Cyber Security

Technology Overview

4.1.1 Cyber Security deals with the evolving cyber threat landscape and highly skilled threat actors. Cyber Security is becoming an increasingly important concern as communications, monitoring and operations of business and critical cyber physical infrastructure increasingly rely on networks and the Internet. Since such information systems are so intrinsically connected, any attack on or compromise of these systems by malicious users can cause catastrophic economic damage or affect human lives.

4.1.2 Cyber-attacks can also disrupt critical public infrastructure like utilities (e.g. power, water, gas) and communications (e.g. public communication networks, sensor networks).

4.1.3 It is therefore critical to ensure robust security of systems, uphold privacy and confidentiality, and enable adaptive self-recovery and response capabilities in the event of any system security breach.

4.1.4 Comprehensive security management involves three goals and three phases. These security solutions should work to achieve the following three goals:

(1) Confidentiality: Preventing unauthorised access of private information.

(2) Integrity: Keeping data accurate, consistent and secure over its life.

(3) Availability: Ensuring system and data is readily accessible.

4.1.5 The goals can be accomplished in three phases:

(1) Preparation (Before incident)

(2) Response (During incident)

(3) Recovery (After incident)

4.1.6 The following are major threat groups that can compromise cyber security.

(1) State-sponsored: The Actor or group is employed by the government or large organisations. They typically conduct intelligence gathering and economic espionage over a long period of time.

(2) Cyber criminals/terrorists: Cyber criminals are usually financially motivated, while terrorists seek destruction with a for propagandistic goals. They are increasingly more sophisticated and mature in their operations.

(3) Hacktivists: They are usually issue or cause-driven. They are often not destructive.

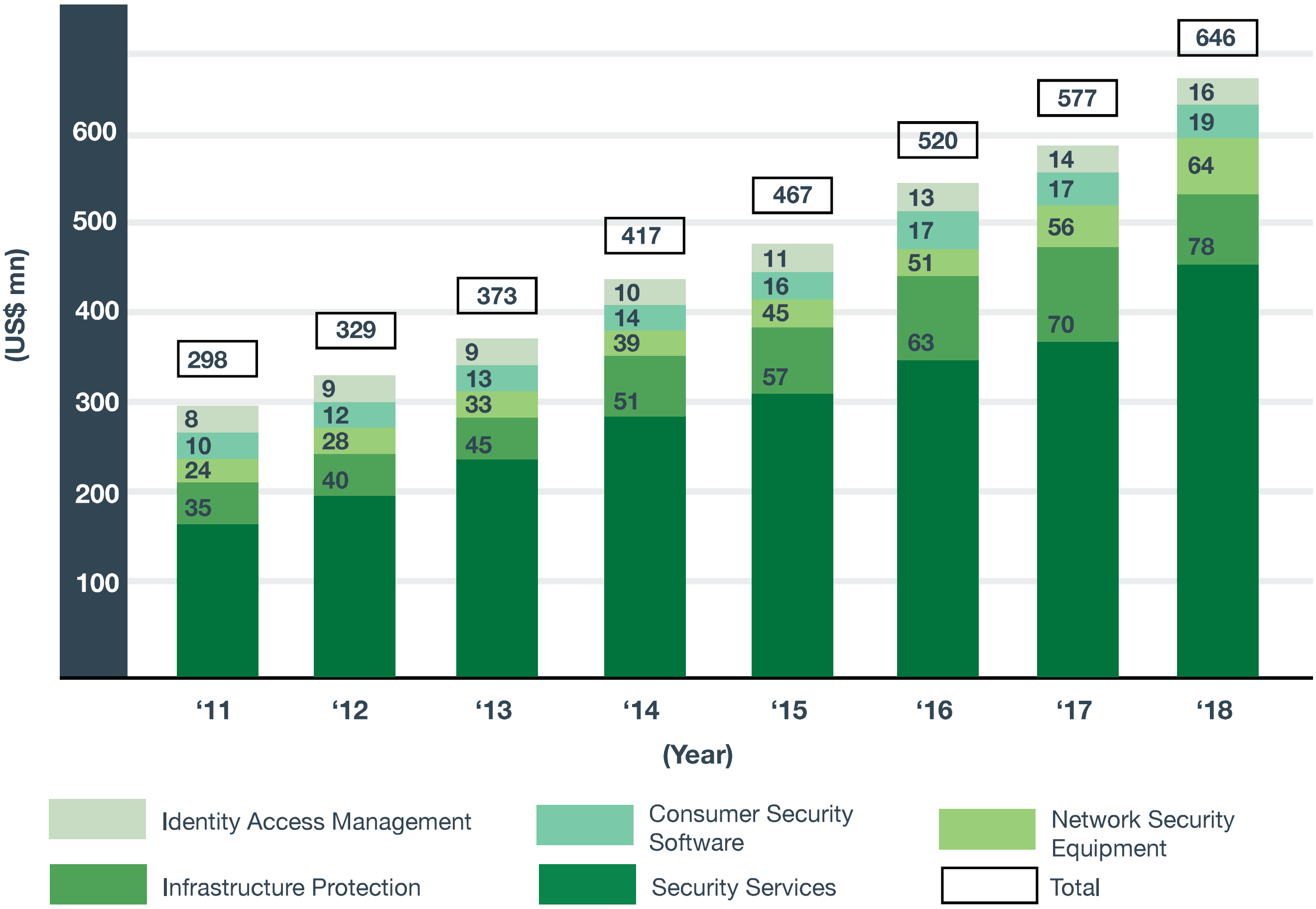
4.1.7 Cyber Security affects system end-users, owners, infrastructure providers and regulatory bodies, all of whom have varying interests in having secure systems. End-users, with new mobile options to access these systems them readily available on-demand, and expect effective and reliable function without compromise on confidentiality and privacy.

Market Size

4.2.1 With the global mobile transaction volume and value is expected grow around 42 per cent annually between 2011 and 2016[16], the threat of cybercrime in the mobile space will become greater too. Cybercrime is estimated to cost the global economy about US$375 billion to US$575 billion yearly, which is about 15 per cent to 20 per cent of the Internet's value[17]. This calls for effective protection of users' data, finances and financial transactions from cyber criminals.

4.2.2 The global market for Cyber Security is expected to reach US$102 billion in 2018, and Singapore's addressable market globally is expected to exceed US$600 million in 2018[18].

Singapore's Addressable Cyber Security Market Globally, 2011-18
CAGR = Compound Annual Growth Rate



4.2.3 Investment in Cyber Security by public institutions and venture capitalists in last few years were mostly in monitoring, detection and protection technologies, and privacy and confidentiality preserving. Private Mergers and Acquisitions focused more on monitoring, detection and protection technologies[19].

Trends

4.3.1 Mobile: There are more than a million malware apps and up to 2.3 million grayware apps that display undesirable behaviour[20], and this number is expected to increase as mobile users increasingly perform financial transactions online. 2014 saw a resurgence of scam campaigns through SMSes that target victims mainly scraped off classified ad websites. Wearable fitness and personal health devices have been breached with proof of concept attacks, and researchers have demonstrated how implanted insulin pumps can be lethally hacked to administer incorrect dosages from up to 100m away. It is also worrying that nearly 20 per cent of readily available healthcare apps transmit user credentials without encryption, and more than half do not have privacy policies.

4.3.2 Web Threats: High profile vulnerabilities are used to compromise servers instead of end points. For instance the "HeartBleed" vulnerability in the OpenSSL cryptographic software library crippled 17 per cent of SSL web servers and massively affected businesses and individuals. "Shellshock" hijacks Bash to execute code in variables. Such attacks often come easily in public Wi-Fi hotspots. Given their widespread existence, they become very hot targets for attackers and are exploited within hours of disclosure.

4.3.3 Targeted Attacks: There are now hacking tools to target specific sectors. "Reign" provided powerful tools to spy on governments, infrastructure operators and businesses, and its sophistication suggests a significant investment of resources. "Trula" used spear-phishing and watering hole attacks to target governments and embassies. "Dragonfly", a cyber-espionage campaign attack against 84 countries, targets the energy sector and crippled a number of them.

4.3.4 Advanced Persistent Threats (APTs): APTs operate in the public and private sectors for espionage purposes. For instance, the DarkHotel APT, warned about in late 2014, lurked within servers and Wi-Fi networks at luxury hotels targeting unsuspecting business and Government executives who check in[21]. Once infected, the malware will sit quietly for six months before communicating with its command-and-control server. It will then delete itself from the hotel's servers days after the targeted executive left the hotel. Although this vulnerability appeared in May 2012, there is evidence that DarkHotel had already been in operation since 2007.

4.3.5 Hacking and Activism (Hacktivism): Hacktivists use cyber-attacks to voice their displeasure over political, social and moral issues, and has become more rampant over the past few years. Verizon has said that hacktivists stole about 58 per cent of data in addition to usual acts of website defacement and denial of service attacks[22].

In November 2013, hactivist group "Anonymous" attacked websites of government to voice their displeasure over the earlier-announced Internet licensing framework. Anonymous had also launched cyber-attacks in other countries. These include attacks on the Ferguson police website over the shooting of Michael Brown[23], attacks on the Pakistani government websites over political reasons[24] and the attacks on Israeli government websites over Operation Protective Edge[25].

Companies and governments around the world are thus urged to address the vulnerabilities of their systems and strengthen their defences against hacktivists' cyber-attacks.

Technology Roadmap

4.4.1 This table reflects the industry's view of the likely evolution and mainstream adoption of Cyber Security.

Demand Drivers	1-2 Years	3-5 Years	>5 Years
Preparation – Systems/ Networks Design & Analysis	**Security By Design**	**Non Traditional Designs**	**Formal Methods in Security Designs**
	• Secured system design/ Security design life cycle (SDLC) • Advanced network security • Secure coding • Schema for specifying system security	• Alternative system architectures	• Provably secure system architectures • Top-to-bottom formal analysis of systems trustworthiness
Preparation – Security Testing & Diagnostics	**Component Testing tools**	**Application Testing tools**	**Automated System Testing tools**
	• Simulation environments for analysis of trustworthy systems • Tools for embedded/industrial systems testing	• Web application testing	• Tools for verifying trustworthiness of composite systems • Automated tools for testing all system dependencies under a wide range of conditions
Preparation – Privacy & Confi-dentiality Preserving	**Improved Confidentiality**	**Advanced Federated Authentication**	**Confidentiality in Dynamic Data**
	• Advanced Data Encryption including Auditability • Advanced data anonymisation without affecting data quality • Mobile identification, authentication & obfuscation	• Federated identity management • Advanced anti-bot measures • Dynamic authentication and trust establishment for ad-hoc networks environments • Usable authentication and management of access controls	• Privacy reserved data analytics • Dynamic Data Masking • Encrypted data search without revealing query • Private information retrieval
Response – Monitoring, Detection & Protection	**Improved Security Management**	**Advanced Analytics & Detection**	**Self-Protection Systems**
	• Vulnerability management • Advanced Network Traffic Analysis • Actionable Cyber Intelligence • Unified threat management • Malware detection • Security for supply chain • Intrusion detection • Security information and event management^{T} • Firewall ^{T}	• Malware detection & endpoint containment • Mobile data protection • Data leak protection • Security as a Service • Risk analysis platform • Comprehensive Advanced Persistent Threats detection • Big data intelligence for security • Real-time security analytics	• Hardened industrial devices to detect malicious events in sensor and control data in critical infrastructure • Trustworthy systems with integrated analysis tools • New cryptography techniques for protection against many different kinds of threats • Software–defined security • Self-healing systems • Containment of cyber security attacks

^{T} is classified as Technology, otherwise as Capability.
Industry has differing views on the timeframe for mainstream adoption for some technologies.

Recover and Revise – Attack Attribution, Forensics & Recovery	Attack Visualisation	Correlated Multi Sources Visualisation	Intelligent Attacks Management
	• Elementary visualisation of (systems & network) attack events • Extraction of hidden evidence from information system • Case management to track incidences	• Visualisation of auto correlated multiple sources of attack events	• Systems that predict and respond to attackers' intent • Scalable visualisation, visualisation with accurate geolocation and zoomable visualisation at varying levels of details • Accurate Attribution • Intelligent analytical tools that correlate multiple events over time at a large scale

^{T} is classified as Technology, otherwise as Capability.
Industry has differing views on the timeframe for mainstream adoption for some technologies.

R&D Opportunities

4.5.1 R&D opportunities have been included in an ongoing National Cyber Security R&D programme[26] which aims to improve the trustworthiness of cyber infrastructures and emphasise security, reliability, resiliency and usability. These programmes provide funding to support research efforts on both technological and human-science aspects of Cyber Security.