The Secure Data Centre

Telin Singapore 3rd Advisory Council Roundtable 2H2017

www.telin.sg

Introduction

Security is a hot-button topic today, especially when it comes to cybersecurity in our heavily digitized society. In Singapore, the Government has publicly ramped up cybersecurity measures with initiatives that include setting up an academy to boost the skills of cybersecurity professionals, among others.

It is against this backdrop that council members of the Telin Singapore Advisory Council (TSAC) gathered once again in November 2017 to discuss the factors that make up a secure data centre. The wide-ranging roundtable discussion covered topics including essential considerations to properly secure physical infrastructure, the value of deterrence, the role of the network, and the importance of having an open and forward-looking attitude towards security.

Telin Singapore will draw on the insights and feedback obtained from the roundtable to beef up its security posture, rollout new capabilities to address security pain points, and tweak processes and communication to improve its position as the operator of choice for organizations that genuinely care about their infrastructure security.

Contents

Council Members

Victor John Carey is the director and owner of AT Advanced Technologies in Singapore. With 30 years of experience of which the majority are in Southeast Asia, Victor is an Uptime Institute (UTI) accredited tier designer with expertise in data centres, microelectronics facilities and buildings with stringent noise control requirements. His company offers design, integrated systems testing and UTI accreditation support for high tech buildings including data centres, and was also engaged in the commissioning management and support for the UTI accreditation of Telin-3 in 2016.

Akito Kurokawa is the APAC network strategy manager at Netflix, a global, leading Internet television company, specialising in partner engagement, quality of experience, interconnections and network architecture. He has extensive experience in the Asia Pacific working on various network roles for almost two decades including stints at global OTT providers, a global data centre provider, and a global internet service provider.

John Lee is the co-founder and COO of Vodien Internet Solutions, and is responsible for all aspects of operations, sales and customer care. He works closely with the product and technical divisions of Vodien, and helps to guide the company's sales strategies, focusing on promotional campaigns that drive the company's growth. As part of the overall drive to increase customer satisfaction, John ensures only the highest levels of service and support to all customers.

Lim Boon Chuan is the managing director of Webzilla Singapore, an enterprise hosting company with a presence in North America, Europe and Southeast Asia. Boon Chuan was the founder of 8 to Infinity prior to its acquisition by XBT Holding, which owns Webzilla. Boon Chuan is just as passionate about web hosting services today, and he delights in providing customers with what they need to succeed.

Terence Lim the director and co-founder of RED Technologies, and has more than 20 years' experience in the IT and Telecom industry where he is involved in the design, build and maintenance of infrastructure. RED Technologies specialises in fibre network build and maintenance, data centre remote hands support, IT project management and its associated service support and has a presence in Singapore, Hong Kong and Malaysia.

Victor Yuk is the CEO of Wizlearn Technologies, a leading e-learning solutions company in Singapore. Victor started work at Wizlearn Technologies as a system administrator, and subsequently became the vice president of operations where he led a team of 25 solution architects, system and software engineers. Victor initiated several major e-learning projects which led to an increased adoption of such systems in schools, corporate companies and government agencies.

Securing the data centre

The secure infrastructure

It was quickly evident that the secure data centre means different things to different members. Akito Kurokawa was quick to delineate it into two separate aspects: Security controls to manage and protect the cloud or on-premises deployment, and a robust infrastructure design to defend against crippling distributed denial of service (DDoS) attacks.

"Our cloud security team has a very different view on security," said Kurokawa. "You want to have at least two cloud instances that are separate regions, which could be two places in Singapore: East and West [of the island]. Or, Singapore and Indonesia. You need to have that kind of regional diversity, to make sure that one is available if the other is not," he said.

Kurokawa pointed to an opportunity to assist organisations with hybrid deployments, which he sees as a rising trend. "A lot of people don't understand how to move from a traditional data centre to a hybrid solution," he noted.

Victor John Carey's chief concerns about security, on the other hand, lies in the data centre's physical infrastructure. He said, "When I think of security, I think traditional [data centre] security in terms of CCTV, biometric scanners, infrastructure hardware, rather than [data theft] and cyberattacks. We deal with intruders, terrorist attacks, not cyberattacks where someone gets into the facility, causing problems from within."

The data centre advantage

When it comes to physical security, Vic Carey noted that organizations are generally happy once key security capabilities are in place. Referring to the Monetary Authority of Singapore's (MAS) Threat and Vulnerability Risk Assessment (TVRA) guidelines, he noted: "I don't think they look a lot beyond what the TVRA report says. People just see TVRA and they're happy. CCTV, perimeter security, perimeter fencing, that's the level that I see people scrutinizing to."

He recounted his experience at a data centre in Hong Kong that required all visitors to produce their passports to identify themselves: "They didn't rely on electronic security, they made you show your passport at the point of entry. I know it's old fashioned, but it's as safe as anything. [Visitors] have to show the passport with a photo ID before they could enter."

"It's like a two-form authentication," mused Terence Lim, agreeing that a mix of digital and analogue controls may work best. "In most data centres, they would have a list of authorized people who can access it; upon registration, [security personnel] first verifies that I am authorized to come in."

Lim thinks the independent, around-the-clock security of colocation data centres gives them an advantage over an on-premises data centre, which is typically located within less secure commercial buildings. He noted that he once attended a talk by a prominent white hat hacker who demonstrated the cloning of security access passes with nothing more than a home-made wireless card reader. Properly disguised, the hacker was able to steal certain types of access credentials by simply walking near to a victim.

On post-attack analysis

An important consideration that council members highlighted was the importance of the post-attack analysis in the wake of a security breach. "Understanding how a problem happened helps mitigate it the next time round," said Vic Carey. "Anytime you have a problem, it is important to establish the root cause of the problem. You can't mitigate [a problem] unless you know what it was. Did the guy who gained illegal access steal an [access pass] or copied it?"

Understanding the cause of an attack aside, some security measures such as keycodes may simply be too weak to be used alone, said Vic Carey. "Years ago, I stayed at a place secured with a keypad. It wasn't a data centre, but it was a supposedly secure place. Somebody apparently watched from a pair of binoculars and was able to gain entry."

Are there specific security procedures or measures that council members consider crucial for a proper post-attack analysis? "Everything is important," said Lim, with accountability and traceability being key considerations.

"An instruction is being sent out to someone to perform a task. You need to have some form of record in terms of what he's done. What are the information he received? And did he carry out the task based on instructions? These are the bases to even start with the investigation," he explained. "I think anything that needs to be carried out needs to be recorded, including physical access information. When did you go in and come out?"

The value of deterrence

"A lot of people [commit cybercrime] because they think they can get away with it", said Kurokawa. "With proper identity and access management, you can keep the right kind of logs to identify who could be accountable for a breach. When that happens, there is a lower chance of that breach happening because there is going to be repercussions. If you are going to get caught, then you won't do it, right?"

Speaking on cybersecurity in general, he elaborated on the type of security measures that businesses could incorporate to strengthen their safeguards, such as physical security measures and the use of data loss prevention software.

"If there is a malicious copying of files, at least you can say: 'That account was the reason for the breach.' That individual using that account might say, 'Oh, somebody stole my credential' – which does not automatically preclude it being his fault – but at least you have identified the hole and ensured there is accountability," he said.

Deterrence is the reason why some organizations ask for cages even within colocation data centres, agreed Vic Carey. Tenants use it to secure their own area within the data centre under their own set of locks, and typically top it off with an independent CCTV system as an additional layer of deterrence.

Can there be too much security?

Can there be such a thing as too much security though? Kurokawa highlighted his experience of going through frustrating security procedures at some facilities. This can be exacerbated by systems that don't work perfectly, such as biometric scanners that fail or take too long to validate, or when visitors forget to bring along the requisite documentation. While in agreement that it can be a hassle, council members in general felt that any inconvenience is par for the course.

"I think customers do expect that there will be no easy access to the building," said Vic Carey. "In a colocation data centre, you expect to have to change passes, you expect to be escorted, they expect it to be monitored by CCTV… it's the industry norm. And colocation providers [expect] to get photo identification and a name list in advance. I think most people do practice it. I think it is the expectation."

Complaints about security systems can be an indirect compliment and increases the confidence of executives about the security of a company's data, observed Victor Yuk. "If any of my guys go down to the data centre, I will be informed as well. It works for me, because anything can happen; like one of my guys could be compromised."

"In terms of physical access, if you forget the passport, then the fault lies with you. Subsequently you have to remember that's the SOP [standard operating procedure]," said Yuk. He also pointed to how the latest facial recognition systems tend to be faster and more accurate than before, and can alleviate inconvenience while increasing security.

Securing the network

The importance of the network

What would a hypothetical attack on the data centre look like? Council members felt that it is far easier to disrupt or tap communication links than to gain unauthorized admittance to a physical data centre. "I feel [an attack will come by means] of tapping into the network pipes to monitor their traffic. What is really inside the data centre don't really matter. You can get all the things you need from what is being communicated," said John Lee.

Lim compared the data centre to the human brain, which can't do much without a body. "Everything is processed inside [but] you have the pipes and power going into the facility. Sometimes I feel that some of the providers need to pay more attention to such infrastructure. Without the connectivity, it is just another [expensive] building."

People often look at the security of the data centre, and how they can defend against forcible or discreet attacks against the physical facility, but often neglect network security, said Vic Carey. "If terrorists knew about the security measures... they won't attack a data centre. It's too difficult. It's the network infrastructure security that is, in my view, the most important consideration," he said.

Defending the network

But how can data centres defend against network attacks on the cybersecurity front? The most obvious would be through offering protection against the likes of distributed denial-of-service (DDoS) attacks, or the encryption of inter-data centre pipes.

Kurokawa feels that this is where data centre operators can step in: "Rather than having individual [companies] implement DDoS measures themselves, it is always better to do it at scale. It makes more business sense. If everyone wanted to build their own network, there's going to be a lot of wasted capacity. In the long run it is cheaper for everyone."

Lee, however, offered a contrarian viewpoint about the data centre delving too deeply into the cybersecurity sphere, noting that while protection against volumetric DDoS attacks may work, operators are unlikely to have the competency to properly handle cybersecurity. He said that most DDoS attacks are highly targeted affairs against specific web sites or systems, and could be probed by hackers to test their capability to disrupt live websites.

"We won't want the data centres to take care of cyber defences because they won't be contractually liable for it. This will work probably for volumetric DDOS attacks, but not if you talk about services other than DDOS. The data centre operator won't know about your specific needs and requirements as well as yourself." he asked.

On rapid recovery and SLA

Delving deeper into the theme of DDoS attacks, Yuk highlighted the importance of rapid recovery to his business. Unlike a streaming service or e-commerce site where uptime is critical, he explained that he has greater leeway to put up a maintenance page as the outage is being addressed – highlighting the different levels of tolerance to network-related issues.

"I think our basic principal is how fast we recover. [My clients] are fine with a maintenance page, provided we recover quickly. The ability to quickly get back on our feet typically results in hackers losing interest quickly," he said.

DDoS attacks have not been an issue for Yuk since he engaged the services of anti-DDoS providers, barring heavier forms of volumetric attacks in the future. Considering that website defacement used to be one of the biggest headaches, he suggested that future threats are unlikely to be recognizable: “I see now the security trend is moving towards threats such as ransomware, and completely new forms of attacks.”

When it comes to the network, enterprises may prefer tapping into a data centre operator’s connectivity over rolling out their own. Yuk thinks this could be an opportunity for Telin Singapore to offer value added networking capabilities, noting that some businesses may prefer relying on their providers to provide network diversity.

“If you build your own fibre network. There is usually no service level agreement (SLA) for the fibre. [However], there is an SLA for a virtual private cloud. Some organizations might prefer that,” noted Kurokawa.

Standing above the rest

Culture of openness

All things being equal, how can Telin Singapore position itself such that it stands out from the competition on the security front? It boils down to a culture of openness and a spirit of ownership, according to council members. Yuk says he values providers that take ownership and have an attitude of continuous improvement, and who communicates the improvements to customers.

“The whole organization need to take responsibility [for security]. It goes all the way up to the top. When something happens, don’t just blame the rank and file workers who are simply doing what they have been told,” said Yuk. Instead, providers should regularly update their standard operating procedures (SOP) to ensure that the requisite checks and balances are in place.

“We can make one mistake, but it should not be repeated. We put in countermeasures, we put in the SOPs, we mitigate it,” he said. Yuk agreed that it gives him confidence when providers take ownership in such a manner. Together with a positive mindset towards security, these factors are what tell him that he has chosen the right provider.

Educating the customers

Yuk suggested educating customers through electronic newsletters to keep them in the loop about security improvements. This approach has the added advantage of being readily shareable with other business leaders in need of similar solutions, he says.

“With all the new government requirements and the tightening of security, it would be good to send out as an email newsletter if you have implemented something to improve security," said Yuk. He acknowledged that though not all information can be shared publicly, he thinks there are ways around it: "You may not have to mention the confidential details, but mention the improvements in place."

Lim agreed on the need to educate customers, pointing out that Telin Singapore is a technology company: "You need to educate the market about how a certain technology is going to help the company. You need to lead by example, to say that we are willing to take that step and be at the forefront of technology."

While no news is often good news where colocation is concerned, the complete absence of news is a double-edged sword as customers start to forget the importance of the provider, noted Lim. He said: "What are we going to do to prevent certain security attacks from happening? If Telin Singapore is using it and they know how to prevent it, I think it adds confidence to the client. They will think: 'They are already using it, and they know what they are doing'."

Leveraging one's strengths

Telin Singapore is in a unique position of strength as a telecommunications provider and data centre operator, said Lim. He observed that not all telecommunication providers have access to their own data centre facilities, and that they can be lacklustre when it comes to offering genuine redundancy and reliability.

"You'll be surprised some of them put little emphasis on preventive solutions [against failures]. They just say: 'Don't worry, we have diverse network' but which may not necessarily be the case. If a [saboteur] knows what he is doing and which part of the network to disable, then the data centre can be reduced to a shell without connectivity," he said.

A new way of selling

In closing, Lee threw out a curveball by suggesting the idea of disrupting the colocation industry with cloud-like transparency in pricing. The idea struck a chord with council members, who recounted the often-lengthy lead times to get pricing information.

"Why are data centre providers not moving into the cloud market where there is transparency in pricing? The cloud is so popular because of transparency. It is never about what you are doing, it's just because of price. If you can get the right price, the right product, you win the [business]," he said.

"Data centre operators [currently] have the mindset that they are in a backward industry. They think: 'Contact the account manager, leave your contact details, and we will get back to you'," he said, noting that quotations can take months to materialize in some instances.

Conclusion: Establishing trust, building relationship

While there is no consensus of what constitutes a truly secure data centre, an environment of openness without finger-pointing is an essential ingredient, says council members. And though they acknowledged that security measures can be a hassle at times, they also consider it as a necessary aspect of keeping a facility properly secured.

Council members are in favour of timely updates from their providers about the various security improvements and pre-emptive measures as they are adopted. Ultimately, improved communication is the linchpin of establishing a strong relationship of trust between the provider and its customers.

About Telin Singapore

Telin Singapore, a subsidiary of PT Telkom Group, is the data centre provider of choice through best-in-class, integrated solutions. Telin Singapore currently manages flexible, modular and scalable data centre facilities in Singapore that are enhanced by proprietary-owned, seamless submarine cables connectivity from Indonesia and Singapore to the rest of the world. Telin Singapore's Tier III & Tier IV certified data centre facilities embrace the company's commitment to deliver world-class ICT solutions that are scalable and flexible to fit any customer's needs.

For more information, please visit www.telin.sg.