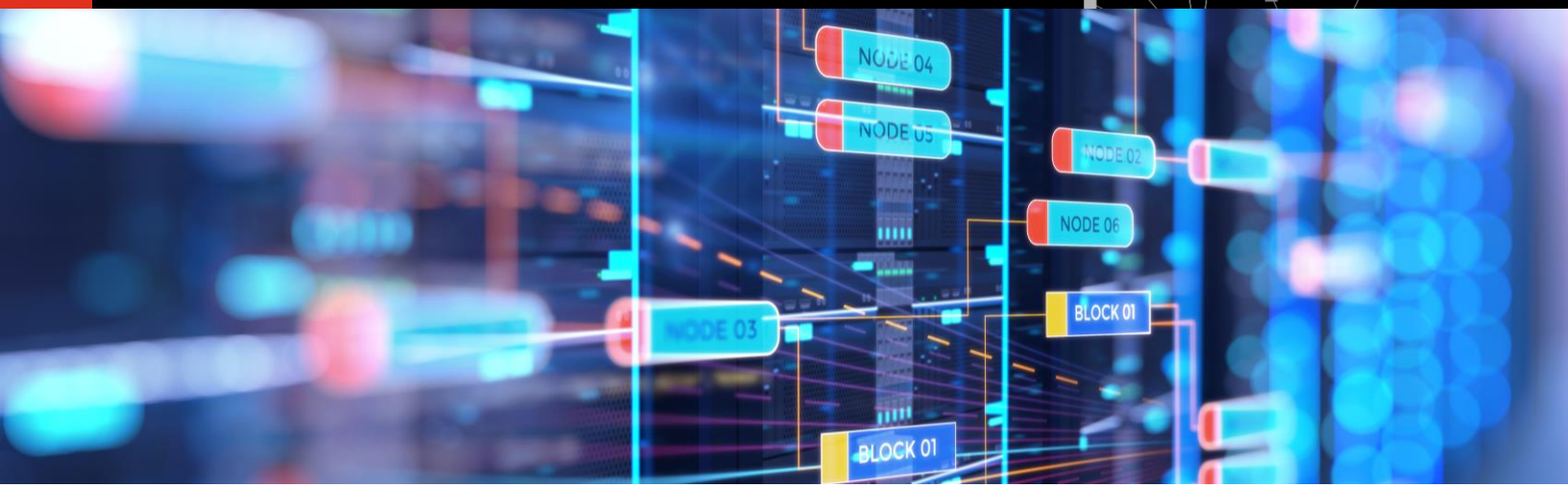
September 2020

COVID-19 – How boards can keep up with cyber risks



Business models are changing in response to the COVID-19 pandemic, and that has driven changes in cybersecurity needs. With many employees working from home and the rise in phishing, ransomware, and business email compromise schemes, companies have had to address increased security vulnerabilities. At the same time, they may be expanding their digital footprint with the adoption of new technologies further increasing cyber risks. Security functions have been—and continue to be—in fire fighting mode. Boards will want to understand their company's cyber strategy and how underlying programs have adapted to address the company's changing activities and business risks. These efforts should focus on the company's resiliency during uncertain times.

pwc

www.pwc.com/us/governanceinsightscenter

Here are the top areas where boards will want to focus.

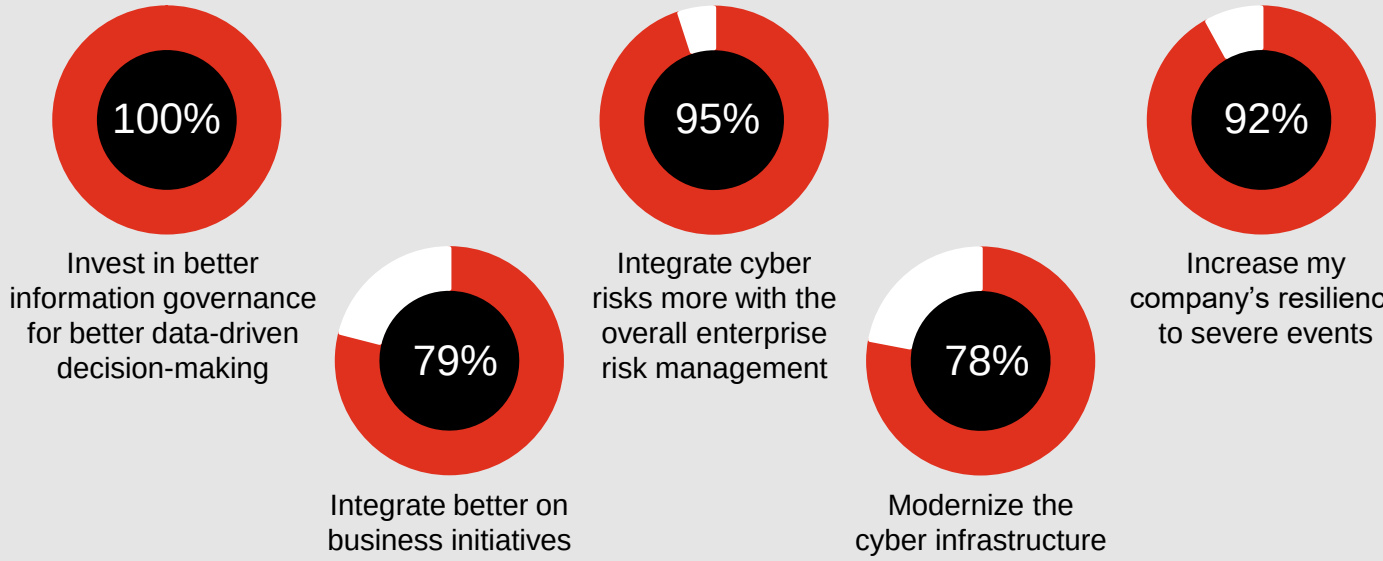
1. **Hitting the mark:** As companies' business objectives and risk profiles have changed in response to the pandemic, boards will want to ensure that management has aligned the cyber strategy with the current business and threat environment.
2. **Piecing together the puzzle:** Board reporting should be holistic and consistent to make it easier for directors to effectively understand and monitor cyber risk management.
3. **Making room at the table:** Relying on management for information is core to how board members discharge their responsibilities, but getting the views of others can provide greater insights.
4. **Building a better mousetrap:** With the frequency of crises, management's response plan should continue to evolve based on lessons learned. And boards will want to maintain their oversight in this area as it does.
5. **Opening the blinds:** As boards oversee the company's environmental, social, and governance (ESG) efforts, they will want to look for ways to be more transparent about their oversight activities related to data security and privacy.

Five areas for boards to focus

1. **Hitting the mark:** *As companies' business objectives and risk profiles have changed in response to the pandemic, boards will want to ensure that management has aligned the cyber strategy with the current business and threat environment.*

   Amid the pandemic, many companies have shifted gears and changed their business objectives by offering new or different products and services. Others have changed their operations to meet new customer demands or address shortfalls in service. Many have accelerated digital efforts to engage with customers, employees, and others in innovative ways, adding to their ever-increasing technology footprint. They are doing this against a drastic shift in cyber risks with rising malicious attacks and vulnerabilities arising from employees' remote work. In this new environment, boards should be getting insight from the CISO on how the company's cyber strategy is aligned with current business objectives. They should understand what new risks have emerged and mitigating actions taken, as well as how the overall cyber risk profile has changed. If the company is using new technologies, is the CISO engaged and managing potential new risks? In this way, they can be comfortable that the company's cyber program is keeping pace with the latest business and threat environment.

CISOs speak out on changes to cyber strategy based on pandemic learnings



Q: Based on what you have learned and experienced during the crisis, which of the following changes to your cybersecurity strategy, if any, are you planning to make? (Please rank up to three. Indexed score.)
Base: 141
Source: PwC, *Digital Trust Insights Pulse Survey*, June 2020.

2. Piecing together the puzzle: *Board reporting should be holistic and consistent to make it easier for directors to effectively understand and monitor cyber risk management.*

For many boards, directors hear from the CISO on a quarterly or semi-annual basis. But too often these discussions don't cover all the key topics or address them in a consistent format, making it hard for a board to really understand the cyber risk program. Key topics boards will want covered can include an understanding of the company's cyber strategy, gaps in maturity against a known security framework, recent security events, status of regulatory compliance projects, third-party risk management, cyber insurance coverage, and cyber budget and resources. Dashboard reporting can be helpful to crisply convey the status of risk mitigation efforts. Importantly, the reporting needs consistency so that the board can understand how key risks are being addressed or have changed. An emerging practice for some boards is to hold private sessions with the CISO to have a candid and confidential conversation about these key topics and better understand sensitivities around key risks, talent, and allocation of resources.



50% increase in the frequency of interaction between the board and CISO since the pandemic

Source: PwC, *Digital Trust Insights Pulse Survey*, June 2020.

3. **Making room at the table:** *Relying on management for information is core to how board members discharge their responsibilities, but getting the views of others can provide greater insights.*

   While boards rely heavily on company management for information and perspectives, getting insights from others is critical. Third parties can provide additional insights about the company's cybersecurity program. Management may hire third parties to perform cyber readiness assessments, penetration testing, or other activities. Boards or committees should consider periodically requesting presentations from these individuals to understand their findings and get answers to any questions directors may have. Boards may also get perspectives from government, industry organizations, and other sources about the current threat environment, common threat schemes experienced at other companies, and even benchmarking data.

4. **Building a better mousetrap:** *With the frequency of crises, management's response plan should continue to evolve based on lessons learned. And boards will want to maintain their oversight in this area as it does.*

   Companies are increasingly faced with the reality that security incidents and successful cyber breaches will happen. As boards will want to be involved in any response to a major incident, they will want to make sure that the crisis response plan is updated and enhanced and ready to be deployed when a major event occurs. An event might be a cyber breach or another type of crisis like COVID-19 or a natural disaster. When a crisis does occur, another area for boards to push management on is whether crisis response plans are updated for lessons learned from these events. The goal of taking time to reflect and discuss crisis activities should be for the company to be better prepared for when the next one occurs, which could be a successful cyber breach.

5. **Opening the blinds:** *As boards oversee the company's ESG efforts, they will want to look for ways to be more transparent about their oversight activities related to data security and privacy.*

   As ESG has become a hot button issue for institutional investors and other stakeholders, consider expanding the disclosures related to the board's role in overseeing cyber and privacy risks, which can be considered material "social" and "governance" risks for many companies and boards. Benchmark your proxy disclosure against peers to see if there are any learnings, and even look at disclosures of companies that have weathered a breach to provide additional insights and actions that may be valuable for your board or company to consider.

In today's environment, boards should expect their CISO to step up and bring innovative solutions to improve data security and resiliency while also keeping a close eye on security costs and budgets.

Stepping up oversight amid a changing landscape

The pandemic has elevated cyber risk levels at companies. But these risks can be managed by ensuring the cyber strategy is aligned to the business objectives, prioritizing and addressing the latest significant risks, and continuing to improve the incident response plan to build cyber resilience. Boards have an important role to play in overseeing whether these management-level activities are happening, and they should be taking steps now to make sure the company's cyber program continues to keep pace with the current business and threat environment.

Contact us for more information

Paula Loop
Governance Insights Center Leader
paula.loop@pwc.com

Sean Joyce
Global and US Cybersecurity, Privacy & Forensics Leader
sean.joyce@pwc.com

Barbara Berlin
Managing Director, Governance Insights Center
barbara.berlin@pwc.com

Joe Nocera
Cyber & Privacy Innovation Institute Leader
joseph.nocera@pwc.com

© 2020 PwC. All rights reserved. PwC refers to the US member firm or one of its subsidiaries or affiliates, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.