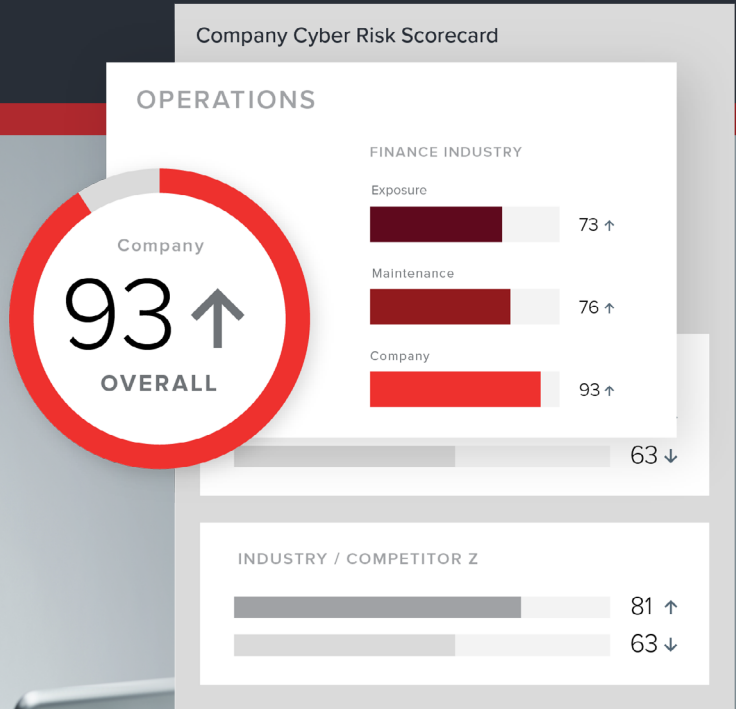




# ASSESSING YOUR CYBER RISK SCORE

Better Risk Assessment and Analysis Using a Cyber Risk Scorecard



# The Importance of Cyber Risk Awareness

Cybersecurity threats are dynamic and constantly evolving. The financial, reputational and structural damage wrought by a cyber breach can be hard to recover from. For boards, vigilance is key.

Without the right tools, it can be nearly impossible to keep up. Irrespective of industry or location, cybersecurity is a critical business issue and will be a key focus for boards in the months and years ahead.

Indeed, Gartner's [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) – a clear indicator of high-level organizational changes that are already being made “in response to the greater risk created by the expanded digital footprint of organizations during the [COVID-19] pandemic.”

As organizations continue on the path to a digitally led future, boards must ensure they take the right steps and put the right measures in place to ensure the transition goes as smoothly as possible. Boards must be cognizant of any vulnerabilities – from potential data breaches to third-party partnerships – that may present risk if preemptive measures are not put in place.

## 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 important secure collaboration and communication are in a virtual environment.
- Increasing scrutiny from investors, higher expectations from consumers and a growing number of stakeholder considerations that need to be taken into account .
- 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 order for a cyber risk strategy to be effective, directors need access to relevant cybersecurity data, presented in an intuitive format that allows for rapid assessment and informed decisions that improve cyber posture.

A cyber risk scorecard offers this functionality, particularly when presented within the board management software with which directors are already familiar. Clear and succinct data helps directors identify relevant, actionable intelligence and apply that intelligence to future decision-making – whether that’s taking steps to improve cybersecurity posture or taking measures to enhance preparedness for a cyberattack — or simply to create a common understanding and enable productive conversations at all levels within the organization.



“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

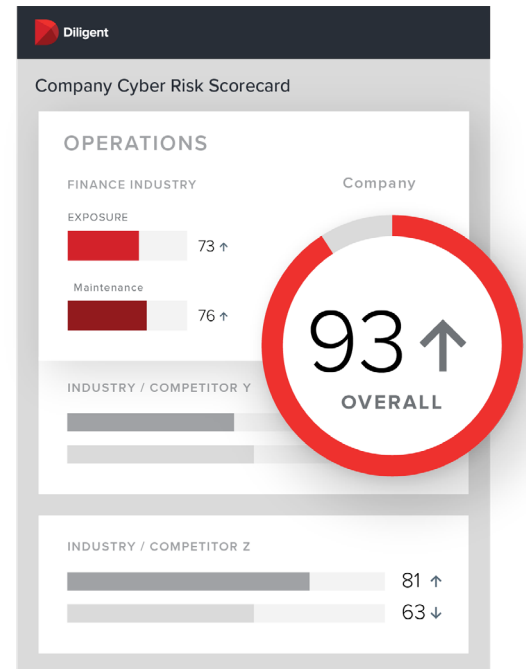
- ❑ Push for alignment across the organization, from legal to technology to data security. An integrated approach at board level and below will lead to a quicker, more effective response to threats.
- ❑ A good board leads by example, making sure that their own communications are secure and protected. By embedding cybersecurity in their own processes, they illustrate the importance of such an approach to the organization as a whole. Cybersecurity needs to be viewed as an enterprise-wide risk management issue – and not just as a problem for the IT department.
- ❑ Implement a solution for clearly measuring and communicating cyber risk. This is a vital step amid an increasingly complex risk landscape. Utilizing 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 own governance and focus on cybersecurity, the board can set the tone for the rest of the organization. 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 color-coded flags can act as eyes and ears, driving board members to ask better questions:

- **What gaps exist in our cybersecurity framework?**
- **Does the service provider we're considering have vulnerabilities that could put our organization at risk?**
- **What is the risk level of our current third-party providers?**
- **How do our cybersecurity capabilities stack up against those of our competition?**
- **How does the board know the organization 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. Yet, for reporting and planning purposes, the most useful piece of information is often a simple, easily understandable score. A cyber risk score carries many benefits. Through a simple, hierarchical grading system – whether composed of letters or numbers – it 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 make better, more informed cybersecurity decisions, and to make those decisions more quickly.



## 4 Scenarios Requiring a Cyber Risk Scorecard

### 1 MEASURING THE ORGANIZATION'S CYBER RISK

A cyber risk scorecard should evaluate an organization'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. In addition, continuous monitoring of such a scoring system enables boards to see where progress has been made, and to measure the impact of that progress on the wider organization.

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

### The Realities of a Cyber Breach

SolarWinds, a major IT firm that provides software for entities ranging from Fortune 500 companies to the U.S. government, was [recently the subject](#) of a massive cybersecurity attack that spread to its clients – with the breach going undetected for months. Up to 18,000 of SolarWinds' customers unwittingly installed software updates that included hacked code, executed so stealthily that some victims may never know if they were hacked or not. Re-securing compromised systems will be astronomically expensive and could take years.

### 2 BENCHMARKING AGAINST PEERS

The ability to quickly assess the security posture of industry peers and competitors allows boards to understand exactly where they sit in comparison to others in their field, what they could be doing better and where they maintain an advantage over the competition. Being able to drill down into specific security issues across a peer group offers an instantaneous way to compare and contrast cybersecurity readiness.

Organizations regularly examine other companies' KPIs in sales, profits or productivity and consequently improve internal performance by reallocating resources and prioritizing certain objectives. Applying the same processes to cyber risk analysis can be beneficial. Being aware of where your competitors stand not only helps to plug security gaps in your organization, but also helps to drive innovation and push processes forward. Leveraging that data can help to create an action plan and set short- and long-term goals centered on raising cybersecurity to the same or a higher level as that of 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 organization 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 organization'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 jeopardizes 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. Unless cyberthreats are identified and addressed early in the process, these threats have the potential to jeopardize a deal's anticipated value.

A data breach suffered by a third party can wreak havoc on all organizations connected to it. In 2018, the data of more than 2.65 million Atrium Health patients [was breached](#) when the servers of its billing vendor, AccuDoc Solutions, were breached. Similarly, the personal data of at least 30,000 U.S. Department of Defense workers was exposed when a third-party vendor used for booking travel [was hacked](#).

“[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 some risks can be mediated and managed – and often dealt with internally – a tarnished corporate image can take years to rebuild. Thus, it's vital that organizations manage their reputations carefully.

A cyber risk scorecard offers consistent visibility into potential threats and vulnerabilities that could disrupt business operations. It allows organizations to detect potential gaps in security while also 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.

In 2017, [Verizon acquired Yahoo](#) for \$4.48B, but the deal almost fell through over [two data breach](#) scandals that came to light during negotiations. Yahoo revealed that it had suffered two separate data breaches that it had not made public. Verizon went ahead with the acquisition of Yahoo, but knocked \$350 million off the purchase price. Verizon also agreed to share legal liability for the breaches with Yahoo. It was a costly inheritance, and, coupled with the PR fallout, it damaged the deal's value in innumerable ways.



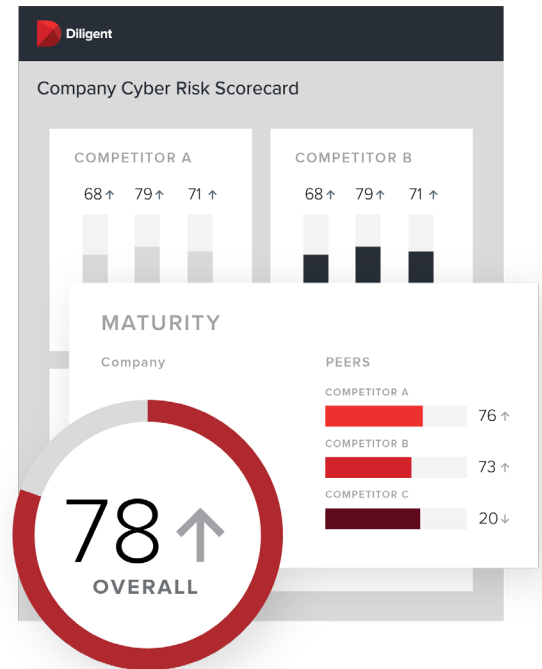
# Diligent's Cyber Risk Scorecard Provides a Comprehensive Cyber Health Snapshot

A proactive approach to cyber risk management is imperative to continued organizational 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 – a crucial component when it comes to cyber risk. The information presented is easily digestible, allowing not only greater understanding but better reporting and easier analysis. It's also intuitive in the way it measures cybersecurity, sourcing its data and information from a number of 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 organization itself, with peers, over time and across key factors driving the score. Organizations 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 Diligent's Cyber Risk Scorecard – powered by the World Economic Forum-recognized SecurityScorecard – directors can 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.
- Prioritize which actions to take and identify what infrastructure and software need to be addressed.
- Manage reputational risks, identify trends and access their historical cyber risk scores.



## VIEW THE ORGANIZATION FROM AN OUTSIDER'S PERSPECTIVE

Diligent's Cyber Risk Scorecard helps identify vulnerabilities, as well as highlighting 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 based on a simple A-F scale. Organizations 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 help 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, so it can evaluate over 1.6 million companies.

Diligent's Cyber Risk Scorecard continuously monitors the security of your organization 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 organizational 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, unsecure 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 in a timely manner.
- **Endpoint Security:** Endpoint security refers to the protection involved regarding an organization'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 all over the world. The incoming infected IP addresses are then processed and attributed to corporate enterprises through an 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 organization's IP reputation.
- **Hacker Chatter:** Cyber Risk Scorecard continuously collects multiple streams of underground chatter, including hard-to-access or private hacker forums. Organizations and IPs that are discussed or targeted are identified.
- **Leaked Information:** Cyber Risk Scorecard identifies sensitive information that is exposed as part of a data breach or leak, keylogger dump, pastebin dump or database dump, and via other information repositories. It then maps that information back to the companies that own the data.








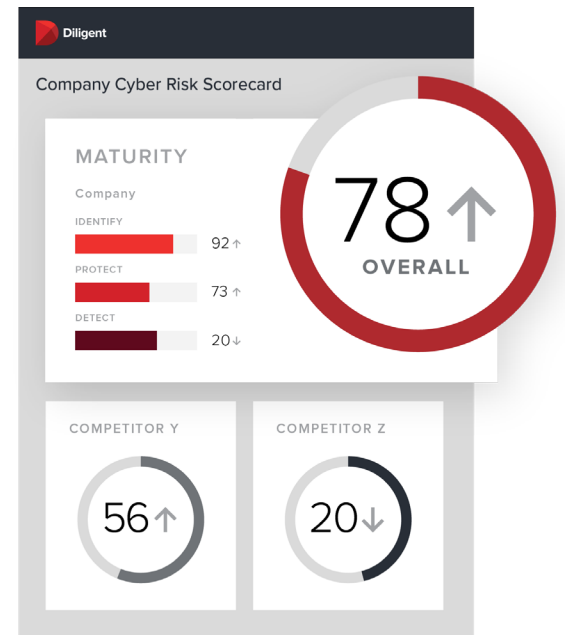
# Cyber Risk Scorecard and the Broader Governance Ecosystem

A well-managed solution to established and incoming cyberthreats is only one facet of a modern approach to corporate governance. 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 synergistically with the rest of the Diligent modern governance platform, creating a stronger, more secure and more digitally robust organization poised to thrive. With Cyber Risk Scorecard, organizations benefit from:

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



Directors, executives and governance professionals are facing 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 not only essential for continued security and digital resilience, but also for future potential and organizational 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 organizations 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 organizations across the globe



### 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: **+1-877-434-5443** • Email: **info@diligent.com** • Visit: **diligent.com**