IBM Security

Rethinking data security in the time of covid-19

Foreword

Security is critical to business growth in a hybrid multicloud environment

The security landscape has evolved significantly over the past decade, more-so with the change in working norms during the last year. We are seeing cloud adoption gaining traction among enterprises as it transforms from being viewed as a cost-reduction initiative to a business innovation enabler. According to an IBM-commissioned study by McKinsey, 94% of organisations use not just one, but multiple cloud environments to support their business. This has added to the increasing fragmentation of the security market.

Today, cybersecurity is one of the top concerns for organisations as a hybrid multicloud environment increases the complexity of performing core security tasks, from threat management and remediation to regulatory compliance. These organisations have data security lapses that leave them vulnerable to data breaches. A SANS Institute survey stated that more than 55% of security teams struggle with integration between security analytics tools and cloud infrastructure.

With employees working outside the office firewall in the covid-19 environment, securing data is an absolute necessity.

Malicious cyber activities and exposure of company assets aren't just pandemic-induced. Compromised credentials, cloud misconfiguration, or third-party software vulnerabilities are major contributors to malicious breaches[1] and have kept IT teams working overtime. This makes securing data a tough ask.

A key challenge in the implementation of data privacy and protection is the identification and categorisation of the growing avalanche of data and regulatory compliance. By tapping into advanced data security solutions, we can reduce security concerns without adding extra pressure on our IT personnel.

However, the onus of security—even for cyber resilient companies—doesn't just lie with our IT or security teams anymore. Having stringent security tools isn't enough to dodge cyberattacks.

As companies integrate artificial intelligence (AI), machine learning (ML), and cloud apps into their operations, the intersection with people is a vulnerable security link that needs to be strengthened. Organisations need to be cognisant of the "human" factor and train their employees regarding security protocols to prevent inadvertent lapses. About 23% of data breaches are a result of human error.

Today, as more and more of our employees work remotely, it is no longer a question of just how secure our data security solution is, but rather who is accessing it and how?

Armed with a cyber-elite specialist team and one of the most advanced and integrated portfolios of enterprise data security products and services, IBM helps organisations prevent unauthorised access to data in a hybrid multicloud world.

IBM works with businesses across the region to effectively leverage AI and data analytics to prevent potential breaches to secure privileged accounts. From protecting business data while maintaining compliance to retaining customers via a robust customer identity program, we partner with our clients to future-proof their cybersecurity strategy.

Matthew Glitzer
Vice President,
IBM Security,
APAC

IBM

1 Cost of a Data Breach Report 2020, Ponemon Institute and IBM Security, Jul 2020

WRITTEN BY

The Economist INTELLIGENCE UNIT

Rethinking data security in the time of covid-19

Through interviews with CxOs across Asia, The Economist Intelligence Unit examines the remote work and cybersecurity challenges that covid-19 has brought to the competitive landscape.

Cybersecurity is not a new concern for companies, but the onset of the covid-19 pandemic has made many people more attuned to the role it plays. "There is a bigger threat," confirms Jihong He, chief corporate strategy officer and data centre chief executive at CapitaLand, a Singapore real-estate company. New ways of working have brought new opportunity for cyber criminals. Ms He says regular company-wide data protection drills have now become standard. "We have always been aware of this issue but I would say awareness of the threat has increased and we are also raising our inner bar."

Indeed, hackers have started working overtime, much like their remote-working corporate targets. In the US, the FBI reported a spike from about 1,000 daily cybersecurity complaints before the pandemic to between 3,000 and 4,000 per day.[2] INTERPOL's cybercrime analysis during covid-19 also has shown a target shift "from individuals and small businesses to major corporations, governments and critical infrastructure."[3] For Asia specifically, David Koh, the commissioner of cybersecurity and chief executive at the Cyber Security Agency of Singapore, spoke at a roundtable event for the Center for East Asia Policy Studies, explaining that covid-19 has brought a convergence of three major trends: "1) an acceleration in digitalisation and increased exposure of assets and infrastructure to cyberattacks; 2) an increase in collective risk profiles due to an expanded teleworking environment; and 3) a global surge in malicious cyber activities."[4]

To gain a deeper understanding of how these trends are affecting business in Asia, The Economist Intelligence Unit spoke with regional C-suite leaders to better gauge the local challenge. Views between IT and non-IT functions showed close alignment, from the CIO to the COO.

Indeed, hackers have started working overtime, much like their remote-working corporate targets.

Ms He says the situation has prompted her company to add layers of security to ensure activities such as downloading data are recorded in a central server and to make transferring it "much more difficult than before".

Bupa, a global healthcare insurer, has fended off two sophisticated attacks in recent months. To counteract threats, the company implemented remote monitoring to track staff behaviour and scope out malware attacks, according to Sami Yalavac, the company's Australia and New Zealand CIO. Mr Yalavac says a larger digital transformation programme has been under way for several years, but the renewed focus on security has sharpened people's senses to risk. New policies include the use of secure exchange portals and regular exercises to encourage responsible behaviour and preparedness.

2 The Hill, "FBI sees spike in cyber crime reports during coronavirus pandemic," April 16th 2020, https://thehill.com/policy/cybersecurity/493198-fbi-sees-spike-in-cyber-crime-reports-during-coronavirus-pandemic
3 INTERPOL, "INTERPOL report shows alarming rate of cyberattacks during COVID-19," August 4th 2020, https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19
4 Brookings, "Experts discuss the growth of cyber threats amid the pandemic", December 28th 2020, https://www.brookings.edu/blog/order-from-chaos/2020/12/28/experts-discuss-the-growth-of-cyber-threats-amid-the-pandemic/

At FWD, a Hong Kong-based insurance group with operations across Asia, Simeon Preston, the company's group chief operating officer, has not seen the need to introduce new security policies over the past year, "but we've emphasised what we have much more. We've reminded people of their obligations." And to battle an increasingly common attack, the company added a button to its email system that allows workers to report suspected phishing attempts. "That email then gets quarantined."

The issue is compounded by the ever-expanding amount of data and, in some cases, lack of awareness.

Ratan Jyoti, chief information security officer for Ujjivan Financial Services in India, also sees staff as a vital part of security. "Continuous engagement with employees on awareness is important," he says, "and involving them in all activities like data scoping, categorising and tagging, etc, helps both IT and [the wider] business to solve many challenges."

Security has a lot to do with the intersection of where people interface with technology but companies are also starting to bring in artificial intelligence (AI) and machine learning (ML) to have a bigger hand in mitigating external threats. "I think it will play more and more of a role in identifying the early stages of any attack and stopping it at the source," Mr Yalavac says. "AI and automation [are] now a necessity for success" in user behaviour analysis and threat intelligence, agrees Mr Jyoti.

Wong Sze Keed, CEO of AIA Singapore, says that among other tactics, AIA has been "ramping up the monitoring of suspicious network activity and threat intelligence on emerging cyber threats including ransomware and malicious backdoors—the frequency of which was heightened during the pandemic, as noted by the Cyber Security Agency of Singapore."

The cloud is also largely seen as essential, but there are caveats. These financial, health and insurance companies handle highly sensitive data and "everything is on the cloud these days", Bupa's Mr Yalavac says. "How you're accessing it, who's accessing it and how it travels. These are considerations a company needs to think about."

For CapitaLand, the cloud is becoming increasingly important for data storage, says Ms He. "Choosing the right cloud player is very important. They need to have strict cybersecurity and really treat customer privacy as a priority," she adds.

Mr Preston says advances in the way people are using the cloud have minimised risk. "It was seen as a form of infrastructure four years ago or so," he says. "So then you were exposing yourself to more risk but now we're using cloud-native applications, not just moving ours up to the cloud. We believe we are benefiting from the enormous cybersecurity resources that service providers are building in."

"We make sure of everything we put onto the cloud, that we have our own layers of cybersecurity," he adds. "You can benefit from extra layers but you have a responsibility to ensure that everything is protected."

Consensus among our CxOs appears to be on two main challenges in implementing data privacy and protection. "The biggest issue is identifying and categorising your data," Mr Yalavac says. Mr Jyoti agrees: "Getting visibility to all data in the network has been a tiresome challenge for us. This is not a one-time activity and needs continual monitoring and coverage."

The issue is compounded by the ever-expanding amount of data and, in some cases, lack of awareness. Then there are the ever-changing regulatory goalposts. "Regulators are ratcheting up

requirements so the challenge is to stay ahead of those," notes Mr Preston. "The demand for the data we hold is increasing all the time. As you hold more data in the cloud, more of that is exposed... It's an arms race."

With massive data breaches, such as the headline-grabbing ones at Adobe, Equifax and eBay in the past decade (affecting almost a half billion people combined), clean-up tasks are extensive. And the hit to consumer trust can be an even greater cost. Regulations, technology and corporate policy are all part of the defence.

Central to achieving it is ensuring the whole organisation—not just the IT department—sees data security as a priority. Mr Yalavac says Bupa's training starts with the board and involves identifying "security champions" in every team. "Data classification activities across departments—as well as allowing data owners to categorise—helped not only to achieve the classification task but made [staff] realise what data they owned and helped in archiving unwanted data," says Mr Jyoti. "For operations, this helped in many ways from reclaiming the storage space to improving backup strategy."

"You have to create the right incentive for individuals to take it seriously," Mr Yalavac says. "We share personal stories, organisational stories, examples like people losing their retirement funds. You don't want to be the reason your company is in the headlines." Too often, he says, boards "throw money at security teams" but fail to seed understanding beyond that part of the company. At Bupa, he says maintaining constant pressure has paid off.

Ultimately, cybersecurity can't be a drag on business activities. The goal should be to simplify operations while ensuring that the security systems' architecture remains resilient. "Security should be an enabler rather than a blocker," Mr Yalavac says. That means understanding what each segment of data means from a privacy perspective and how to store it. At FWD, Mr Preston says "data privacy is a first-line responsibility among all managers, not just the IT department."

"You have to create the right incentive for individuals to take it seriously."

Sami Yalavac, Australia and New Zealand CIO, Bupa

Our CxO interviews consistently point to holistic strategies that involve far more of an organisation than the IT department. New technological tools, such as AI, ML and more cloud applications, will certainly be integrated into company operations, but the intersection with people is likely to remain a vulnerable security link. "It is not just one department's responsibility to protect," says Mr Jyoti, "what's needed is collaborative understanding and responsibility."

David Blecken was the author of the report and Jason Wincuinas was the editor. Additional insights for this article were obtained from in-depth interviews with experts. Our thanks are due to the following individuals:

- Jihong He, chief corporate strategy officer and data centre chief executive, CapitaLand
- Ratan Jyoti, chief information security officer, Ujjivan Financial Services
- Wong Sze Keed, Chief Executive Officer, AIA Singapore
- Simeon Preston, chief operating officer ASEAN, FWD Life
- Sami Yalavac, chief information officer Australia and New Zealand, Bupa