Kroll | A Division of DUFF & PHELPS

Data Breaches in the Healthcare Industry

BY BRIAN LAPIDUS AND LOUISA VOGELENZANG

Introduction

As custodians of vast amounts of highly-sensitive personal information, healthcare providers globally have continued to experience more data breaches than any other sector—a trend that's only accelerated as a result of COVID-19. The data points held by providers—Medicare numbers, date of birth, credit card information, medical insurance and driving license numbers—are rich fodder for cybercriminals, especially considering they're often tied to even more sensitive information such as medical diagnoses and history.

By the last account, Australia's healthcare industry experienced more data breaches than any other industry, accounting for 22% of notifiable data breaches between January to June 2020 as stated in the Notifiable Data Breaches Report by the Office of the Australian Information Commissioner (OAIC)[1]. While we are yet to understand the full ramifications of COVID-19 for the healthcare industry, as providers continue to digitise and transition online, the threat of cybercriminals and the risk of experiencing a data breach has only intensified.

The provision of quality care is often dependent on the efficient passing of information between healthcare providers, and can involve scenarios where security and data privacy become priority number two behind the delivery of emergency care – scenarios that cybercriminals will often work to exploit for financial gain.

In addition to privacy concerns, in a worst case scenario, cyber risk and clinical risk have the potential to intersect with tragic consequences – a 2020 cyber attack (ransomware) on a hospital in Europe caused network outages that forced a hospital to reroute patients to emergency care elsewhere. The disruption led to delays to emergency treatment for a patient and the local authorities have opened a death investigation.[2,3] Not all data breaches start with a cyber attack – according to the report by OAIC, 57% of notifiable data breaches reported by Australian health service providers during the period of January to June 2020 were due to an unintended action by an individual that led to a data breach.

However, with 40% of data breaches in Australian healthcare caused by malicious or criminal attack and with health systems outdated making it easier for threat actors to gain access,[4] only one in three health organisations have embedded awareness and training into their policies and procedures.[5]

1 https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-report-january-june-2020/

2 https://www.bbc.com/news/technology-54204356

3 https://www.reuters.com/article/germany-cyber/prosecutors-open-homicide-case-after-hacker-attack-on-german-hospital-idUKL8N2GF3HW

4 https://www.unsw.adfa.edu.au/school-of-engineering-and-information-technology/school-of-engineering-and-information-technology/news/strained-health-systems-struggle-keep-hackers

5 https://www.digitalhealth.gov.au/about-the-agency/digital-health-cyber-security-centre/information-security-guide-for-small-healthcare-businesses/HD127%20Information%20Security%20Guide%20for%20small%20healthcare%20businesses%20(co-branded%20with%20Stay%20Smart%20Online)%20Online%20Version.pdf

Yet despite this reality, patients continue to place a high level of trust in healthcare organisations—not only trusting them with their care and the care of their loved ones but also trusting them with the care of the data they provide to them. A recent report on Australian community attitudes to privacy found that healthcare remained the most trusted industry between 2007 – 2020[6] when compared to others including federal government departments, financial institutions and companies.

In an increasingly challenging cyber security landscape, healthcare providers must be prepared for a data breach to ensure they're in the best defensible position when a cyberattack inevitably occurs.

Over the past 17 years, Kroll's Cyber Risk practice has managed data breaches for over 1,600 healthcare institutions worldwide, and since 2019, has engaged with 14 million patients to help mitigate any risks stemming from data breach incidents.

In our experience, healthcare data breaches (when compared to data breaches in other industries) generate higher levels of anxiety in the impacted population given the nature of the information that has been potentially compromised, a richer variety of issues given the complexity of the data compromised, and more inbound phone calls to our call centres and investigators/restoration specialists by impacted patients or consumers.

Our extensive experience with data breaches in healthcare in the U.S., Europe and Canada has provided helpful insights into what effective breach management by a healthcare provider looks like and what impact that breaches can have on a patient's sentiment towards that healthcare provider.

This whitepaper examines how cyber security threats and data breaches in the healthcare industry have evolved since COVID-19 and assesses recent public incidents and two anonymised healthcare breach case studies in order to better understand the landscape and consider best approaches for the healthcare industry moving forward.

[6] https://www.oaic.gov.au/assets/engage-with-us/research/acaps-2020/Australian-Community-Attitudes-to-Privacy-Survey-2020.pdf

The Impact of COVID-19 on Healthcare's Cyber Security Landscape

There's no denying the significant impact that the pandemic has had on the vulnerability of the healthcare sector to cyberattacks, with Kroll observing an 86% increase in healthcare breach notification cases globally between March - September 2020, when compared to the same period in 2019.

Coupled with the growing sophistication of cyber-criminals, this has created fertile ground for cyberattacks, which have robbed 24,000 Australians of their personal details this year alone.[7]

For the healthcare industry specifically—an industry at the frontline of the pandemic—this new risk landscape, which continues to evolve at pace, characterised by multiple points of vulnerability that cybercriminals will exploit if given the chance. These include:

1. **The rapid shift to remote working** meant many organisations took shortcuts with the security of their networks or adopted systems that weren't necessarily designed with corporate levels of security in mind. Simultaneously, cybercriminals sought to exploit remote workers in order to gain access to insecure networks.

2. **An expansion in telehealth services** allowed healthcare providers to ensure continuity of care for patients unable to attend in-person appointments, but at the same time accentuated providers' digital footprints and placed patient data at an elevated risk.

3. **A workforce under intense stress and pressure** has likely naturally increased the potential for human error, such as sending personal information to the wrong person, not BCC-ing or loss of a data storage device. As reflected in the OAIC report, 57% of the reported notifiable data breaches by health service providers were due to unintended action by an individual, as compared to 24% across all sectors during the same period. In addition to this, threat actors can more easily exploit those who may be (understandably) distracted via convincing phishing emails. Phishing was the top cyber incident resulting in data breaches in the health sector in Australia according to the latest OAIC report.[7]

4. **The interoperability of Australia's healthcare industry** can amplify the impact of a cyberattack or data breach—one of the system's greatest assets can be turned into a weakness if subjugated by cybercriminals.

5. **Personal protective equipment (PPE) shortages** pushed healthcare workers online in search of supplies, where gray marketers worked on illegitimate websites to gain access to healthcare networks in order to compromise data.

[7] https://www.scamwatch.gov.au/types-of-scams/current-covid-19-coronavirus-scams

Expansion in Telehealth

While some of these vulnerabilities are likely to dissipate as the COVID-19 situation improves and we ultimately progress through the recovery, the surge in demand for telehealth services will more than likely remain a permanent feature of Australia's healthcare system.

During the height of the pandemic in Australia, governments across the world sought ways of strengthening the capacity of the healthcare system amid changed and evolving circumstances. The Australian Federal Government rapidly expanded access to telehealth to help reduce community transmission of the coronavirus, and protect patients and healthcare workers, and ensure continued access to healthcare services.

Temporary items were added to the Medicare Benefits Schedule (MBS), enabling patients to access a range of telehealth services at home via video or telephone. For general practitioners, bulk billing incentives were doubled for telehealth appointments, and eligible clinics were able to upgrade their NBN connection for free to help manage the surge in demand for telehealth services.

Since then, experts and advocacy groups have continued to push for these temporary changes to be made permanent, arguing that telehealth is underutilised and could play an important role in chronic disease management going forward.

But what are the implications for the security of patient data?

Considering the stronger reliance on technology platforms that telehealth services depend on, the healthcare profession must at the same time ramp up its focus on the cyber security risks that are part and parcel of the online world. This will ensure that the move online doesn't come at the expense of patient data privacy and security.

In its transition to telehealth, much of the healthcare industry is rapidly adopting a cloud-first model within their IT infrastructure, and the security of these systems must adapt accordingly to reflect modern healthcare services. Yet, many in the industry continue to work with legacy medical Internet of Things devices that are riddled with security vulnerabilities well understood and easily navigated by cybercriminals.

The security of telehealth solutions will depend on many factors, including the configuration of the solution (e.g., on-premise, Software-as-a-Service SaaS-based), data storage locations, authentication, video encryption, video recording and integration with electronic health record (EHR) systems. Many of these solutions are SaaS-based, which for the un-initiated, makes it more difficult to obtain a complete understanding of how well the solution is secured.

For healthcare providers looking to make telehealth services a permanent fixture of their offering, it is essential they have a good third-party risk assessment program to ensure all security risks are considered from the start, and contracts with third-party vendors are reviewed for security-related provisions, and general terms and conditions.

High-Profile Data Breach Cases in the Healthcare Industry

When considering the cyber security landscape that healthcare industries are currently dealing with, it is useful to look at several high-profile cases that have been reported since the start of the pandemic.

An assessment of these incidents indicates the measures and methods used by cybercriminals to gain access to valuable health data, and the types of data they're in pursuit of, furthermore, it highlights some vulnerabilities of healthcare providers and provides insights around the best lines of defense, and what providers must do in order to safeguard their networks, and the confidential patient records they host, in order to support the delivery of safe patient care.

The diagram below provides a snapshot of several healthcare data breach incidents that have occurred since the start of the pandemic.

Apparent in the examples is the prominence of ransomware, phishing and malicious software as common forms of cyber security incidents experienced by the healthcare industry.

MARKET: WORLDWIDE

Incident:
Fake HIV test results and COVID-19 conspiracy theories used to target insurance, healthcare and pharmaceutical companies worldwide

Details:
Cybercriminals used fake HIV test results and COVID-19 conspiracy theories to infiltrate the computer systems of healthcare companies worldwide. Hackers impersonated top U.S. medical centres to send out phishing emails, luring recipients into opening malicious content embedded

Nature of Attack:
Phishing attack with emails embedded with malware

Key Vulnerabilities:
Email verification, remote workforce

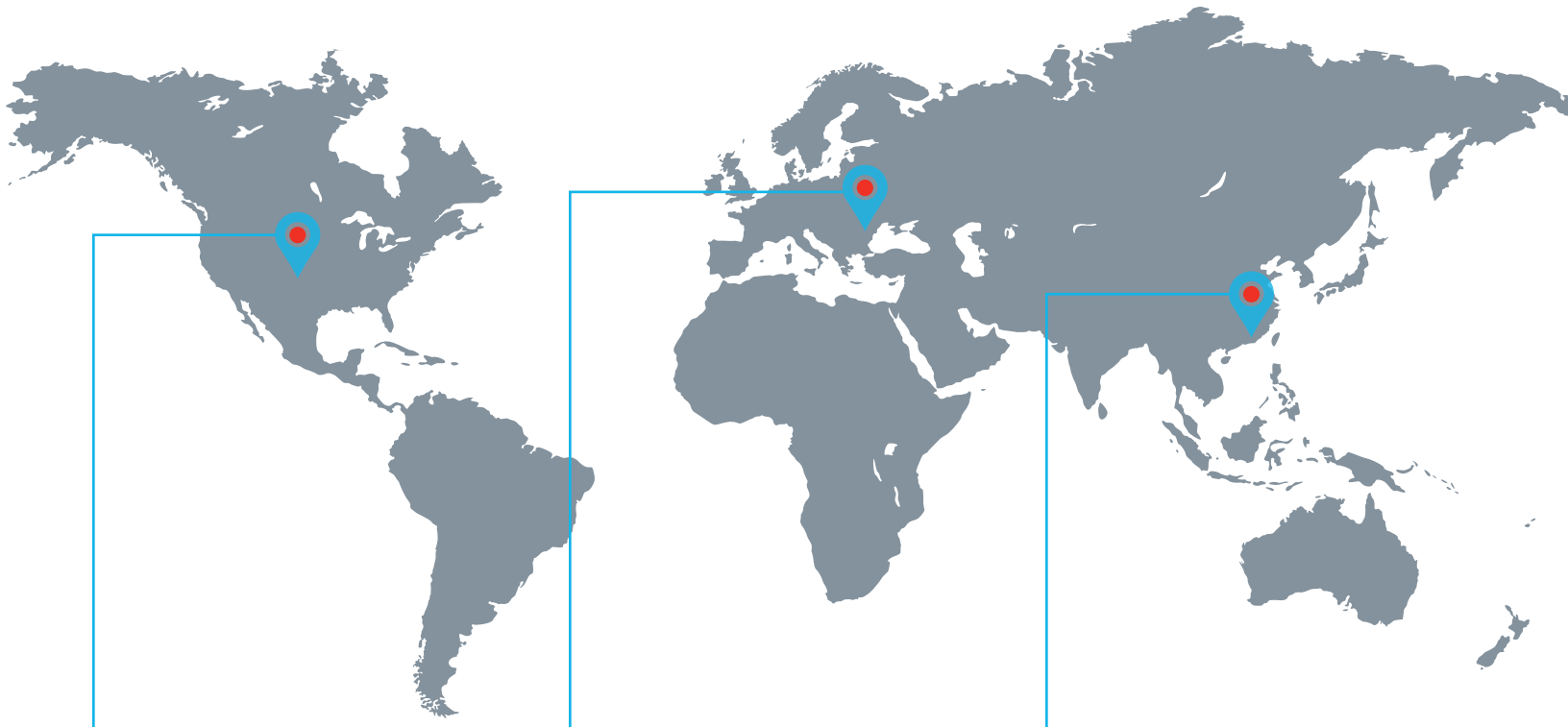
MARKET: WORLDWIDE

Incident:
Hospital and healthcare company's computer system attack

Details:
Hundreds of U.S. health system sites were disrupted as a result of a cyber security attack. The attack resulted in ambulance diversions and impacted facilities, including lab tests

Nature of Attack:
Ryuk ransomware is suspected, but full details have not been confirmed

Key Vulnerabilities:
Unreported



MARKET: U.S.

Incident:
Community based healthcare company data breach

Details:
An employee responded to a phishing email, which gave the attackers access to hundreds of thousands of patient records

Nature of Attack:
Phishing attack that provided the attackers with the login credentials of the victim employee

Key Vulnerabilities:
Human manipulation

MARKET: EMEA

Incident:
Cyberattack disrupted operations at a local hospital resulting delay in emergency treatment[2,3]

Details:
Cyberattack caused network outages, forcing rerouting of emergency care patients to other hospitals. Death investigation into the incident opened by local authorities. If proven, this could be the first fatality directly attributed to a ransomware attack

Nature of Attack:
Ransomware infected dozens of servers at the hospital. The hackers were able to exploit a Citrix vulnerability which the hospital had not patched in time

Key Vulnerabilities: Insecure Systems

MARKET: APAC

Incident:
Care operator hit by cyberattack

Details:
An overseas third party infiltrated and copied data from internal systems. Staff and patient details were released publicly as a result

Nature of Attack:
Ransomware infected IT system to disrupt operations. Personal data was copied, some were released on the dark web

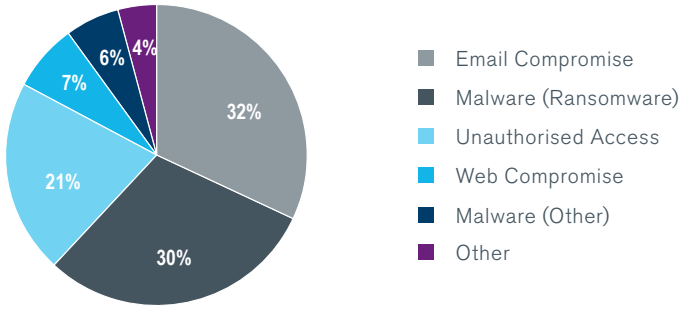
Key Vulnerabilities:
Unreported

[2] https://www.bbc.com/news/technology-54204356

[3] https://www.reuters.com/article/germany-cyber/prosecutors-open-homicide-case-after-hacker-attack-on-german-hospital-idUKL8N2GF3HW

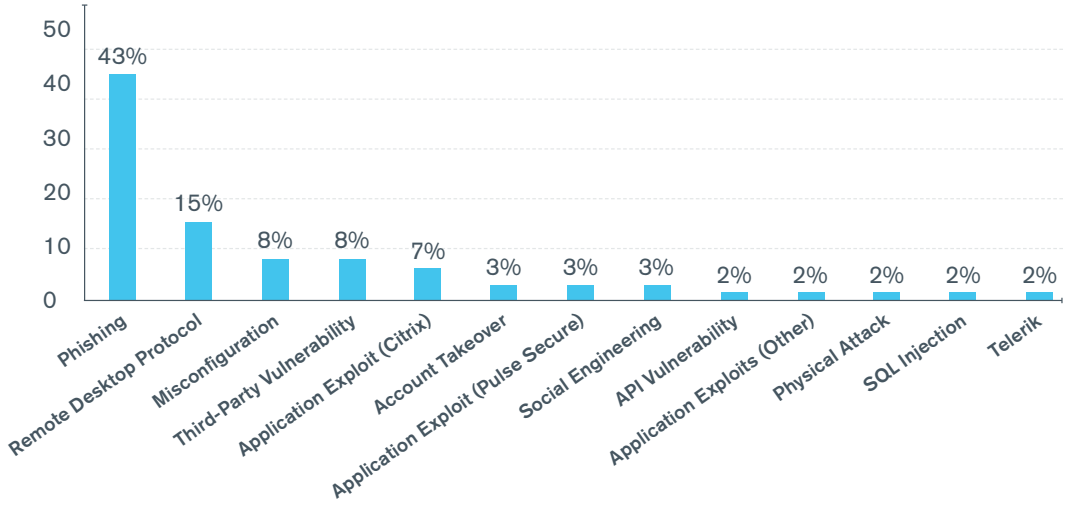
The latest Kroll case data for 2020 (January 1, 2020 through to September 1, 2020) on the most commonly observed threat incident types in healthcare indicates that business email compromise was the leading incident response case seen, closely followed by malware (ransomware).

HEALTHCARE ANALYSIS: MOST COMMONLY OBSERVED THREAT INCIDENT TYPES



The leading cause of malware (including ransomware) infection was phishing (43%) followed by remote desktop protocol (15%).

INCIDENCE OF INFECTION VECTORS



The goal of cybercriminals is ultimately to derive value from data stolen during cyberattacks, with data values on the dark web varying from USD 1 for a US social security number to USD 2000 for a passport. The price of health records fluctuates with some studies attributing price drops to supply and demand trends.[8] Recent investigation and analysis by Privacy Australia indicates that medical records can be worth any-thing from AUD 1 to AUD 1000 depending on how complete they are, but they also acknowledges that prices vary significantly.[9]

The examples demonstrate the nature of reporting on data breaches in the healthcare industry, predominately focused around the size and extent of the attack or breach, how the perpetrators gained access and what information was retrieved. Yet once the "news" value of the incident dies down, little is said about what goes on in the aftermath to effectively manage the data breach notification process and the steps taken to help restore the reputation of the impacted provider.

The following case studies provide a more in-depth "behind the scenes" look at what is involved when managing a data breach experienced by a healthcare provider, based on Kroll's extensive global fieldwork.

[8] https://www.cyberscoop.com/dark-web-health-records-price-dropping/

[9] https://privacyaustralia.net/dark%20web%20personal%20data/

Breach Case Study 1

Scope: Patient medical record theft leading to health identity fraud
Number of Impacted Patients: Initially 500,000 patients

The Healthcare Organisation's Perspective

A desktop computer was stolen from the unlocked car of an IT employee at a large hospital. It was determined that the computer housed nearly 500,000 patient records containing names, date of birth, identification numbers, addresses, and information on patient medical history. When the client called Kroll, they were focused on procuring urgent breach notification services only—further investigation had not been considered at this time. However, as hospital officials an insider stealing equipment from the facility, Kroll recommended a full investigation that would include interviews with employees, and a thorough evaluation of current security measures to identify any areas of deficiency and risk.

The investigation began with a forensic interview with the said IT employee while investigators traced his footsteps to determine if anything else had gone missing. Concurrently, the Kroll team scoured pawn shops, checked with local authorities, and closely monitored physical equipment moving in and out of the facility for the duration of the investigation. All activities were carefully documented. The investigation ultimately revealed that no other staff had stolen equipment and that the hospital had only lost the single desktop.

While the investigation was underway, Kroll helped the hospital prepare for data breach notification. This involved:

- Assembling extensive up-to-date records of individuals impacted by the breach
- Running the data against a registry to identify the deceased
- Checking for updated addresses
- Deduplicating data
- Deploying call centre services

The Patient's Perspective

One of the patients impacted by this breach was an 85-year-old woman. Following the breach, she received a document in the mail stating that she had undergone a cosmetic procedure. It turned out someone else had claimed the procedure on her insurance using her stolen identity information.

Working with one of Kroll's licensed investigators and restoration specialists, the patient was able to notate her medical records tied to the identity theft issue that had occurred. Working with her insurance company, our investigator was able to successfully assist this patient to remove the procedure from her medical history and insurance claims file, in order to avoid the patient having to deal with the impact the procedure could have on future medical procedures and claims. By identifying the patient as a victim of identity theft on her medical record, Kroll was able to reduce future risk.

Breach Case Study 2

Scope: Healthcare breach that disclosed patient diagnosis and medication information
Number of Impacted Patients: 900,000

The Healthcare Organisation's Perspective

A healthcare organisation reported the theft of dozens of unencrypted hard drives, which contained a large number of audio and video files. Before the client could begin notification, the stolen data needed to be reconstructed and then individually analysed to determine the scope and extent of the incident. The client engaged Kroll to establish a clear picture of the event and manage the response process as it was concerned it would not be able to meet the tight deadlines for notification.

Kroll conducted a thorough investigation into the event and recovered the stolen data from backup tapes. After reconstructing the data, Kroll determined that more than one million files required data analysis to accurately define the scope of the exposure. Kroll accelerated the process by employing a combination of proprietary technologies and human reviewers who worked around the clock to identify the type of data compromised and which stakeholders would need to be notified.

Kroll identified over 900,000 individuals who needed to be notified about the incident—a complex population that featured special groups, including minors and deceased individuals. Kroll worked with the client to deploy the notification process in phases based on the severity of risk, providing guidance along the way to ensure the client met regulatory obligations. Kroll provided consumer remediation solutions on behalf of the client, performing both credit- and non-credit-related investigations to identify suspicious activity and fraudulent use of information.

Kroll spent nearly 87,000 hours on data analysis staffed by hundreds of analysts to pinpoint the scope of the event and expedite notification. This assistance enabled the client to focus on business continuity, without having to divert critical resources away from revenue-generating operations.

Kroll guided its client through the controlled execution of a timely notification strategy. In total, 28 unique population groups were identified and notified, in compliance with applicable state and federal laws.

The Patient's Perspective

Kroll's call centre handled inbound calls tied to the 900,000 notification letters distributed to impacted individuals. Because the breached records contained data for the past decade, the impacted group was diverse and some individuals required a unique engagement approach.

One of the patients impacted in this breach was a 36 year old man who had undergone medical testing regarding an undiagnosable set of symptoms. After receiving a letter regarding the data breach via priority post that had been customised to his population group (patients who had the medical diagnosis, prescription data, and/or financial payment information) he decided to call into the call centre. While this patient was concerned about others learning of his diagnosis and being privy to the medications that he was prescribed, he was even more concerned that the information held which included financial data, could be used to "scam" him financially as he had been the victim of identity theft after a suspected data breach of his personal information 10 years ago, something that had led to additional identity theft episodes in the following years.

Upon calling in to the toll-free number provided, the Kroll agent was able to assist him with the process of turning on the remediation services such as identity theft and credit monitoring. This gave him re-assurance that someone was watching his accounts to ensure criminals were not using the stolen data to commit fraud again.

Kroll helped the client demonstrate its long-term commitment to safeguarding constituent privacy. Based on the results from Kroll's follow-up risk assessment, the client implemented several steps to strengthen its overall security protocols to reduce the risk of a future data loss event.

Getting It Right for Healthcare Providers and Patients

Effective breach management is complex and varies considerably case-by-case. Leveraging decades of experience, Kroll has developed clear guidance around best practices when it comes to managing data breaches in the healthcare industry, while also envisaging where key trends are headed and what providers can do to help mitigate the wide-ranging consequences of a data breach.

Effective Communication is Key

In the first hours (and even days and weeks) of a crisis, breach victims and the organisation impacted don't often have a complete picture of the incident that has occurred. During this period of discovery, with ambiguity rampant, breaches can be made worse by misguided communication efforts that take too long, fail to come off as transparent, or provide information that must be corrected as the forensic investigation uncovers new details about the incident and the extent of data exposure.

In the event of a breach, organisations that have in place a carefully considered and holistic crisis communications plan are able to act immediately, which includes taking pivotal steps aimed at maintaining or restoring trust among the impacted population. Ensuring communication with stakeholders is frequent, informative, transparent and reassuring is critical.

A robust data breach response plan that is regularly tested and outlines who should, and how to, communicate a data breach to impacted stakeholders is the first step.

Do Not Judge a Breach by its Size

While the size of a data breach is almost always reported on, it's important to note that the size of the impacted population doesn't necessarily reflect the impact that the breach will have on the organisation or stakeholders involved. Beyond the number of impacted stakeholders, the type of data accessed is a key determinant of a breach's impact and the longer-term implications for the healthcare provider.

The impact of a data breach always varies on a case-by-case basis, and some consequences are not as easily foreseeable as others.

In terms of the financial costs involved, the results are in. The average total cost of a data breach in Australia in 2020 was estimated to be $3.35 million—or $163 per lost or stolen record—an increase of 9.8% year-on-year.[10] However, beyond the impact to a business's bottom line, the loss of consumer confidence and trust resulting from a breach, while harder to quantify, can be even more devastating and long-lasting for the organisation involved.

[10] https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/

A 2020 study revealed that Australian organisations see damage to brand and reputation as the biggest risk to not managing consumer data properly, followed by cybercrime,[11] indicating a clear awareness of the consequences of not effectively safeguarding consumer data. However, in reality, we know that awareness of threats and risks may not necessarily translate to the application of best practice.

Therefore, providers must keep in mind that for data-rich industries like healthcare, consumer confidence and trust is not solely based on the services provided, but also a belief that personal information is adequately safeguarded. Providers must take measures to ensure this is the case.

Going Beyond Compliance

According to a 2020 survey on consumer privacy sentiment, four out of five consumers expect compensation for breaches of privacy, amid widespread anxiety about identify theft, misuse of data and a lack of consumer protections. Data security breaches are now Australians' biggest concern, with nearly 90 per cent considering privacy extremely or very important when choosing a digital service. Identity theft and fraud, and data security and data breaches were cited as the two biggest privacy risks by Australian consumers.[12]

What's more, 50 per cent consider their data privacy to be more at risk in a COVID-19 environment.

While it is clear community expectations around data privacy are growing, there are also myriad legal obligations that organisations that manage customer data must comply with.

On October 30, 2020, the Australian government kicked off a review of the Privacy Act including effectiveness of the notifiable date breach scheme. Potential amendments to the Australian Privacy Act are just the latest addition to what is fast becoming a high-pressure, increasingly regulated cyber security landscape.

While this new regulatory landscape is taking shape, establishing digital trust—that is, consumers' confidence in the ability of organisations to effectively secure the privacy of individuals' data—must take on a new level of focus for healthcare providers, to not only meet their legal obligations but also must go the extra mile to safeguard consumer trust.

This is critical at a time when consumers want and expect more and are more willing than ever to take their business elsewhere. Similar sentiment was echoed in a recent call to action from the Australian Information Commissioner and Privacy Commissioner, Angelene Falk.

"We encourage entities to move beyond compliance, to effectively support consumers. While the law obliges entities regulated under the Privacy Act to provide transparent and useful information to consumers, it is those entities who focus on the consumer and navigate beyond compliance—to support affected individuals to take steps to minimise or prevent harm in a meaningful way—who will differentiate themselves and maintain trust over time."[13]

[11] https://www.governanceinstitute.com.au/advocacy/survey-reports/digital-trust-survey/

[12] https://www.oaic.gov.au/engage-with-us/research/australian-community-attitudes-to-privacy-survey-2020-landing-page/2020-australian-community-attitudes-to-privacy-survey/

[13] https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-scheme-12month-insights-report/

Another 2020 study[14] also found that nearly half of Australian consumers would pay more to do business with an organisation that is committed to protecting their personal data.

Healthcare entities must move beyond compliance to ensure their trusted status with patients is not eroded by the consequences of breaches of their personal information.

Conclusion

As the gatekeepers of patient records and sensitive data points, the healthcare industry plays a fundamental role in ensuring the privacy and security of patient health information.

Poor data stewardship that results in a data breach can have crippling consequences for both the healthcare providers and their patients involved. The consumer trust – and more specifically the digital trust – that is lost in the event of a data breach cannot be restored overnight.

Healthcare industries are being forced to navigate a period of intense change and uncertainty while remaining the world's front line of defence against the rapidly evolving COVID-19 pandemic. Cybercriminals are not characteristically civic-minded and have continued to exploit pandemic-induced vulnerabilities for financial gain.

While many healthcare organisations have sought to fight back, investing significantly in their people, technology and general security measures, the capabilities of cybercriminals continue to outpace their efforts.

Effectively managing a data breach incident from start to finish is the domain of highly experienced specialists and forensic experts who can combine global best practice with local knowledge and expertise.

Proactively addressing cyber risk must form part of good governance for all Australian organisations as for most, the incidence of a data breach is not a matter of "if" but "when".

[14] https://www.itwire.com/guest-articles/australian-consumers-put-a-price-on-privacy-almost-half-would-pay-more-to-do-business-with-an-organisation-committed-to-protecting-their-personal-data.html

Kroll | A Division of DUFF & PHELPS

CONTACTS

Brian Lapidus
Managing Director and Global Breach Notification Leader Identity Theft and Breach Notification

blapidus@kroll.com

Louisa Vogelenzang
Associate Managing Director APAC Lead - Identity Theft and Breach Notification

louisa.vogelenzang@kroll.com

TALK TO A KROLL EXPERT TODAY

Australia
T: +61 1800 870 399

North America
T: +1 877 300 6816

Hong Kong
T: +852 800 908 015

UK
T: +44 0 808 101 2168

Singapore
T: +65 800 101 3633

Additional hotlines at:
kroll.com/hotline

Or via email:
CyberResponse@kroll.com

About Kroll
Kroll is the leading global provider of risk solutions. For more than 45 years, Kroll has helped clients make confident risk management decisions about people, assets, operations and security through a wide range of investigations, cyber security, due diligence and compliance, physical and operational security, and data and information management services. For more information, visit www.kroll.com.

About Duff & Phelps
Duff & Phelps is the world's premier provider of governance, risk and transparency solutions. We work with clients across diverse sectors in the areas of valuation, corporate finance, disputes and investigations, cyber security, claims administration and regulatory compliance. With Kroll, the leading global provider of risk solutions, and Prime Clerk, the leader in complex business services and claims administration, our firm has nearly 4,000 professionals in 25 countries around the world.
For more information, visit www.duffandphelps.com.