ComputerWeekly.com | TechTarget

E-guide

CW+ Content

Managing data breaches

Your expert guide to data breaches in APAC

In this e-guide

In this e-guide:

With over 146 billion records expected to be stolen over the next five years, enterprises can no longer rest on their laurels when it comes to protecting the data under their care. As recent events show, the impact of data breaches can be severe, not just in terms of monetary losses but also reputational damage. In this e-guide, read about the data breaches that have occurred across the region in recent years and the lessons you can learn to respond better to data breaches, which are all but inevitable at every organisation large and small.

In this e-guide

Experts: A breach response plan is a must in 2019

Mekhala Roy, associate features writer

With the frequency of mega breaches continuing to rise, several security experts believe the best approach is accepting the fact that companies are likely to get breached at some point.

Embracing this mindset will allow companies to focus on what their breach response is going to be like, said Jon Siegler, co-founder and chief product officer at Chicago-based SaaS startup LogicGate.

"The market is really going to judge you on how you respond," Siegler said during an IT GRC Forum webinar titled "Critical actions to survive a data breach in 2019 and beyond." "How do you respond to that incident and being prepared and having that [breach response] plan in place is really going to help."

In the event of a breach, the key is speed and as much transparency in the disclosure process when communicating with customers. That's according to Stephen Boyer, co-founder and CTO at Boston-based security ratings vendor BitSight. This is where having a breach response plan comes in handy, he said.

In this e-guide

"Companies really need to be much more efficient in [communicating a data breach] because otherwise it becomes overwhelming for those who have had the issue but also for those with whom that organization is engaging, so they can answer those questions and then take the business mitigation actions that they're going to need to do," Boyer said. "Without communication, worry and doubt fill the void."

The way that an organization is breached is oftentimes based on something very fundamental that they overlooked, a detail that someone did not follow up on, or a human error, Boyer explained.

Justin Fier, director of cyber intelligence and analytics at Cambridge, U.K.-based cybersecurity startup Darktrace, said companies should deploy tools that give them better visibility and ability to detect and take action quicker than they have in the past, but shy away from overinvesting in "shiny-blinky things for one-off problems."

"Probably the biggest frustration is collecting too many tools and then only having one or two people on the team know how to use each one of those tools," Fier said. "There's really no good spread of knowledge transfer across the entire stack, which leaves a major vulnerability when doing incident response."

Fier advised companies to move away from legacy approaches to security.

In this e-guide

"What worked just three or four years ago does not work today, and unfortunately I just don't see a lot of companies adapting to the new cyber world that we live in," Fier said. "Machines are getting faster, we're consuming more and more data, IoT has exploded, yet we're still using the same [security] practices that we used three years ago."

Developing an effective breach response plan

A breach response plan provides a guideline for companies to follow each time a data breach is discovered, LogicGate's Siegler said during the webinar.

But a C-level executive sponsorship is imperative for a breach response plan to be taken seriously. Having that formal process in place and making sure everybody is on the same page is critically important, he added.

A breach response also has to be led from a business perspective because data breaches impact the business and not just IT, he said.

Assembling a team to devise a breach response plan is a cross-functional exercise, Siegler stressed. Too many breach responses fail when led solely by their IT department, he said.

"You want somebody to be that response manager, somebody with product management skills who can wrangle different people across the organization, who's able to communicate those plans, address any remediation that need to

In this e-guide

occur immediately and then communicate out to regulatory agencies or to your customers," Siegler said.

When crafting a breach response plan, companies often involve information security or privacy functions, Siegler said. The general counsel needs to be involved from early on, he added. Companies working on creating software or technology would want to include infrastructure and DevOps teams to help understand and mitigate any issues, include marketing or public relations for communications, and customer service to be able to directly communicate with the customers.

It is equally important for companies to test their breach response plan, just like they would test their business continuity and disaster recovery plans, and run through it like going through a real breach, he added.

Next Article

In this e-guide

Data breaches in Australia show no sign of abating

Beverley Head

In the three months to the end of December 2018, Australian authorities were alerted to 262 data breaches which potentially exposed Australians' personal information – the vast majority classed as resulting from malicious or criminal actions.

The nation's notifiable data breach scheme turns one year old on February 22, and in its first four quarterly reports (the first covering only a partial period) the Office of the Australian Privacy Commissioner dealt with 812 notifications of breaches deemed serious enough to potentially cause serious harm to an individual.

In one case reported last quarter, more than a million Australians would have been potentially impacted. And, while in most cases the personal data compromised was contact information, people's tax file numbers were put at risk in 46 separate breaches during the quarter.

In this e-guide

The leading sectors affected were private health service providers, finance, legal, accounting and management services, private education providers, as well as mining and manufacturing.

Announcing the report, Australian Information Commissioner and Privacy Commissioner Angelene Falk said preventing data breaches and improving cyber security had to remain a priority for all organisations handling personal information.

While 64% of breaches were traced to malicious or criminal attacks, 33% were blamed on human error and 3% on system faults.

Given the use of techniques such as phishing to gain access to systems, Falk called for employees to be aware of the common tricks used by cyber criminals to steal usernames and passwords, while consumers were advised to be alert to scams and regularly change their passwords.

Small and mid-sized firms are particularly at risk, according to Phil Kernick, co-founder and chief technology officer of CQR Consulting, who said medium-sized businesses were guilty of often slack cyber security. He predicted there would be an enforceable action against at least one Australian company in the coming year.

Aura Information Security country manager Michael Warnock meanwhile warned that many mid-sized businesses will remain a happy hunting ground for

In this e-guide

cyber criminals as management teams remain reluctant to invest in high tech protection.

At the same time, they just do not expect an attack will happen to them, so they refrain from elevating the issue on their training agendas.

"The harsh reality is, cyber attacks will continue to grow in both frequency and complexity over the coming year," he said. "Both business and IT teams should accept the threat is present, implement ongoing training to teach employees to recognise potential threats, adopt responsible data protection behaviour and allocate sufficient funds to cover protection measures that commensurate with their organisation's risk profile."

According to Paul Trulove, chief product officer of identity governance company SailPoint, Australian organisations are struggling to see and understand the risks associated with compromised user credentials, as demonstrated by 43% of cyber incidents involving phishing, 8% resulting from brute-force attacks and 24% from compromised or stolen credentials.

"The report reiterates that an organisation's users have become the easiest route into an organisation for hackers," he said.

Next Article

In this e-guide

Personal data of 46.2 million Malaysia mobile subscribers leaked

Aaron Tan, senior editor, APAC

The personal data of more than 46 million mobile phone users in Malaysia was reportedly leaked online in possibly the biggest data breach in the Southeast Asian country.

According to Malaysian technology news website Lowyat.net, the leaked data comprised personal details such as e-mail and billing addresses as well as SIM card information of pre-paid and post-paid mobile subscribers of at least 12 telcos and mobile virtual network operators.

Additionally, the personal data of users of job portal Jobstreet.com, as well as a slew of medical organisations such as the Malaysian Medical Council and the Malaysian Dental Association, was compromised.

The massive data breach first came to light on October 18, when Lowyat was alerted to databases containing the leaked data that had been put up for sale for an undisclosed amount of bitcoin on its online forums.

Based on the dates in the data, the breach was likely to have occurred between 2014 and 2015, according to a Lowyat report. It is uncertain how the breach occurred, though investigations by the local police are ongoing.

In this e-guide

"All aspects are still under investigation, so we do not want to make any conclusions that will only complicate the situation," Mazlan Ismail, chief operating officer of the Malaysian Communications and Multimedia Commission (MCMC), told the Bernama news agency.

Mazlan revealed the MCMC had met with the affected telcos to seek their cooperation and keep them updated on the situation. "This is to ensure that they understand what is happening now, especially when the police, through the Commercial Crime Investigation Department visit them to investigate," he said.

On its Facebook page, the MCMC had called for the public to avoid making speculations on the data breach until the authorities complete the investigations.

Sanjay Aurora, Darktrace's Asia-Pacific managing director, said this latest breach is yet another example of a 'low and slow' attack that stays dormant inside networks for years, without anyone noticing.

"Traditional defences predicated on chasing after yesterday's attack fail to spot and stop stealthy 'low and slow' attacks of this type. Lateral movements are incredibly difficult to catch, with attackers spending an average of 260 days in a network before striking," he said.

Aurora said machine learning technology that learns on the job and dynamically recalibrates assumptions in the face of new information will detect and stop similar attacks. He also called for a cultural change against widespread victim-

In this e-guide

blaming that could deter organisations from coming forward with the evidence of crimes.

With mounting data breaches around the globe, Asia-Pacific countries such as Singapore and Australia are either planning to enact data breach notification requirements or have already done so.
Although Malaysia has personal data protection laws that require organisations to guard the personal data of individuals against loss, misuse, modification, unauthorised or accidental access, among other obligations, it does not mandate organisations to report data breaches.

Ng Kai Koon, a former director of government affairs at Symantec Asia-Pacific and Japan, had called for Malaysia to implement data breach notification rules as early as 2012, noting that this would instil consumer confidence in the country's data protection regime in spite of the regulatory overheads and costs to businesses.

Next Article

In this e-guide

Huge Singapore data breach shows need for new approach

Warwick Ashford, security editor

Personal data of 1.5 million citizens, including prime minister Lee Hsien Loong, has been stolen from a government health database in Singapore in a "deliberate, targeted and well-planned attack", according to health ministry.

Those affected visited SingHealth's specialist outpatient clinics and polyclinics from 1 May 2015 to 4 July 2018, but while data includes names, addresses, gender and date of birth, no medical records were involved apart from details of medicines dispensed to about 160,000 patients, the health ministry said in a statement.

According to the statement, no records were amended or deleted and no other patient records, such as diagnosis, test results or doctors' notes, were breached, but that the attackers "specifically and repeatedly" targeted Prime Minister Lee Hsien Loong's personal particulars and information on his outpatient dispensed medicines.

In this e-guide

The Cyber Security Agency of Singapore said its investigation shows that the cyber attackers accessed the SingHealth IT system through an initial breach on a particular front-end workstation.

They subsequently managed to obtain privileged account credentials to gain privileged access to the database, the agency said, adding that upon discovery, the breach was immediately contained, preventing further loss of data.

As part of government moves to tighten the security of SingHealth's IT systems, no computers used for health IT system are being allowed to access the internet, additional controls have been placed on workstations and servers, user and systems accounts have been reset, and additional system monitoring controls have been installed.

Similar measures are being put in place for IT systems across the public healthcare sector against this threat, the government said.

Fraser Kyne, European chief technology officer at Bromium, said the breach is "very serious" given the sensitivity of the data accessed and the sheer volume of records involved.
"This breach once again highlights how today's cyber security is a house of cards – it just takes one person to click on the wrong thing for the whole thing to come crashing down.

In this e-guide

"Only when we admit that we cannot detect and stop threats, and instead start focusing on minimising harm, can we ever hope to disrupt hackers," he said. "The simple fact is that if the endpoint was isolated, the hacker would have had nowhere to go and nothing to steal."

The incident also highlights the fact that networks and endpoints can no longer be trusted, said Kyne, because attackers will inevitably find a way in.

"Air-gapping can be an effective solution, but it is impractical when you have multiple employees trying to access a business critical application. Instead, we need to shrink protection to application level.

"By protecting applications that store our most sensitive and critical data, even if the device or network is compromised, that application cannot be touched as it will be invisible to the device and network," he said.

Threat detection

Javvad Malik, security advocate at AlienVault, said the breach drives home the importance for all companies across all verticals, particularly those which deal with personal data of any kind, to have effective threat detection and incident response controls in place so any such breaches can be detected quickly and stopped from turning into a large incident.

James Hadley, CEO and founder of Immersive Labs, said a breach of any type can never be underestimated.

In this e-guide

"However, as this incident has resulted in the loss of health records, the consequences could be devastating for individuals.

"It is no longer acceptable to stick with traditional means of security and leave the protection of data down to those seen to be elite in the field.

"Every organisation, from businesses to hospitals, must create a cyber-skilled workforce to ensure they are ahead of the bad guys and make breaches like this more difficult to come by," he said. "Taking on cyber security skills at this kind of scale should be a major priority."

Next Article

In this e-guide

Over 146 billion records to be stolen over next five years

Aaron Tan, senior editor, APAC

More than 33 billion records will be stolen by cyber criminals in 2023 alone, despite data protection laws mandating strong measures to protect personal and financial data, a study has found.

The figure represents an increase of 175% over the 12 billion records expected to be compromised in 2018, resulting in cumulative losses of more than 146 billion records over the next five years, according to research by Juniper Research.

However, average levels of cyber security expenditure will remain relatively static. Spending by small businesses in 2018 will only make up 13% of the overall cyber security market in 2018, despite more than 99% of all companies being small businesses.

In addition, the cost of breaches can exceed millions of dollars, dwarfing the turnover of such businesses.

Juniper said many of these companies use consumer-grade products, spending on average under $500 per year on cyber security. With many such businesses

In this e-guide

currently rolling out digital transformation initiatives, this will leave them vulnerable to newer forms of malware which require more advanced cyber security, beyond simple endpoint protection.

"Juniper's strategic analysis of 48 leading cyber security companies shows that artificial intelligence and predictive analytics are now table stakes for this market," said Juniper senior analyst James Moar. "These technologies need to be made available to all businesses, regardless of size".

Additionally, the research firm found that the US will become a more prominent target over the next five years. Juniper expects over half of all data breaches globally to occur in the US by 2023.

This is because the US has much national and international consumer and corporate data in a disparate range of institutions and regulations, making it easier to find and exploit systemic weaknesses, Juniper said.

Outside the US, countries such as Singapore, Malaysia and Australia have had their share of data breaches in recent years.

In July 2018, the Singapore government revealed that the non-medical personal information of around1.5 million patients who had visited specialist outpatient clinics and polyclinics in a public healthcare group had been illegally accessed and copied in a deliberate, targeted and well-planned cyber attack.

In this e-guide

The data taken included names, national identity card numbers, addresses and dates of birth. Information on the outpatient dispensed medicines of about 160,000 patients was also exfiltrated through an initial breach on a front-end workstation.

Notably, security budgets for organisations in Singapore were the highest among five nations recently surveyed by Osterman Research, which found that the security budget for a 2,500-employee Singapore organisation was more than S$1.3m (US$950,000) in 2017 and will grow to more than S$1.4m in 2018.

While security budgets in Singapore were the highest in the study, they will also grow at the slowest rate in 2018 at only 7.1%, less than half of the global average of 14.8%.

In addition, Singapore organisations reported the second-lowest spending among the nations surveyed when it comes to remediating a major security event – one that would cause significant disruption to an organisation's operations, such as a widespread ransomware attack.

According to Osterman Research, Singapore organisations would spend an average of nearly S$260,000 to resolve such an incident, lower than the global average of S$391,448.

Next Article

In this e-guide

Australia's data breaches are a 'sign of naiveté'

Beverley Head

One in 20 Amazon Web Services (AWS) S3 cloud storage services had been set up with such lax security that the data stored in them could be read by anyone.

That was just one of the findings of the latest *Cloud adoption and risk* report released by cyber security company McAfee at its user conference in Sydney.

According to Rajiv Gupta, senior vice-president of cloud security at McAfee, Australian enterprises might be slightly less exposed – but not because they are more diligent about cloud security.

Instead, it was because they had been rather slower than their global counterparts in embracing cloud infrastructure and platform services, he said.

Gupta also said companies that had once believed they had "reasonable transparency" into their data and how it was secured had had that belief "shattered" by the transition to cloud – but not because cloud suppliers were less diligent about security.

In this e-guide

Rather, Gupta said this was because businesses did not take precautions to ensure their data remained secure and private, in a sign of "naiveté rather than bad intentions".

"Cloud configurations are new and confusing," he said. "But I am surprised how widespread this is. Any S3 bucket left open could be on the front pages of the newspaper."

In 2017, Australia's national broadcaster inadvertently exposed sensitive data hosted on S3, following similar incidents in the US.

And more data breaches are coming to light following Australia's mandatory data breach notification legislation, which came into effect earlier this year.

In its latest quarterly report, released this week, the Office of the Australian Information Commissioner revealed that 245 organisations had experienced data breaches affecting personal information in the three months up to the end of September 2018, with 57% of breaches attributed to malicious or criminal attacks.

McAfee's analysis showed that, at present, 21% of all files held on public cloud services hold some sensitive data, and sharing data with a publicly accessible link increased by 23% last year. Threats in Microsoft Office 365, for example, soared by 63% over the past 12 months, said McAfee.

In this e-guide

Speaking at the Sydney conference, McAfee's senior vice-president and chief marketing officer, Allison Cerra, called for businesses that are tackling growing cyber security challenges to navigate the threat, technology and regulatory landscapes as they moved critical applications to the cloud.

Cerra pointed to McAfee's Mvision suite of cyber security tools, which will eventually include a cloud-focused tool.

The company said the suite's newest module for endpoint detection and incident response would be released in the first quarter of 2019, but gave no indication of when the cloud module will be due.

A further challenge faced by many organisations, particularly in Australia, is the shortage of cyber security skills as cited by nearly four out of five respondents to McAfee's skills survey.

However, 63% were unable to specify which skills were missing, while two in five people working in cyber security roles in Australia today have no formal qualification in the area, according to McAfee.

Next Article

In this e-guide

SingHealth and IT supplier fined $1m for data breach

Aaron Tan, senior editor, APAC

Singapore's Personal Data Protection Commission (PDPC) has fined SingHealth and its IT supplier a total of S$1m (US$739,410) for failing to protect the personal data of 1.5 million patients that were stolen in the city-state's largest data breach to date.

The PDPC said its investigations into the data breach arising from the unprecedented attack on SingHealth's patient database system found that SingHealth's IT supplier, Integrated Health Information Systems (IHiS), had failed to take adequate security measures to protect the personal data in its possession.

As for SingHealth, the PDPC found that SingHealth employees handling security incidents were unfamiliar with incident response processes, and were overly dependent on IHiS. They also failed to take further steps to understand the significance of the information provided by IHiS after it was surfaced, it added.

PDPC has imposed a "financial penalty" of S$750,000 on IHiS and S$250,000 on SingHealth – the highest amounts imposed so far.

In this e-guide

In a statement explaining the grounds of its decision, the PDPC noted that if organisations delegate work to suppliers, their role as data controllers requires them to be responsible for the personal data that they have collected from customers.

In meting out the fine, the PDPC said it took into account the fact that the data breach was the largest in Singapore so far, as well as the sensitive and confidential nature of the compromised data.

The PDPC said IHiS and SingHealth were cooperative throughout the investigations and took immediate remedial actions.

It also recognised that both organisations were victims of a skilled and sophisticated threat actor bearing the characteristics of an advanced persistent threat (APT) group, using numerous advanced, customised and stealthy tools and carrying out its attack over a period of more than 10 months.

Under Singapore's Personal Data Protection Act, organisations are required to protect the personal data in their possession or under their control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks. Those that fail to do so could face a financial penalty of up to S$1m.

In this e-guide

Defence-in-depth

In the aftermath of the SingHealth data breach, Singapore's minister in charge of cyber security S. Iswaran said in Parliament on 15 January 2019 that the government will ensure its IT and database systems are secure, and that the personal data it collects is well-protected.

This includes adopting a 'defence-in-depth' strategy, with multiple layers of cyber defences to impede an attacker. Iswaran said these layers of defence "cascade from the perimeter to within our systems, as we recognise that a sophisticated and determined attacker, given enough time and resources, may find a way through".

"This is why we also have capabilities in our layered defence that enable swift detection of a breach, and decisive response," he added.

In this e-guide

Getting more CW+ exclusive content

As a CW+ member, you have access to TechTarget's entire portfolio of 140+ websites. CW+ access directs you to previously unavailable "platinum members-only resources" that are guaranteed to save you the time and effort of having to track such premium content down on your own, ultimately helping you to solve your toughest IT challenges more effectively—and faster—than ever before.

Take full advantage of your membership by visiting www.computerweekly.com/eproducts

Images; stock.adobe.com