DIGITAL TRANSFORMATION, ENTERPRISE CYBERSECURITY, SAFER BUSINESS

Corporate boards need more members who ‘get’ cybersecurity

ART BY You X Ventures

Company boards need to know enough about cybersecurity to govern effectively, but four in 10 boards admit they should know more.

4 minute read

AUTHOR
Sherry Jones

SHARE ARTICLE

Meanwhile, data breaches keep going up. The past year saw a record number of cyberattacks. There were more than five thousand cybersecurity incidents reported worldwide in the first nine months, a one-third increase on the same period in 2018. The number of records exposed more than doubled, to near eight billion.

Cost is rising, too. Kaspersky's 2019 survey found the average price tag of an enterprise cybersecurity incident is now 1.41 million US dollars. It increases each year.

Lawmakers and regulators are noticing the rising risk. So are investors and shareholders – in 2019, former directors and officers at Yahoo! settled with shareholders for 29 million US dollars. The shareholders had sued them for failing in their duties after a breach of *three billion* customer accounts.

Boards have come a long way from the days when cybersecurity was just the IT department's concern. But if, as the NACD survey suggests, 60 percent of boards know enough to govern their company's cybersecurity, 40 percent don't. That's a lot of boards who admit to not knowing their endpoint from their elbow.

Cyber knowledge should be the rule, not the exception

As cyberattacks and data breaches become more frequent and cause more damage, the need for effective cybersecurity governance becomes more business-critical.

> Information security expertise is no longer a nice-to-have. All boards and business leaders need it – from startup advisers to corporate directors.

Take, for example, the popular risk management model "three lines of defense," from the Institute of Internal Auditors (IIA). It outlines who's in charge of keeping entities digitally secure. For 20 years, the three lines were operational managers, risk and compliance management and internal audit. A 2020 update to "three lines of defense" will specify a role for the board: "Governance, organizational success and value creation."

The same thing's happening at the Federal Financial Institutions Examination Council (FFIEC). Last November, its updated Business Continuity Management guide, assigned the board and senior management ultimate responsibility for minimizing disruption to critical business functions. Malicious threat actors often cause these disruptions.

The same organization's Information Security guide says the board should "reasonably understand" the business case for information security and the implications of security risks, and guide management accordingly.

But are these expectations realistic?

To most outside the field, cybersecurity is a mystery. How will board members learn enough to ask the right questions and give the Chief Information Security Officer (CISO) direction?

Companies with digitally savvy boards do better

Knowing boards need help in their role as security watchdog, organizations like the World Economic Forum (WEF) and the NACD have advice.

The NACD has also issued a list of five core principles for boards' cybersecurity risk oversight. Number one: A thorough understanding of cybersecurity and risk mitigation.

But it seems boards need help making sense of cyber.

Only 24 percent of US boards of companies with more than a billion US dollars in annual revenue are "digitally savvy," according to a 2019 Massachusetts Institute of Technology (MIT) report. The report also says the companies with the digitally savvy boards had 38 percent higher revenue growth and 34 percent higher return on assets.

The bar is high. To qualify a board as digitally savvy, the study authors recommend not one, but three technology-minded directors or advisors.

It's easy to misunderstand or fail to listen to one tech-savvy director. For real change, there must be a critical mass.

The remaining 76 percent of boards in the study lacked expertise in even common digital technology. For them, getting up to speed on cybersecurity will be hard. But it's possible, if they're willing to ask for help.

Start recruiting cybersecurity and tech experts to boards

"Every board, no matter the industry, status or size, should include at least one cybersecurity expert among its membership," says William Killgallon, Executive Head of Security Risk and Crisis Management at GE Digital.

cybersecurity expert on their board.

Killgallon is on several boards. He says his expertise made the difference in one startup’s fundraising: “Venture capitalists asked pointed questions about security and privacy, especially data protection,” he says. Company leaders had done their homework and recruited Killgallon to the board. They got the funding.

“The money wouldn’t have come without investor confidence that the leadership teams had, at the very least, done due diligence on cybersecurity and risk. Cyber-proficient board members who are also excellent communicators can teach the rest what they need to know,” Killgallon points out.

Today, cybersecurity expertise has become as essential to boards as understanding business requirements. Kaspersky CISO Andrey Evdokimov says having both is a win-win: knowing how the business functions *and* how IT and security work in the context of business.

“Too often, management hasn’t identified the organization’s critical business functions – those that must remain up and running for the business to work. The organization’s own CISO or cybersecurity managed service provider may not be able to put a dollar figure to the cost of a debilitating cyberattack.

“Many enterprises don’t have a resilience plan. These should set recovery time goals for key functions and map network interdependencies, making sure critical systems can be restored fast, in the right order. To govern effectively, boards must hold its cybersecurity management accountable for the answers to these questions”, Evdokimov says.

> Infosecurity management is not for dummies. It’s for upper intermediates in business process management.
>
> — **Andrey Evdokimov**
>
> Chief Information Security Officer, Kaspersky

How boards can go from cyber-questioning to cyber-smart

New regulation will keep driving boards' shift from cyber-questioning to cyber-smart.

Nowadays, 58 percent of countries have data protection and privacy laws. The European Union's General Data Protection Regulation (GDPR) required strict data privacy practices in EU nations and those doing business with EU residents. The US state of California's Consumer Privacy Act (CCPA) followed suit in 2020. All include boards in the chain of accountability.

And in the US, the Cybersecurity Disclosure Act of 2019 awaits debate in the Senate. If enacted, it would require every publicly traded company to disclose whether any board member has expertise in cybersecurity. If the board includes no such experts, the company must explain why.

Why, indeed? In a time when everything and everyone is becoming digitally connected, boards must too.

Bringing a cyber-expert (or three) to the table – or having closer connections to experienced InfoSec professionals and the board – may do much to protect your organization's systems and your customers' data.

When it comes to cybersecurity, a little knowledge goes a long way.

This article reflects the opinion of the author.

Share article

Keywords:

SUGGESTED ARTICLES

security bytes data breaches

DATA BREACHES

Advice from the pros: How to deal with a data breach

Knowledge is power! Courageous infosec pros share their experiences of dealing with a data breach.

janitor cleaning an office

TALENT

If we do our job, nothing happens

You wouldn’t fire your cleaners if your office was spotless. The same’s true of cybersecurity: we must get better at managing the virtual dirt on our networks.

rocket economics report

FINANCE AND BUDGETS

The real cost of data breaches in 2019 (and how to avoid them)

Data breaches can devastate your business. Read Kaspersky’s 2019 IT Security Economics report to find out how to defend against them.

AUTHOR INFO

Sherry Jones

ghostwriting.

in

MORE ARTICLES BY SHERRY JONES →

About Secure Futures

Secure Futures magazine is your go-to business guide for opinions, trends and insight into the world of technology and cybersecurity. We help your business to bring on the future. Brought to you by Kaspersky, the global cybersecurity experts.

Got an idea for a story you'd like us to cover? Contact the Editor.

What's coming next?

Be first to find out what's happening in tech, leadership and cybersecurity.

STAY AHEAD

Kaspersky Anti-Virus

Kaspersky Internet Security

Kaspersky Total Security

Kaspersky Security Cloud

Kaspersky Security Cloud – Free

All Products

Small Business Products

1-50 EMPLOYEES

Kaspersky Small Office Security

Kaspersky Endpoint Security Cloud

All Products

Medium Business Products

51-999 EMPLOYEES

Kaspersky Endpoint Security Cloud

Kaspersky Endpoint Security for Business Select

Kaspersky Endpoint Security for Business Advanced

All Products

Enterprise Solutions

1000 EMPLOYEES

Cybersecurity Services

Threat Management and Defense

Endpoint Security

Hybrid Cloud Security

• Privacy Policy • Anti-Corruption Policy • License Agreement

Contact Us • About Us • Partners • Blog • Resource Center • Press Releases • Trust Kaspersky

Securelist • Threatpost • Eugene Personal Blog

Global