ECONOMIST IMPACT

Managing cyber risk for a secure future

Sponsored by BT

Executive summary

"Managing Cyber Risk for a Secure Future" was a keynote session at Economist Impact's Innovation@Work Virtual Week USA, featuring Kevin Brown, managing director of BT Security, who spoke about the changing cyber-security landscape and how companies are mitigating cyber-threats to further enable their digital transformation journeys.

Scene-setting: The cyber-security landscape after the pandemic

The quantity and complexity of cyber-security challenges are evolving rapidly across sectors and regions, owing to the growing sophistication of cyber-criminals and the increased digitalisation of firms' operations, which have caused connected systems and infrastructure to proliferate. The growing threat of cyber-attacks has made a new mentality commonplace, where firms now assume that they will be, and likely already have been, targeted by cyber-criminals. By extension, executives must also assume that some of these attempted attacks will have been successful, sometimes without their knowledge.

Firms must now face the fact that there is no such thing as 100% security. In the modern business world, it is inevitable that there will be cyber-security breaches. The key now is for organisations to understand their risk appetite and tailor their response to cyber-threats accordingly.

The covid-19 pandemic has also transformed the security landscape, accelerating a number of cyber-security trends that were already well underway. For instance, the adoption of remote working at breakneck speed dramatically enlarged the threat surface of organisations. Traditional security models involving perimeters around self-managed corporate networks simply ceased to be workable as cloud adoption massively accelerated. Additionally, changes to how and where people access data, and where that data is stored, have all greatly increased the complexity of security considerations.

"We find ourselves as a very large target when it comes to cyber-attacks. We typically see around 6,500 cyber-attacks per day, which come from a mix of nation states, cyber-criminals, hacktivists or good old-fashioned rogue individuals."

Kevin Brown
managing director, **BT Security**

Top of the agenda: Focusing on cyber-security

In combination, increasing cyber-threats and the changes to working conditions during the pandemic have resulted in sharply increased awareness of cyber-security across the business world. Growing media coverage of cyber-security issues—particularly of a handful of high-profile incidents that have served as cautionary tales for executives with an eye on reputation management—has added to this awareness. Attacks affecting hospital operations and health-care systems became news headlines, as did the Colonial Pipeline ransomware attack of 2021 and the SolarWinds cyber-attack of 2020.

For many in the cyber-security industry, the SolarWinds hack in particular shows how the digital landscape has changed. The incident has become infamous not only for how much access the attackers gained to a huge number of organisations, but also for its going undetected for much longer than many thought was possible. The breadth and severity of the hack continues to have unfolding repercussions, which has contributed to executives' shift in mindset to incorporate the assumption that their organisation has already been compromised by one or more hostile actors.

The way forward: Navigating a changed world

Given the rapid development of cyber risks and the subsequent renewal of interest in cyber-security, many organisations are now asking themselves: what more can we do?

Even those that have invested enormous amounts of time and resources into their cyber-security efforts need to reassess how secure they are, especially given the rise of remote and hybrid work. Part of the challenge is often how to develop cyber-security tools and processes that are fit for a dynamic, constantly evolving landscape of technologies, work practices and threats.

One difficulty for organisations seeking to keep up with cyber-threats is that while they are dynamic, and while cyber-criminals often adapt and change their approaches to evade discovery, cyber-security benchmarking remains a fairly static field. Benchmarking technologies often only capture a moment in time rather than providing a holistic and current view of security threats. When those threats are constantly evolving, organisations need tools that can evaluate their protections dynamically so they do not have to rely on assessments made six months or even a year ago.

At BT, the key to gauging threats has been to invest in Safe Security, a company whose technology allows businesses to make real-time assessments of their cyber-security risks. The technology also incorporates baseline scenarios for different industries, countries and regions to better allow companies to objectively assess their own cyber-security risks in comparison to those of others.

The platform also lets companies calculate the financial cost of cyber-incidents. This functionality has come in response to the growing interest in cyber-security from executive teams and company boards, who are increasingly aware of their duties to be in control of such an important risk factor for their organisations. Allowing companies to quantify cyber risks makes it easier to identify which business strategies can be adopted, and which investments made, to counter them.

"When the threats are constantly changing, how can an organisation really trust that their security protections really are the right protections?"

Kevin Brown
managing director, **BT Security**

Creating an enabling environment for security

While the new cyber-security environment is creating new challenges for companies in multiple sectors, security has gone from being seen as a "blocker", restricting certain business ambitions or quashing new ideas that look too risky, to being seen as an enabler of business plans.

This development partly stems from an increased understanding of cyber-security, and partly from organisations now knowing that they ignore cyber-security at their peril. From start-ups and small and medium-sized enterprises practising basic online and data hygiene to multinational corporations grappling daily with an increased threat level, organisations are no longer looking at cyber-security purely from a technical perspective. Rather, they are embedding it throughout their operations, involving people and processes as well as technology.

When whole organisations successfully embed cyber-awareness, cyber-security becomes an enabler that lets them make better use of new technologies and seize new opportunities. Firms gain competitive advantage by being able to quantify and mitigate the risks from cyber-attacks so that no risk is unanticipated. Organisations that adopt and implement effective cyber-security controls are also better able to reduce the reputational risk that comes with becoming the next high-profile cyber-victim.

Fully embedding cyber-security also makes it easier for businesses to adapt quickly to the changing technology landscape, where artificial intelligence, quantum computing and the internet of things will create new opportunities to thrive. While cyber-criminals will also be able to adapt to these advanced technologies, companies that maintain a proactive approach will be better placed to respond to nimble attackers.

Economist Impact
Economist Impact is a part of The Economist Group, publisher of *The Economist* newspaper. Sharing *The Economist*'s commitment to informed, impartial and independent debate, we are recognised the world over as a leading provider of highly interactive meetings—including industry conferences, private gatherings and government roundtables—for senior executives seeking new insights into important strategic issues.

20 Cabot Square, London, E14 4QW, United Kingdom
events.economist.com