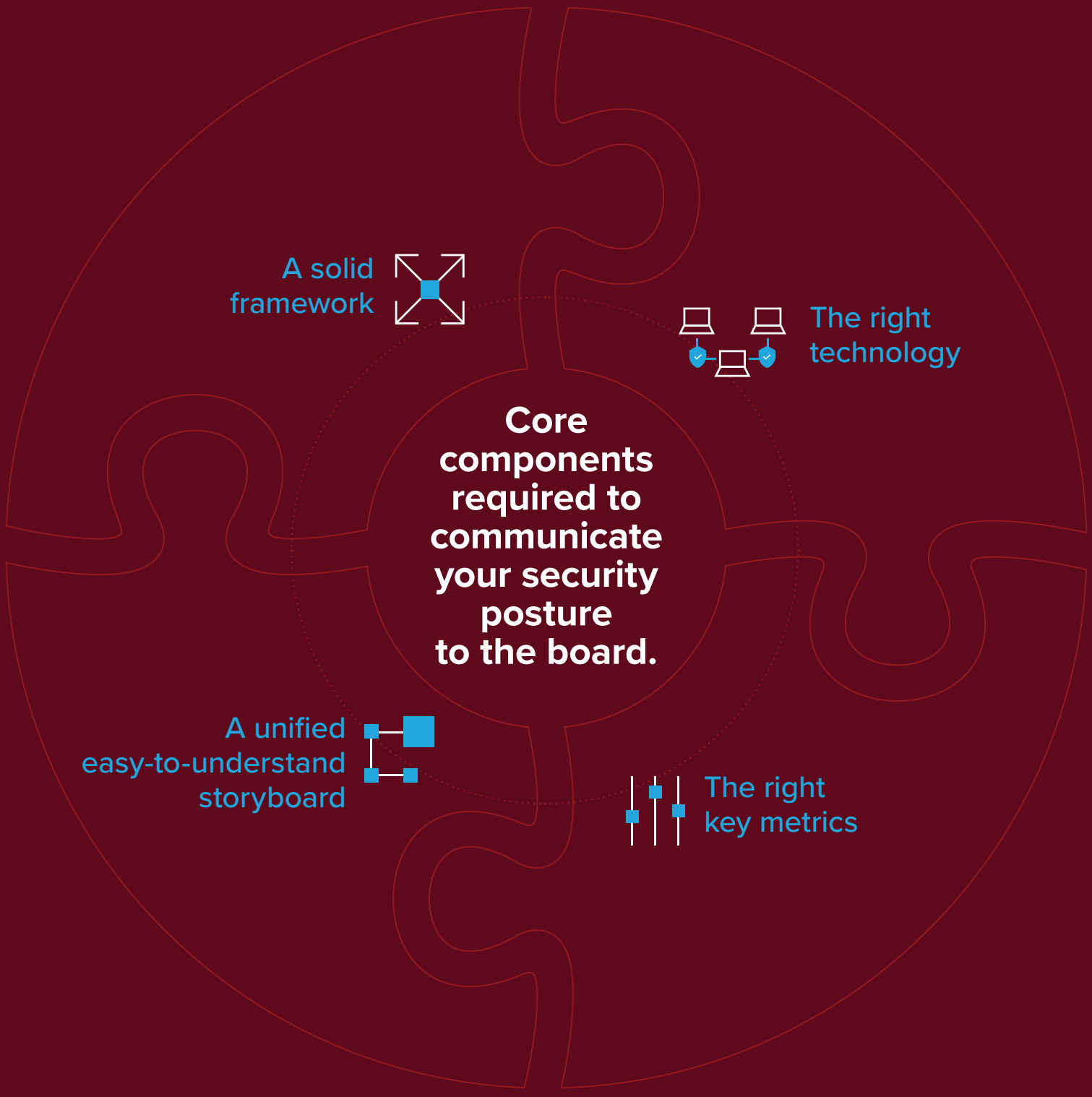
Communicate the Business Impact

Instead of using fear or uncertainty as a strategy, CISOs should present cybersecurity risk as a business problem. Boards don't want excessive detail, so CISOs have to avoid overwhelming them with long reports or technical jargon. This is where a single, unified, easy-to-understand dashboard can help. Ideally, one that's updated in real time, displaying the key metrics that you identified.

Use the Right Management Framework

The NIST Cybersecurity Framework is commonly used by CISOs because it simplifies security in a language that the board can relate to: capabilities before, during and after an attack:

- Identify risk systems, assets, data and capabilities before an attack
- Protect your organization by developing and implementing appropriate safeguards
- Detect a cybersecurity event
- Respond to the cybersecurity attack
- Recover by developing and implementing activities for resilience and restoring capabilities or services


A solid framework
The right technology
Core components required to communicate your security posture to the board.
A unified easy-to-understand storyboard
The right key metrics

Diligent

Select the Cybersecurity Metrics that Matter Most to the Board

When presenting to the board, CISOs should speak to cybersecurity risk as a strategic business opportunity. Some tips:

Focus on the Data That Drives Decisions

Don't track metrics simply for the sake of tracking metrics. If a metric isn't enabling business decisions or influencing behavior, don't waste your time on it.

Establish a Baseline of What Is a Low, Medium and High Risk

Despite cybersecurity risk frameworks like NIST, there is little standardization in information security. Based on your organization's policies and risk appetite, you can set up a baseline and thresholds to help you prioritize risks (and easily articulate them in the boardroom).

Look at the Speed of Risk Reduction

It's important to go beyond basic "count" metrics. For example, rather than reporting the number of critical vulnerabilities, focus on the number that are still open after 60 days.

Be Prepared to Compare

The board will often want to know how your organization's security posture stacks up against the competition. Using a benchmarking tool such as Cyber Risk Scorecard from Diligent can enable you to see (and share) the security score of your organization, competitors and the industry overall.

Prepare for Questions Posed by the Board

While it's impossible to predict every question the board may ask, here are some common ones:

1. **What's our organization's security posture?**

   In other words: what's our maturity level before, during and after a cyberattack?

2. **What's our customers' view of the risk?**

   For example, if Amazon's website goes down, it hugely impacts their customers, while a technology company is more focused on protecting the integrity of its technology platform.

3. **Do we have the right certifications?**

   To be compliant, organizations may have to meet certain regulations, (e.g., the Sarbanes-Oxley Act, HIPAA, FedRAMP, SOC 2, etc.).

4. **How can we quantify risk in dollar figures?**

   This includes how much a data breach will cost an organization and how much cyber risk insurance costs.

5. **What are we doing to mitigate third-party risk to protect our supply chain?**

   Third-party risks are only increasing, especially with more organizations relying on emerging technologies like cloud computing.

6. **What are we doing to safeguard customer information and maintain privacy?**

   The board might ask about controlling access to sensitive data, current security technologies, physical security methods and so on.

7. **What are some scenarios that could damage our reputation?**

   For example, could an ex-employee access a social media account and post something inappropriate?

8. **Do we have a PR strategy to help us with damage control if we need it?**

   There's a big benefit to having an established relationship with a PR company rather than frantically searching for one after a disaster.

Diligent

The CISO has a huge responsibility in a climate of escalating cyber risk.

The role can no longer be solely about technical architecture and responses to breaches. Today's CISOs require solid business and communication skills to bring value to the boardroom – and across the organization.

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.

For more information or to request a demo:
Email: info@diligent.com | Visit: diligent.com