Diligent

CISOs in the Boardroom

Table of contents

Diligent

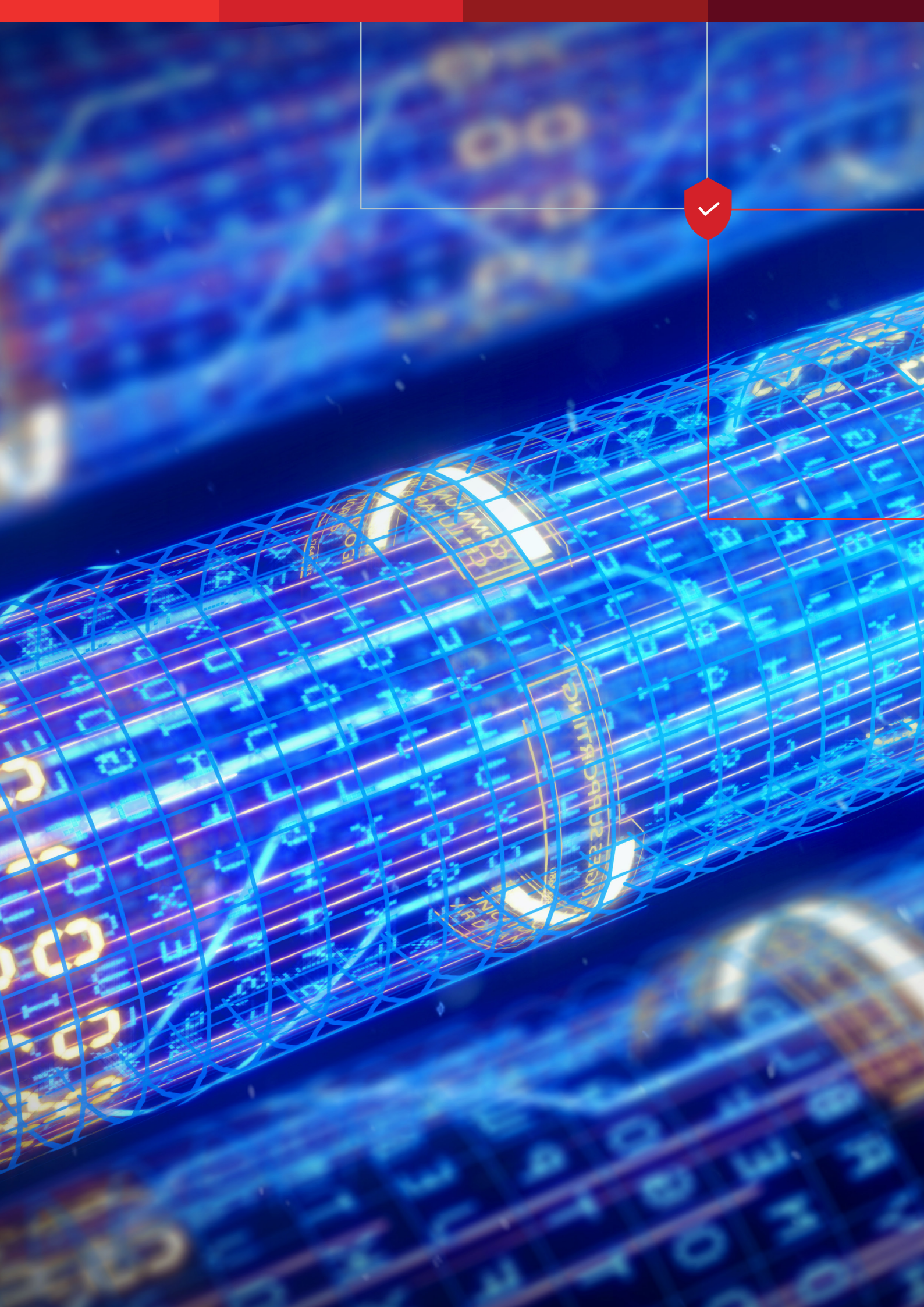
The Evolution of the CISO

The chief information security officer (CISO) is running faster than ever to keep up with the demands of a role that's evolved dramatically since "the world's first CISO" Steve Katz started at Citibank in the 1970s.

In the early years, the CISO role was largely reactive, responding to security threats and data breaches after they happened. The CISO was also a frequent scapegoat when a data breach occurred, blamed by higher-ups who didn't understand that these attacks weren't preventable.

But today's CISO has stepped out of the server room and into the boardroom. The re-defined CISO role is now much more strategic. It combines cybersecurity and IT expertise, business acumen, and the ability to communicate complex objectives and issues to non-technical board members. Boards are finally realizing that cybersecurity breaches are inevitable, and that strong detection and response tactics are the best way to protect an organization.

This eBook outlines some of the current challenges CISOs face and provides practical solutions to help them thrive as strategic partners with a reserved seat at the table.



Diligent

The CISO & the CIO

The chief information officer (CIO) typically oversees the operational IT needs of an organization, whether it's policy and procedure development or budgeting; a CISO monitors and analyzes potential risks to an organization.

However, the responsibility of the CISO has grown beyond the CIO. While the CISO may still report to the CIO, they now also interact with the board, and an organization's key customers often want to talk to the CISO directly about cybersecurity issues.

In fact, some organizations have actually separated security from the CIO role to minimize conflict and better meet business objectives. In 2018, a PwC study concluded that only around 24% of CISOs report to the CIO, with 40% of CISO's now reporting directly to the CEO.[1]

There may be a power struggle as CIOs attempt to balance security with speed to market, while CISOs emphasize and scrutinize security.[2] The CIO plays the role of innovating, increasing productivity, and improving the user experience, while the CISO could be cast as the villain restricting growth and adoption.

To work collaboratively, rather than combatively, there needs to be communication, respect, and a clear delineation of responsibilities between the CISO and CIO.

[1] **PwC**, 2018, Global state of information security® survey
[2] **CSO**, 2019, What is a CISO? Responsibilities and requirements for this vital leadership role

Diligent

The CISO's Top Challenges

It's clear that the scope of the CISO role is constantly changing. Cybersecurity incidents are increasing—both from outside forces and malicious insiders—and so are regulatory requirements.

In a survey of 200 organizations,[3] 80% claimed they had experienced at least one cybersecurity incident over the last 12 months that was so severe it required a board-level meeting.

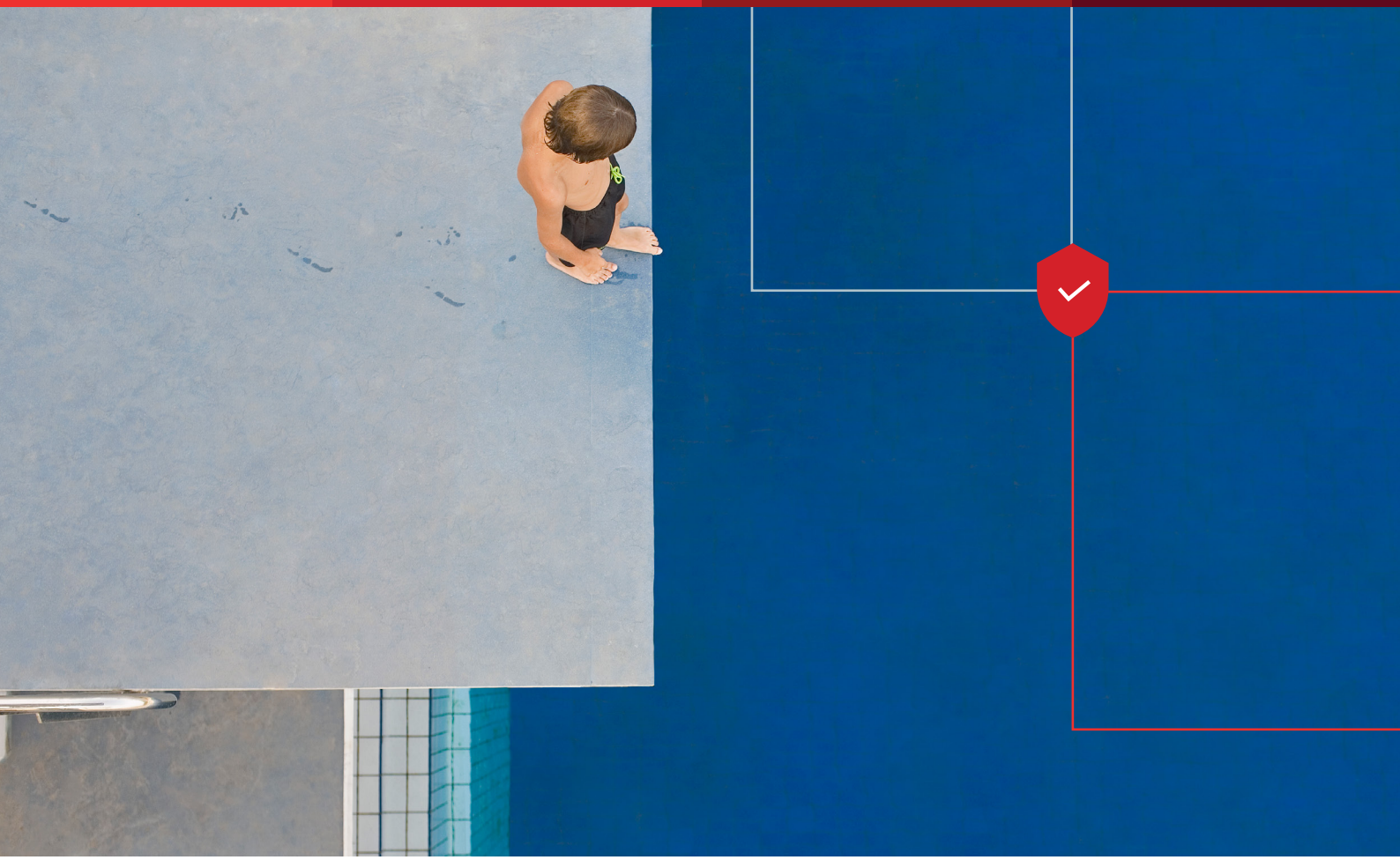
Here are six of the top challenges for CISOs:

01 **Difficulty hiring & retaining talent.** Because the demand for IT security professionals has surpassed global supply, positions can be hard to fill. Without a solid support team, the CISO can be distracted from critical issues and lack the resources to properly manage cyber risks.

02 **The speed of change.** Organizations hurry to stay one step ahead of the competition, better serve customers, and use new technologies—especially cloud-based ones. This, coupled with the pace of mergers and acquisitions, has created a virtually borderless world of data fraught with cybersecurity and third-party risks.

03 **Data from many sources.** CISOs generally have two sets of dashboards:one for internal stakeholders and one for external stakeholders. Both should be based on the same underlying data, but this isn't always the case. From spreadsheets to BI tools, CISOs can have data streaming in from many different sources, making it hard to consolidate information and present meaningful dashboards to the C-suite.

[3] **IronNet**, 2019, New survey finds vast majority of IT security pros willing to share threat intel to improve overall collective defense efforts



04 **Uncertainty over which metrics to present.** There's no shortage of metrics available to security professionals, and it's easy to get into the weeds when reporting and sharing data. If CISOs aren't focused on the right metrics and using data consistently to drive decisions, they can't confidently back up their recommendations to the board.

05 **Budget constraints.** IBM puts the average cost of a data breach at $3.92 million.[4] But ironically, cybersecurity budgets haven't typically been a high-priority spend for organizations. While cybersecurity risks are now at the top of the agenda, CISOs still have difficulties securing larger budgets, often because they can't guarantee a clear return on investment. Smaller organizations and local governments generally lack the budgets to properly mitigate threats.

06 **Communication challenges.** CISOs and boards speak different languages. The board doesn't care about technical details, while the CISO is immersed in them. A CISO may struggle while trying to articulate risk in terms that will be meaningful to board members.

[4] **IBM**, 2018, Cost of a data breach study: Benchmark

Diligent

The Cyber Security Risk Landscape

New technologies are a double-edged sword for organizations.

Innovation spurs growth and helps maintain a competitive advantage, but introduces risks. (And the "old" risks aren't going anywhere; classic approaches to hacking like ransomware and phishing schemes continue to pose serious threats.)

Some of the top cybersecurity risks to organizations include:

CLOUD COMPUTING & UNCONTROLLED CLOUD EXPANSION

According to a survey of 250 security directors,[5] this risk was the one they were most worried about. As more and more organizations migrate data and operations to the cloud, cyber criminals will increasingly target cloud providers. It's not just cloud computing in general that CISOs worry about, but uncontrolled cloud expansion by lines of business.

THIRD PARTIES & VENDORS

Risk exposure begins when organizations give third-party vendors access to their facilities, networks, and data—often with far less care and concern than they reserve for direct vendors. When a third-party vendor is compromised, an organization can experience devastating financial, reputational, regulatory, operational, and strategic consequences.

THE INTERNET OF THINGS (IoT)

From smart thermostats to vending machines, the IoT is everywhere. Routers and connected cameras make up 90% of infected devices,[6] with hackers stealing data, intercepting communications, or wiping devices. If an unsecured device is on the same network as other devices, it's a gateway for further exploitation.

[5] **IronNet**, **Kaspersky**, 2018, What it takes to be a CISO: Success and leadership in corporate IT security
[6] **Symantec**, 2019, Internet security threat report

SOCIAL ENGINEERING ATTACKS

Verizon[7] examined 41,686 security incidents and 2,013 data breaches and found that 33% of them featured social attacks, with phishing the most common type of attack.

HUMAN ERROR

Cyber criminals rely heavily on people's mistakes to complete all sorts of attacks. If an employee clicks on a malicious link and falls prey to a phishing attempt, or a systems administrator has poor patch management practices, attackers can infiltrate the organization's network.

ARTIFICIAL INTELLIGENCE (AI)

While AI can be greatly beneficial, it can also be used against organizations. For example, criminals used AI-based software to impersonate an executive's voice and call the CEO to ask for an urgent transfer of funds. The unaware CEO of the unnamed UK-based energy firm transferred €220,000 to a fraudulent account.[8]

[7] **Verizon**, 2019, Data breach investigations report
[8] **Wall Street Journal**, 2019, Fraudsters used AI to mimic CEO's voice in unusual cybercrime case

Diligent

Solutions for CISOs

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 to the board, 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

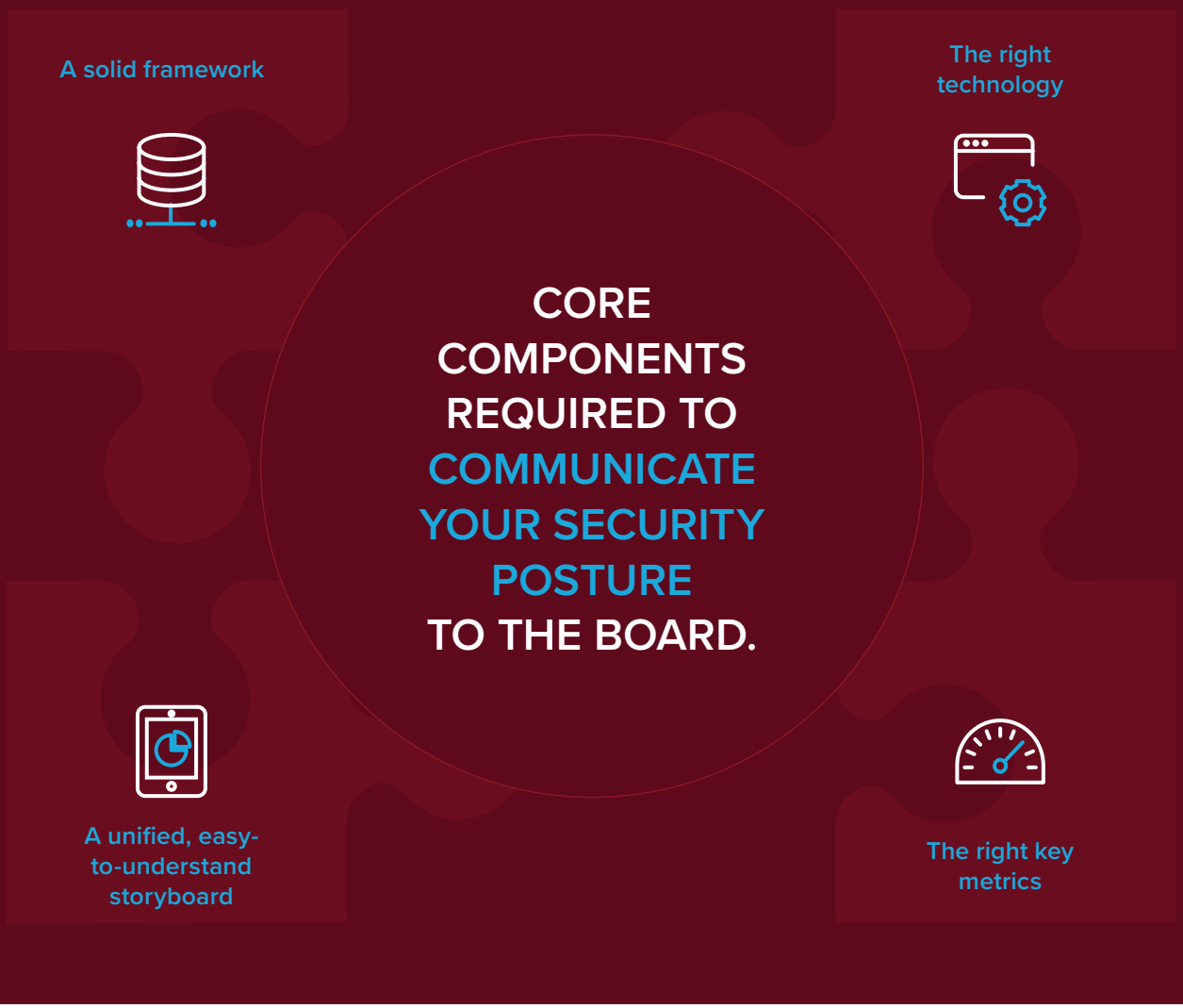
- Organize metrics by departments (e.g., governance, security ops).
- Select the metrics that influence behavior.
- Establish a baseline of what is a low, medium, and high risk, based on your policies and risk appetite.
- Focus on the speed of incident closure, not only the incident count (e.g., look at the number of critical vulnerabilities still open after 60 days vs. just the number of critical vulnerabilities).

MAKE SURE YOU HAVE THE RIGHT TECHNOLOGY

Can you merge data from different tools—not just security and GRC tools, but ERP systems? It's essential that your tech solution is able to process data through an analytics engine, put it on a schedule, and create storyboards for easy data sharing.

PARTNER & COMMUNICATE CLEARLY WITH THE BOARD

The CISO role is now a business-focused one. Rather than using fear or uncertainty as a strategy, CISOs should present cybersecurity risk as a business problem. Boards don't care about excessive detail, so CISOs have to avoid overwhelming everyone 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 earlier.



USE THE RIGHT RISK MANAGEMENT FRAMEWORK

A good framework will help protect the organization without slowing growth. 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.

01 **Identify** risk systems, assets, data, and capabilities before the attack.

02 **Protect** your organization by developing and implementing appropriate safeguards.

03 **Detect** a cybersecurity event.

04 **Respond** to the cybersecurity attack.

05 **Recover** by developing and implementing activities for resilience and restoring capabilities or services.

Be Prepared to Answer Questions from the Board

While we can't predict what a certain board will ask a CISO, here are some common questions.

1. **What's our organization's security posture?** In other words: what's our maturity level before, during, and after a cyber attack?

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).

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 cause damage to 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

Conclusion

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).

We hope this eBook has helped you understand the challenges and risk landscape CISOs must navigate, often with limited resources. But more importantly, how the new CISO role and intelligent, purpose-built technology like our HighBond platform can create more strategic alignment with organizational objectives.

Diligent

Further Learning

THE EVOLVING ROLE OF THE CISO: FROM RISK MANAGER TO BUSINESS ENABLER

The CISO increasingly has a seat at the table because security is no longer just about risk—it's also about competitive differentiation.
securityroundtable.org/evolving-role-of-the-ciso-risk-manager-to-business-enabler/

CISO EMERITUS STEVE KATZ: WHY THE CISO SHOULD REPORT TO THE CHIEF RISK OFFICER & NOT THE CIO

According to Katz, CISOs need to be "trusted business advisors" that help companies define risk appetites and identify alternative ways to mitigate risk.
hmgstrategy.com/resource-center/articles/2018/02/07/ciso-emeritus-steve-katz-why-the-ciso-should-report-to-the-chief-risk-officer-and-not-the-cio

ONCE CONSIDERED A CAREER KILLER, CISOs WITH BREACH EXPERIENCE NOW PREFERRED

The measure of competence for a CISO is not so much their capacity to prevent every breach, but whether or not they have a company-wide incident-response plan in place.
blog.nacdonline.org/posts/cisos-breach-experience-preferred

SECURITY LEADERS SHARE TIPS FOR BOARDROOM CHATS

Cisco, Oracle, and LinkedIn security leaders share their challenges in communicating with business teams and give advice for how CISOs can navigate this critical relationship.
darkreading.com/risk/security-leaders-share-tips-for-boardroom-chats/d/d-id/1335789

CISO SERIES

Discover successful security strategies and valuable lessons learned from CISOs and Microsoft's top security experts to help you navigate an ever-expanding threat landscape.
microsoft.com/security/blog/ciso-series

Ready to find out how Threat and Vulnerability Management can help you better manage your IT security risk?

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