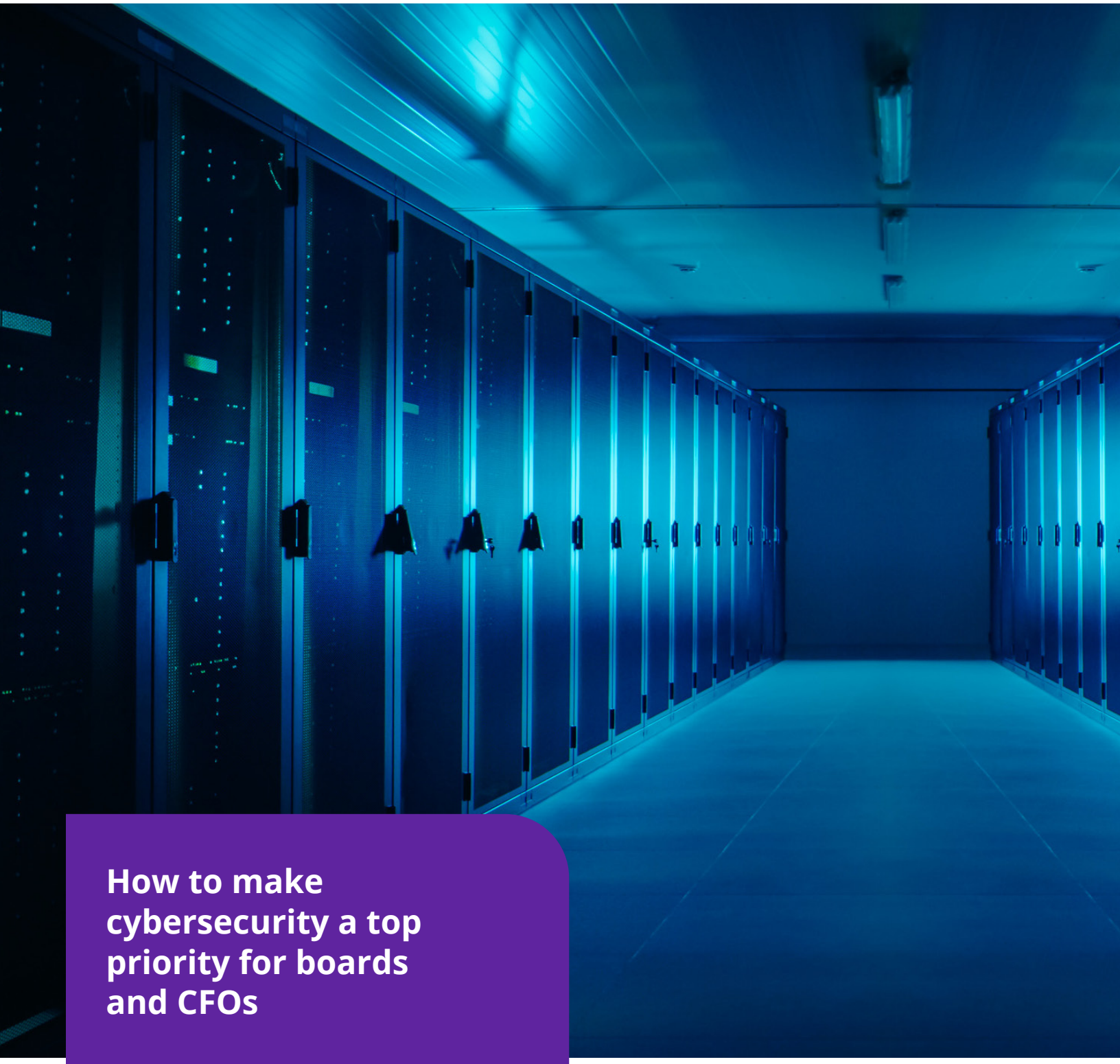
DXC TECHNOLOGY



How to make cybersecurity a top priority for boards and CFOs

By Mark Hughes,
President, Security
DXC Technology

How to make cybersecurity a top priority for boards and CFOs

As an executive responsible for delivering security solutions to our global customers, I see cybersecurity moving higher on the agendas of boards of directors. At a time when most budgets are shrinking, worldwide security spending is expected to grow 8.1% annually and hit $174.7 billion by 2024, according to IDC.

There's a good reason for this. Major data breaches and crippling ransomware attacks can rise to the level of natural disasters — often bringing business to a standstill and damaging the brand, customer loyalty, partner relationships, and more. It's startling to me, but the projected cost of cybercrime — an estimated $6 trillion in 2021 — represents "the greatest transfer of economic wealth in history," according to Cybersecurity Ventures.

To be truly effective, boards and CFOs need to fully understand the risks and view cybersecurity as foundational to almost everything an organization does — starting at the top.

If boards and CFOs learned anything in 2020, it was to expect the unexpected. But to be truly effective, they need to fully understand the risks and view cybersecurity as foundational to almost everything an organization does — starting at the top.

Not just an IT problem

It's important to note that security isn't just about patching and protecting IT systems anymore. We know it's far more embedded into the operational landscape.

Last June, when ransomware locked up the internal networks of one global manufacturer, the company was forced to temporarily shut down production facilities, customer service, and financial services operations.

The other trend I see is the widening range of risks facing large enterprises. A variety of sociotechnical factors such as regulatory environments, social and political change, and culture are affecting the threat landscape.

Policies communicated poorly by management can trigger insider threats and the release of sensitive data. Introducing a new board policy, M&A activity, or an association with a supplier can inadvertently prompt a hacktivist group to deface a corporate website, hijack social media accounts, or shut down services through a distributed denial-of-service attack. Lax data privacy programs may lead to huge penalties in some regions, but just a slap on the wrist in others.

While most boards understand the impact of security on the brand and customer trust — and CFOs have become all too familiar with the costs — chief information security officers (CISOs) still face the daunting task of communicating the constantly changing risk landscape.

Elevating security on the agenda

Our team focuses on helping these leaders understand risks in their terms. Several best practices can help your organization make security a top priority.

Talk about risk and ROI, not threats and vulnerabilities. Security monitoring tools and threat intelligence can paint a good picture of the rise in cyber attacks, but they can't answer the basic question "How safe are we?"

The board needs data to understand cost, reliability, and risk, but CISOs also need to provide a holistic view of risk exposure.

Managing security programs and fending off attackers will always be a tradeoff between cost and risk, but with so much at stake, security decisions need to be made in an informed, strategic, and collaborative way.

A cyber-aware culture starts at the top. With the increase in more sophisticated spearphishing attacks, the leadership team is more vulnerable than ever. CFOs think in terms of weighing risk mitigation costs with potential exposure, so CISOs need to clearly communicate ROI: What's the potential impact on the stock price and shareholder value? What's the potential cost of a vulnerability versus the cost to fix it?

Trying to secure against all possible threats could be cost-prohibitive and could even hamper business innovation and growth. Decisions need to be made in collaboration, striking the right balance between risk priorities and effective security controls.

Find a security champion. In recent years, senior leaders have focused on ways to diversify their boards. In addition to a range of backgrounds and perspectives, boards can also benefit from relevant skills such as investment management, information technology, human resources, and risk management.

A case can also be made for putting a cyber-risk champion on the board, particularly in highly targeted industries such as banking, retail, health care, and utilities. Having a security champion on the board will help keep security front and center. A board member with a security background or prior experience in dealing with major breaches can help less tech-savvy members make sense of rapidly changing risks.

Don't rely on cyber insurance alone. Cyber insurance is a relatively new tool for mitigating risk that generally covers liabilities related to data breaches, including damages, legal fees, notifications to customers, recovering data, and repairing computer systems. However, these policies may not cover the loss of value due to theft of intellectual property or the cost of upgrading software and equipment to prevent attacks.

CFOs and chief risk officers should carefully assess the benefits of cyber insurance versus self-insurance options. In 2018, the city of Atlanta spent $2.7 million to recover from a cyber attack rather than pay the $50,000 ransom demand. Most of the money went to upgrading outdated systems. Cyber insurance makes it easier for the CFO to decide not to pay the ransom, but it can't mitigate reputational damage. Prevention, rapid response, and operational resilience are still the best defenses.

Put agile management processes in place. New vulnerabilities are constantly surfacing, and attackers are continually changing tactics, so security programs need agile management processes to respond.

Organizations need to manage security according to best practices and with resiliency plans in place, in the same way that core systems need disaster recovery plans and backups. Just as companies aim for continuous improvement in operations, customer service, and other key disciplines, the board and CFO should expect the same for security.

Managing security programs and fending off attackers will always be a tradeoff between cost and risk, but with so much at stake, security decisions need to be made in an informed, strategic, and collaborative way. Boards and CFOs are an integral part of that conversation.

DXC sponsor content as seen on Harvard Business Review's website, HBR.org

About the author

Mark Hughes is president of Security at DXC Technology, responsible for DXC's Security business including cyber defense, digital identity, secured infrastructure and security risk management. He previously served as chief executive at BT Security.

Learn more at
dxc.com/threats