HIGH PERFORMANCE SECURITY
REPORT 2017 - SINGAPORE

BUILDING CONFIDENCE

FACING THE CYBERSECURITY CONUNDRUM IN SINGAPORE

Accenture Security

BUILDING SECURITY CONFIDENCE IN SINGAPORE'S CYBER ECOSYSTEM

Being an open and connected economy, Singapore is one of the most vulnerable major business hubs in Asia Pacific to cyber security attacks.

As digital technology becomes increasingly pervasive, there is a growing likelihood of a cyber breach among organizations and government agencies alike. Recognizing the threats and impact a successful cyber-attack can have on the local economy, businesses and government services, Singapore in October 2016 unveiled a cybersecurity strategy to coordinate efforts and facilitate global partnerships to achieve its goals of a resilient and trusted cyber ecosystem.

Being cyber-safe cannot, however, just be a national directive. It requires collaboration by the government, businesses and individuals. Today, cybersecurity is a boardroom issue as the risk of breaches adversely affecting share prices and creating corporate scandals is very real. While cybersecurity awareness is on the rise among organizations in Singapore, investments need to be made in alignment to risks and needs, with the effectiveness of security measurable.

This inaugural High Performance Security Report highlights that businesses in Singapore share misplaced confidence while struggling to identify threats. To grow confidently, it is imperative that security programs continue to improve their capabilities to detect and prevent advanced attack scenarios.

In Singapore's aspiration to be a Smart Nation, a comprehensive cyber defense is not an option. Devising strategic and targeted plans to manage cyber risks as businesses embrace new technologies to innovate and grow is a more realistic choice, and one that is essential for the economy's continued development.

A DANGEROUS DISCONNECT

One in four focused breach attempts get through, yet most organizations in Singapore are "confident" in their ability to protect the enterprise.

Reacting to cyber breaches is an operational reality for most organizations today, and it's accompanied by increasing amounts of chaos and dissonance. A recent Accenture survey[1] of 124 security executives representing large enterprises in Singapore revealed that roughly one in four focused and targeted breach attempts succeeded, yet respondents remain confident that they are doing the right things in terms of cybersecurity, with 77 percent indicating confidence in their cybersecurity strategies. This dissonance may partially result from attempts to toe the company line, but it reveals a cybersecurity disconnect.

While the failure rate in preventing security breaches in Singapore is lower than the global rate of one in three, it is still alarmingly high. And this is amplified when you understand the sheer volume of attacks. In addition to the thousands to millions of random attempts that company networks repel each week, on average, an organization will face more than a hundred focused and targeted breach attempts every year, and respondents in Singapore say one in four of these will result in a successful security breach. That's two to three effective attacks per month.

The length of time taken to detect these security breaches often compounds the problem. Consistent with other studies, 49 percent of Accenture survey respondents in Singapore admit it takes "months" to detect successful breaches (global average: 51 percent), while another 23 percent identify them "within a year" or longer (global average: 17 percent). Additionally, internal security teams discover only 68 percent of effective breaches (global average: 65 percent), with employees, law enforcement and "white hats" (e.g., "ethical" hackers) finding most of the rest.

All in all, security teams in close to half of surveyed companies in Singapore (45 percent) discovered 61 to 70 percent of breach attempts.

Part of the security challenge is prioritizing where to focus resources to effectively protect the organization. Over two-fifths (45 percent) of survey respondents say internal breaches made by malicious insiders have the greatest cybersecurity impact. Even so, only 44 percent of respondents in Singapore are confident in their organizations' abilities to monitor for breaches. That compares with 50 percent in the UK and the global average of 38 percent.

Further, despite this explicit recognition of the impact of internal compromises, many respondents continue to focus on external security issues. For example, 44 percent prioritize heightened capabilities in perimeter-based controls against outsiders (global average: 58 percent), instead of pivoting to address high-impact internal threats. Ultimately, many remain unsure of their ability to manage internal compromises with the greatest cybersecurity impact even as they continue to prioritize external initiatives that produce the lowest return on investment.

1 The global survey polled 2,000 security executives representing companies with annual revenues of US$1 billion or more from 12 industries and 15 countries across North and South America, Europe and Asia Pacific.

One in four focused attacks results in a security breach.

MISPLACED CONFIDENCE DESPITE HIGH-IMPACT BREACHES

One in four focused attacks in Singapore results in a breach; internal compromises have a major impact; and security teams admit they lack the necessary tools to detect breaches (and, in a third of cases, don't discover the breaches at all). Nevertheless, three out of four respondents express confidence in their abilities to protect their organizations from cyberattacks. Not only that, 69 percent say that their organizations have completely embedded cybersecurity into their cultures and 82 percent indicate that it is a board-level concern supported by their top executives.

One potential contributor to this dissonance is that there is still too much emphasis on compliance, in part because it seems more tangible and measurable. Many cybersecurity departments measure performance based on achieving compliance objectives as opposed to mitigating negative business impacts. Security control frameworks and compliance programs are extremely helpful in defining foundational thinking; however, they often fail to reflect real-world dynamics. Just as adhering to generally accepted accounting principles does not ensure protection against financial fraud, cybersecurity compliance alone will not protect a company from successful incursions.

What's more, the sentiment among those surveyed suggests organizations should expect more of the same. For example, given extra budget, 41 to 52 percent of respondents in Singapore would double down on their current cybersecurity priorities — investments that are failing to prevent breaches.

These priorities include protecting the company's reputation (52 percent; global average: 54 percent), safeguarding company information (48 percent; global average: 47 percent), and protecting customer data (41 percent; global average: 44 percent). Far fewer organizations would invest the extra cash in efforts that more directly affect their bottom lines, such as mitigating against financial losses (31 percent; global average: 28 percent) or investing in cybersecurity training (8 percent; global average: 17 percent) — an area Accenture research reveals as an increasingly important cybersecurity pillar. In our "State of Cybersecurity and Digital Trust[2]" research published in June 2016, 31 percent of respondents identified a lack of training or staffing budget as the single biggest inhibitor to cybersecurity readiness.

With the average total IT budget on cybersecurity among organizations in Singapore running at 8.3 percent, it compares well with the global average of 8.2 percent. Companies in France spend the most—9.4 percent—while businesses in the US (8.0 percent) and Australia (7.6 percent) spend the least.

And in Singapore, 23 percent of organizations polled take up to a year or more to detect a successful attack. This compares with the 30 percent in the US and 26 percent in the UK, where enterprises take the same time to discover a successful breach.

But even as two-fifths of organizations in Singapore plan to double down on customer data protection, if given extra budget, cybersecurity strategies among 35 percent of businesses in Singapore focus less on the protecting of consumer information than the global average (49 percent).

Another example of potential cognitive dissonance: While three-quarters of survey respondents in Singapore say they have high cybersecurity confidence levels, far fewer indicate similar confidence in their organization's ability to deal with breaches. For example, only 44 percent claim they have confidence in their organization's ability to monitor for breaches, and 38 percent said the same about minimizing disruptions.

2 The State of Cybersecurity and Digital Trust 2016, Copyright © 2016, Accenture and HfS Research, Ltd https://www.accenture.com/us-en/insight-cybersecurity-digital-trust-2016

FORCING PERCEPTION TO FACE REALITY

To survive in this contradictory and increasingly risky landscape, organizations need to reboot their approaches to cybersecurity.

Protecting a company requires an end-to-end approach that considers threats across the spectrum of the industry-specific value chain and the company's ecosystem, identifying and minimizing business exposure and focusing on protecting priority assets. The following steps can help organizations to overcome limited perceptions and deal effectively with the high-impact cyber threats they face.

DEFINE CYBERSECURITY SUCCESS

Organizations need to answer several critical questions in order to reframe their cybersecurity perceptions and build a new definition of success:

- **Are you confident that you have identified all priority business data assets and their location?**
- **Are you able to defend the organization from a motivated adversary?**
- **Do you have the tools and techniques to react and respond to a targeted attack?**
- **Do you know what the adversary is really after?**
- **How often does your organization "practice" its plan to get better at responses?**
- **How do these attacks affect your business?**
- **Do you have the right alignment, structure, team members, and other resources to execute your cybersecurity mission?**

We believe security organizations need to improve the alignment of their cybersecurity strategies with business imperatives. And while many firms are clearly making progress in compliance and risk management, security programs need to continue to improve their ability to detect and prevent advanced attack scenarios.

PRESSURE-TEST SECURITY CAPABILITIES THE WAY ADVERSARIES DO

Organizations need to establish a realistic assessment of their capabilities to protect against high-impact threats, whether internal or external. Pressure-testing company defenses can help leaders understand whether they can withstand a targeted, focused attack.

PROTECT FROM THE INSIDE OUT – STOP INTERNAL COMPROMISES IN THEIR TRACKS

Many organizations fail to limit internal access to key information, monitor for unusual employee network activities or regularly review access. Adversaries know what they want, but they don't know where key assets live. In contrast, cybersecurity professionals have the advantage of knowing which key assets need to be protected. By prioritizing energy on these key assets organizations can build a more effective cybersecurity foundation: instead of attempting to anticipate a seemingly infinite variety of external breach possibilities, organizations can concentrate on the relatively fewer internal incursions that have the greatest impact.

INVEST TO INNOVATE AND OUTMANEUVER

When it comes to cybersecurity, standing still is no longer an option. Organizations need to innovate continually to stay ahead of potential attackers, which may require redirecting some resources to new strategies and programs rather than investing more in current programs.

But where to invest?

To improve cybersecurity capabilities and strengthen resilience to cyberattacks, organizations can examine the following seven key domains. These alone will not be a cure-all against malicious breach attempts; continual and systematic security investments are still required. Almost one third of enterprises in Singapore plan to at least double their cybersecurity investment in the next three years. That's significantly higher than the global average of 16 percent.

Within each of the following domains, there are sub-domains in which approximately 40 percent of companies in Singapore are competent. No single company, however, is excelling at every sub-domain.

Specifically, enterprises in Singapore and the wider ASEAN economy need to focus on the first four areas to outmaneuver and defeat cyber attackers.

Business alignment assesses cybersecurity incident scenarios to better understand those that could materially affect the business, and identifies key drivers, decision points, and barriers to the development of remediation and transformation strategies.

Governance and leadership focuses on cybersecurity accountability, nurtures a security-minded culture, measures and reports cybersecurity performance, develops attractive cybersecurity incentives for employees and creates a clear-cut cybersecurity chain of command.

Cyber response readiness means having a robust response plan, strong cyber incident communications, tested plans for the protection and recovery of key assets, effective cyber incident escalation paths and the ability to ensure solid stakeholder involvement across all business functions.

Investment efficiency is understanding investments across cybersecurity domains and the allocation of funding and resources. It also compares organizational investments against industry benchmarks, organizational business objectives, and cybersecurity trends. In addition, generating key performance indicators to measure the effectiveness of long-term strategic security investments is key.

Cyber resilience is operational excellence in the face of disruptive cyber adversaries. From technology and process foundations to cyber incidence recovery performance, the company seeks to understand the threat landscape, designs key asset protection approaches and uses "design for resilience" techniques to limit a cyber attack's impact.

The extended ecosystem, which comprises different actors with varying business objectives and operational requirements, should be ready to cooperate during crisis management, develop third-party cybersecurity clauses and agreements, and focus on regulatory compliance.

Strategic threat context explores cybersecurity threats, including an analysis of competitive and geo-political risks, peer monitoring, and other areas to align the security program with the business strategy.

MAKE SECURITY EVERYONE'S JOB AND MAKE IT MEASURABLE

Employees also play a critical role in detecting and potentially preventing breaches. More than half of survey respondents in Singapore said that for breaches not detected by the security team, the company learned about them most frequently from employees. In fact, people represent its first line of defense, which is why organizations need to prioritize training and continually refresh cyber talent across the business.

Making every employee understand and adopt security as a way of life in the office goes beyond ticking boxes for compliance requirements such as firewalls or anti-virus programs. Today, cybersecurity is a boardroom issue as the risk of breaches adversely affecting stock prices and creating corporate scandals is very real. Business and cybersecurity team must therefore have an agreed set of clear metrics to monitor results. Without the ability to quantify security risks and measure success, it would be almost impossible to identify loopholes and respond effectively.

Three in five respondents from Singapore are confident in their ability to measure the impact of a breach compared with the global average of 47 percent.

60% vs. **47%**

SINGAPORE **GLOBAL**

To build a culture of cybersecurity awareness, organizations should view state-of-the-art cybersecurity as an organizational mindset — one capable of continually evolving and adapting to counter changing threats. To foster a culture of cybersecurity and digital trust, organizations must emphasize an adaptive, evolutionary approach to addressing all aspects of security on an ongoing basis. Many enterprise cybersecurity teams still struggle to overcome the gap between the security talent they need and the talent available. In a separate **Accenture survey on digital trust**, 42 percent of respondents said they have sufficient security technology budgets, but need additional budget for hiring security talent and training.

42% OF ORGANIZATIONS NEED ADDITIONAL BUDGET FOR HIRING SECURITY TALENT AND/OR TRAINING.

LEAD FROM THE TOP

While the cybersecurity issue has gained full attention on company agendas, many chief information security officers (CISOs) may feel locked out of the C-suite. This isn't necessarily a conscious snub on the part of organizations; instead, it's a question of the security organization's maturity level. To succeed, many CISOs need to step beyond their comfort zones (e.g. compliance audits, cyber technology) and materially engage with enterprise leadership on a day-to-day basis to effectively discuss the business issues at the core of cybersecurity.

Doing so will require them to speak the language of business in order to make the case that the cybersecurity team represents a critical pillar in the battle to protect company value. At the same time, the CISO needs to build the board's cyber literacy with the goal of making it a priority equal to business risk assessment.

Build the board's cyber literacy with the goal of making it an equal priority to business risk assessment.

BUILD ON PAST LESSONS

Effective cybersecurity requires organizations to achieve greater maturity and improve its ability to protect the business from devastating losses. Fortunately, organizations have done this before, with efforts such as the huge push toward higher quality in products and services over the past three decades. For many organizations, product and services quality remained an afterthought until new competitors arrived offering superior quality at lower prices. When such competition affects the bottom line, organizations quickly began to act and factor quality into the equation. A similar reaction is beginning to happen now with cybersecurity. Enterprises are no longer treating it as an afterthought. As their digital security strategies and organizations mature and new solutions emerge, companies that tie cybersecurity efforts to real business needs will gain justifiable confidence in their ability to deal with cyber threats.

ABOUT ACCENTURE

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world's largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With approximately 384,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at www.accenture.com.

ABOUT ACCENTURE RESEARCH

Accenture Research is a global team of industry and digital analysts who create data-driven insights to identify disruptors, opportunities and risks for Accenture and its clients. Using innovative business research techniques such as economic value modeling, analytics, crowdsourcing, expert networks, surveys, data visualization and research with academic and business partners they create hundreds of points of views published by Accenture every year.

ABOUT THE ACCENTURE GLOBAL HIGH PERFORMANCE SECURITY RESEARCH

In 2016 Accenture Security surveyed 2,000 executives from 12 industries and 15 countries across North and South America, Europe and Asia Pacific. The survey objective was to understand the extent to which companies prioritize security, how comprehensive security plans are, how resilient companies are with regard to security, and the level of spend for security. The survey aimed to measure security capabilities across seven cybersecurity strategy domains identified by Accenture: business alignment, cyber response readiness, strategic threat intelligence, cyber resilience, investment efficiency, governance and leadership, and the extended ecosystem. More than 50 percent of respondents were key decision-makers in cybersecurity strategy and spending, including security, IT and business executives at director level and above at companies with revenues of US$1 billion or more.

CONTRIBUTORS

Kevin Richards, Managing Director, North America
Ryan M. LaSalle, Managing Director, Growth & Strategy
Rik Parker, Managing Director
David M. Cooper, Senior Manager
Joshua Kennedy-White, Managing Director, Asia-Pacific Security
Freddy Wee, Managing Director, ASEAN Security
Mark Du Plessis, Senior Manager, ASEAN Security

16-4213