First Data
beyond the transaction

Asia Pacific Cyber Attack Alert: Why a Better Defense Strategy is Essential

Tapping the latest technology and collaborative efforts are the starting points

The costs, volume, and sophistication of cyber attacks are growing exponentially, and this trend is predicted to continue indefinitely. Asia Pacific is highly susceptible to such attacks, and the region is two times more likely to be targeted by advanced cyber attacks than the rest of the world. The average financial losses due to security incidents are estimated at more than US $1.6 million per company.

The fact is, while attack methods and technologies have evolved tremendously in the past decade, defensive methods and technologies have not. And while the agility of attackers is high and growing, defence mechanisms remain bogged down by rigid processes, slow information diffusion and tedious regulations.

The problem is further exacerbated by changes in the modern world that make systems more vulnerable. Such changes include the move to mobile technologies, greater reliance on general-purpose devices, and greater dependence on external parties such as cloud service providers. The rapid emergence of these technologies has improved efficiency and convenience, but has also increased the number of ways that organizations can be attacked.

For example, the recent Target data breach in the United States started with Target providing its air-conditioning sub-contractor with external network access. Attackers then broke into the retailer's network using network credentials stolen from the sub-contractor. The fact that it was an air-conditioning vendor, and not a high-tech service provider that may usually be associated with technology risks, only emphasizes how hard it is to properly manage these issues.

Asia Pacific as a region needs to focus on four key areas to collectively work on our cyber-preparedness to stay ahead in cyber security.

More effective cyber metrics

It is true that you cannot manage what you cannot measure, but the fact remains that cyber metrics and theories lack maturity and rigour. Even core ideas like "risk" and "vulnerability" are defined differently by different groups. There is no clear, accurate and defensible way to measure success or failure, and this causes enterprises to struggle with making security and risk management decisions. Furthermore, these fundamental problems are only getting worse, since the limited metrics of today are growing even less useful as the world changes.

For example, risk metrics today do a particularly poor job of capturing and analyzing the "domino effect" of attacks spreading through inter-dependent systems, but our systems are becoming more and more inter-dependent with every passing day.

There is a real need for effective real-time cyber metrics that can help put enterprises in a proactive stance regarding cyber security. Effective metrics

Asia Pacific Cyber Attack Alert: Why a Better Defense Strategy is Essential

can help bring visibility and awareness to cyber threats and quantify the need for companies to adopt security best practices.

The key example of this for the next five years is going to be security metrics in a world of distributed vulnerabilities and distributed responsibilities (both within organizations, and more importantly, between organizations), as highlighted in the Target breach. In coming years, companies will increasingly be expected to provide detailed insight into their security posture to their customers.

Furthermore, that insight will need to be near-real-time. Today's "once-a-year testimony" of a company's security posture, like SSAE 16, is better than nothing, but will be seen as increasingly inadequate as the world moves faster and faster. By the end of the decade, vendors will be expected to provide evidence of their security status once a minute, not once a year.

Technologies and processes for faster and more targeted responses

Cyber attacks today can penetrate their target and take over in a few seconds, and the region needs to adopt a security posture that gives us time to respond rapidly, even in the face of lightning-fast attacks.

Recent research has shown typical enterprise response time to be more than 210 days from initial breach to detection, with the majority (64 per cent) taking more than three months to detect system intrusions. Post detection, enterprises on average take a further three months to rectify the damage.

While it is clear that this situation is profoundly inadequate, it can only be improved when organizations have better real-time insight into their world, and better access to faster, smarter, and safer response technologies. Otherwise, organizations will be too slow to notice, or unwilling to act quickly because they fear making things worse.

The necessary insight is the simpler issue, and is just a matter of better data collection and management. The ability to respond more quickly and intelligently is far more challenging, and will require fundamental architectural and systemic changes. One advantage the Asia Pacific has over some western countries is that without the curse of (legacy) infrastructure, it can more quickly and directly adopt these sorts of new networks.

More efficient and defensive use of emerging technologies

Many enterprises are still running dated systems and technologies that are highly vulnerable to cyber attacks. The general lack of security expertise and low adoption of risk management technologies put them at a disadvantage when combating a cyber assault because they are trying to meet 21st century attacks with 20th century defences.

The region needs to engage aggressively with emerging technologies, using them as a shield against cyber criminals. For example, Big Data can be harnessed to monitor risks, bad actors, and the global "cyber weather" in a way that individual attackers will find hard to match.

The value of Big Data will only grow as instrumentation becomes more ubiquitous and intelligent, as part of the Internet of Things. Virtualization and the Cloud can allow for better resource management and resistance to things like Distributed Denial of Service (DDOS) attacks. Even older technologies like encryption will remain powerful defensive tools.

Asia Pacific Cyber Attack Alert: Why a Better Defense Strategy is Essential

Better framework for information sharing

The interconnectedness of Asia Pacific's digital economy means that security is increasingly communal and distributed, which in turn means that there is a heightened need for a timelier, more granular, and more insightful framework for information sharing. Collaborative status and solution-sharing helps enterprises detect potential risks earlier and prevent further cyber attacks. It also makes cyber defense more cost-efficient by distributing costs and reducing duplication.

There has been some weak movement towards such a sharing framework in countries like the US, but there are major concerns around issues such as admission of liability, privacy and intellectual property.

Unfortunately, the US regulatory system is poorly equipped to address such concerns, but the Singaporean system of government is better aligned at a structural level with this sort of top-down and long-term initiative. Singapore's recent partnership with network security company FireEye to equip more security professionals with the expertise to defend, detect and respond to cyber threats is also a move in the right direction.

While these four major action plans are each individually necessary, they also reinforce and support each other: better metrics obviously make information sharing more effective and valuable, and emerging technologies allow for better monitoring and fast-response options. Together, they form important stepping stones in the roadmap for Asia Pacific to become safer and smarter in the 21st century.

Conclusion

Data theft processes evolve quickly, and your approach to security needs to keep up. The best way to protect your business is with a thorough and ongoing data security program. A little preventative work goes a long way, so check with your payments provider on whether they are armed with solutions that will help protect you and your customers.

First Data has a range of security solutions for merchants. Talk to your First Data Business Consultant to learn about affordable, easy to deploy security solutions that can mitigate potential cyber attacks and secure your customers' transactions from start to finish.

For more information, contact your Business Consultant or visit firstdata.com.

Beyond the transaction℠