Help us choose our Top 10 Topics for 2018
www.deloitte.com/lu/InsideRisk2018f

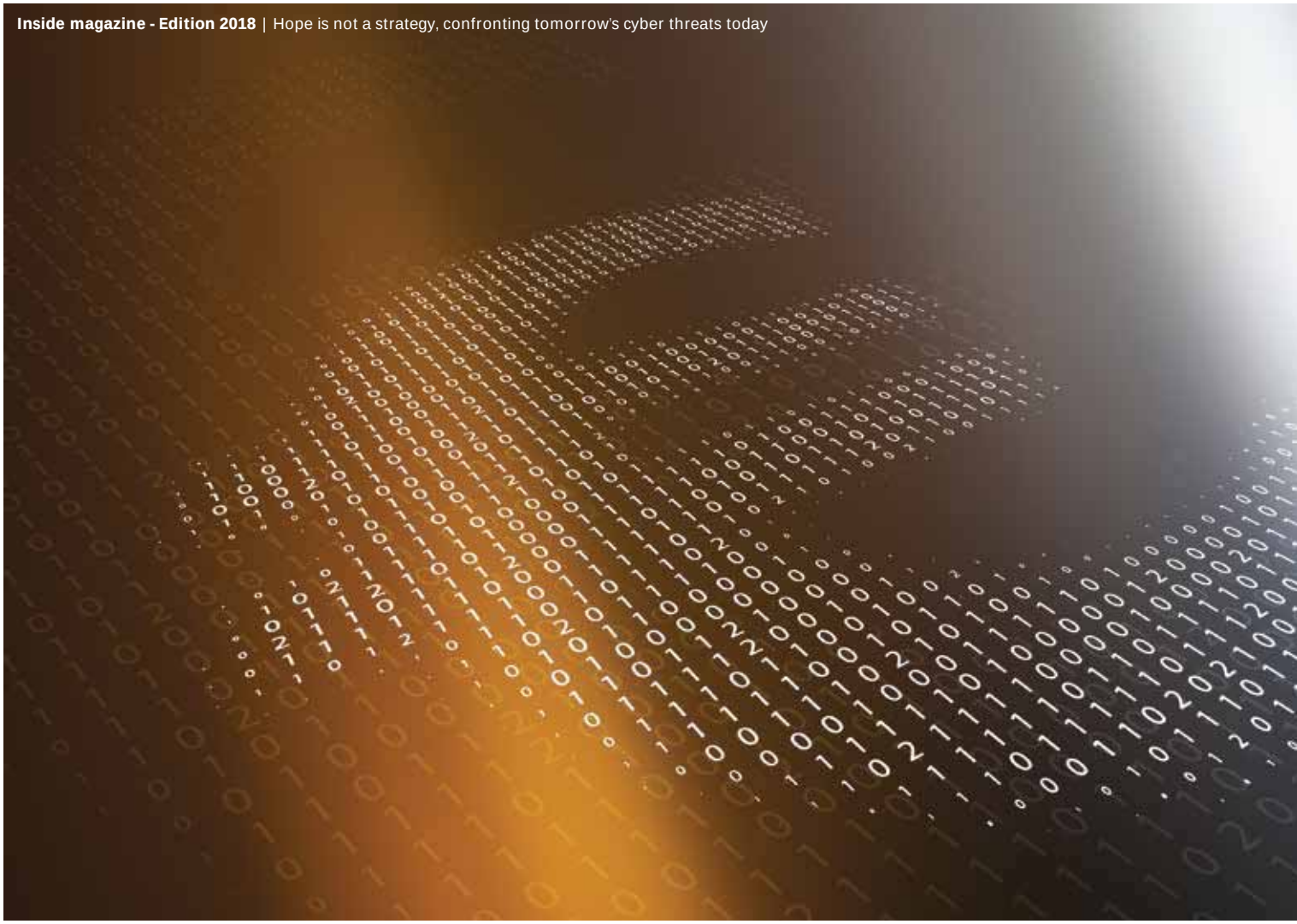
Printed with permission of Deloitte Canada

HOPE is not a strategy

Confronting tomorrow's cyber threats TODAY

Nick Galletto
Partner
Research Leader
Global and Canadian
Cyber Risk Leader
Deloitte Canada

Digital disruption and exponential technologies are creating unprecedented business opportunities, but they also bring risks. Having a strong cyber risk management plan in place can give your organization a competitive advantage and enable it to use cyber risk to power performance.



In the World Economic Forum's The Global Risks Report 2017, cyber risk is recognized as one of the most significant sources of commercial risk, alongside the economy, the environment, and geopolitics.[1] The risks from cyber continue to skyrocket; according to a recent report, by the year 2020 the world will need to cyber-defend 50 times more data than it does today.[2] With new risks emerging daily, organizations must constantly devise new cyber strategies and defenses, and become more resilient as attackers figure out how to get past the cybersecurity that is currently in place.

The good news is that while digital disruption and cybersecurity present serious challenges, those challenges are not insurmountable. To protect themselves from both evolving and emerging cyber threats, organizations need to ensure they have established basic cyber capabilities that can repel today's threats, while at the same time investing in future-proof capabilities that can protect them and enable them to effectively respond to any threats that might emerge in the future.

Digital innovation: a double-edged sword

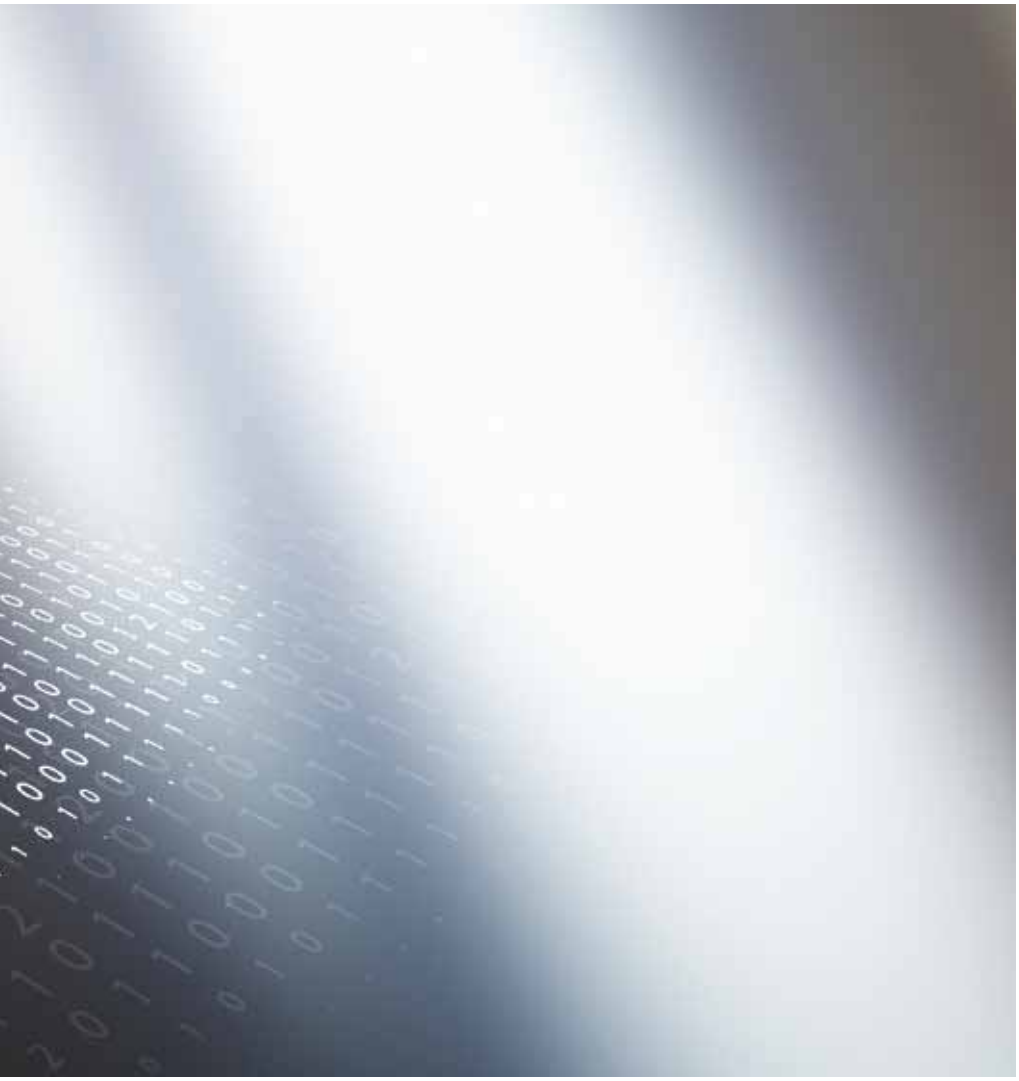
In this new digital world, one of biggest threats facing organizations today, and for the future, is cyber risk. "We always refer to it as the duality of technology," says Nick Galletto, a partner at Deloitte and the Global and Canadian Cyber Risk practice leader. "The same technology that is used to create for good can, in the wrong hands, be used to mount cyber-attacks."

More than an IT issue

Cybersecurity is no longer just an IT issue; it is a business issue and strategic imperative for organizations of all industries and sizes. Innovators in every sector must take the lead by constantly striving to strike a balance between protecting the organization from cyber threats and laying the groundwork for future success by capitalizing on digital technology. That is why taking the lead on cyber capabilities means doing more than addressing the threats that exist now.

1. World Economic Forum, "The Global Risks Report 2017", 12th Edition, http://www3.weforum.org/docs/GRR17_Report_web.pdf Accessed 9 May 2017.

2. Cybersecurity Ventures, "Cybersecurity Market Report," 2016 edition http://cybersecurityventures.com/cybersecurity-market-report/ Accessed 9 May 2017.



The good news is that while digital disruption and cybersecurity present serious challenges, those challenges are not insurmountable.

Prepare for tomorrow's threats today

As new technologies drive digital disruption, they introduce entirely new kinds of cyber threats and amplify existing ones—requiring additional next-level capabilities that companies must start building now.

Even threats an organization thinks it has under control today could threaten it again in the future as those threats evolve and grow in sophistication and complexity. For example, distributed denial of service attacks have been around for many years, yet they are now more prevalent, deceptive, and sophisticated than ever—often being used as a ploy to divert attention from secondary attacks such as data exfiltration, physical attacks, or the implanting of ransomware.

"Organizations are realizing that no one is immune to a cyber-attack, and in response to the increase in large and well-publicized attacks across a number of sectors, there is a greater sense of organizations now starting to better appreciate what the risks are and putting the appropriate measures in place to be better prepared," says Galletto. "We're definitely trending in the right direction."

Suppliers, vendors, partners, and even customers can all be points of entry for an attack—which means that even if an organization itself is highly secure, it could still be vulnerable.

Protect your crown jewels

Although a comprehensive cyber strategy that provides full protection for everything within an organization might sound appealing in theory, in practice it is simply not feasible. Cyber threats are infinite, but cybersecurity budgets and resources are finite. That is why it is essential to set priorities, with your "crown jewels" at the top. These include:

- People: key individuals that might be targeted
- Assets: systems and other assets that are crucial to your business and operations
- Processes: critical business processes that could be disrupted or exploited
- Information: data, information, or intelligence that could be used for fraudulent, illegal, or competitive purposes

Organizations that do not explicitly design their strategies around these crown jewels often end up allocating their resources haphazardly, investing too much in areas that are not very important while investing less in what matters most, leaving those areas dangerously vulnerable.

Mind your ecosystem

Suppliers, vendors, partners, and even customers can all be points of entry for an attack—which means that even if an organization itself is highly secure, it could still be vulnerable. After all, a chain is only as strong as its weakest link. To stay aware, conduct ongoing cybersecurity assessments of your ecosystem to ensure outsiders are not creating unacceptable risk exposure. Also, be part of the solution, sharing information with ecosystem partners and fostering collaboration to fight common adversaries.

Pay attention to the enemy within

Although external attacks get most of the headlines, the fact is many of the biggest cyberthreats are internal—originating from within an organization, or within its extended corporate network. These internal incidents can be even more damaging than attacks from outside. In many cases, the damage is done without malicious intent, and is simply the result of carelessness or poor controls and procedures.

Prepare a resiliency plan

The middle of a crisis is no time to be figuring things out from scratch. To be resilient, you need a plan. You also need to establish effective governance and oversight to coordinate plans and response activities across all stakeholders—including board members and business leaders outside of IT. For most organizations, this comprehensive approach will require a mindset shift from thinking of cyber breaches as an IT risk to understanding that cybersecurity is a strategic business issue and should be addressed as an integral part of the organization's disaster recovery planning.

An effective resiliency plan needs to be developed well in advance, and should be clear and concise enough that people can quickly understand it when the bullets are flying, yet detailed enough to be immediately actionable. The preparation process is continuous—develop threat scenarios, test, evolve, repeat—with the goal of having a response plan that constantly matures and improves to keep pace with emerging threats and changes to the organization's threat landscape.

Cyber threats are infinite, but cybersecurity budgets and resources are finite.

Leverage best practices and cutting-edge insight

The most effective way for an organization to maintain the necessary levels of security is through partnering with external experts in cyber risk management to take the lead on cyber risk. "The threat landscape continues to change," says Galletto. "But the good news is that there are a lot of services out there that can help organizations maintain cyber hygiene basics, while also effectively managing their cyber risk profile."

Leveraging teams of global cyber risk advisers, these experts help organizations build effective cyber risk strategies based on a thorough understanding of their business and industry. The result is a secure, vigilant, and resilient strategy that enables organizations to grow, share, and trust without compromising on compliance.

It can also be useful to establish or join a cyber-threat intelligence (CTI) sharing community. These communities aim to help organizations improve their vigilance posture in a variety of ways, including: enabling cross-sector sharing with similar organizations; leveraging cybersecurity expertise; facilitating open group discussions; improving compliance with regulatory requirements; developing a funding framework; and initiating government relationships. Think of CTI communities as fighting fire with fire. After all, cyber attackers leverage online communities to strengthen their attacks; why not do the same to strengthen your defenses?

In the months and years ahead, digital innovations and exponential technologies will be key drivers of growth and success, providing tremendous opportunities for businesses around the world to create value and gain a competitive advantage.

To thrive in this increasingly digital world, businesses need a robust cyber strategy that can help them become secure, vigilant, and resilient. Hope is not a strategy.

- Recognize that cyber risk is a strategic business issue, not just an IT issue
- Anticipate tomorrow's threats; don't be satisfied solving yesterday's problems
- Identify and protect your crown jewels
- Don't forget about risks from within your own organization and extended enterprise
- Accept the fact that breaches are inevitable and prepare your business to bounce back quickly
- Share insights and leverage expertise beyond your own organization

Cyber risk is growing exponentially, and no company is immune. However, armed with the right strategy and tools, this is a risk you can master.