THE CYBER THREAT LANDSCAPE

By
THNG CHIOK MENG AND WONG YONG HUI

Cyber security threats have risen significantly over the past few years. While many people are aware that cyber security is an issue, there is not necessarily a clear understanding of the threats, let along the preventive measures. They consider it a matter best left to the technical experts. It should not be.

Awareness of the threat landscape can be a first step to understanding the need for every individual to deal with the prevailing cyber threats.

The following pages provide a set of infographics on the fundamentals and trends of cyber threats as follows:

- Cyber attackers: Who are they? Are there ethical hackers? Where from do the hackers attack?
- Cyber attack targets: Which are the industry sectors and business areas being attacked, and where are the sources of these security incidents?
- Types of cyber threats: What are the kinds of cyber threats, in particular, the increasing risk of ransomware?
- Cyber incidents: What are some of the major cyber security incidents and learnings from them.

Much of the data and charts here are drawn from the following reports and indicated by the legend as follows:

PwC : Four related reports:

- The Global State of Information Security Survey 2016 by PWC;
- Turnaround and Transformation in Cybersecurity by PWC;
- Reclaiming Cybersecurity – Singapore insights by PWC

Dimension Data:

- The Executive's Guide to the 2016 Global Threat Intelligence Report by Dimension Data

Thng Chiok Meng is the Deputy Director and Wong Yong Hui is the Assistant Manager of the Group Internal Audit Division of MOH Holdings, the holding company of Singapore's public healthcare clusters. The views in this article are their own.

CYBER ATTACKERS

Who are the cyber attackers?

Cyber attackers are getting more diversified. Twenty years ago, a cyber attack is a highly skilled job. However, with the advancement and readily available tools written by hackers for non-hackers, there are now many amateur hackers.

Attackers can range from some who do not even know what they are hacking as they are merely following a set of instructions, to the other extreme where very sophisticated hackers are funded by a country to launch massive and targeted attacks on other nations.

The table below provides a grouping of the main actors but increasingly, the lines among them are blurring.

Types Of Cyber Attackers

	PROFILE	MOTIVATIONS	TARGETS
State-backed	• Very highly skilled • Vast resources • Focus on long-term cyber campaigns with strategic national interests	• Global competition • National security • Fraud	Other nation states, corporations and certain individuals for the purposes of espionage, intelligence gathering and disrupting critical national infrastructure.
Cyber criminals	• Range of skills, but usually highly skilled • Motivated by financial gains • Activities include stealing credit card numbers, internet banking logins, passwords and personal data.	• Illicit profit • Fraud • Identity theft	Any organisation and anyone whom they can eventually obtain financial benefit from
Hacktivists	• Range of skills, from the lowly skilled to highly skilled • Motivated by political and social change objectives • Some hobbyist hackers may do it for fun and learning • Will disrupt government agencies or corporations or individuals which affect their beliefs	• Ideological • Political cause rather than political gain • Sport	Any country, organisation or individual that stands in the way of their cause
Insiders	• These can be employees or third party contract personnel • Those who are unhappy will use their inside knowledge and access to disrupt operations, cause regulatory breach and create public embarrassment for the company • Some may be white hat hackers employed the company for defensive purposes (see next page)	• Disenfranchised and unhappiness with the organisation • Performing a service to the organisation (white hat)	The organisations that they are formerly or currently employed in, or associated with (through third party contracts which provide them insights and access).

Are there ethical hackers?

Not all hackers are inherently bad. Technical writers often refer to the three hats of hackers based on their ethics:

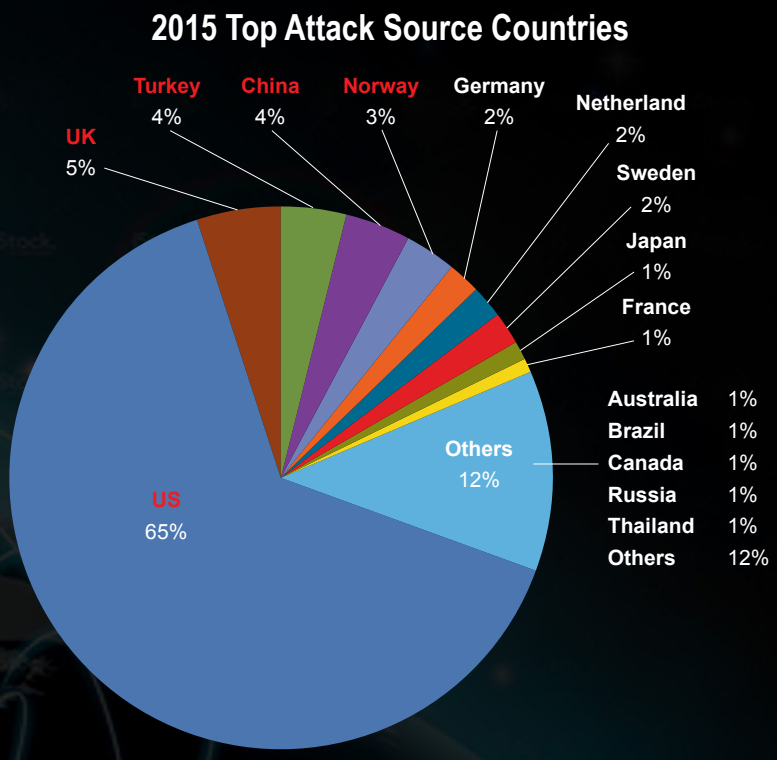
Black Hats: These are usually individuals with extraordinary computing skills but are destructive. They violate computer security for personal gain or pure maliciousness. They fit the widely-held stereotype of hackers as criminals performing illegal activities.

White Hats: These are the "ethical hackers", the professionals who use their abilities for good, ethical and legal purposes. They are often employed to test an organisations's computer security systems and improve their defences.

Grey Hats: These are individuals who may not hack for own personal gain or cause carnage, but may technically commit crimes and do arguably ethical things. For example, a grey hat hacker might attempt to compromise a computer system and then inform the organisation only after the fact, or publicly disclose a security flaw before it is fixed instead of privately informing the organisation about the security flaw.

Where do they attack from?

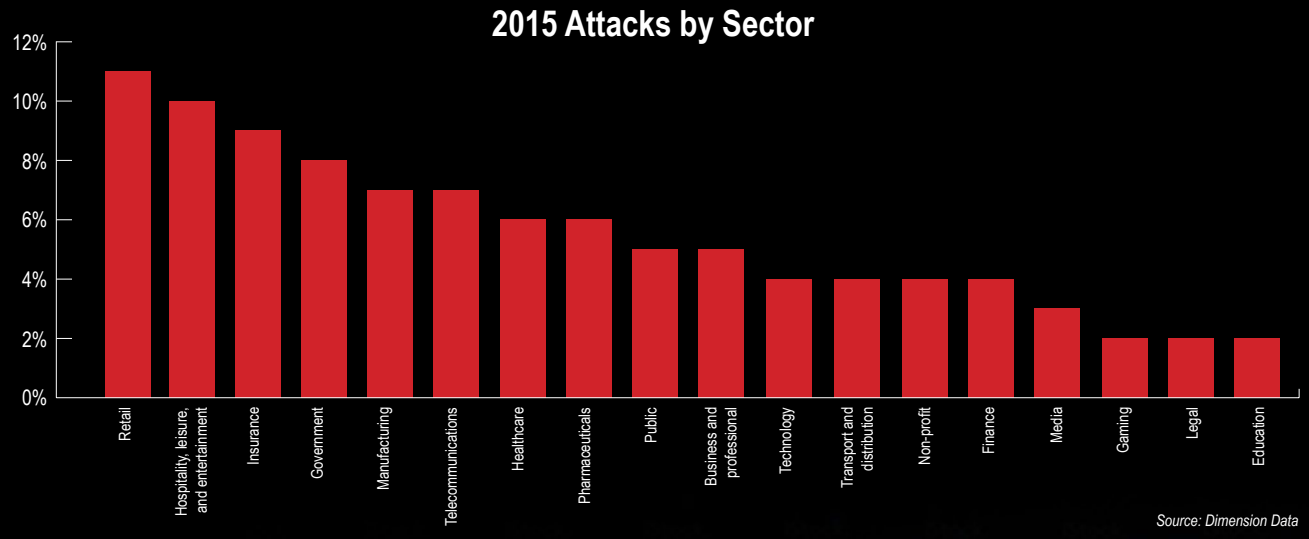
- The top five attack source countries accounted for 81 per cent of all identified attacks in 2015.
- 65 per cent of attacks originate from IP addresses within the US because a significant of the targets are in the US, so attackers often host the attacks locally to avoid geolocation blocking or alerts. Also, US makes it easier with low cost cloud hosting services.
- While the source IP address is based in the US, the actual attacker could be anywhere in the world because of the ease of disguising IP addresses.
- UK, Turkey and China are the primary source of non-US attacks.
- Activity from Turkey included several campaigns against government agencies in Europe.



Source: Dimension Data

CYBER ATTACK TARGETS

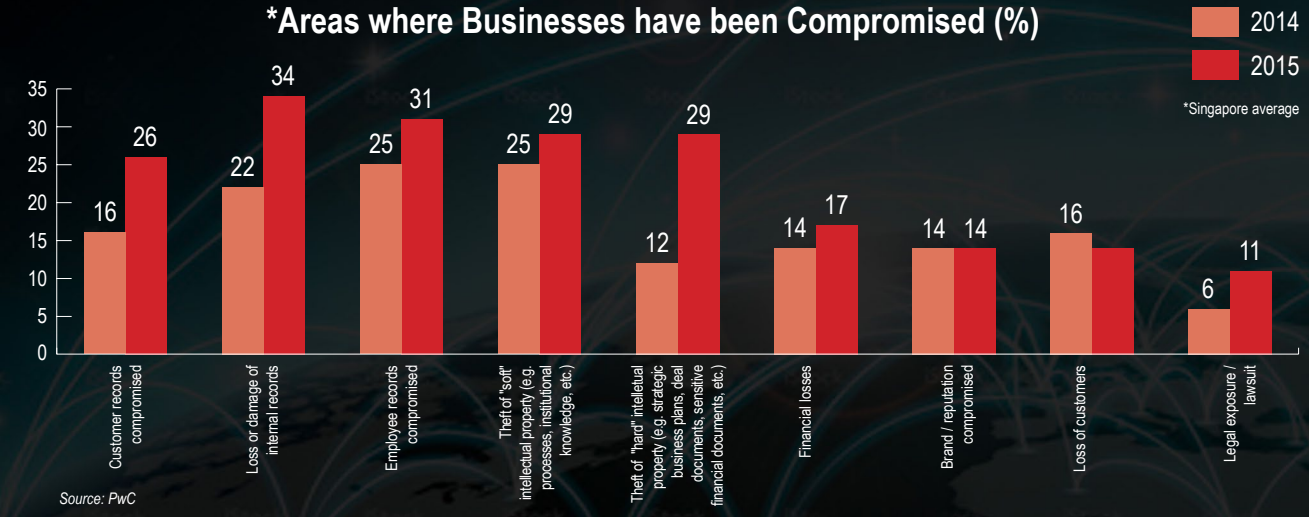
Which industry sectors are more likely to face attacks globally?



Source: Dimension Data

- Organisations in the top five sectors experienced 45 per cent of the attacks.
- The retail sector experienced nearly three times as many attacks as the finance sector.
- The retail companies are popular targets as they process large volumes of personal information (e.g. credit card data) in highly distributed environments with many endpoints and point of sales devices.
- The hospitality, leisure and entertainment sectors similarly process high volumes of sensitive information including credit cards data with sizeable transactions, and loyalty plans with personal information is the target second in rank for cyber attacks.
- The finance sector which experienced 3 per cent of the total number of attacks is more consistent in its defense against cyber attacks.

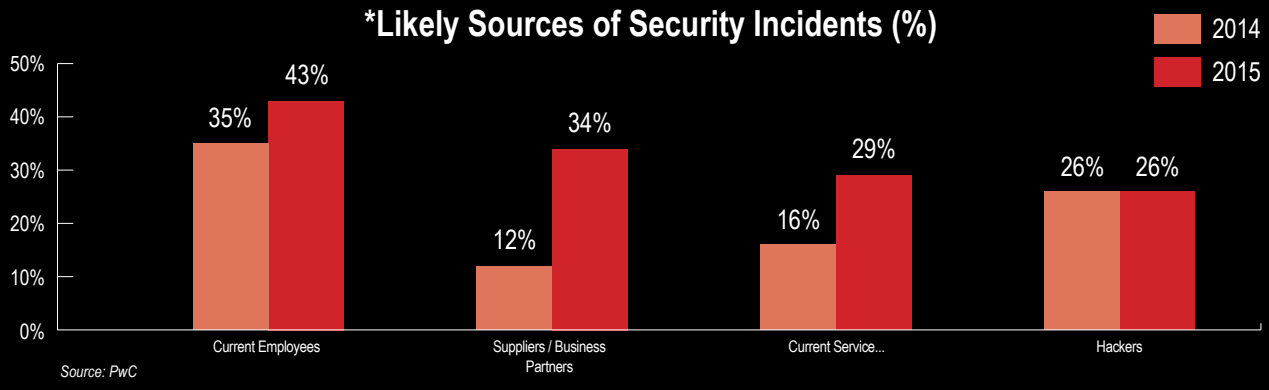
Which are the business areas affected?



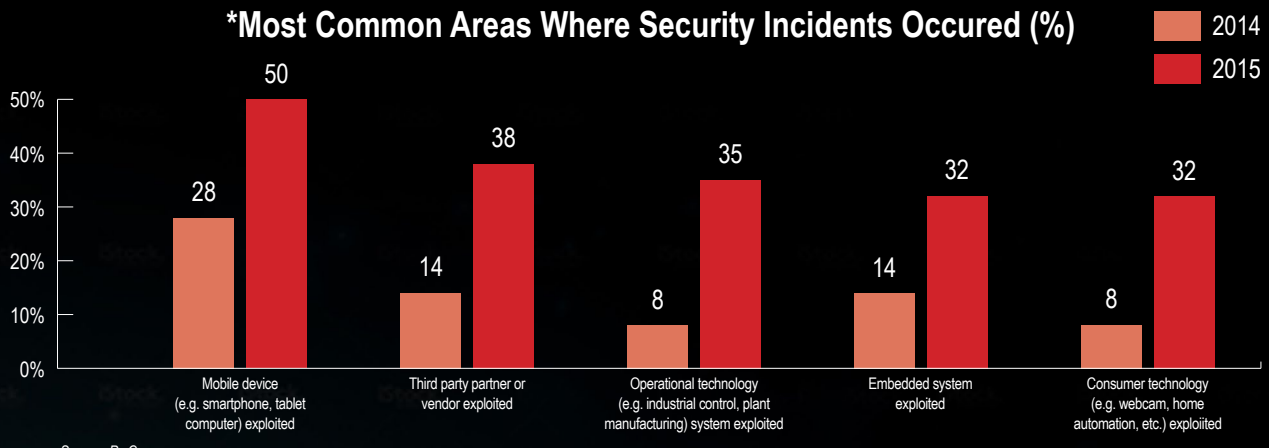
Source: PwC

- There is a significant increase in theft of "hard" intellectual property such as business plans and financial documents.
- Internal, customer and employee records continue to be of higher and increasing risks.

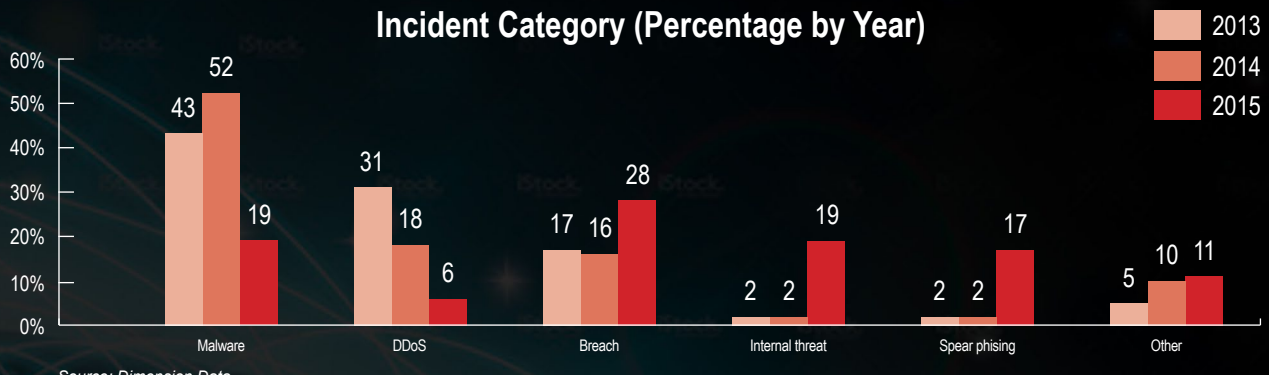
What is the source of security incidents?



Source: PwC



Source: PwC



Source: Dimension Data

- The number of security incidents is increasing. In 2015, 38 per cent more security incidents were detected globally than in 2014.
- Both PwC and DD studies shown that the internal threat are increasing with DD study showing the sudden jump from 2% to 19% from 2014 to 2015.
- While current employees remain the most cited source of compromise, internal-threat incidents attributed to business partners have climbed significantly.
- A significant number of the security incidents are from the exploitation of mobile devices such as smart phones and tablets.
- There is an increase in cyber attacks through more channels including webcam, embedded systems and manufacturing systems.

TYPES OF CYBER THREATS

What are the types of cyber threats?

Know Thy Enemy

Email spoofing		An email from a forged sender address (usually someone familiar to you) to trick you into doing something (e.g. wiring money to a bank account).
Phishing (pronounced as "fishing") and spear-phishing.		As in fishing, a bait (usually in the form of an email or website) is employed to get your personal information (such as Login ID, passwords, credit card numbers). In ordinary phishing, the malicious emails are sent to any random email account. In spear-phishing, the emails are designed to appear to come from someone the recipient knows and trusts.
Brute force attack		A trial-and-error method used to obtain information such as a user password or PIN.
Spam		Unsolicited and mostly useless messages that are sent to a large number of addressees that usually carry advertisements, and sometimes phishing and malwares.
Malware		A generic term that refers to a variety of hostile or intrusive software that includes the computer virus and worm, phishing, spyware and ransomware.
Malvertising		Malware that appears as a benign advertisement on a web page, and is activated when a user clicks on it.
Computer virus		This malware attaches itself to a programme or file, and spreads to other computers as the "infected" program or file is shared. Viruses often perform some harmful type of activity on the infected hosts.
Computer worm		A programme that, when executed, replicates itself in order to spread to other computers, often through a network relying on security failures on the target computer to access it.
Spyware		Software that gathers information about you or your computer without your knowledge, and may send the collected information to another entity. Also referred to as Trojans, adware, and tracking cookies.
Ransomware		See next page.
Denial of service (DOS) & Distributed DOS (DDOS)		Attacks which make a machine or network resource unavailable to intended users. A DDOS attack originates from many devices at once.

What is ransomware?

A "ransomware" is a malware usually sent via a malicious email. Once downloaded into the victim's computer, the malicious software will encrypt and "lock up" the data folders of the victim's computer. The hacker then demands a payment to restore the data.

Ransomware is on the rise in Singapore and across the world in recent times.

The advice from the experts on ransomeware include:

- Do not to click on suspicious URL links, especially those sent from suspicious emails.
- The best form of recovery from ransomware is to restore a backup. So, perform regular backups.
- Configure the file folders in individual PCs to restrict sharing to specific users and not to a generic group such as "everyone".
- Do not pay when held to ransom. You are encouraging such actions, and some hackers may not even release the locked data and insert malicious software that leaves you open to future attacks.

How Ransomware Works

CYBER INCIDENTS

Singapore government: Who is "the Messiah" and "Anonymous"?

In 2013, there was a spate of attacks against the Singapore government and other websites.

A person claiming to speak for activist hack group Anonymous issued an online video warning to "go to war" with the Singapore government over Internet licensing rules. However, the virtual 5 November 2013 day passed with few backing Anonymous' call.

However, "The Messiah", later found to be James Raj Arokiasamy and who claimed links to Anonymous, hacked into one of the Straits Times journalist's blogs. He posted the message "Dear ST: You just got hacked for misleading the people!" because he believed that the reporter had incorrectly chosen to "modify the sentence 'war against the Singapore government' into 'war against Singapore'".

Arokiasamy was caught, and also charged for other cyber intrusions including that of the People's Action Party Community Foundation and City Harvest Church Co-founder Sun Ho's websites. His computer also contained the bank statements of 647 Standard Chartered Bank's customers which were stolen from a server at Fuji Xerox Singapore to which the bank outsourced its statement printing. Arokiasamy was sentenced to 56 months in prison.

Other incidents in that period included the websites of the Prime Minister's Office and the Istana websites being compromised by Mohammad Azhar Tahir and a businessman, Delson Moo, respectively. Tahir was sentenced to two months jail, and Moo was fined $8,000.

In the aftermath of these cyber attacks, the government announced plans for the Cyber Security Agency and the introduction of a new cyber security Bill to be tabled in 2017 to strengthen measures against online crime.

Target: Data breach through third party contractor

In December 2013, Target Corporation, the second largest discount retailer in the US, announced that data from around 70 million credit and debit cards was stolen.

The attacker had first compromised a third-party contractor, Fazio Mechanical Services, who provides Heating, Ventilation and Air Conditioning services to Target. The attacker had then used the contractor's portal, which remotely monitored energy consumption and temperatures at various Target stores, to penetrate Target's internal network. After compromising an internal Windows file server, the hackers installed a malicious software "RAM scraper" in the Point-of-Sale (POS) systems which records unencrypted payment card details.

As the customers' credit cards information contain a person's account number, expiration date, and secret Card Verification Value (CVV) code, hackers could sell this information to credit card counterfeiters who could replicate these credit cards using their own magnet-stripe encoding machines or making online fraudulent purchases.

The Target breach has cost the company over US$160 million, and led to the resignation of its CEO and Board of Directors, as well as significant reputational damage.

Singapore banks: Phishing for PINs, passwords and money

Singapore was ranked third globally for spear-phishing attacks, according to Symantec's annual Internet Security Threats 2015 report.

In 2014, a phishing site (http://home.e-posbsg.com) was created to impersonate the real POSB Internet banking website (http://www.posb.com.sg) in order to steal customer identity names, personal identification numbers (PINs) and one-time passwords (OTPs).

In 2015, OCBC encountered a phishing attack through a fake banking portal. Customers performing a simple check of their bank accounts would risk having their cash cleaned out if their computers were infected by the malicious software.

In the same year, the CSA warned about phishing emails purported to be from support@gebiz.gov.sg. GeBIZ is a government-to-business public e-procurement business centre where suppliers can conduct electronic commerce with the Singapore government. The fraudulent email advised GeBIZ trading partners to complete a one-time account update on the phishing page which stole their user names and passwords when they signed in.

SingPass: Breach of user accounts through weak passwords

SingPass is an account management system set up in 2003 for every citizen to access the 340-plus e-government services. There are 3.3 million SingPass account holders in Singapore.

In June 2014, IDA announced that potentially more than 1,560 user ids and passwords had been accessed without the users' permission, potentially compromising the security of citizens' personal data. The passwords of all these users were then reset and the users notified.

In January 2016, James Sim Guan Liang, a former administrative assistant, was jailed five years and two months for cracking the passwords of 293 SingPass account holders and selling the details to a China-based syndicate to produce sham Singapore visa applications. Sim had realised that there was no strong password control for SingPass password. He spent thousands of hours on his computer cracking the passwords of SingPass accounts. All his 293 victims had used their NRIC number as their passwords.

Following these incidents, IDA implemented Two Factor Authentication (2FA) for SingPass login by July 2016. SingPass users are now required to use one-time-password (OTP) to transact with e-government services.

Bangladesh Central Bank: Stealing US$63 million

In February 2016, thieves tried to illegally transfer nearly US$1 billion from Bangladesh Bank to several fictitious bank accounts around the world via the SWIFT International Payment network. In the event, five transactions issued by hackers, worth US$101m and withdrawn from a Bangladesh Bank account at the Federal Reserve Bank of New York, succeeded. US$20m was traced to Sri Lanka (since recovered) and US$81m to the Philippines (about US$18m recovered). The Federal Reserve Bank of NY blocked the remaining thirty transactions, amounting to US$850m, at the request of Bangladesh Bank.

The theft shows how the criminals carefully studied the operation of a business and system, and devoted substantial resources and efforts to carry out a large-scale attack. The hackers had installed a malware at Bangladesh Bank's Dhaka headquarters in January 2016 and gathered information on the bank's operational procedures for international payments and fund operations.

The FBI, authorities in Dhaka and private forensic experts are investigating the incident. Investigators have found "footprints" and malware of hackers, and evidence of insider support.