Diligent

Assessing your cyber risk score

Better risk assessment and analysis using a cyber risk scorecard

The importance of cyber risk awareness

One thing is certain about cyber risk: that threats are dynamic and continually evolving. The financial, reputational and structural damage wrought by a cyber breach can be devastating. 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. Irrespective of industry or location, cybersecurity is a critical business issue and an area for board focus in the months and years ahead.

Indeed, Gartner's recent 2020 Board of Directors survey predicts that some 40% of boards will have a dedicated cybersecurity committee by 2025, up from fewer than 10% today. It's a clear indicator that high-level organisational changes are already underway. As Gartner notes, in part, it's a response to "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 they take proper steps and put suitable measures in place to ensure the transition goes as smoothly as possible. Boards must be aware of any vulnerabilities – from potential data breaches to third-party partnerships – that may present a risk without pre-emptive safeguards.

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

- Digital transformation, which entails a shift toward technology-driven operations, and a simultaneous movement away from manual, paper-based legacy processes
- A marked increase in remote working, highlighting how vital secure collaboration and communication are in a virtual environment
- Taking into account 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.

"More abundant and better-resourced cybercriminals and cyber activists, and increasingly sophisticated and emboldened state actors, mean Australia is quite literally under constant cyber attack."

Andrew Penn, CEO, Telstra

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. A failure 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 presented in an intuitive format. This information will enable rapid risk assessments and well-considered decisions that improve cyber posture.

A cyber risk scorecard offers this functionality, especially when presented within the board's existing board management software package. Clear and concise data helps directors identify relevant, actionable intelligence and apply that intelligence to their decision-making. Those decisions may include taking steps to improve cybersecurity posture, taking measures to enhance preparedness for a cyberattack, or creating a shared understanding to enable productive conversations at all levels within the organisation.

"Connected technologies are now right at the heart of the lives of most Australians and increasingly pivotal in shaping our economy, our society and our prospects for the future."

Andrew Penn, CEO, Telstra

Battling cyber risk: best practices for boards

- **Push for alignment across the organisation,** from legal to technology to data security. A joined-up approach at board-level and below will lead to a quicker, more effective response to threats.
- **A good board leads by example**, making sure that their communications are secure and protected. By embedding cybersecurity in their processes, they illustrate the importance of such an approach to the 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 step is vital step 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 organisation. Is cybersecurity a constant item on the agenda or just a passing thought? 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 is the risk level of our current third-party providers?
- 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 continually evolving and changing. As important as it is to keep up with any emerging threats, the most valuable piece of information is often a simple, easily understandable score for reporting and progression purposes. A cyber risk score carries many benefits.

A simple, hierarchical grading system – whether letters or numbers – improves executive-level reporting, elevates cybersecurity reporting and aligns it with business needs. Armed with that score and the visibility it provides, the board is empowered to make better, more informed cybersecurity decisions and to make those decisions more quickly.

4 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. It provides 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 view progress and measure its impact on the organisation.

A board that uses a cyber risk scorecard will find itself in a position to proactively manage and prioritise security risks, as well as make informed, data-driven business decisions.

Australian businesses are bracing for more cyber attacks **from criminal organisations and state-based actors.**

Likely targets include critical infrastructure, such as the power grid, and critical services, such as hospitals. Cloud services are another likely target, as their usage has increased thanks to workers shifting to work-from-home arrangements in response to the COVID-19 pandemic.

2. Benchmarking against peers

The ability to quickly assess the security posture of industry peers and competitive organisations allows boards to understand:

- Where they sit in comparison to others in their field
- What they could be doing better
- Where they maintain an advantage over the competition.

The ability to drill 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 objectives. Applying the same processes to cyber risk analysis can be beneficial. Being aware of where your competitors stand helps to plug security gaps in your organisation and helps to 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.

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 acquiring another company means taking on its digital operations, which can bring new and potentially deal-altering cybersecurity risks. Without identifying and addressing cyber threats early in the process, they can jeopardise a deal's anticipated value.

"[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

A data breach suffered by a third party can wreak havoc on all organisations connected to it.

In the first half of 2020 the overall number of Notifiable Data Breaches was down 3% on the previous half-year, but 61% were from malicious or criminal attack. Healthcare continues to be the most targeted sector, followed by finance (22% and 14% of breaches, respectively). Most affect fewer than 5000 people but 5% affected more – with two cases exceeding 1 million and one exceeding 10 million people globally.

4. Managing reputational risks

Reputational risk is potentially the most damaging of all. Whereas more traditional hazards 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 continuous visibility into potential threats and vulnerabilities that have the power to disrupt business operations. It allows organisations to detect potential gaps in security while ensuring that any vendors they are working with are always in compliance with relevant regulations. This, in turn, allows organisations to address third-party reputational risks in real-time.

Reputational risk emerged as a genuine business concern **around a decade ago.**

In 2014 the Australian Institute of Company Directors (AICD) has identified reputational damage as a 'top threat'. Deliotte Risk Services managing partner Harvey Christophers said at the time, "Reputational risk was ranked third three years ago, but today it is the top strategic risk".

Australia is the world's sixth-most targeted country according to recent data. AustCyber's latest report estimates that a major incident could cost $30bn and destroy more than 160,000 jobs. These figures are only direct losses so do not include the impact of reputational harm. These harms include customers or business partners losing trust in an organisation's ability to protect their data and taking their trust elsewhere – and their custom, investments and contracts along with it. The risks are very real, so businesses must take equally real steps to counter them.

Diligent's Cyber Risk Scorecard provides a comprehensive cyber health snapshot

A proactive approach to cyber risk management is imperative to continue organisational success.

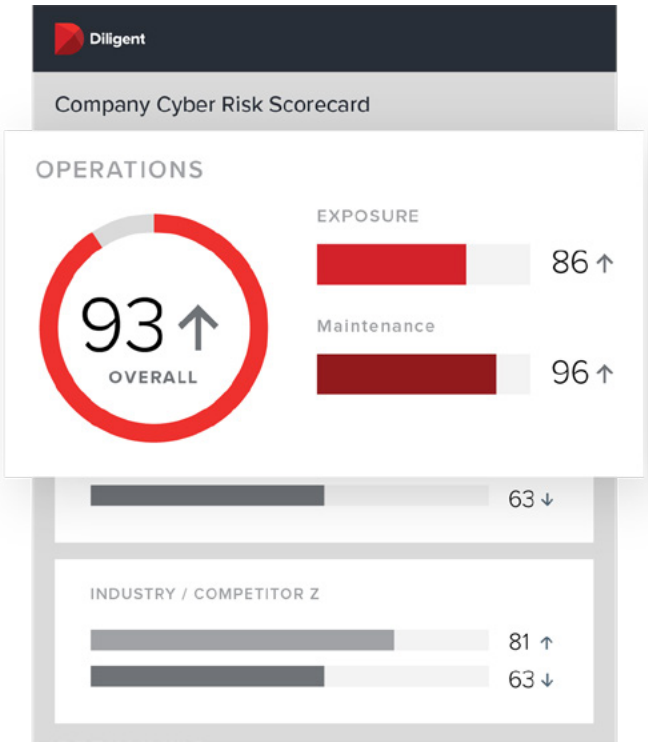
Diligent's Cyber Risk Scorecard offers board members a level of visibility they didn't have previously. It's always up to date and always accessible – making it a crucial tool for managing cyber risk. The information presented is easily digestible, allowing for greater understanding, better reporting and easier analysis. It presents cybersecurity evaluations intuitively, sourcing data and information from several 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 itself, with peers, over time and across key factors driving the score. Organisations who 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-recognized SecurityScorecard – directors can fortify their organisations and ably navigate an evolving and complex digital landscape by:

- Accessing their cyber risk score and comparing it against peer and Diligent-managed competitive groups.
- Understanding their cybersecurity posture against industry benchmarks, as well as the top three security factors contributing to that score.
- Prioritising which actions to take and identifying which infrastructure and software to address.
- Managing reputational risks, identifying trends and accessing their historical cyber risk scores.

The Cyber Risk Scorecard comprehensively measures and quickly communicates security risk, 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 while benchmarking the organisation against custom peer groups and Diligent-managed competitor groups. Additionally, they can monitor up to five peers' cyber risk scores.

It's an invaluable tool for managing risk and protecting your organisation. If you're not using it, we urge you to begin exploring your options today.



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 Scorecard draws its ratings from many 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 Scorecard's reports, it contains a wealth of data, human analysis and machine learning, and it evaluates 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 notifiable data breach terminology

- **Financial details:** Information relating to an individual's finances, for example, bank account or credit card numbers.
- **Tax File Number (TFN):** An individual's personal reference number in the tax and superannuation systems, issued by the Australian Taxation Office.
- **Identity information:** Information that is used to confirm an individual's identity, such as a passport number, driver's licence number or other government identifier.
- **Contact information**: Information that is used to contact an individual, for example, home address, phone number or email address.
- **Health information:** As defined in section 6 of the Privacy Act.
- **Other sensitive information:** Sensitive information, other than health information, as defined in section 6 of the Privacy Act. For example, sexual orientation, political or religious views.

Breach categories

- **Human error:** An unintended action by an individual directly resulting in a data breach, for example inadvertent disclosure caused by sending a document containing personal information to the incorrect recipient.
- **PI sent to wrong recipient (email):** Personal information sent to the wrong recipient via email, for example, as a result of misaddressed email or incorrect address on file.
- **PI sent to wrong recipient (fax):** Personal information sent to the wrong recipient via facsimile machine, for example, as a result of fax number incorrectly entered or wrong fax number on file.
- **PI sent to wrong recipient (mail):** Personal information sent to the wrong recipient via postal mail, for example, as a result of a transcribing error or wrong address on files.
- **PI sent to wrong recipient (other):** Personal information sent to the wrong recipient via channels other than email, fax or mail, for example, delivery by hand or uploading to web portal.
- **Failure to use BCC when sending email:** Sending an email to a group by including all recipient emails addresses in the 'To' field, thereby disclosing all recipient email address to all recipients.
- **Insecure disposal:** Disposing of personal information in a manner that could lead to its unauthorised disclosure, for example, using a public rubbish bin to dispose of customer records instead of a secure document disposal bin.
- **Loss of paperwork/data storage device:** Loss of a physical asset containing personal information, for example, leaving a folder or a laptop on a bus.
- **Unauthorised disclosure (failure to redact):** Failure to effectively remove or de-identify personal information from a record before disclosing it.
- **Unauthorised disclosure (verbal):** Disclosing personal information verbally without authorisation, for example, calling it out in a waiting room.
- **Unauthorised disclosure (unintended release or publication):** Unauthorised disclosure of personal information in a written format, including paper documents or online.
- **Malicious or criminal attack**: A malicious or criminal attack deliberately crafted to exploit known vulnerabilities for financial or other gain.
- **Theft of paperwork or data storage device:** Theft of paperwork or data storage device
- **Social engineering/impersonation:** An attack that relies heavily on human interaction to manipulate people into breaking normal security procedures and best practices in order to gain access to systems, networks or physical locations.
- **Rogue employee/insider threat:** An attack by an employee or insider acting against the interests of their employer or other entity.
- **Cyber incident:** A cyber incident targets computer information systems, infrastructures, computer networks or personal computer devices.
- **Malware:** Software which is specifically designed to disrupt, damage, or gain unauthorised access to a computer system.
- **Ransomware:** A type of malicious software designed to block access to data or a computer system until a sum of money is paid or other conditions are met.

- **Phishing (compromised credentials):** An attack in which the target is contacted by email or text message by someone posing as a legitimate institution to lure individuals into providing personal information, sensitive information or passwords.
- **Brute-force attack (compromised credentials):** Automated software is used to generate a large number of consecutive guesses as to the value of the desired data, for example passwords.
- **Compromised or stolen credentials (method unknown):** Credentials are compromised or stolen by methods unknown.
- **Hacking (other means):** Exploiting a software or security weakness to gain access to a system or network, other than by way of phishing, brute-force attack or malware.
- **System fault:** A business or technology process error not caused by direct human error.

SOURCE: Notifiable Data Breaches Report: January–June 2020

Cyber risk scorecard and the broader governance ecosystem

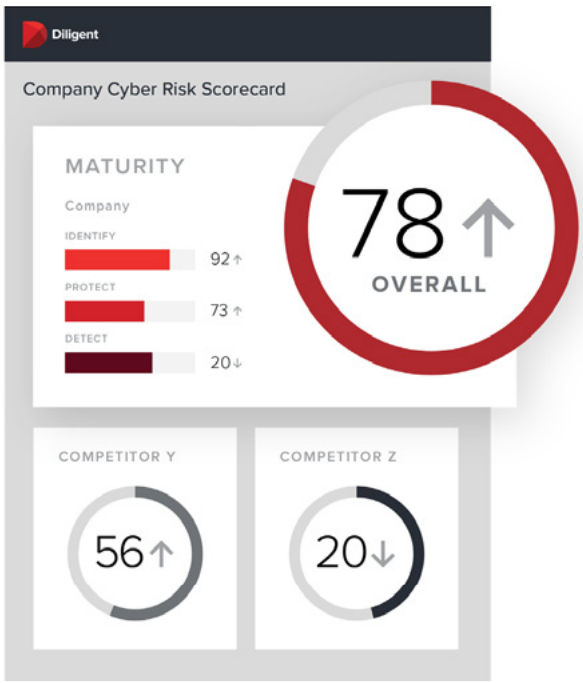
A well-managed solution to established and incoming cyber threats is only one facet of a modern corporate governance approach. Cybersecurity, by its very nature, demands a digital solution.

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. The 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.



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.

Ready to see Diligent's Cyber Risk Scorecard in action? Contact us to schedule a demo:

Email: info@diligent.com
Website: diligent.com/au

Phone:
Australia: 1 800 646 207
New Zealand: 0800 434 5443
Singapore: +65 6932 2638
Hong Kong: +852 3008 5657
India: 000-800-100-4374
China: 400-120-9359

Diligent