RISK ADVISORY

BOARD RISK MANAGEMENT:

HELPING YOUR CISO TACKLE EMERGING CYBERSECURITY CHALLENGES

RSM

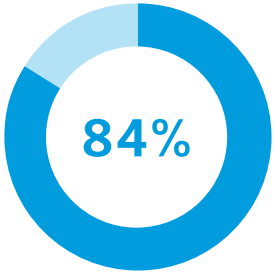
THE POWER OF BEING UNDERSTOOD
AUDIT | TAX | CONSULTING

CONTENTS

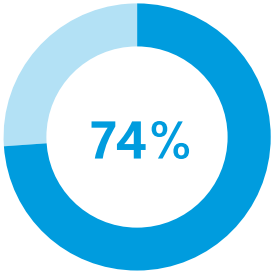
Modern businesses rely on a complex mix of technology systems for daily operations and progression toward strategic goals. These systems once resided within the walls of the organization, but today they extend far beyond and are exposed to constant threats that could directly harm the business.

Where does board risk management fit in? Board members have supported the embrace of technology to improve the customer experience, rein in costs, increase competitiveness and more, but they also need to recognize that digital transformation itself makes organizations more vulnerable to new cybersecurity risks.

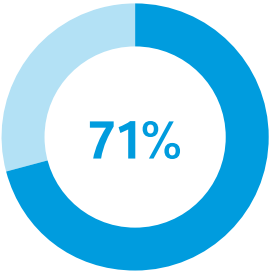
WHY BOARD MEMBERS SUPPORT DIGITAL TRANSFORMATION



Improved customer experience



Cost effectiveness



Having better data to drive growth

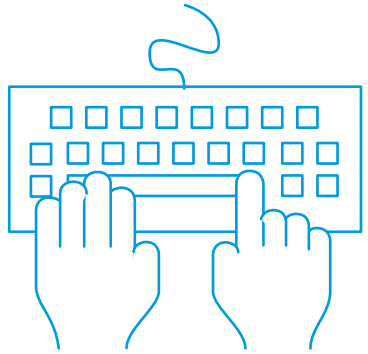
Source: Survey of board members by RSM and Corporate Board Member

CONTENTS

When cybersecurity isn't integrated into the business or effectively managed, it can derail digital transformation and put brand reputation, customer and business data, and capital at risk. Even daily operations could be brought to an abrupt halt by a cybersecurity incident.

In this environment, board members can no longer treat cybersecurity as simply a function within the enterprise. Cybersecurity is the enterprise because businesses can't create value and maintain competitiveness without stable, protected systems and data.

Proactive board members can help their CISOs reduce cyber risk by getting to know the top challenges they face.



64% of board members say they are increasing oversight of digital transformation and cybersecurity as a result of the changing business landscape.

1
2
3
4
5

CHALLENGE NO. 1:

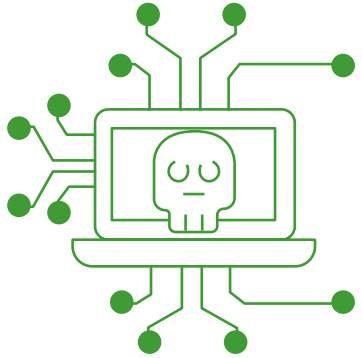
Lack of resources

Funding for cybersecurity often gets trimmed to divert funds to other priorities. Considering that growing threats such as ransomware can expose sensitive data and freeze operations entirely, cutting cybersecurity resources rarely is a good business move. Cybersecurity is an ongoing, perennial need — part of operations, not capital expenditures.

In addition to funding, there's a shortage of qualified cybersecurity professionals, who are in a position to be picky about their employer and command top dollar. Trying to keep these skills on staff can drain time and energy away from more strategic CISO initiatives.

It's critical to help your CISO find skills solutions so that they have qualified personnel and can minimize their efforts in managing continuity. Many CISOs are recognizing the benefits of strong partnerships with trusted managed services providers to help tackle the talent issue.

Finally, CISOs rarely have a seat at the table for big strategic decisions because cybersecurity is seen as a background function that's always there and can be applied "after." This is an outdated, inefficient and potentially dangerous view. Nothing can get done without technology, so CISOs should be part of any strategic decision making to make sure systems are protected and available during any changes.



42% of executives at larger middle market organizations reported a data breach in the last year, compared with 16% at smaller counterparts.

Source: RSM MMBI Cybersecurity Report 2021

HOW TO SUPPORT YOUR CISO

- Hold C-suite leaders accountable for involving the CISO in strategic plans and big changes to raise awareness of cybersecurity concerns as early as possible.
- Ask your CISO directly for information on their resource and funding needs, as well as risks that the security team is unable to remediate themselves.
- Encourage and approve the use of vetted third-party services that can mitigate cybersecurity skills gaps.

1
2
3
4
5

CHALLENGE NO. 2:

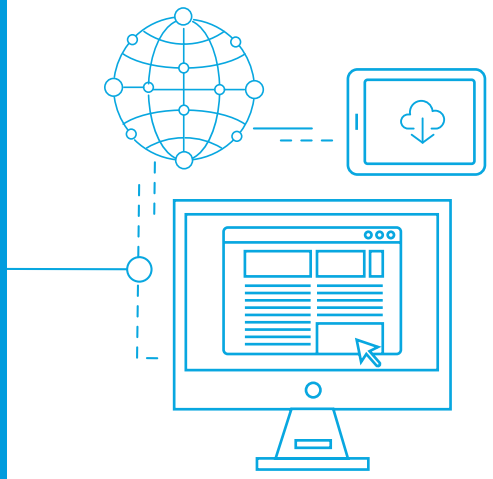
More opportunities for cybercriminals

Cybercrime is on the rise because cyberattacks have become easier to pull off, and businesses are facing increasing vulnerabilities. It's a perfect storm of factors feeding this surge — from changing workforce models to legitimate technological advances that criminals exploit.

One chilling example of growing sophistication is Ransomware-as-a-Service, in which ransomware has been turned into an outsourceable business model.

Person A can buy a ransomware service from Person B that enables them to penetrate an organization's system. While there are still some hackers motivated by activism or politics, this corporatization of cybercrime as a business has opened the door to criminals who are not necessarily technology savvy.

64% of middle market executives anticipate that unauthorized users will attempt to access data or systems in 2021.



Source: RSM U.S. Middle Market Business Index Cybersecurity Special Report 2021

CHALLENGE NO. 3:

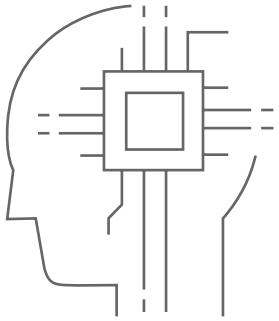
Managing the rate of change in business and technology

Business change never ceases. Businesses are introducing new technologies, and new competitors and markets arise. Workforce trends shift how people work, too. For example, the pandemic accelerated the pace of digital transformation and led to the increase of remote, hybrid and distributed workforce models. This trend has put more work on the plate of CISOs and their teams. Without the right resources, many are struggling to keep up.

Sometimes the tools may already be in place, but they aren't configured optimally so that the organization is taking full advantage of the functionality. This could be due to a skills gap or simply a matter of not enough time and resources to spend on optimization.

CISOs also must contend with a culture of indifference among front-line employees who may not recognize their role and responsibility in protecting the business. Adding to this challenge is hybrid work environments. Even employees who understand the importance of cybersecurity may let their guard down when working from home or a coffeehouse.

This could be because the enterprise itself treats cybersecurity as a siloed function rather than a fabric that touches all. The human factor — and getting buy-in from every employee — is the number one resource that enterprises have to improve cybersecurity and prevent cybercrime.



HOW TO SUPPORT YOUR CISO

- Prioritize questions about cybersecurity during periods of fast change and transition.
- Engage your CISO in blue-sky thinking. Present a hypothetical budget and ask them how they would spend it.
- Hold business leaders accountable for cybersecurity planning related to using cloud vendors and services.
- Support efforts to raise awareness about cybersecurity roles and responsibilities throughout the organization and the consequences for not complying with requirements.

CHALLENGE NO. 4:

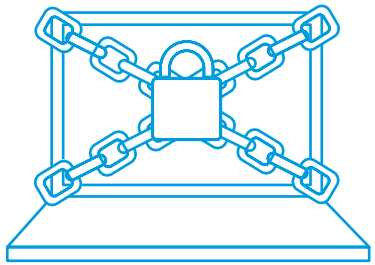
External influences

Finally, CISOs face outside forces that impact cybersecurity but can't be explicitly controlled. The shortage of qualified cybersecurity professionals is one such example. Regulations are another. They are always changing and can vary by state or country, an added stressor for businesses operating across multiple locations.

Managing this highly complex and dynamic mix of requirements can require heavy resources that could otherwise be focused on fighting cybercrime.

Other outside forces include destabilizing elements, such as activists ("hacktivists") who attack companies to make a social or political point and foreign state actors who target businesses for geopolitical purposes.

Another outside element is the board itself. When a big attack hits the news but cybersecurity isn't on your radar, you may call upon your CISO to learn what they are doing to protect the business. In reality, your CISO is likely doing all they can with the resources on hand, but they need more consistent support versus periodic prioritization.



28% of middle market executives claimed that their company experienced a breach, the highest level since RSM began tracking data in 2015 and a sharp rise from 18% the prior year.

GDPR INFLUENCE

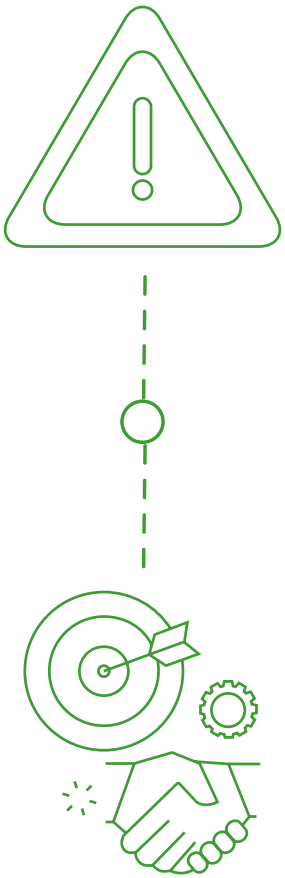
More than a dozen U.S. states have implemented data privacy laws since the General Data Protection Regulation (GDPR) was implemented in 2018.

Know your responsibilities

Cybercrime is growing faster than ever, and as a board member, it's your responsibility to understand your role in preventing it. Supporting your CISO sends the message that you've prioritized the protection of your organization's most valuable assets — its people, data and systems.

Specifically, here are your responsibilities:

- **1.** Being aware of and approving the risk appetite of your organization. Don't leave this for IT or cyber teams to determine without your oversight.
- **2.** Fully understanding the cost vs. potential risk reduction when considering budgetary requests. Ensure that the organization is spending the level of resources on the highest-risk items.
- **3.** Facilitating an organizational culture that is on board and active in cybersecurity initiatives. This work will impact not only employees, but also customers, vendors and potentially other groups.



Empower your CISO

But with such a dynamic and challenging external environment, most organizations can't cover all cybersecurity needs on their own. They need a partner who can fill in the missing pieces or provide enterprise-wide cybersecurity capabilities.

Outsourcing all or some of your cybersecurity to a third-party provider such as RSM can empower your CISO with cutting-edge technology, professional continuity and years of experience preventing cybercrime.

Contact RSM for a board-level consultation on your cyber risks.

LEARN MORE

+1 800 274 3978
rsmus.com

eb-nt-ras-all-10202119--EBK-CISO

RSM