AMERICAN CHAMBER OF COMMERCE

2019 CYBERSECURITY SURVEY

EXECUTIVE SUMMARY

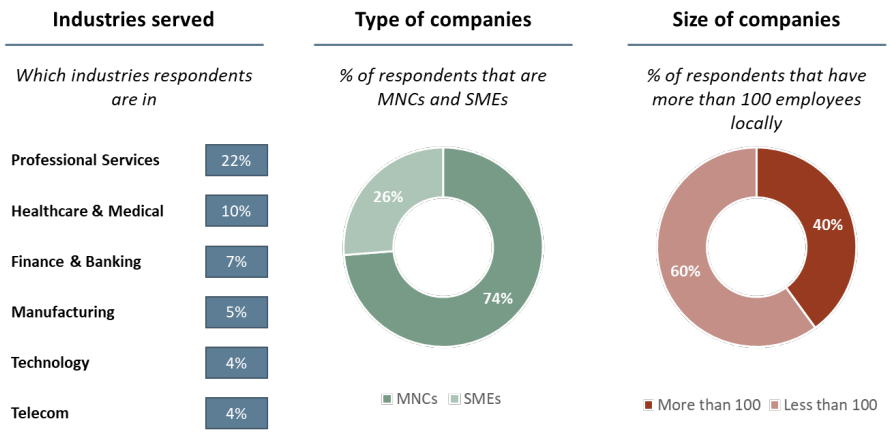
A thriving ecosystem of cybersecurity products, services, and strategies fueled by a growing awareness of the damages and liabilities arising from cyber breaches are increasingly dominating C-Suite and Boardroom conversations around enterprise risk. In July 2019, AmCham conducted an online survey of its members to better understand how cybersecurity is affecting businesses in Singapore.

Our survey revealed that cybersecurity remains a key concern for business leaders. While respondents report a myriad of cybersecurity threats and experiences, there is a discernable pattern: malware, phishing and insider threats continue to pose significant security challenges to organizations. To get ahead, forward-thinking organizations must invest in diverse talent with new skills and viewpoints to augment traditional information security teams; solutions that lead with artificial intelligence and automation; and security structures that take into account an organization's unique culture and threat profile.

METHODOLOGY AND DEMOGRAPHICS

An online survey of executives was conducted from July 2019 to August 2019. Questions targeted key areas of concern ranging from locally-based cybersecurity practitioners, technology investment, and workforce awareness. Over 70% of the surveyed respondents were from multi-national companies operating in a wide range of industries spanning professional services and consulting, healthcare, finance and banking, manufacturing and engineering. All companies surveyed had a local presence in Singapore with 60% having more than 100 employees locally.

EXHIBIT 1: SURVEY DEMOGRAPHICS



FINDINGS

Our analysis of the survey data identifies four (4) key findings.

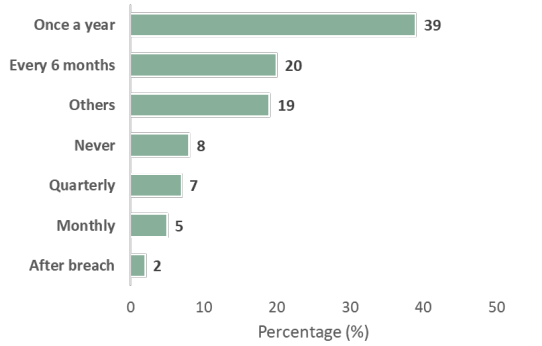
1. ***Cyber risk has elevated to the boardroom.*** Cybersecurity has grown in significance amongst corporate boards and senior management due to the potential for severe consequences arising from security failures, particularly as concerns revenue generation, operational integrity, and brand reputation. In our survey, over 70% of respondents shared that cybersecurity initiatives were driven directly from their board of directors or senior management. As cyber threats become increasingly prevalent, companies should continue to prioritize cyber risk management as a key enabler for driving business growth and performance.

2. ***Malware and phishing remain top cyber concerns.*** Over 80% of respondents cited malware and phishing as the top cyber-threats faced by businesses today. This is not surprising as phishing emails are inexpensive to generate and can be accurate in targeting recipients. While most companies (79%) have deployed mitigating security controls, such as endpoint protection, the rise of new adversary technologies, such as AI-enhanced malware, will make detection increasingly difficult. Looking ahead, phishing is likely to dominate the cyber threat landscape as it will remain an effective approach for compromising the integrity of an organization. Companies should invest in advanced security defensive efforts, such as cyber analytics and Advanced Threat Hunt, as a means to force bad actors to seek other vulnerabilities and means of exploitation.

3. **Cyber awareness remains low on the agenda.** The majority of respondents reported they conduct cyber awareness trainings only once a year. As priority is placed on Cybersecurity initiatives from the Boardroom, a top-down approach to raising awareness is necessary to instill a security-conscious culture. The predominance of internal staff hired to defend against security incidents suggests that companies would be wise to proactively invest in training to better understand the latest threats and how to prevent and/or mitigate against those threats.

EXHIBIT 2: CYBERSECURITY AWARENESS

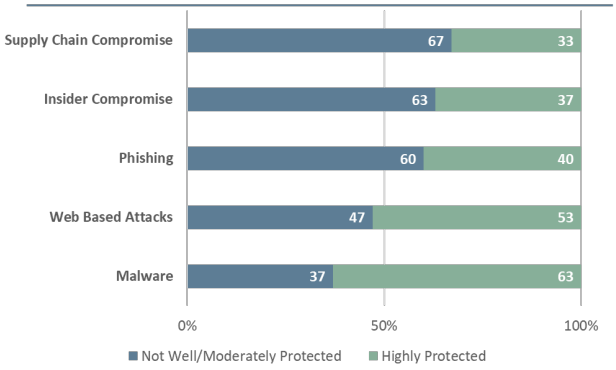
Q: How often do your employees in the Singapore office undergo cyber security awareness training?



4. ***Insider attacks are on the rise.*** Over sixty percent of the companies surveyed feel they are vulnerable to insider threats arising from current and former employees, contractors, as well as third-party vendors/partners. Insider attacks are certainly on the rise; Verizon's 2018 Data Breach Investigation Report stated that such attacks account for 28% of all data breaches. As systems become more interconnected, companies should focus on enhancing relevant controls, such as Identity Access Management and Privilege Access Management, as well as leverage user entity behavior analytics to enhance detection and response efforts.

EXHIBIT 3: INSIDER THREATS

Q: Rate how you feel your company is protected against the following threats?



About AmCham

Established in 1973, the American Chamber of Commerce in Singapore (AmCham) is the largest and the most active international business association in Singapore and Southeast Asia, with over 5,200 members representing more than 700 companies. Our Chamber is comprised of 13 industry-specific committees and conducts nearly 250 events per year. AmCham is a forward-thinking, business-progressive association. Our mission is to create value for our members by providing advocacy, business insights, and connections. Our membership includes American companies and Singaporean and third-country companies with significant U.S. business interests. AmCham is an independent, non-partisan business organization. We are a member of the 28-chamber-strong AmChams of Asia Pacific (AAP). Our goal is to provide the information and facilitate the access and connections that give members insight into the local, regional, and global operating environment, enhance their professional capabilities, and enable them to make well-informed business decisions.

About Booz Allen

Booz Allen Hamilton has been at the forefront of strategy and technology for more than 100 years. Today, the firm provides management and technology consulting and engineering services to leading Fortune 500 corporations, governments, and not-for-profits across the globe. Booz Allen partners with public and private sector clients to solve their most difficult challenges through a combination of consulting, analytics, mission operations, technology, systems delivery, cybersecurity, engineering, and innovation expertise. With international headquarters in McLean, Virginia, the firm employs more than 25,800 people globally and had revenue of $6.70 billion for the 12 months ended March 31, 2019. To learn more, visit BoozAllen.com. (NYSE: BAH)