Protected data sharing and Life Sciences in the Asia Pacific: From treatment to prevention

In the last decade, "big data" and "data & analytics" dominated the life sciences sector, and with increasing digitization and liberation of data, the sharing of medical information will take center stage going forward. But it comes with great responsibility, particularly from a security and privacy perspective because health data is highly valued, especially by hackers.

While personal identity numbers can fetch around U$15 on the dark web, personal health records are worth upwards of U$100 each because identity theft becomes more specific to the individual. The SingHealth incident, where 1.5 million patient records were exposed, goes to show no one is safe.

How can life sciences companies prevent threats to their own data and that of partner stakeholders from derailing growth ambitions and advancements in connected care? How should they tackle the shift in mindset such that cyber security becomes an enabler of innovation, rather than an inhibitor?

Security by design

In a study conducted by Forbes Insights and KPMG on cyber security in life sciences (Forbes Insights-KPMG study)[1], findings indicate that while life sciences organizations are elevating cyber security as a strategic imperative, it is at a pace that lags behind the desired adoption of broader digital technologies. Further, according to the International Association of Privacy Professionals, life sciences organizations spend about US$8 million on privacy compliance programs annually although it is expected to be more like US$15 million for digitally-transformed companies, and upwards of US$2 million for fast-growing biotechs.

"Healthcare breaches around the world are unfortunate," said Rob Suarez, Global Head of Product Security at BD (Becton, Dickinson and Company). "But it is an opportunity for the industry to come together to make an impact. There must be continuous efforts to improve security by design, taking into account the clinical workflows and patient experience. Industry collaboration is the key to progress as there will never be enough resources individually."

"It's a multi-faceted evolution for vertical industries like life sciences," observed Christopher Martin, Asia Pacific Director for Access Partnership, a global technology policy consulting firm. "Not only are they improving internal systems to be more secure, but there is a realization that engaging with other sectors and governments on cyber regulation is imperative to ensure policy does not conflict with business."

The lack of proper cyber security programs at the organizational level is hurting business and consumers in numerous ways. These range from the halting of clinical trials due to poor technology infrastructure and fear of intellectual property (IP) theft, to valuation concerns during mergers & acquisitions when one of the companies reveals data privacy violations, and the removal or recall of medical devices from data streaming services because of tampering concerns. Common among these examples are the concepts of data sharing, Internet of Things (IoT) and underlying it all, the people element.

Data sharing for the win

Forward-looking life sciences companies are betting their future on being integrated, data-driven service organizations rather than as mere product sellers. Many are looking for new sources of data, even direct from consumers through wearables and social media[2]. Unfortunately, as breaches have shown, while data is valuable and available, ineffective governance will prevent open sharing. The damage arising from data loss include reputational, regulatory and eventually, the removal of social license to hold such information.

"The fourth industrial revolution is data driven," remarked Floor van der Wind, a member of the KPMG Life Sciences Digital Enablement team in Singapore. "The value of data tends to increase as digitalization increases and organizations are starting to actively explore the possibilities of sharing data to enhance innovation and growth. One such example is Google Maps, which now serves as a platform for Google's partners to do business."

However, laws governing data localization threaten to undo much of the progress made in areas like telemedicine and remote servicing of medical devices, Caitlin Asjes, Director of Public Affairs for BD Greater Asia, pointed out. "Data localization denies small and mid-sized companies the many benefits, including increased security, that come with more advanced technologies that are available when using the cloud."

Progress in innovation for life sciences companies will see them mature from data analysis to data sharing across borders, with competitors, on the cloud and in real-time. While this may sound daunting for some, 76% of the participants in the Forbes Insights-KPMG study believe moving to the cloud actually improves their security profile. However, nearly half of these same executives have not increased cyber security budgets despite their knowledge of high-profile breaches.

[1] Life sciences innovation and cyber security: Inseparable, KPMG, 2017. Retrieved from: *https://institutes.kpmg.us/healthcare-life-sciences/articles/2017/innovation-cyber-security-inseparable.html*

[2] Consumerization of genetic testing, KPMG, 21 November 2018; Retrieved from: *https://home.kpmg/sg/en/home/insights/2018/11/consumerization-of-genetic-testing.html*

Organizations are sharing sensitive and confidential information with:

Clinical research partners (e.g., universities)	77%
Contract manufacturers	51%
Marketing/detailing organizations	45%
Contract sales people	30%
Staffing agencies/ contractors	24%
Business process outsourcers	10%

BD's portfolio, which now includes over 200 products with software embedded, is trending toward IoT-enabled technologies, hence the laser focus on cyber security initiatives and emphasis on medical device security and transparency. The company regularly publishes results from cyber security vulnerability assessments (CVAs), and outlines the procedures on their website. "No device will ever be 100% secure because the landscape is constantly evolving," said Asjes. "We need to work with our customers to ensure we stay ahead of the threats."

IoT: Interest of Thieves?

Hospital and care provision infrastructure is increasingly reliant on medical device integration and vice versa. Thus, putting in place a secure network is in the best interest of all parties as cyber attacks can take many forms. It can be through a medical device connected to the hospital's IT system, through inappropriate access to sensitive information or device tampering.

Taking a collaborative approach to cyber security and privacy is ideal and starts with the design phase. Of the companies that participated in the Forbes Insights-KPMG study, while 92% indicated they are integrating privacy principles during product development, only 15% conduct regular software engineer training on secure development and programming.

"Unlike information security programs focused on preventing theft of IP or protecting a company's internal data, product cyber security focuses on keeping devices safe when they are in the customer's environment," shared Asjes. "We can put all the safety features in the world on a product, but if a customer chooses to write the password on a sticky note and place it on top of the device, it will never be secure. As such, medical device manufacturers not only need to ensure the safety features built into the product are practical and effective, they also need to better engage with and educate customers on protecting their device and data."

Don't overlook the people factor

Companies are continuing to invest in cyber security, focusing on software/technology and improved governance and polices. And interestingly, of all the efforts associated with improved cyber protection for life sciences companies, only 9% of respondents in the Forbes Insights-KPMG study cited greater staffing as a priority. Additionally, just 38% conduct cyber training for leadership, 34% carry out employee response drills, and 28% host desktop drills for the IT department.

While IP loss/leakage remains foremost on the minds of executives, most life sciences organizations are only able to monitor a small percentage of their employee and third-party bases. Not many are directing efforts at insider detection which is much more difficult than tracing external threats. As such, one of the most immediate challenges is getting relevant parts of the organization to work under a unified approach. At BD, trained cyber security personnel are part of the business and product teams. "The goal is to empower everyone at BD to deliver the highest quality products and services," said Suarez. "To avoid disrupting innovation, we use our existing well-defined protocols plus the embedded team approach. And this must occur from initial design stage. For example, our R&D people are reviewing software for coding bugs and these are natural opportunities to insert cyber security discussions, and to have these same experts look for security vulnerabilities."

Two-thirds of employee-based security threats are actually accidental rather than activities with malicious intent[3]. In this regard, organizations must help employees understand that cyber security programs are designed to protect them and their patients and should not be perceived as initiatives driven by mistrust of employees. Programs that fail to create this positive position may give rise to disgruntled employees and become part of the problem it is attempting to solve.

"Our ambition for cyber security is to shift from a mentality of moving out of fear to following a plan of focus, action and multi-stakeholder engagement," said Suarez.

[3] Insider threat in life sciences, KPMG, May 2018. Retrieved from: *https://institutes.kpmg.us/content/dam/institutes/en/healthcare-life-sciences/pdfs/2018/insider-threat-in-lifesciences.pdf*

What's your game plan?

Life sciences companies must evolve their cyber security programs from "treatment" (reactive) to "prevention" (proactive). This entails integrating data security principles into the broader organization growth strategy and in some cases, even as-a-service itself to customers.

As the recent UL certification for its flow cytometry device indicates, BD is demonstrating increased rigor in addressing cyber security because of its connection to patient safety and privacy shared Suarez. "Cyber security is the next frontier in patient safety," Asjes added. "We are not only responsible for keeping our patients physically safe, but also keeping their personal data safe."

"Multi-stakeholder engagement is critical to improving the overall cyber security environment," said Martin. "No one can do it alone. But because threats are evolving rapidly, we're seeing knee-jerk reactions from governments; implementing regulations, some of which are ill-informed. At the same time, governments are eager to hear how industries are tackling cyber security threats and incorporating those lessons into better policy responses."

Ultimately, when it comes to cyber security, there is no substitute for good planning and management. It requires a holistic view of people, processes and technology, and cyber teams must continuously monitor and allow their program to evolve as new cyber threats emerge. Over the years, KPMG has assisted countless clients in building cyber confidence by working with them through their cyber strategy and governance, organizational transformation, cyber defense and cyber response. Additionally, KPMG has invested in technologies and collaboration spaces where their clients' cyber security program, systems and readiness are put to the test.

Acknowledgements

Rob Suarez
Director, Product Security
BD (Becton, Dickinson and Company)

Caitlin Asjes
Director Public Affairs, Greater Asia
BD (Becton, Dickinson and Company)

Christopher Martin
Director, Asia-Pacific
Access Partnership

KPMG Healthcare and Life Sciences Practice:
Ajay Sanganeria, Chris Hardesty,
Owen Hawkes, Floor van der Wind

Contact us

Ajay Sanganeria
Partner, Life Sciences
T: +65 6213 2292
E: asanganeria@kpmg.com.sg

Chris Hardesty
Director, Life Sciences
T: +65 9824 2924
E: chrishardesty@kpmg.com.sg

Join the conversation

Life Sciences Breakroom
linkedin.com/groups/10392062/

kpmg.com.sg

kpmg.com/socialmedia

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.