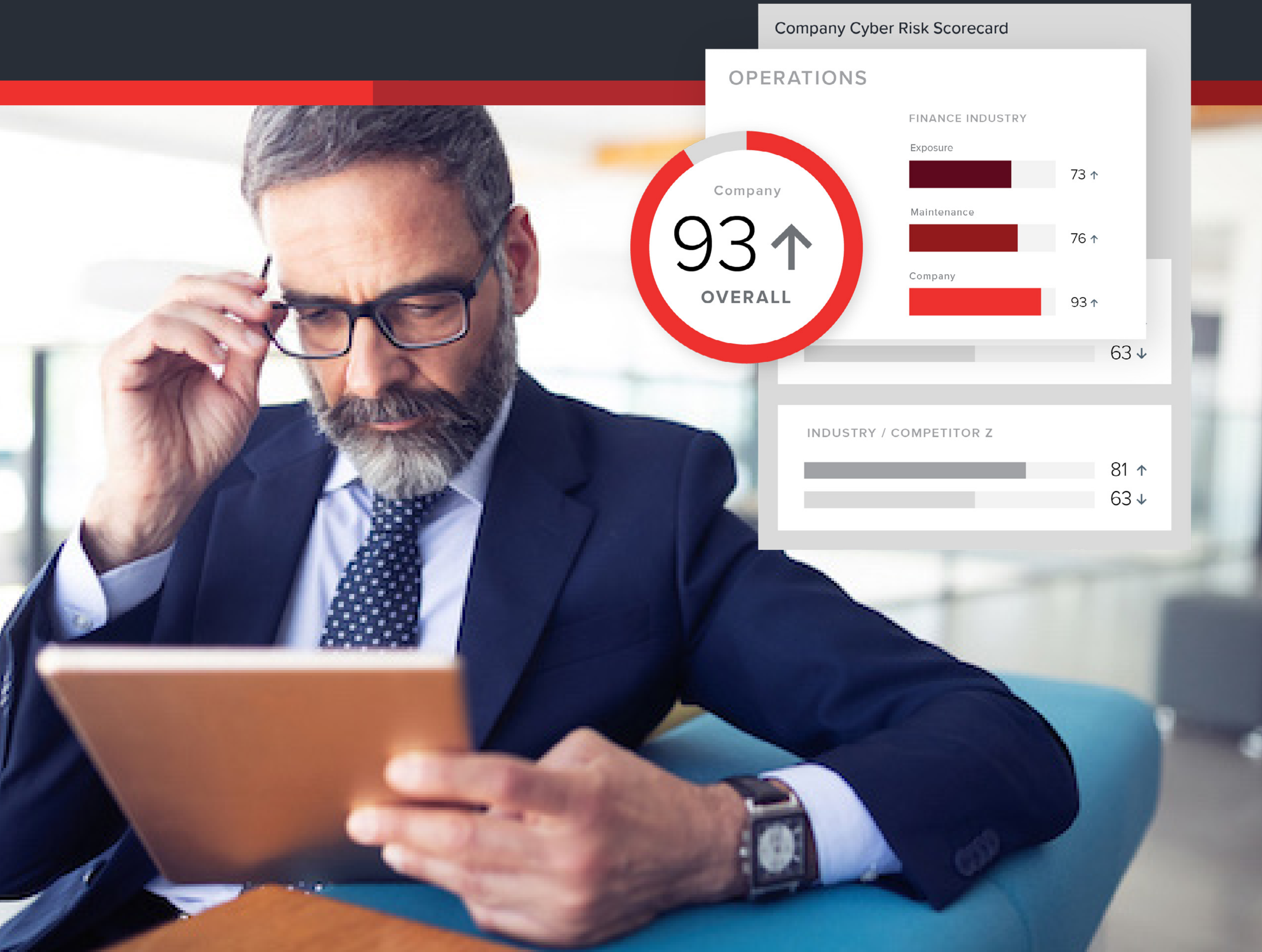
Diligent

ASSESSING YOUR CYBER RISK SCORE

Better Risk Assessment and Analysis Using a Cyber Risk Scorecard



The Importance of Cyber Risk Awareness

One certainty about cyber risk is that threats are dynamic and constantly evolving. Recovering from a cyber breach's financial, reputational and structural damage can be difficult. For boards, vigilance is critical.

Today's cybersecurity landscape is one where challenges are rapidly multiplying and, without the right tools, it can be nearly impossible to keep up. Regardless of industry or location, cybersecurity is a critical business issue and will be a crucial focus for boards in the months and years ahead.

Gartner's recent 2020 Board of Directors survey predicts that some 40% of boards will have a dedicated cybersecurity committee by 2025 (up from less than 10% today). This increase is a clear indicator of high-level organisational changes that are already underway, accelerated by "the greater risk created by the expanded digital footprint of organisations during the [COVID-19] pandemic."

As organisations continue on the path to a digitally-led future, boards must ensure the transition goes as smoothly as possible. They must be aware of any vulnerabilities – from potential data breaches to third-party partnerships – that may present risks if pre-emptive measures are not in place.

The correct approach to managing cyber risk requires a better understanding of several factors, including:

- Digital transformation, entailing a shift toward technology-driven operations, and a simultaneous movement away from manual, paper-based processes.
- A marked increase in remote working, highlighting secure collaboration and communication's importance in a virtual environment.
- Increasing scrutiny from investors, higher expectations from consumers, and a growing number of stakeholder considerations.
- A regulatory focus on third-party monitoring.
- The impact of reputational risk and its associated financial ramifications.

Ultimately, staying acutely aware of cyber risks is one of the most pressing issues for boards today.

> "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

Effective Risk Oversight Starts at the Top

In the face of unpredictable cyber risks, organisations must fortify their defences and identify and prioritise the most suitable systems, models, and processes. Failing to put protective measures in place leaves businesses particularly vulnerable to attack and leaves them lagging behind more security-conscious peers. A reactive approach to cyber risk is also likely to have a severe reputational impact on an organisation.

For a cyber risk strategy to be effective, directors need access to the relevant cybersecurity data in an intuitive format that allows for rapid assessment and informed decisions.

A cyber risk scorecard offers this functionality. Presenting it within the board's existing board management software package further enhances its usefulness. Clear and concise data helps directors identify relevant, actionable intelligence and apply that intelligence to future decisions. That may mean taking steps to improve cybersecurity posture or deploying measures to enhance preparedness for a cyberattack. It could also mean creating a shared understanding at all levels within the organisation to enable productive conversations about risks and risk management.

> "There is not a single major business decision [today] that does not include cybersecurity considerations. [They should] be woven into the entire process."
>
> **Larry Clinton**
> President, Internet Security Alliance

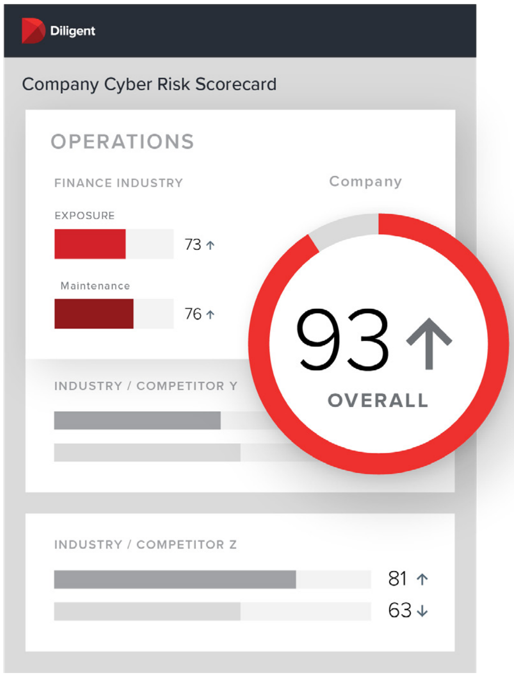
Battling Cyber Risk: Best Practices for Boards

- □ Push for alignment across the organisation, from legal to technology to data security. An integrated approach will lead to quicker, more effective threat responses.
- □ A good board leads by example, making sure that its communications are secure and protected. Embedding cybersecurity in its processes illustrates its importance to the entire organisation. Cybersecurity must be understood as an enterprise-wide risk management issue, not just a problem for the IT department.
- □ Implement a solution for clearly measuring and communicating cyber risk. This is vital amid an increasingly complex risk landscape. Using an informational scorecard – with all risk-related data coherently presented in one place – ensures focus and allows for credible reporting.
- □ Ensure that a detailed, well-drilled, and watertight cybersecurity response plan is in place: the more rapid a response, the less likely the potential for long-term damage.
- □ Lead from the top. Through its governance and focus on cybersecurity, the board can set the tone for the entire organisation. Is cybersecurity a regular item on the agenda? With strategy and risk management sitting high on many board priority lists, conversations on those issues should not happen without a significant focus on technology and security.

A Cyber Risk Scorecard Drives Better Cyber Risk Management

When it comes to cybersecurity, ratings, graphs, and colour-coded flags can act as eyes and ears, driving board members to ask better questions, such as:

- **What gaps exist in our cybersecurity framework?**
- **Does the service provider we're considering have vulnerabilities that can put our organisation at risk?**
- **What are our current third-party providers' risk levels?**
- **How do our cybersecurity capabilities stack up against our competition?**
- **How does the board know the organisation is improving its cybersecurity and compliance posture?**
- **Does the business we're about to acquire have cybersecurity issues that could impact the deal?**



Cybersecurity risks are constantly evolving and changing. As important as it is to keep up with any emerging threats, for reporting and progression purposes the most useful piece of information is often a simple, easily understandable score. A cyber risk score carries many benefits. A simple, hierarchical grading system, whether letters or numbers, improves executive-level reporting and elevates cybersecurity reporting and aligns it with business needs. Armed with that score and the visibility it provides, the board is empowered to more quickly make better, more informed cybersecurity decisions.

Four Scenarios Requiring a Cyber Risk Scorecard

1 MEASURING THE ORGANISATION’S CYBER RISK

A cyber risk scorecard should evaluate an organisation’s security risk using data-driven, continuously updated metrics that provide visibility into security control deficits and potential vulnerabilities throughout the supply chain ecosystem.

Armed with this knowledge, boards can enact changes to shore up weak points. Further, continuous monitoring of such a scoring system enables boards to see where progress has been made and measure its impact on the organisation.

A board with the visibility offered by a cyber risk scorecard will find itself able to proactively manage and prioritise security risks and make informed, data-driven business decisions.

The Realities of a Cyber Breach

In 2020 Ambulance Tasmania’s paging system was breached, meaning that the details of every callout since November has been published online, on a website with more than 26,000 pages.

As of January 2021, the information was ‘live’ and being updated every time an ambulance was dispatched. The site has since been taken offline.

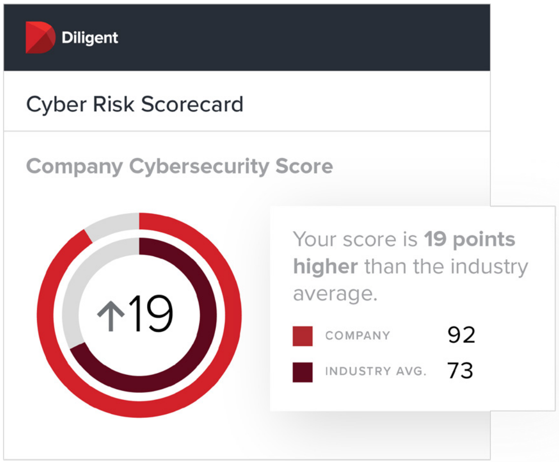
The published data included personal details and condition, incident locations, HIV status, mental health callouts, gender and age. More than half a billion dollars has been allocated to upgrade the state’s emergency communications network.

2 BENCHMARKING AGAINST PEERS

The ability to quickly assess industry peers’ and competitive organisations’ security postures is significant. It allows boards to understand exactly where they sit compared to others in their field, what they could be doing better and where they maintain an advantage over the competition. Drilling down into specific security issues across a peer group offers a fast way to compare and contrast cybersecurity readiness.

Organisations regularly examine other companies’ KPIs in sales, profits, or productivity to improve internal performance by reallocating resources and prioritising specific objectives. Applying the same processes to cyber risk analysis can be similarly beneficial.

Being aware of where your competitors stand helps plug security gaps in your organisation. It can also help drive innovation and push processes forward. Using that data can help create an action plan and set short and long-term goals centred on raising cybersecurity to the same or a higher level as top-performing competitors.



Diligent

Cyber Risk Scorecard

Company Cybersecurity Score

↑19

Your score is **19 points higher** than the industry average.

🟥 COMPANY	92
■ INDUSTRY AVG.	73

3 UNDERTAKING DUE DILIGENCE

Gartner's Innovation Insight for Security Rating Services report states that, by 2022, "Security ratings will become as important as credit ratings when assessing the risk of business relationships." Comprehensive due diligence requires obtaining insights into the cyber health of any vendors or companies the board's organisation intends to do business with – whether they are potential or current partners or vendors or potential acquisition targets.

Having the ability to continuously identify, monitor and manage risk throughout the vendor ecosystem is critical to continued success. Ultimately, an organisation's cybersecurity is only as strong as the weakest link in its entire network. A vulnerability anywhere in that supply chain not only escalates enterprise risk but jeopardises productivity, profitability, and reputation.

Similarly, investing in, partnering with or buying another company means taking on its digital operations, which can bring new and potentially deal-altering cybersecurity risks. Identifying and addressing cyber threats early in the process can neutralise their potential to jeopardise a deal's anticipated value.

Notifiable breaches increasing

Australia's Notifiable Data Breach (NDB) scheme was established in 2018. In the event of a breach, organisations covered by the Privacy Act 1988 must notify the Office of the Australian Information Commissioner (OIAC), and the individuals affected.

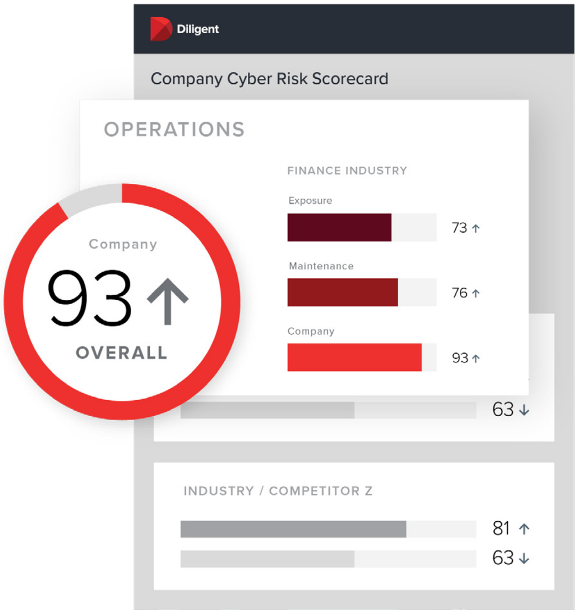
For the July–December 2020 period there were 539 notifications (up 5% from the previous period), of which 58% were due to malicious or criminal attack. Healthcare remains the highest-reporting sector, with 123 notifications, followed by finance, with 80, then education (40), legal, accounting and management services (38) and government (33).

> "[By 2022,] security ratings will become as important as credit ratings when assessing the risk of business relationships."
>
> Innovation Insight for Security Rating Services
> Gartner

4 MANAGING REPUTATIONAL RISKS

Reputational risk is perhaps the most damaging risk of all. Whereas more traditional risks can be mediated and managed – and often dealt with internally – a tarnished corporate image can take years to rebuild. As such, organisations must manage their reputation carefully.

A cyber risk scorecard offers consistent visibility into potential threats and vulnerabilities that have the power to disrupt business operations. It allows organisations to detect potential gaps in security whilst ensuring that any vendors they are working with are always in compliance with relevant regulations – enabling the capacity to address third-party reputational risk in real-time.



Data breaches affect us all

While healthcare is the most-targeted sector by criminals, data breaches occur across all industries. Not all attacks come from criminals; in the second half of 2020 58% of notifiable breaches were due to malicious actors, while 38% were due user error. This may reflect carelessness, but it can also indicate poor internal processes, a weak security culture or inadequate training.

Diligent’s Cyber Risk Scorecard Provides a Comprehensive Cyber Health Snapshot

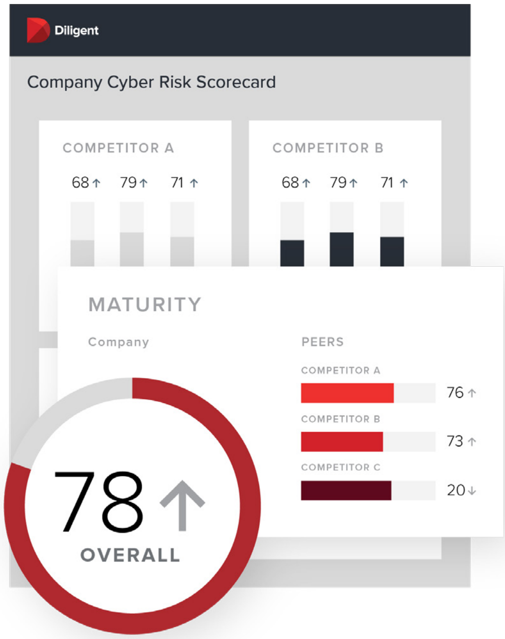
A proactive approach to cyber risk management is imperative to continued organisational success. Diligent’s Cyber Risk Scorecard offers board members a level of visibility they didn’t have previously. It’s always up to date and always accessible, which is crucial for cyber risk management.

The information presented is easily digestible, allowing for greater understanding, better reporting and easier analysis. Its cybersecurity measurements are intuitive, sourcing its data and information from many touchpoints and distilling its findings into a coherent, visual display. Diligent’s Cyber Risk Scorecard offers accurate security ratings that can help detect critical issues within the organisation, with peers, over time and across critical factors driving the score.

Organisations that choose to dive in further can access an even deeper level of information across vendor relationships, M&A transactions, private equity deals, credit underwriting, and financial sales and trading.

With the Cyber Risk Scorecard – powered by the World Economic Forum-recognised SecurityScorecard – directors can fortify their organisations and ably navigate an evolving and complex digital landscape:

- Access their cyber risk score and compare it against peer and Diligent-managed competitive groups.
- Understand their cybersecurity posture against industry benchmarks, as well as the top three security factors contributing to that score.
- Prioritise which actions to take and identify what infrastructure and software must be addressed.
- Manage reputational risks, identify trends and access their historical cyber risk scores.



Cyber Risk Scorecard comprehensively measures and quickly communicates security risks, curating insights via a visual dashboard that outlines network and system vulnerabilities alongside critical and common risks. Directors can prioritise the cybersecurity gaps that need remedying most immediately whilst benchmarking the organisation against custom peer groups and Diligent-managed competitor groups. Additionally, they can monitor the cyber risk scores of up to five peers.

VIEW THE ORGANISATION FROM AN OUTSIDER'S PERSPECTIVE

Cyber Risk Scorecard helps to identify vulnerabilities and highlight active exploits and advanced cyber threats – and all from an 'outside-in' perspective, letting boards see what a hacker sees. With heightened visibility and direct access to information, boards can keep pace and stay informed.

Cyber Risk Scorecard grades companies with a simple A–F scale. Organisations with an F rating are 7.7 times more likely to experience a data breach than those with an A rating. When part of a comprehensive risk oversight strategy, these ratings can effectively highlight cybersecurity vulnerabilities and prevent data breaches.

To provide the most comprehensive overview possible, the ratings are drawn from a multitude of factors, including DNS health, IP reputation, web application security, network security, leaked information, hacker chatter, endpoint security and patching cadence. Despite the clarity and visual simplicity of the information presented within the Scorecard, it contains a wealth of data, human analysis, and machine learning to evaluate over 1.6 million companies.

Diligent's Cyber Risk Scorecard continuously monitors your organisation's security and displays the most critical risk issues your company faces, sorted by severity. It will automatically generate a recommended remediation plan informed by your own organisational goals and procedures, helping you to put the best processes in place.

Understanding Cybersecurity Terminology

- **Network Security:** Examples of network security hacks include exploiting vulnerabilities such as open access points, unsecured or misconfigured SSL certificates, or database vulnerabilities and security holes that can stem from the lack of proper security measures.
- **DNS Health:** This generally refers to measurements of Domain Name System configuration settings, as well as the presence of recommended configurations
- **Patching Cadence:** This measures how a company patches its operating systems, services, applications, software and hardware, and whether it is doing so promptly.
- **Endpoint Security:** Endpoint security refers to the protection of an organisation's laptops, desktops, mobile devices, and all employee devices that access that company's network.
- **IP Reputation:** Cyber Risk Scorecard ingests millions of malware signals from commandeered Command and Control (C2) infrastructures from all over the world. The incoming infected IP addresses are then processed and attributed to corporate enterprises through our IP attribution algorithm. The quantity and duration of malware infections are used as the determining factor for these calculations, providing a data point for the overall assessment of an organisation's IP reputation.
- **Hacker Chatter:** Cyber Risk Scorecard continuously collects multiple streams of underground chatter, including hard-to-access or private hacker forums, and identifies organisations and IPs that are discussed or targeted.
- **Leaked Information:** Cyber Risk Scorecard identifies all sensitive information exposed as part of a data breach or leak, keylogger dumps, pastebin dumps or database dumps, and via other information repositories. It then maps that information back to the companies that own the data.

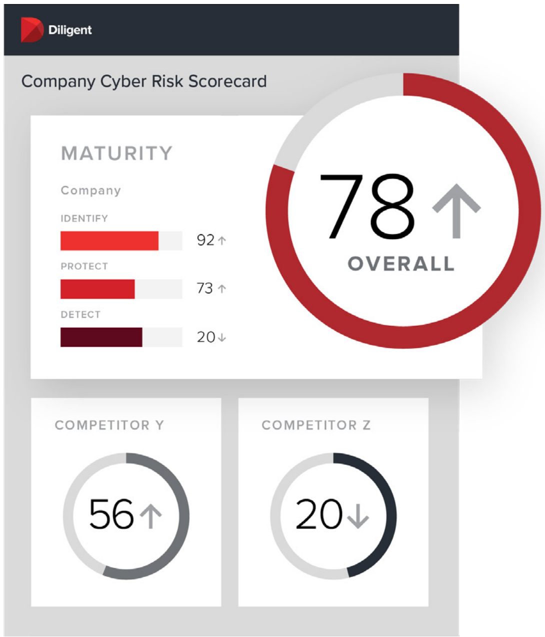
Cyber Risk Scorecard and the Broader Governance Ecosystem

A well-managed solution to established and incoming cyber threats is only one facet of a modern corporate governance approach. Cybersecurity, by its very nature, demands a digital solution.

Furthermore, as boards transition to new styles of oversight, they are embracing new information channels. While the concept of 'risk dashboards' has been around for a while, it is time for boards to demand access to them. Cyber Risk Scorecard offers this intuitive dashboard functionality.

Cyber Risk Scorecard works in synergy with the rest of the Diligent modern governance platform, creating a stronger, more secure, and more digitally robust organisation poised to thrive. With Cyber Risk Scorecard, organisations benefit from:

- Continued security and digital resilience
- Enhanced knowledge around important issues, from data stewardship to supply chain security
- Organisational stability
- Future investment potential
- Long-term prosperity



Directors, executives and governance professionals face a modern governance imperative: They need to navigate complexities and make challenging and rapid decisions. A suite of solutions that mitigate risk, enhance operations, and keep leaders informed is essential for continued security and digital resilience and future potential and organisational stability.

Ready to see Diligent's Cyber Risk Scorecard in action? Schedule a demo.

REQUEST A DEMO ▶

Diligent

a MODERN GOVERNANCE company

About Diligent

Diligent is the pioneer in modern governance. Our trusted, cloud-based applications streamline the day-to-day work of board management and committees, support secure collaboration, manage subsidiary and entity data, and deliver insights that empower company leaders to make better decisions in today's complex landscape. With the largest global network of corporate directors and executives, Diligent is relied on by more than 19,000 organisations and nearly 700,000 leaders in over 90 countries. With award-winning customer service across the globe, Diligent serves more than 50% of the Fortune 1000, 70% of the FTSE 100 and 65% of the ASX.

Trusted by over 700,000 leaders and 19,000 organisations across the globe

CREDIT CORPORATION · AUSTRALIAN RED CROSS · General Mills · Liberty Mutual. · Domino's

Highest security standards

- 256-bit encryption
- Remote locking
- Two-factor authentication

Industry-leading support

- 24/7/365 support
- White glove service
- Unlimited user training

Compliance Attestations

- ASAE 18 audits
- ISO-certified
- Third-party security testing

For more information or to request a demo:

Call: **1-800-646-207** • Email: **info@diligent.com** • Visit: **diligent.com/au**