



The Dark Web of deceit

Page 16



Trekking in a clear and present danger cyber world

Page 32



Business futures for directors

Page 52



**SID
Annual
Corporate
Governance
Roundup
2016**

It's that time of the year again to catch up with your fellow directors and on the year's happenings at the **SID Corporate Governance Roundup 2016**

Date : Wednesday, 24 November 2016

Venue : Antica Ballroom, Orchard Parade Hotel

Program : 09.30 am Registration / coffee

10.00 am Annual Corporate
Governance Roundup

12.00 pm Lunch
Collection of *Boardroom
Matters Volume 3*

1.15 pm End of Annual CG Roundup
event

Cost: \$60 for SID members

\$90 for non-members

All attendees will receive a complimentary copy of *Boardroom Matters - Volume 3*, worth \$38.

Register for the event at www.sid.org.sg

The Corporate Governance Roundup event has now become a regular on the directorship scene.

It is for those who want a quick refresher on the year's happenings and know what to expect in 2017 on matters such as regulatory updates, digital and value creation, board diversity, cyber security, stewardship principles, professional development, corporate governance codes and excellence, and audit committee implications. The subjects will be presented by SID Council members in the traditional roundup fashion.

The event is also an opportunity to meet up and network with your fellow directors in a convivial atmosphere, and the roundup precedes the AGM for members.

Organised by:



Venue Sponsor:



Far East Organization

INSPIRING BETTER LIVES

Celebrating **5** years in Singapore

It's not "if" but "when"



By **WILLIE CHENG**
Chairman, SID



DIRECTIONS

This has become the catchphrase to describe the pervasiveness of cyber attacks.

At the recent SID Directors' Conference, the Chief Executive of Cyber Security Agency David Koh quipped that the only safe computer is the one that is still in the box – in other words, unopened and uninstalled.

The frightening thing is not that a cyber attack is inevitable. It is that the frequency and intensity of such attacks are rising. Hence, it's also not just "when" but "how often and relentlessly" one can expect to be attacked.

What then are companies to do?

Experts on the subject are united on several fronts.

First, companies should do what they can to prevent breaches, notwithstanding that attacks will happen.

As breaches are inevitable, being prepared also means shoring up mechanisms that detect and respond to the breaches. According to the Mandiant M-Trends report, in 2015, the average time before a breach is detected by companies is 146 days. As recent high profile cases show, untold damage can be inflicted on a company during this period.

This issue of the Directors' Bulletin follows from the last issue, as well as the recent Directors' Conference

on Digital Disruption, to focus on cyber threats, the dark side of technology disruption.

We kick off the issue by surveying the landscape of cyber threats, and taking a peek at the Dark Web, a murky corner of the internet which few are aware, and which is the source of many of the tools used in cyber attacks (pages 6 to 19).

Subsequent articles examine how individuals, companies and the nation are, and should be, responding to cyber threats.

This issue also features several major SID events on corporate governance that took place in the last three months: the SGTI launch (page 60), the KPMG-SGX survey on corporate governance disclosures (page 66), the Chinese corporate governance seminar (page 58), and the Singapore Corporate Awards (page 54). And, of course, we have highlights of our flagship Directors' Conference (page 38).

In addition, with the support of the SGX, we introduce a new section that lists SID members who are taking on new directorships in listed companies (page 75).

As we wrap up 2016, I hope to see you at our major events in the last quarter which include the launch of the Singapore Directorship Report (18 October), the launch of the Board Guide (11 November), and the annual corporate governance round-up and AGM (24 November). ■

SID Brand and Communications Committee

CHAIRMAN

Wong Su Yen

DEPUTY CHAIRMAN

Wilson Chew

MEMBERS

Chan Yu Meng

Mylinh Cheung

Mike Gray

Gary Harvey

Sameer Khan

Sonya Maderia

Marie-Helene Mansard

Dennis Mark

Wayne Soo

Leonard Stornes

Jean-Emmanuel Turquois

Victor Yeo

Annabelle Yip

PUBLISHER

Singapore Institute of Directors

168 Robinson Road #09-06/07

Capital Tower

Singapore 068912

Tel: +65 6422 1188

Fax: +65 6422 1199

Email: secretariat@sid.org.sg

Website: www.sid.org.sg

EDITOR

Adlena Wong

EDITORIAL COORDINATORS

Joyce Koh

Chia Yi Hui

DESIGN

Epiphany Design

PRINTER

Entraco Printing Pte Ltd

CONTENTS



FEATURES

- 6 The cyber threat landscape
- 16 The Dark Web of deceit
- 22 Cyber attacks: Staying ahead of the bad guys
- 26 Building digital services upon a secure foundation
- 32 Trekking in a clear and present danger cyber world
- 36 Seizing the cyber security challenge with data stewardship
- 38 *SID Directors' Conference 2016*
An immersive digitally disruptive experience
- 54 *2016 Singapore Corporate Awards*
Celebrating the best in corporate governance, "Oscar" style
- 58 Singapore corporate governance and directorship (Chinese) seminar
- 60 The Singapore Governance & Transparency Index
- 66 The State of Corporate Governance Disclosures Forum



COLUMNS

- 20 INNOVATION
Cyber terrorism: fact or fiction?
- 30 BOARDROOM MATTERS
Affording information security
- 52 EXPANDING HORIZONS
Business futures for directors
- 76 AFTER HOURS
Walk a mile in my shoes

SID NEWS

- 50 The secrets & art of cyber security
- 70 Building a high impact board
- 71 Fair process leadership in the boardroom
- 72 Board Chairmen's Conversation: Beyond the hype of IoT
- 73 AC Chairmen: IA at the speed of business with data analytics
RC Chairmen: Bridging the gap with shareholders on pay

- 74 Black Swans: Predicting the unpredictable
CG experts come together to enhance the ASEAN Corporate Governance Scorecard
- 75 Director Appointments and National Day Awards 2016
- 79 Photo Gallery Of Past Events
- 82 Welcome to the family


SID CALENDAR

- 78 SID's Q3 events
(July 2016 – September 2016)
- 80 Upcoming events

A person wearing a dark hoodie is shown from the chest up, making a hand gesture with their right hand. The background is a dark blue and black space with a glowing globe at the bottom. Numerous bright blue and white lines arc across the globe, representing a global network or data flow. The overall lighting is a mix of dark blues, blacks, and bright oranges and reds from the text.

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 alone 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 the 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 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: Three related reports:

- *The Global State of Information Security Survey 2016* by PwC;
- *Turnaround and Transformation in Cyber Security* by PwC;
- *Reclaiming Cyber Security – 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 they?

Cyber attackers are getting more diversified. Twenty years ago, a cyber attack was 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	<ul style="list-style-type: none"> • Very highly skilled • Vast resources • Focus on long-term cyber campaigns with strategic national interests 	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Range of skills, but usually highly skilled • Motivated by financial gains • Activities include stealing credit card numbers, internet banking logins, passwords and personal data. 	<ul style="list-style-type: none"> • Illicit profit • Fraud • Identity theft 	Any organisation and anyone whom they can eventually obtain financial benefit from.
Hacktivist	<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • Ideological • Political cause rather than political gain • Sport 	Any country, organisation or individual that stands in the way of their cause.
Insiders	<ul style="list-style-type: none"> • These can be employees or third-party contract-personnel • Those who are unhappy will use their inside knowledge and access to disrupt operations, causing regulatory breach and create public embarrassment for the company • Some may be white hat hackers employed the company for defensive purposes (see page 9) 	<ul style="list-style-type: none"> • 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 organisation’s computer security systems and improve their defences.

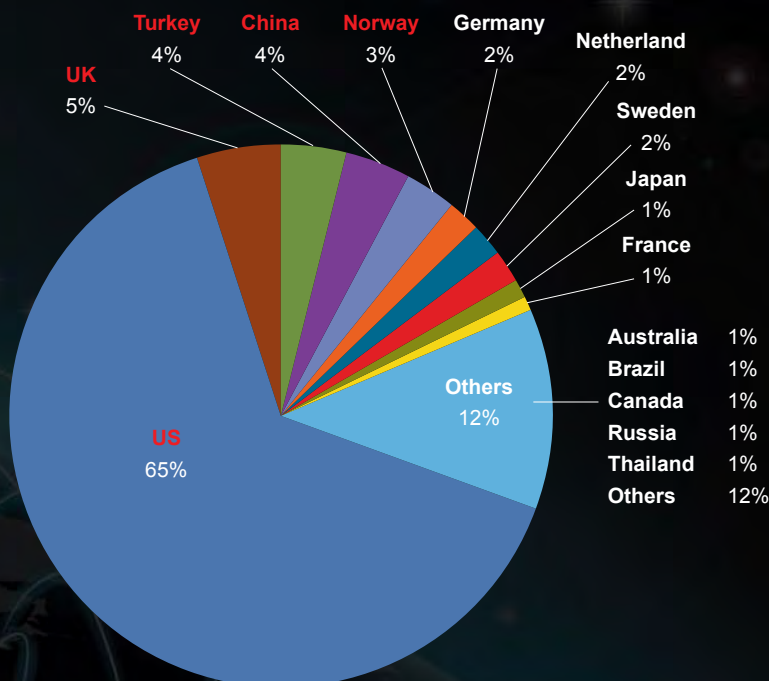


Grey Hats: These are individuals who may not hack for own personal gain or cause carnage, but may technically commit crimes and do arguably ethical things. For example, a grey hat hacker might attempt to compromise a computer system and then inform the organisation only after the fact, or publicly disclose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

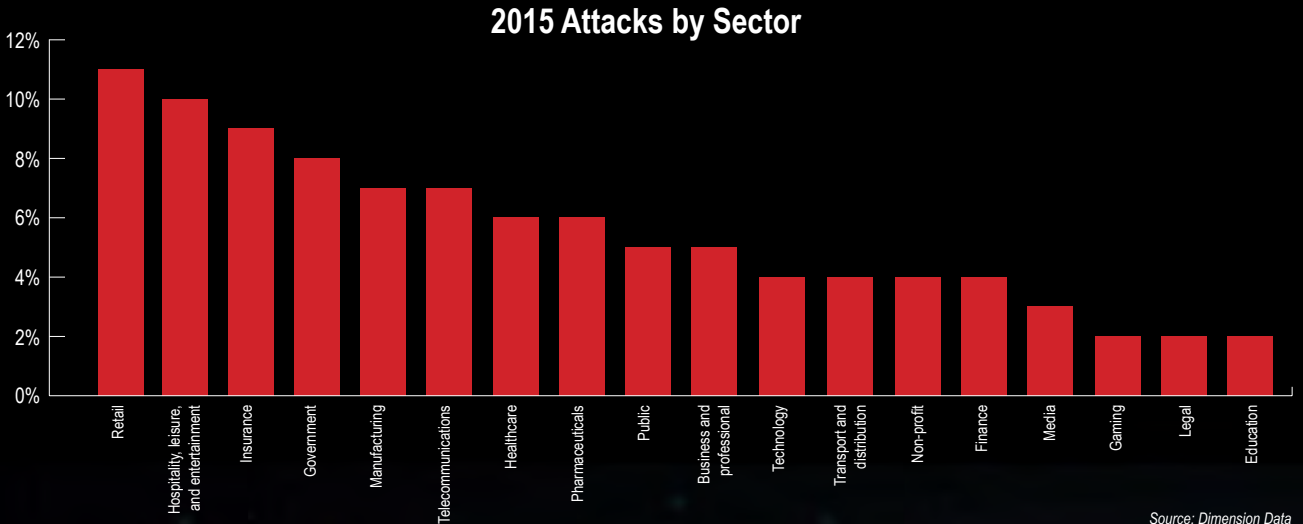
2015 Top Attack Source Countries



Source: Dimension Data

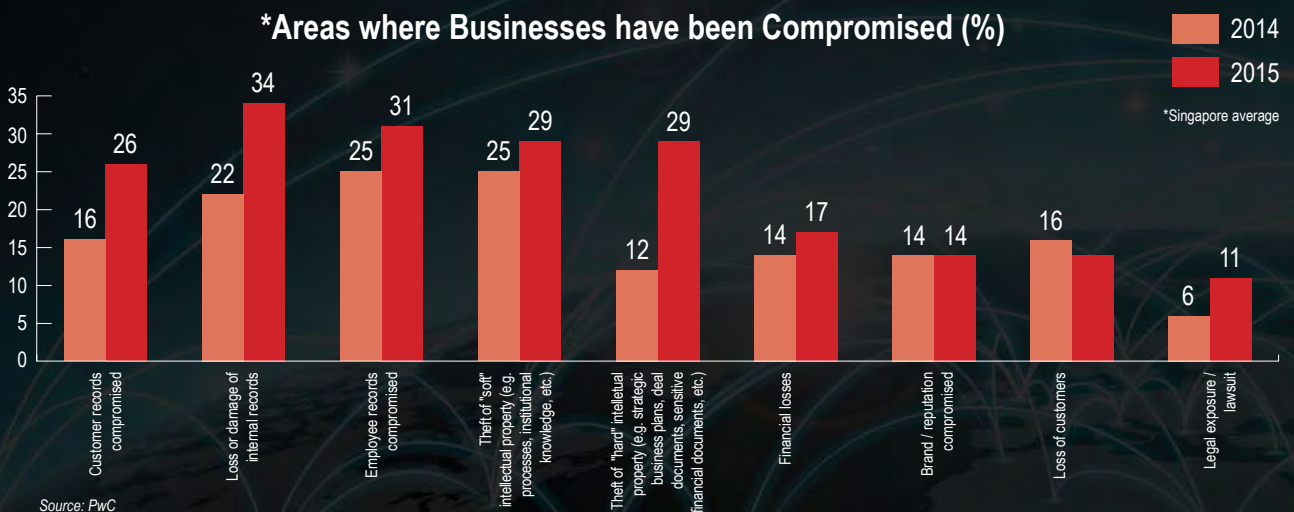
CYBER ATTACK TARGETS

Which industry sectors are more likely to face attacks globally?



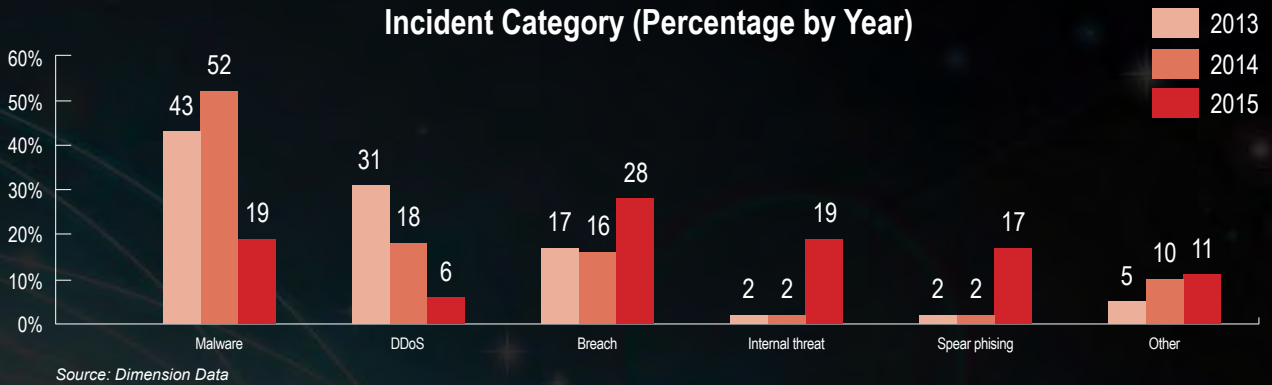
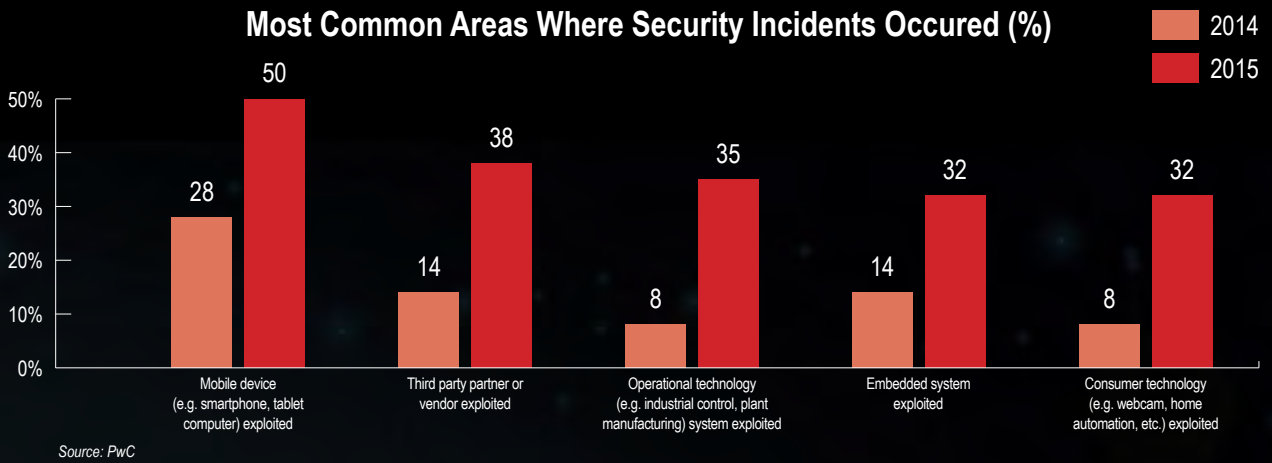
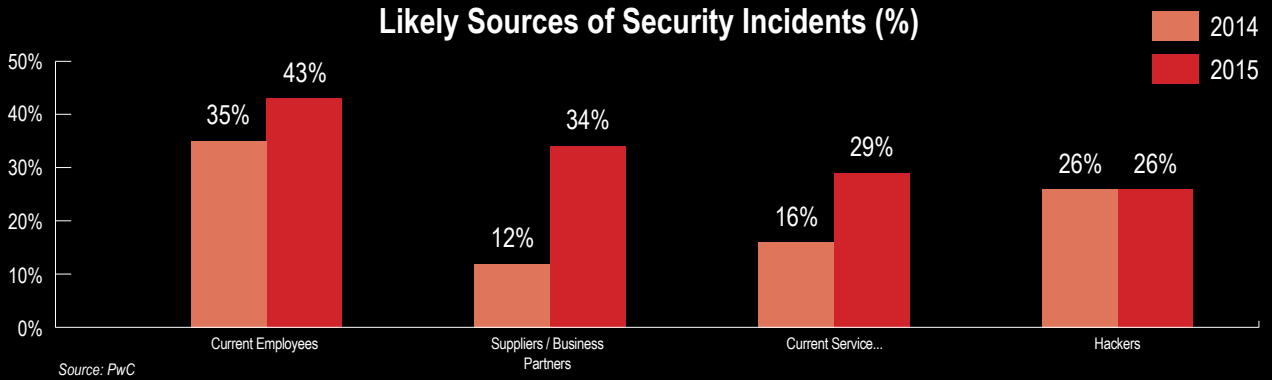
- Organisations in the top six sectors experienced 52 per cent of the attacks.
- The retail sector experienced nearly three times as many attacks as the finance sector.
- The retail companies are popular targets as they process large volumes of personal information (e.g. credit card data) in highly distributed environments with many endpoints and point-of-sale 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 three per cent of the total number of attacks is more consistent in its defense against cyber attacks.

Which are the business areas affected?



- 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?



- 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 show that the internal threats are increasing with the DD study showing the sudden jump from two per cent to 19 per cent 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 smartphones 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, some form of bait (usually in the form of an email or website) is employed to get your personal information (such as login IDs, 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 page 13.
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 ransomware include:

- Do not 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 websites: 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 being compromised by Mohammad Azhar Tahir and a businessman, Delson Moo, respectively. Tahir was sentenced to two months jail, and Moo was fined S\$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-posb.com>) was created to impersonate the real POSB Internet banking website (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. ■



The Dark Web of deceit

By
GERRY CHNG

The Internet already provides us with so much information, but is there more than meets the eye? Deep within the recesses of the Internet is the Dark Web, where data is encrypted and users remain anonymous. Is it a place for good or for bad?

The Internet. A vast expanse of interconnected systems offering a seemingly endless treasure trove of information.

Usually, search engines are our first resort when we look for information. These search engines trawl the Internet and create sophisticated search indices by applying advanced algorithms. The pages that are found with search engines are known as part of the “Surface Web”.

Over the years, those who try to determine the extent of the Internet reveal what we have long suspected: the Surface Web accounts for only one to four per cent of what is out there on the World Wide Web.

Go deep

There are, in fact, much more resources on the Internet that can be accessed only if the URL address is known. Examples of such pages are private corporate resources that are only meant to be accessed by employees or contractors, or simply resources that are not linked in from other pages.

These form what is known as the “Deep Web”, the part of the Internet that has not been indexed by search engines.

On its own, the Deep Web is not ill-intentioned. It is what it is: a place that can only be accessed if you know the URL. No special permits or tools are needed to pry it open.

SURFACE WEB

Google Bing
Wikipedia Yahoo

DEEP WEB

Medical records Intranet
Legal documents Graphic media
Academic information Subscription databases
Financial records Multilingual databases
Scientific reports Password-protected pages
Government reports Conference proceedings

DARK WEB

Illegal information Private communications
Drug trafficking sites TOR-encrypted sites
Hacking groups and services

The Dark Web rises

However, residing within the Deep Web is a much shadier part of the Internet, called the “Dark Web” or “Dark Net”.

The physical world equivalent will be the dark alleys that most will wisely not venture unless they are feeling adventurous, or are a familiar part of that community.

The Dark Web is where shady businesses thrive. Examples include:

- Sales of drugs and illegal items,
- Pornography (particularly child pornography which is illegal in most places with coordinated policing by the Interpol and various governments),
- BitCoin-related financial services,
- Hacking services (see the table “Available for sale in hackers’ paradise”)
- Pirated software

Accessing the Dark Web

When accessing a page using a conventional browser, the browser follows a direct network route to the destination. Assuming there are no special steps taken to make the connection anonymous (e.g. through VPN or anonymous proxy services), the destination resource is able to know the Internet address one is accessing the service from. Likewise, the user is able to determine the Internet address of the resource he or she is trying to access.

Obviously, this ease of mutual identification does not serve well for the Dark Web community. This part of the Internet is not meant to be directly accessible even with knowing the URL. To protect their own anonymity, such resources are only available to verified members of the community, and through the Tor network.

Tor is a free software that enables anonymous communication. The name is an acronym derived from the original mid-1990s software project, “The Onion Router” which was used to protect the security of US intelligence communications conducted online.

When using a specialised Tor browser, the anonymity of the data transport is achieved by encrypting the payload and routing it through a random list of relay servers distributed throughout the world. Each relay “peels away” one layer of the onion to reveal which relay server to subsequently forward to. Each relay only knows this much, just enough to route the encrypted package along.

This helps to create the cloak of anonymity that operators within the Dark Web seek to make it harder for law enforcers to track them down.

Just like in the physical world, we also do see law enforcement and threat intelligence operators within the Dark Web. Their objective is to gather relevant threat intelligence and perhaps even to avail of its product and services for law enforcement purposes.

The digital black market

The anonymity of the Dark Web creates a perfect environment for different trades to exist with lowered risk of discovery.

A prominent example was the Silk Road digital marketplace, which was allegedly founded and run by Ross William Ulbricht under the pseudonym, “Dread Pirate Roberts”. Launched in 2011, Silk Road was an online marketplace for selling illegal drugs, accessible only through the Dark Web. It was shut down in 2013 by the FBI along with the arrest of Ulbricht.

We have also seen the rise of a thriving trade serving the hacker community with a matured

Available For Sale In Hackers' Paradise

Zero-day exploit information	These are hitherto unpublished vulnerabilities in software, which can be sold to individuals or entities for their own purposes. They are called “zero-day exploits” because they are yet to be made known publicly.
Exploit kits	The zero-day exploits can be packaged together into exploit kits that can be sold to either individuals, hacking groups, or other entities for their purposes of breaking into other systems. Usually, such exploit kits combine several capabilities so that there are more than one possible vector in gaining unauthorised access to the victims.
Stolen credit card details	Magnetic stripe information stored on credit cards that are stolen can be sold for the purpose of credit card fraud or duplication of such cards. It is envisioned that this category of malicious activities will disappear soon with the adoption of EMV chips on credit cards.
Stolen personal information	Stolen personal information can be sold and subsequently resold, possibly along with the exploit kits. The information serves as a pool of victims that can be targeted either in general phishing or spear-phishing (a more targeted form of defrauding victims over emails).
Hacking and surveillance services	Sometimes, a buyer does not want to be bothered with the tools and process, and only wants specific outcomes. Such services can also be bought for a price from digital black marketplaces.

supply chain and business models, so much so that the Dark Web has also been referred to as a “hackers’ paradise” with products and services such as those shown in the table.

The increasing number and sophistication of tools and services available in the Dark Web has made cyber attacks a stark reality of the digital era. It is no longer possible to assume that with the right preventive measures, one can hope to prevent being a victim of a cyber attack. It all depends on the value of the information that is at stake, and how much the hacker is prepared to invest to get the most relevant or best exploit kit or services.

Enterprises should thus diversify their security expenditure to cover not just preventive measures, but also to ensure that they have the right detection and response capabilities.

What sets apart the digitally responsible organization from the rest is taking the right informed decisions to embrace the opportunities that the digital age brings, while in doing so, recognise the risks and put in the appropriate measures to safeguard the future of the business. ■

Gerry Chng is Partner, Advisory Services, EY. The views reflected in this article are the views of the author and do not necessarily reflect the views of the global EY organisation or its member firms.

Cyber terrorism: fact or fiction?



By **ROBERT CHEW**
Council Member, SID

An article in the June 2016 edition of New York Magazine described the scenario of how a massive, multi-pronged online attack on New York City could take place:

On December 4, 2017, at a little before nine in the morning, ... a hired SUV suddenly swerved to the left, ... pinning a sedan against a concrete median. A taxi ran into the SUV's rear fender and spun into the next lane, forcing a school-bus driver to slam on his brakes. Within minutes, nothing was moving ... Moments later, on the George Washington Bridge, an SUV veered in front of an 18-wheeler, causing it to jackknife across all four lanes and block traffic heading into the city.

The crashes were not a coincidence. Within minutes, there were pileups ... At the center of each accident was an SUV of the same make and model, but as the calls came in to the city's 911 centers in the Bronx and Brooklyn, the operators simply chalked them up to Monday-morning road rage. No one had yet realized that New York City had just been hit by a cyber attack.



INNOVATION

A third-year resident in the emergency room at Columbia University Medical Center ... walked through the hospital as a television was airing images from the accident on the George Washington Bridge; that meant several crash victims would soon be heading her way. When she got to her computer, she tried logging into the network to check on the patients who were already there, but she was greeted with an error message that read WE'RE NOT LOOKING FOR BITCOINS THIS TIME.

No longer the stuff of novels

What reads like a techno-thriller novel was meant to be a thought-provoking exercise, except the unnerving thing about it is that most, if not all, of what the article envisioned have already happened.

In July 2015, two researchers Chris Valasek and Charlie Miller demonstrated that they could launch attacks against the software systems that powered a 2014 Jeep Cherokee. They bombarded the passenger cabin with loud music, blurred the windshield with wiper fluid and, worryingly, forced the car to decelerate while on the Interstate Highway.



In March 2016, KrebsonSecurity.com, a site on internet security matters written by former *Washington Post* staffer Brian Krebs, reported that Kentucky's Methodist Hospital was on lockdown after an outbreak of the Locky ransomware encrypted data on a number of systems at the facility. At the same time, the BBC reported that two other Californian hospitals – Chino Valley Medical Center and Desert Valley Hospital – had also experienced ransomware attacks.

The *New York Magazine* article invoked high drama of a coordinated multi-vector attack on New York City to illustrate a point. As we move more and more things online, thinking we are moving into the future, we might one day be rudely awakened by the very real possibility of a war zone instead.

Granted, we may not be in that war zone yet but we are certainly entering a new era of cyber security. With every bit of information getting digitalised, everything going the way of IoT (Internet of Things), vehicles becoming driverless and autonomous, and medical devices getting implanted in our bodies, we create irresistible targets for those who want to spy and steal, disrupt and destruct, and a wide spectrum of illegal activities. Cyber threats are no longer just annoying but alarming, rendering both the information and physical world unsafe.

Fighting the invisible enemies

As Singapore steps up efforts to become a Smart Nation, the need to address the challenges of cyber security becomes ever greater. Foremost among these challenges is sourcing, developing and training information security professionals with the combination of business and technical savvy needed to combat the growing cyber threats. Unfortunately, this profession has evolved largely in reaction to threats and so, we are missing an entire generation.

We are not alone in this. In November 2015, the *Financial Times* reported that the global

demand for cyber security experts is forecast to outstrip supply by a third before the end of the decade, with companies struggling against what one senior industry figure has called the “largest human capital shortage in the world”.

In addition, traditional security methods are not keeping up with cyber attackers. As a result, researchers are now developing systems to automate the response – systems that tap Artificial Intelligence (AI) to create radically different and potentially far more sophisticated defence models. These techniques revolve around technologies such as big data, pattern mapping and matching, cognitive computing, and deep learning methods that simulate the way the human mind works. The goal is to better identify suspicious patterns and behaviour, and build security frameworks that are more resilient and adaptable.

At the recent hacker conference, DEFCON 2016, the US Defense Advanced Research Projects Agency (DARPA) ran its Cyber Grand Challenge. Seven teams competed to build AI “bots” to find, diagnose and fix software flaws. These “bots” also have to defend themselves against other teams attacking the vulnerable code on their own servers while trying to launch counterattacks.

DARPA has repeatedly delivered game-changing capabilities using such competitions, including icons of modern society such as the Internet, automated voice recognition and language translation, and the Global Positioning System receivers small enough to embed in our mobile phones.

The outcome of DARPA Cyber Grand Challenge could radically change the way we deal with software vulnerabilities and cyber threats. We may see here yet another case of digital disruption that is a work in progress. ■



CYBER ATTACKS: Staying ahead of the bad guys

By

BENEDICT TAN

Chief Information Officer, SingHealth

With the number of cyber attacks increasing, it might seem like one's turn is next. While no one can be 100 per cent attack-proof, there are precautions and measures that individuals and organisations can and should take.

Cyberspace lies at the heart of today's society. It impacts our personal lives, businesses and government.

Unfortunately, cyber risks are also a reality of this environment. Cyber attacks can range from installing spyware on a PC to attempts to cripple an organisation, and even destroy the infrastructure of an entire nation.

Organisations and individuals cannot afford to ignore these cyber threats. Knowing what we are up against will be a good start.

The attacks can range from simple email spoofing to phishing and all kinds of malware. The most recent attacks have been "ransomware" where hackers break into a system to lock up and encrypt the data files and then demand a payment (usually money or bitcoins) to restore the system and data files. [Ed: see page 12 for a list of the common attacks.]

Without doubt, most organisations would have put in place measures to deal with cyber security. With the increasing pace and complexity of attacks, whether this is enough is the question. The range

of measures that an organisation should adopt to counter cyber attacks is provided in the next two pages, “Defending the organisation”.

However, cyber defence is everyone’s responsibility. All staff should be educated with real life examples and made aware of how they can play their role in cyber defence. This would include reminding them to:

- Create strong passwords and remember them (not stick them beside the computer). See box on “The importance of passwords”.
- Never give or share their passwords.
- Not open any attachments or click on any links in emails from someone whom they are unfamiliar with. When in doubt, they should check with their IT colleagues. With internet

shopping and purchase getting more and more popular, cyber criminals are riding on this trend to send unsuspecting cyber shoppers phishing emails, luring them to a site on the pretext of checking their delivery.

- Be careful of “odd” emails. For example, a common scam is an email from a known party (whose email id was hacked into or is being spoofed) asking for a small sum of money for an emergency – call back the sender and check (do not respond via email).
- Backup their data and files regularly to an offline storage. (The only way to recover from a ransomware attack is to pay the ransom or to restore the locked files from a backup copy).
- Install appropriate anti-malware and do not delay security updates.

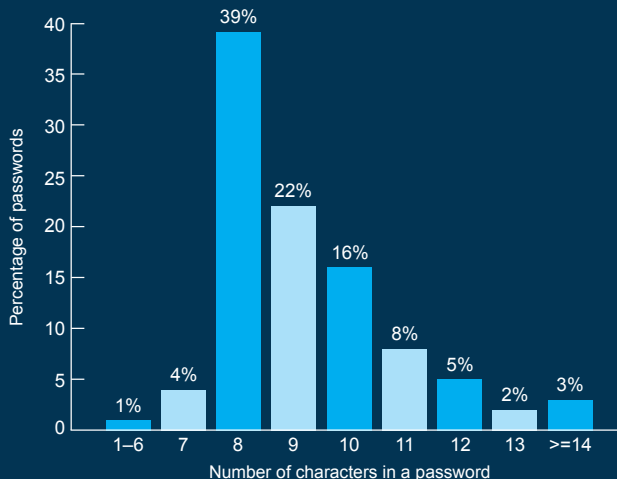
THE IMPORTANCE OF PASSWORDS

The use of common and weak passwords is a major reason for successful cyber attacks. A 2015 study by Trustwave Global Security found that after sampling 500,000 hashed passwords gathered through thousands of penetration tests, an astonishing 51 per cent of them could be cracked within 24 hours and 88 per cent within two weeks.

The top ten commonly-used passwords were found to be:

1. Password1
2. Welcome1
3. P@ssword
4. Summer1!
5. Password
6. Fa\$hion1
7. Hello123
8. Welcome123
9. 123456q@
10. P@ssword1

The common password lengths



Here are three tips on having a strong password:

- The longer the password, the harder it is to crack. Consider a 12-character password or longer.
- Avoid any dictionary word, names and places. Any word on its own is bad. Even combinations of known words should be avoided.
- Mix it all up. Use variations of upper and lower case letters, numbers and letters, punctuation marks and symbols.

DEFENDING THE ORGANISATION



1. Secure the borders

If the organisational network has connections to the internet, the following should be installed:

- **Firewall.** This is the wall around the cyber perimeter. Incoming and outgoing traffic are monitored and permitted ones (based on predetermined rules) can only travel through doors, called ports.
- **Intrusion detection and prevention system.** This is like the border guards monitoring traffic that passes through the ports to identify malicious activity and attempt to block it.
- **Web proxy.** A proxy acts as an intermediary for all communication between an organisation and the internet universe. It protects the organisation by substituting the internet address of the organisation with a pseudo address when communicating with external entities in the internet. Without the actual address, cyber criminals will be more challenged to locate the organisation.
- **Anti-spam.** This software scans through all messages coming in to your organisation's email server and block spam messages from coming through. They usually deposit these blocked emails into a spam folder where the intended recipients can occasionally check if legitimate emails that should not have been but are also blocked. Typically, more than 98 per cent of the emails an organisation received are spams.

Some organisations segregate their internet access and enterprise networks. For example, IDA recently announced that there will be no internet access for public officers' work computers by June 2017. This is arguably the most secure measure against external cyber attacks. However, organisations contemplating this approach will have to weigh the benefits of this added security against any potential drop in productivity and additional infrastructure costs (for example, issuing staff with more than one device, and having a separate network for internet access).

2. Tighten security within borders

The internal network and software should be kept secure and robust through measures such as:

- **Install Network Access Control (NAC).** With NAC, unauthorised devices will be disallowed from connecting to the internal network, even if they use a valid user ID. This prevents cyber criminals who managed to gain physical access into the premises to access computer resources and data assets through the network, as well as malicious software which can be introduced through an unauthorised endpoint (for example, inadvertently or otherwise being brought in by a staff).
- **Keep enterprise software up-to-date.** Major vendors such as Microsoft and Apple release patches regularly to remediate detected vulnerabilities in their software.

- **Regularly review and audit user IDs, access levels and actual accesses.** Put in place a process to regularly review user IDs. Remove those that are dormant or belong to employees who have resigned. Ensure that staff are given the right access levels to do their work, not any higher. Finally, audit actual accesses to identify any unusual activities.

3. Protect the endpoints

Despite all the protection at the border, cyber perpetrators will always find a way to get through. Thus, the organisation needs to shore up defenses at the end-points, i.e. the devices such as notebooks, desktop computers and tablets. These include:

- **Install anti-virus software in all the endpoints.** These software detect viruses through the viruses' signature that are stored in a signature file. Companies that supply the anti-virus software update the signature file regularly with new virus signatures. Hence it is important that the IT Department keep these files updated in all the end-points. There are advanced forms of malwares known as "Advanced Persistent Threats", which will require the installation of Advanced Threat Protection software to detect and neutralise them.
- **Control administrator rights.** Most malwares require "administrator rights" to embed itself in the end-points and to conduct their malicious work. Administrator rights allow unfettered access to all system folders and files; this is not needed by all staff. By limiting the number of user IDs with administrator rights, the organisation effectively limits the number of vulnerable end-points.
- **Implement a regular password change policy.** Every user without exception should be required to change their passwords, ideally every three months. Passwords should be

required to comprise special characters and numbers to make it difficult to hack.

- **Encrypt all endpoints hard disks.** That way, the information stored on the disk will be safe even if the endpoint is hacked into.
- **Limit endpoint connections.** Many organisations disable the endpoints' USB ports and allow only authorised USB devices to be connected. This is to prevent malwares being introduced into the organisation through USB storage devices.

4. Prepare for breach

Despite the best of precautions, the ingenuity and persistence of cyber attackers should never be underestimated. The organisation should put in place resources and processes to control the damage and recover from an attack. These should include:

- **Contact points.** There should be one or more contact point for staff to report and seek help if their devices are compromised. This can be the IT helpdesk line.
- **A recovery team.** There should be trained personnel in place that can be mobilised to immediately respond to the attack. The response would usually involve isolating the infected device, and investigations to determine the route of penetration. Vulnerabilities must be remediated promptly. For example, if the attack was through an email, all emails from the same source should be quarantined.
- **Incident escalation and management.** Depending on the type and extent of the breach, several of the organisation's resources will need to be mobilised to contain the breach and handle public communications. Establishing an incident escalation and management procedure will avoid confusion and provide a structured approach to manage any breaches. ■



Building digital services upon a secure foundation

Organisations can no longer stand still in the face of continuing and new cyber threats. What can, and should boards do?

By

TAN WEN SZE

Assistant Director, Strategy, Cyber Security Agency of Singapore

Cyber threat is borderless. Companies are vulnerable to the increasingly sophisticated cyber crime syndicates and nation-state hackers.

These groups of attackers are developing cheaper and better ways to exploit security loopholes. At the same time, new networked technologies may increase the attack surface. For example, cloud-based transactions and

remote access to enterprise systems can be new channels for breaches, so a comprehensive risk assessment is important when deploying them.

Time to get your defences up

Cyber security strategies have to evolve in tandem with technological change. The Singapore government, as many others around the world, is responding to the growing threat (see box, “What Singapore is doing in cyber security”).



What Singapore is doing in cyber security

Many governments are putting in resources to strengthen the countries' resilience against cyber attacks. In Singapore, Dr Yaacob Ibrahim, Minister-in-charge of Cyber Security, has stated that the government will increase cyber security expenditure as a share of its IT budget to at least eight per cent in the long term.

Recognising the lack of skilled resources is a challenge faced by many companies, the Government is developing schemes to expand the cyber security manpower pool and level up technical competencies.

With the introduction of cyber security diplomas by Ngee Ann and Republic Polytechnics, all five polytechnics now offer cyber security courses. The universities also offer cyber security specialisations such as National University of Singapore's Bachelor of Computing in Information Security and Singapore Institute for Technology's Bachelor of Engineering in Information Security.

Schemes have been launched to help fresh graduates and mid-career professionals enter the cyber security profession. For example, the Cyber Security Associates and Technologists Programme (CSAT) developed by CSA and IDA help new entrants up-skill through on-the-job training programmes led by companies which are CSAT training partners.

Government agencies are partnering leading industry players to enhance Singapore's cyber security capability development. For instance, FireEye's Asia Pacific Centre of Excellence, in collaboration with Infocomm Development Authority of Singapore, provides manpower training programmes for expert level skills in the area of cyber threat intelligence. The Association of Information Security Professionals and CREST International are partnering the Cyber Security Agency of Singapore to set up a local certification centre to raise professional standards in penetration testing and incident response.

Companies have to follow suit. The good news is more organisations are aware of cyber risks and are increasing their cyber security budgets. According to the PwC, CIO and CSO Global State of Information Security Survey 2016, firms worldwide increased their cyber security budgets by 24 per cent in 2015.

A well-architected system gives defence tools a better security return on investment. Companies should start by architecting the system to the defenders' advantage and ensuring that cyber defenders understand their own network and activity better than the adversary.

Good practices include maintaining an authorised inventory of assets to enable monitoring, restricting administrative privileges, performing continuous monitoring and ensuring timely patching to remove vulnerabilities.

Organisations should be cognizant of the need for a layered defence. Security cannot be built on the assumption that systems have well-defined boundaries which can be defended by perimeter security tools such as firewalls.

Additional defences have to be placed around more granular assets at the application and data

levels. Examples include data encryption and application control.

Cyber defences also have to be continually updated against new threats. For example, recent high profile cases were dominated by data loss. In 2015, cyber criminals using data modification for ransom was trending.

Bringing cyber security from the backroom to the boardroom

A company that raises its defences sufficiently to change the cost equation of a threat actor can reduce, although not eliminate, its own cyber risk. In managing risks, the board is the fourth line of defence for the company.

The board can be more active and proactive in cyber security:

1. The board can elevate cyber risk from an IT risk to an enterprise risk. Cyber breaches can result in financial and reputational damage that can set back a company's strategic goals and undermine the confidence of customers, investors and business partners. Addressing cyber risks requires a systematic approach at the enterprise level as these risks are found across the company – from the online shop-front to the networked supply chain, from internal enterprise systems to outsourced cloud services, from traditional computer networks to smart office automation systems. The PwC-CIO-CSO *Global State of Information Security Survey 2016* indicates that there was boards are increasingly involved, with around 45 per cent of the survey participants' boards taking part in the overall security strategy.
2. Directors should increase their level of cyber security literacy. Business units can be called upon to provide cyber risk assessments and reviews of their current policies, processes and budgets to protect key assets to the board. The expertise of enterprise risk management

and internal audit teams can be leveraged to provide a macro view of cyber risks specific to the company and facilitate discussions on interdependencies, prioritisation, resourcing, controls and overall resilience. Industry experts can be engaged to provide broad technology and cyber security trend briefings.

3. The board can advocate a mindset of "assuming breaches". While good cyber defences can prevent and stop most cyber incidents, they can still be breached by determined and sophisticated attackers, who will continually hunt for weaknesses to exploit. Furthermore, malware can operate quietly in the background until the opportune time, at which point the successful cyber attack may cause widespread damage across the networks more quickly than typical crises. Poorly thought through responses may result in more damage than the actual attack. Whether investors and customers retain confidence in the company depends on the company's communication as much as it does the severity of the attack. Time and resources should be invested to construct and test incident response plans.
4. The board should continuously engage management on cyber security. This will help the management and staff recognise that the board is concerned. While no universal set of questions can unearth all vulnerabilities, those listed in the box, "Cyber security questions that directors should ask of management" will be a good way for directors to engage with management.

Becoming cyber resilient

Successful cyber attacks are inevitable – even the most technologically sophisticated countries and organisations have fallen victims to this first-world invention. Petty cyber incidents are a fact of (digitally-enabled) life. Nonetheless, if we keep keeping on, improving our cyber security strategies and staying vigilant, we can cyber risk and ultimately strengthen our resilience in the event of successful cyber attacks. ■

Cyber security questions that directors should ask of management



Assessing risks

- What are the cyber security risks of top revenue generating assets?
- What are the cyber risks that our vendors and third-party service providers expose us to? Do our contracts with them have cyber security requirements?
- What are the implications of successful breaches – business continuity, legal, financial, reputational?



Assessing cyber security maturity

- What is our budget for cyber security?
- How is cyber security governance managed within the company?
- Does our cyber security programme cover technology, people and processes?
- What are the guidelines and processes to ensure that security is considered when we acquire, design, implement, and modify systems?
- What are the different tiers of security for our systems? How are they applied to critical assets?
- How do we configure our systems for security? For example, do we use a whitelist rather than blacklist approach for applications and users? Do we have an effective policy for restricting administrator privileges? Do we know our systems well enough to detect suspicious activity?
- What are the processes for maintaining security? For example, do we close newly discovered vulnerabilities through timely and regular patching?
- How do we validate the security posture of our systems?
- How has our cyber defence model evolved to address new technologies and emerging threats?



Planning ahead

- When building new services on next-generation digital infrastructure, what are the potential cyber risks?
- Does the roadmap for investing in next-generation services include cyber security measures?



Incident response

- When was the last time we had a cyber incident, or, what was our most significant near miss? How was it discovered, and how did we respond?
- Do we have cyber incident response drawer plans? Have these been tested?
- When and what will we communicate to investors and customers after a cyber incident has occurred?
- When and how do we engage government regulators and/or law enforcement agencies after a cyber incident has occurred?

Affording information security



By **LYN BOXALL**
Professional Development
committee member, SID

SID
SINGAPORE
INSTITUTE OF
DIRECTORS

BOARDROOM
MATTERS

One of the hot issues in play today is cyber security, especially the rising threats and costs.

Although the two terms are used interchangeably, cyber security is actually a subset of information security. The former has taken on focus and interest because of high profile attacks. However, information security – which is about the protection of information and information systems, including those in the cyber realm – is still an important and vulnerable target.

According to PwC's *Global State of Information Security Survey 2016*, information security threats have intensified over the last year with 38 per cent more security incidents in 2015 than the previous year. The survey also shows that average information security budgets have gone up 24 per cent in response.

The increased cost raises concerns about the continuing affordability of information security, especially for smaller companies. And despite the increased incidence of breaches, many companies remain hesitant about the expenditure.

This can be a grave mistake.

The aftermath of a breach

The experience is that the financial cost of a data breach can be huge.

According to the Ponemon Institute's *Global Cost of Data Breach 2016* study, the average total cost of a breach is US\$4 million, up 29 per cent since 2013. In fact, companies lose US\$158 per

compromised record, with breaches in regulated industries such as banking, costing more.

Beyond the immediate financial impact, there can be reputational damage, loss of customers, lower stock prices and regulatory sanctions.

The regulatory implications of data breaches should not be underestimated. In April 2016, the Personal Data Protection Commission (PDPC) of Singapore fined K Box and its IT vendor S\$50,000 and S\$10,000, respectively, after the personal data of 317,000 of the karaoke chain's clients were compromised and disclosed online.

Regulators step in

Indeed, there is a growing trend across the world of regulators taking a more active role in setting data security standards, and holding businesses to a greater level of scrutiny for data breaches.

In the last quarter of 2015, the Monetary Authority of Singapore (MAS) issued circulars on cyber security to the financial institutions it supervises. These covered technical and internal control processes that should be implemented, as well as cyber security training for directors and senior management.

While MAS provides financial institutions with a high watermark for managing cyber risks, the Personal Data Protection Act (PDPA) sets the baseline requirements for all organisations in Singapore. Specifically, the PDPA which came into force in 2014, requires every organisation to take reasonable security arrangements to protect personal data.

In 2017, the Singapore government will table a Cyber Security Bill in Parliament to keep pace with the evolving cyber security landscape. The Bill will empower the Cyber Security Agency to keep oversight of cyber incidents and raise the standards of cyber security providers in Singapore.

A business issue

Beyond these technology and regulatory considerations, it cannot be stressed enough that cyber security is a business issue. An attack can cause real and untold damage to the business.

That being so, the board must ensure that management satisfactorily addresses cyber threats. These are fundamental strategic issues as they pose severe financial and reputation risks.

Improving affordability

However, the cost of information security is an important consideration. Here, boards need to ensure that management properly and sensibly weighs the cost to protect against the cost of a breach.

In finding the right balance, boards can look into a number of areas to improve the affordability of information security.

The first is to require management to implement a well thought-out information security policy to protect confidential information in both electronic and hard-copy form.

For example, in the K Box case, the PDPC identified several basic technical issues such as weak passwords, unencrypted email, and lack of security systems testing. These should be part of any basic information security policy.

Studies also show that more than half of data breaches are directly attributable to careless or disgruntled staff. Staff carelessness includes not following or having proper information security policies. Disgruntled staff can cause data breaches when safeguards are not in place



to protect against actions aimed at damaging the company. Only about 20 percent of data breaches are attributable to pure cyber security attacks, i.e., those that do not involve staff, whether complicit or unwitting.

Most crucially, instead of merely creating an awareness of security and controls, companies need to create a security culture based on actively changing behaviour. This can be achieved through inculcating a belief that all staff are responsible for information security, not just those in the IT department. This should be accompanied by auditing compliance and ensuring policy enforcement. K Box, for instance, had a fairly typical password policy but in the absence of enforcement, one staff member's password comprised of a single letter, and that of the website administrator's was "admin". A whistle blowing mechanism reinforces a security culture.

Another layer of defence is cyber insurance, which is evolving as rapidly as technology. What is considered core coverage today was not available several years ago. Thus, first-party insurance is now available for data destruction, denial of service attacks, theft and extortion. Other areas of coverage include crisis management, forensic investigations, data restoration, and business interruption. ■

Boardroom Matters is a weekly column by SID for The Business Times and its online financial portal, BT Invest, where this article was first and recently published.



Trekking in a clear and present danger cyber world

By

BILL CHANG

CEO, Group Enterprise, Singtel

You know that the issue of cyber security is in the spotlight of the business world when regulators make it mandatory for boards to be educated and trained in the area and to also take part in cyber drills so they are better prepared in case of a breach.

Such new requirements are a move following an increasing trend of cyber attacks – which have been cited as one of the top five risks facing economies in the World Economic Forum’s Global Risks Report 2016 – across the world.

And the frightening news is these cyber attacks are being carried out in greater sophistication, scale and frequency, while companies are struggling

to catch up in understanding the nature of these threats and keeping up with them. Company boards and top management are increasingly recognising that cyber threats are one of the top three risks that their organisations can face and is an issue that no longer sits in the jurisdiction of the chief information officers (CIOs) alone.

From boardroom to ops room

Rather, board directors have to provide the oversight and governance with management in cyber risk assessment as part of their overall enterprise risk management framework.

To be able to do so, boards and the management themselves need to be trained in the areas of



cyber security. Such trainings should therefore be comprehensive and endeavour to cover areas like greater awareness of cyber risks, risk assessments with the decisions and investments made to mitigate them, the on-going review with management (given the very fast pace of cyber threat evolution) on the cyber defence strategy and ensure adequate funding is allocated while reviewing the associated level of risk tolerance.

The training should also help boards and management build a framework to set a culture of cyber security readiness, what to request for periodic updates with management to help evolve their cyber security maturity curve over time.

Beyond training boards and management, it is also key to train their CIOs, CISOs (Chief Information Security Officers) and cyber security operations staff. This is to continuously sharpen their defence skills in the midst of a fast-changing cyber threat landscape.

Additionally, the board should also assess the skills and experience of their bench to ensure they have the adequate digital and cyber talent.

What is encouraging is boards are starting to realise the importance of talent needed to not only help the company leverage digital technologies to accelerate growth and transform their business but also to advise and provide the

key oversight and governance with management in cyber security.

Within and beyond company walls

Today, six out of 10 cyber breaches are a result of internal lapses, which could either be caused by a weak enforcement of policies, employee negligence or involves the latter with malicious intent.

In a recent Singtel-Trustwave survey conducted in Singapore, areas in which lapses can occur include a general lack of security training, unauthorised files transfers and weak passwords, among others (see diagram “Internet threat concerns among Singapore companies”). There is a therefore need for progressive internal user education to be more aware of the “dos and don’ts” in cyber security, otherwise sensitive systems can be seriously compromised.

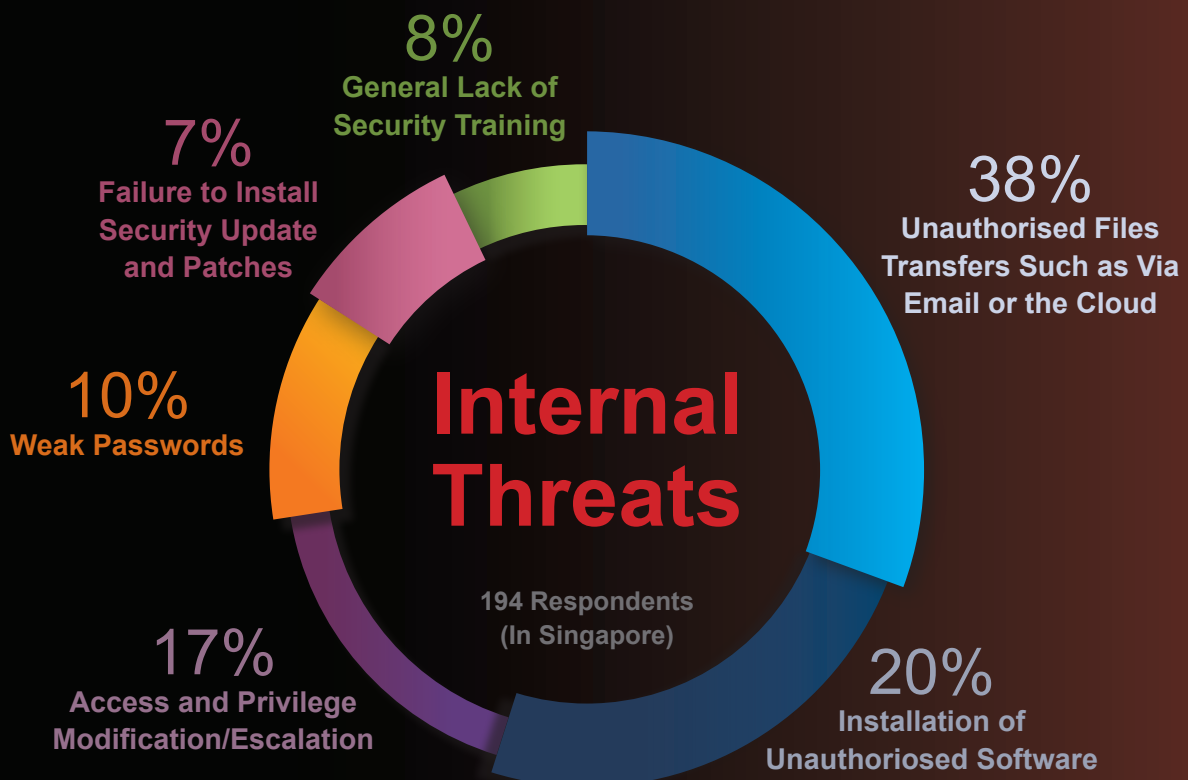
CISOs also have a key role in advising and reviewing with their boards the areas of priority in order to enhance their cyber defences as it would be too costly to defend everything that the enterprise covers.

Companies have to look at their supply chain where cyber risks are at an equal, if not higher chance of occurring, oft-times due to negligence and lapses by contractors and suppliers. The breach by its sub-contractor that cost US retailer, Target, 70 million customer records, is a good example.

Changing mindsets

Beyond awareness, risk assessment and tolerance, boards should also be trained to cover the post breach crisis management and communications process. In many high profile breach cases, the poor handling of post breach

Internal Threat Concerns Among Companies In Singapore



Source: Singtel Trustwave Security Pressures Report 2016

crisis management and engagement with stakeholders actually resulted in the destruction of the company's value, loss of trust with customers, even incurred serious probes and penalties from regulators and class action suits from shareholders.

For many companies, the extent of the breach and how it even occurred is often unknown, at least during the initial stages, and this is often made insurmountable when the breach is made public.

Succumbing to the pressure, most companies make the mistake of giving partial or even incorrect information, resulting in further loss of stakeholder confidence.

Boards and management should be trained in the post cyber breach management to develop their protocols, developing their data narrative, even regularly updating and conducting drills between boards and management not with the mindset if a cyber breach would happen but when it will happen.

Cyber talent shortage

The increasing reliance of the world on sharing and exchanging information and operating on the Internet can only mean an accelerated exposure to the clear and present dangers the cyber world has to bring. And when danger mounts, people to protect us from the cyber menace are needed more and more. However, there appears to be a shortage of these "soldiers" to defend us from these invisible enemies. As of 2016, the world is one million short of cyber-trained professionals and this number is set to swell to six million by 2019, according to Forbes.

In Singapore, our total cyber security professionals make up only one per cent of our overall ICT workforce.

This will not be sufficient for Singapore's needs as we strive towards our vision to be a Smart

Nation, which will require much higher numbers of cyber security professionals to battle in a number of fronts. Compounding to that challenge, more businesses are also accelerating their digital transformation, which means they will also require more cyber defenders to hold their forts.

Towards this end, the *National Cyber security Master Plan 2018* recently announced by Dr Yaacob Ibrahim, Minister of Communications and Information, seeks to grow Singapore's pool of ICT security experts. Some of these initiatives include:

- Promotion of R&D to attract and cultivate more cyber security expertise
- The Company-Led Training Programme for Fresh Professionals by IDA to develop ICT security specialists
- The Singtel Cyber Security Institute to offer holistic training for company boards, management, technology and operations personnel to deal with cyber attacks.
- The Cyber Security for Directors course offered as part of the SID's Business Future series.

So in a very tight cyber talent market globally, it is key that companies invest in the on-going training and development of their boards, management and cyber professionals to better defend themselves and also retain their rare talent.

For companies without the core talent of cyber professionals and have to defend themselves against ongoing cyber threats, they should consider partnering with a managed security service provider (MSSP). In this aspect, they have to consider MSSPs with deep and global capabilities, considering the nature of this global threat phenomenon that we will face for a long time to come. ■



Seizing the cyber security challenge with data stewardship

By

SIOBHAN GORMAN

Director, Brunswick Group

In today's digital world, the data a company holds brings both risks and rewards. Companies need to develop a strong data narrative that shows customers they are good stewards of the data their company holds, while also putting plans in place to manage and mitigate cyber crises in the future.

The challenge of data stewardship is particularly acute in Singapore, where awareness of cyber threats is high.

In a seven-country survey conducted by Brunswick this year, Singapore consumers voiced the highest level of concern about the security of their data. With 93 per cent of consumers expressing concern, Singapore consumers are worried more about data security than the economy, healthcare, or job security.

These concerns translate into business risks. Consumers increasingly expect companies to protect their data and are quick to blame companies that lose it.

In fact, Singaporean consumers are more sensitive to data protection than their counterparts elsewhere: 66 per cent of consumers in Singapore say that companies should be doing more to protect their data, while globally, the number of consumers who believe companies should be doing more is 62 per cent. What's more: 56 per cent of consumers in Singapore say they would boycott a company that was hacked.

These views are matched with declining trust in companies to keep their data secure and a corresponding belief that companies are to blame for data breaches, with 74 per cent of consumers in Singapore saying they will blame a company

for a hacking incident – that is two and a half times the proportion who would blame the hackers themselves.

This number is remarkable and should give boards and corporate leaders pause, given the growing frequency of hacking incidents, even of companies that take strong security precautions. Increasingly, these incidents are becoming public.

They are expensive, as well. Recent estimates project that each cyber attack could set back a company by US\$3.8 million, and the reputational cost of every stolen record valued at US\$154.

Cyber hygiene

Smart companies are now planning for these business risks, which can become significant reputational challenges when not managed effectively. Some of the best ways to mitigate cyber risks are the most basic: Update your security software regularly and have a cyber crisis response plan.

U.S. government officials estimate that 80 per cent of hacking can be prevented with basic cyber “hygiene,” which is keeping firewalls and other security programs updated with security patches. Implementing basic access controls, so it is harder for a hacker to gain access to the company’s crown jewels, is also a useful step to take.

Implementing these and other best practices will not only improve company security, but will also enable a company to develop a data narrative that provides reassurance to customers that it is being a responsible steward of their data.

Cyber responsiveness

Developing response plans – both for operations and communications--based on the most likely and most damaging cyber scenarios for a company will also serve multiple purposes. Having a plan will help a company lead confidently through its crisis, even if the plan doesn’t cover every eventuality.

The process of assembling the plan will bring together key players across a company to discuss the company’s most pressing cyber issues. Oftentimes, clients have found that the process of putting a cyber crisis response plan together is at least as valuable as the plan, itself.

However, having a plan is not enough. It is critical to see how the plan works – and better to test that in a simulation than when the crisis hits. So, regularly holding simulations to test and adjust cyber crisis response plans is important. Just as critical, is having the right people at the table. Simulations should involve leadership across the company, and the best ones include board members who can inject a board perspective into the decision-making process.

Extending the cyber education effort beyond leadership to employees is another step leading companies are now taking. These programs are not one-and-done online courses but rather multifaceted campaigns that are tailored to the corporate culture and measured regularly for effectiveness.

Cyber differentiation

In answering the majority of Singapore consumers who say they are not doing enough to protect their data, companies also have an opportunity. Those who prioritise the protection of consumer data and communicate that effectively to their customers will differentiate themselves from competitors and earn their customers’ trust.

Developing a company narrative and building a company’s initiatives around it to show how the company is prioritising data protection is a key way to build consumer trust on this issue. It puts a company on a firm footing, should it need to explain or defend its actions in public. “We did all we could,” is a much stronger response than, “We didn’t see it coming.” ■

SID Directors' Conference 2016

An immersive digitally disruptive experience

More than 900 local and international company directors, and government and business leaders checked in at the seventh annual SID Directors' Conference on 5 September 2016 on the theme of "Digital Disruption".

The setting of the event was clearly digital. Attendees were first greeted by a gigantic screen highlighting the conference when they arrived at the ground floor lobby of Suntec Singapore Convention and Exhibition Centre where the event was held.

The event hall for the plenary session initially appeared to be a regular conference set up with banners and projection screens. However, when the opening video played, the three walls circumscribing the stage "collapsed" and images of disruptive technologies burst forth from the 180-degree panoramic screens lining the walls to depict the opportunities and threats for companies in the digital age.

SID Chairman Willie Cheng's opening address used the immersive audio-visual and screens



to good effect as he emphasised making digital a key part of the boardroom agenda with an augmented reality presentation.

Dr John Seely Brown, a.k.a. as “Chief of Confusion” was then seen in what looked like his living room in Silicon Valley bantering via video-conferencing with emcee-host and SID Council Member Wilson Chew. Dr Brown then delivered his keynote address via holographic projection appearing on a “holo-podium” on the stage, before being teleported live onto the stage in the blink of an eye. The teleportation sequence alluded to the rapidity and unpredictability of today’s era of technological disruption, what Dr Brown termed “The Big Shift”.

Dr Yaacob Ibrahim, Minister for Communications and Information and Minister In Charge of Cyber Security was the guest-of-honour at the event. He underscored the opportunities and challenges that technological disruption brings, and cited how the Government is studying closely the implications of this phenomenon for Singapore.

Minister Ibrahim also witnessed the signing of two Memorandums of Intent between IDA and Surbana Jurong, and between IDA and Lendlease.

Following the GOH and keynote addresses, three plenary panels took place on the topics of the board agenda, digital transformation, and cyber threats. Throughout the plenary sessions, attendees were encouraged to post questions to speakers and panelists and participate in the polls, which they could easily do via the SID Conference mobile app that was launched for the first time at the event.

In the afternoon, attendees had lunch in the “Digital Den”, an exhibition on how to respond to the challenges of the digital age. In addition, they could attend eight breakout sessions on various aspects of digital disruption.

All in, the Conference featured more than 50 speakers, several of which came from Australia, Europe, the US and South Africa to share their perspectives at this event. Feedback on the event has proven to be very positive.



Plenary Speakers

A new “white water” world

“The 21st century infrastructure is driven by continual exponential advances of computation, storage and bandwidth, with no stability in sight. Be prepared for a rapid set of punctuated jumps for the next 20 to 40 years. Institutional architecture and even our ways of knowing will have to be re-thought. This Big Shift in the reordering of the way we live, learn, socialise, play and work is akin to the sport of whitewater rafting. The world is getting increasingly fast and rapidly connected; it is important to know your own centre of gravity, have balance and authenticity, to respond in the moment.”

Dr John Seely Brown, Chief of Confusion and Co-Chairman at Deloitte Centre for the Edge



The board’s dual roles in digital disruption

“Digital disruption plays to both roles of the board. Innovation and digital transformation harks to the board’s performance role. Risk management of the threat of cyber attacks and the threat of irrelevance from being digitally disrupted, harks to the board’s conformance role.”

Mr Willie Cheng, Chairman, SID



Decisive leadership is needed to respond to disruption

“It is hard to take the threat of disruption seriously until it begins to impact your bottom-line. But not acting until then would have lost you a significant first-mover advantage – one that can only be gained by disrupting your own business. Sometimes it is a matter of resources and trust... Ultimately, culture does matter. Efforts to be future-ready live and die by leaders setting the right priorities, incentives, and expectations, thereby building a culture of innovation and risk-taking.”

Dr Yaacob Ibrahim, Minister for Communications & Information



Left to right: Mr Pooh Joe Keen (Surbana Jurong); Mr Khoong Hock Yun (IDA), Minister Yaacob Ibrahim, Mr Willie Cheng (SID), and Mr Richard Paine (Lendlease) at MOI signing.

Plenary Panel 1

Board Agenda: Digital Disruption



Left to right: John Seely Brown, Robert Yap, Jacqueline Poh, Koh Boon Hwee, John Senior.

“Digital disruption is less about technology, but more about transforming business models. There is a lot of technology out there but how we decide we use it in business is what makes the difference. For instance, with Singapore’s vision of the Smart Nation, we are looking at how technology can be used to transform the way the Government engages with citizens on a one-to-one basis through digital government. Separately we are looking at more efficient mobility, optimizing the running of the city ‘as a machine’. These different approaches to the use of technology are not the same.”

Ms Jacqueline Poh, Managing Director, IDA

“There are two societal impacts of digital disruption that would impact boards. The first is the increasing divide between the haves and the have-nots in an increasing digital economy. The lion share of the value-add from technology will go to those who understand and produce the technology, not those who are merely using the technology. The second is in manufacturing which with robotics, artificial intelligence, sensors, etc, will reduce the number of workers needed. Manufacturing today employs about 20 to 25 per cent of the workforce. It would not be too far away when this could fall to 10 per cent and governments will have to deal with the political fallout, which will eventually affect businesses.”

Mr Koh Boon Hwee, Managing Partner, Credence

“Always be paranoid, because you don’t know what will change your business next. We are currently using drones to count inventory and one of the first to adopt this technology... At the end of the day, it is all about pushing the organisation to take (these technologies) on.”

Dr Robert Yap, Executive Chairman, YCH Group

“Boards need to think more expansively to envisage how their industry or business model could be disrupted.”

Mr John Senior, Senior Partner, Telecom, Media and Technology Practice, Bain & Company

“As each company seeks to respond to digital disruption, don’t overlook the fact that we are all part of the broader ecosystems, so one of the catches is that you may not have to make all the investments yourself. The question is how do you build rapidly strategic networks that actually have complementary resources to let you actually build something that is real but also gives you agility at the end?”

Dr John Seely Brown, Chief of Confusion and Co-Chairman at Deloitte Centre for the Edge

Plenary Panel 2

Cyber Threats: The Dark Side Of Technology



Left to right: David Koh, Bill Chang, Tom Srail, Siim Sikkut, Khoo Boon Hui.

“Data protection is not dissimilar to homeland security. Recognising and internalising this can help you mitigate and recover when an attack happens. In the US, we see boards benchmarking themselves against competitors and industry players – that’s the bare minimum that a company needs to have.”

Mr Tom Srail, Technology Media & Telecommunications Practice Leader, Willis Towers Watson

“Today, not a single country or industry has been spared from security breaches. Some companies take a long time to discover a breach. Prevention alone is a lost cause. Companies need to plan as though a breach is going to happen. They need to have fast detection, and also the strongest defense possible on the very critical components.”

Mr Bill Chang, CEO, Group Enterprise, Singtel

“Four years ago, a good friend of mine, Robert Mueller who was Director of the FBI said, ‘... there are only two types of companies: those that have been hacked and those that will be.’ Last year, John Chambers, Chairman of Cisco said, ‘There are two types of companies: those that have been hacked, and those that don’t know they have been hacked.’ In a way, this illustrates how the landscape of cyber threats has dramatically changed.”

Mr Khoo Boon Hui, Former President, INTERPOL, and Director, ST Engineering

“Given our dependence on cyber, businesses that are reliant on confidence and reliability need to look not just at the return on investment in cyber, but the cost of failure if a breach occurs. There is no such thing as 100% security. It’s a three-way balance between security, usability and cost. Boards and senior management need to make a risk assessment that will balance among these three aspects. The reality is that these are decisions that are core to your business, and they need to be made at the highest level, not just from within your IT department. These discussions on cyber security issues should be elevated from the backroom to the boardroom.”

Mr David Koh, Chief Executive, Cyber Security Agency of Singapore

“Estonia, with its population of 1.3 million people, is very reliant on IT. Our citizens have digital IDs, they handle all their affairs digitally and even can vote for parliament from anywhere in the world over the internet. We were also the first country to be cyber attacked on a large scale, and that was a wake-up call for Estonia. However, we used this as a chance and learning opportunity to strengthen ourselves further. Instead of taking steps back, we moved forward with the digitisation of the country. The Estonian government invests a lot into cyber security and information sharing, partnering closely with private sectors by sharing resources and defending systems and networks together.”

Mr Siim Sikkut, Digital Policy Adviser, Government Office of Estonia

Plenary Panel 3

Digital Transformation: The Bright Side Of Technology



Left to right: Khoong Hock Yun, Sumitra Pasupathy, Julian Persaud, Bruce Liang, Helius Guimaraes, Scott Gibson (standing).

“There is no such thing as a digital strategy, just a strategy in a digital world. Customers behaviour has changed from one that is loyal to brand, to one that is loyal to experience.”

Mr Scott Gibson, Group Executive, Digital Practice, Dimension Data

“Healthcare is not a laggard in technology adoption. Due to high barriers to entry and complex ecosystem, disruption will likely be more evolutionary than revolutionary. Healthcare changes should be led by both the private and public sectors, and by having the incumbents work with insurgents and the best consumer tech companies out there.”

Mr Bruce Liang, CIO, MOH Holdings

“Rio Tinto’s ‘Mine of the Future’ programme is using next-generation systems and technologies to drive Rio Tinto to become a global leader in fully integrated, automated mining. By improving employee safety, increasing productivity in large-scale surface mining, extracting more ore from complex orebodies, lowering energy consumption and reducing environmental impact, we hope to build our sustainable competitive advantage and enable us to deliver greater value.”

Mr Helius Guimaraes, General Manager for Enterprise Architecture & Emerging Technologies, Rio Tinto

“Airbnb did not set out to be a disruptor. In 2008, the co-founders found themselves broke and were just renting out their apartments to earn extra money – that’s how Airbnb was born. Today, we have two million homes in more than 190 countries; the notion of having strangers stay in your homes is no longer a strange concept.”

Mr Julian Persaud, Regional Director, Asia Pacific, Airbnb

“There are three significant ways that technology has disrupted the social sector: process innovation, scaling up of social solutions, and increasing philanthropy and social investments. Technology in the hands of a powerful social entrepreneur can create large systemic disruption to solving social challenges.”

Ms Sumitra Pasupathy, Country Director, Ashoka

“Our smart nation vision seeks to use technologies to help enable Singapore’s continued economic and social growth while reducing the proportional higher demand for limited resources like manpower, land, energy, water. As an industry enabler, IMDA works with our ICT industry in a range of industries, such our urban logistics programme in the retail and logistics sector, use of block chain technologies in International Trade, and personalised learning in education.”

Mr Khoong Hock Yun, Assistant Chief Executive, Development Group, IDA

Breakout 1 & 2

Smart Nation: New Ways of Commerce & Working

In the breakout sessions on Smart Nation, various IDA staff shared some of the pilots and initiatives that are underway to enable Singaporeans to tackle tomorrow's problems today.

For the logistics and supply chain sector, Mr Heng Wei Yeow, Assistant Director of the Logistics, Manufacturing and Retail Sector of IDA described how new eCommerce technologies have helped overcome traditional issues such as delayed orders, loading docks congestion, inventory stock-out and inefficiencies in truck utilization. As a result, goods are able to arrive at the destination on a timely basis, reducing wastage and costs to the companies.



For the retail sector, Mr New Soon Tee, Director of the Logistics, Manufacturing and Retail Sector of IDA showed how the shared platforms set up by IDA allowed SMEs to adopt new technologies more readily. Technologies such as the virtual fitting room changes the customer shopping experience significantly, while generating additional shopping data for analytics purposes. More accurate point-of-sales data also helps retailers gain better insights on the consumer buying patterns via advanced analytics.



For the trade finance function in banking, Mr Yip Shue Heng, Director of the Services Sector of IDA explained that new trail technologies such as blockchain is a game changer protocol. His advice is to consider these new blockchain technologies when transactions are untrusted, where multiple parties are involved in completing a transaction inefficiently, and when there is an irrefutable audit trail. Benefits from implementing these new trade finance technologies include the reduction of duplicate invoices, enhancement of trade security, and the strengthening of controls.



Finally, Ms Lee Chein Inn, Deputy Director of Next Generation Services Development Division of IDA shared insights on how technologies have been used to change the way we work. IDA has started establishing smart work centres equipped with collaboration technologies, near to homes, to reduce down time due to commute. By implementing these new technologies, alternative workplaces have been established to meet the changing needs of workers in Singapore today.



Breakout 3

Cyber Attacks: How Secure Are Your Company And Data?

Speakers on the cyber attacks panel each had their own take on the present and future of cyber attacks. However, as Mr Vincent Loy summarised, all agreed that cyber security is a pressing issue, one which must be addressed strategically by the board.

Mr Guido Crucq spoke about the “Cyber Kill Chain” structure of cyber attacks, and how the scope of threats is a function of tools, time and skills, amplified by motivation. Mr Shade Sanford reiterated that cyber security has moved from server rooms to boardrooms, and that boards need five foundational elements: strategy and governance, technology, human capital, audit, and response exercises. Mr Ong Hian Leong described the advantages of the NIST cyber security framework. Mr Michael Timms spoke of the practical security application of machine learning and the future of cyber security.



Left to right:

- Mr Shade Sanford, Vice President, Booz Allen Hamilton
- Mr Guido Crucq, General Manager, Security Business Unit, NTT
- Mr Vincent Loy, Leader of Financial Crime and Cyber, Singapore & Asia Pacific, PwC
- Mr Ong Hian Leong, Managing Director and Director, Technology Department, GIC
- Mr Michael Timms, Solution Product Manager, Symantec

Breakout 4

The Boardroom Of The Future

Directors need to get into IT (or information technology) was the message of this panel.

Mr Irving Low started the panel by pointing out how boardrooms are left behind even as their companies are automating their operations. Mr Nathan Birtle highlighted that there are tools for boards to manage and annotate documents, for collaboration and action. Mr Lim Chin Hu said that such automated boardroom tools are commonplace in overseas companies and urge Singapore companies to adopt them too.

Mr Scott Russell shared about advanced tools that allow directors to consider “future scenarios” through interaction with “live” information, drilling down information, and posing “what if” questions. Mr Kevin Shepherdson brought up the issue of visibility and transparency, to assess the compliance status of regulations and strengthen governance. This, too, could be facilitated with automated boardroom systems.



Left to right:

- Mr Irving Low, Partner, KPMG
- Mr Lim Chin Hu, Director, Telstra and Citibank
- Mr Scott Russell, President and Managing Director, SAP South-east Asia
- Mr Kevin Shepherdson, CEO and Founder, Straits Interactive
- Mr Nathan Birtle, Vice President, EMEA, Diligent

Breakout 5

Digital Disruption In Banking: Reimagining The future Of Financial Services With Fintech

Fintech is a “sexy buzzy” word which the panel demystified. For a start, the audience learnt that it has actually been around for decades. Ms Janet Young observed how it has grown from a US\$2 billion to a US\$20b industry over five years, and most rapidly in Singapore over the last 2.5 years.

On the startup versus incumbent battle of disruption, she explained how some banks like UOB take a collaborative approach to fintech startups. Mr Markus wished for banks to shorten their procurement process so that new fintech startups can be quickly integrated. MAS intends to grow the fintech sector and encourages incumbent banks to be part of this. He said that making banks open up their front end with APIs is key for mass adoption.



Left to right:

- Ms Janet Young, Head of Group Channels and Digitalisation, UOB
- Mr Sopnendu Mohanty, Chief FinTech Officer, MAS
- Mr Markus Gnirck, Co-founder, Startupbootcamp FinTech and Partner, Tryb
- Mr Mark Carter, Chief Commercial Officer, Fastacash
- Mr Jeremy Tan, Founder and CEO, Korvac Holdings

Breakout 6

Digital Disruption In Hospitality: Losing Sleep Over More And Cheaper Room

Panelists discussed the causes and challenges of digital disruption in hospitality. They covered issues around reducing the costs of travel for the consumers, disintermediation of the “middle men”, and the investments needed to build the new platforms and transform business models.

Mr Loh Lik Peng spoke of the three root causes of the digital disruption in hospitality: rapid pace of change, the sharing economy, and social sharing. Mr Clement Wong shared his experience in using technology to connect travel related businesses such as tours and attractions to enhance the tourist experience. Mr Simon Fiquet illustrated how digital technology has given consumers choices and global reach at scale. He sees huge growth potential as increasing number of consumers goes mobile. Mr Luke Soon contended that the guest experience is the new battleground for hotels and travel companies.



Left to right:

- Mr Loh Lik Peng, Founder, Unlisted Collection
- Mr Robert Hecker, Managing Director, Horwath HTL
- Mr Clement Wong, CEO, BeMyGuest
- Mr Simon Fiquet, General Manager, SEA & India, Expedia
- Mr Luke Soon, Executive Director, Customer Experience Lead Advisory Services – ASEAN, EY

Breakout 7**Digital Disruption In Retail: Of Ecommerce, Omnichannel And Mobile**

The retail industry had always lived with disruption, only this time, it was about the convergence of technology and skills, with culture being key to success, said members of the panel.

Roger Egan felt that the retail market in Singapore was big, with the grocery market alone being S\$16 billion, which required businesses to scale up fast, and to engage people with technology in their DNA. Dr Terry O' Connor believed that it was necessary to invest in the core competencies of any retail business, as well as to create the right culture. Ms Emma Heap felt that the key to success today was efficient delivery of services, and that an informal and non-hierarchical culture in which people could take risks and ask the right questions works best.



Left to right:

- Dr Terry O' Connor, Group CEO, Courts Asia
- Mr Roger Egan, CEO, RedMart
- Ms Sarah Boyd, CEO, Guardian Health & Beauty
- Ms Emma Heap, Managing Director, Foodpanda Singapore

Breakout 8**Digital Disruption In Public Transport: Taxiing To A Car-Less Future**

From pirate taxis to licensed taxis, to apps like Grab, and next to driverless cars. That's how the panel recapped the disruption that is occurring in the ride-hailing industry as Dr Lee Kwok Cheong facilitated a lively discussion on the implications of Grab and Uber on taxi operators, taxi drivers and commuters.

Mr Leow Yew Chin explained LTA's vision for a "car-lite" Singapore, and its focus on public safety and mass public transportation. Mr Reuben Lai shared how Grab and its data collection efforts were first started for safety purposes in Malaysia. Mr Tony Heng described the higher cost of the infrastructure to handle taxi booking and payments of the traditional taxi operator compared to Uber and Grab which use smart phones. Mr Ang Hin Kee pointed out while electronic payment may be convenient for commuters, many taxi drivers prefer cash payments.

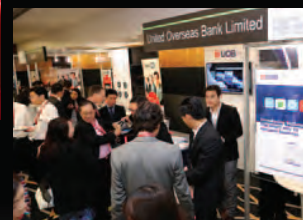


Left to right:

- Mr Leow Yew Chin, Director, Public Transport Promotion & Services, LTA
- Mr Ang Hin Kee, Executive Advisor, National Taxi Association
- Mr Reuben Lai, Group Head of Business Development & Partnerships, Grab
- Mr Tony Heng, Managing Director, SMRT Taxis and Private Hire Services
- Dr Lee Kwok Cheong, CEO, SIM Global Education

Digital Den

In the afternoon, participants had lunch in a trade fair setting where they interacted with 27 organisations showcasing their technologies, products, services and means by which they have or can be used to survive and thrive in the digital age.



Scene & Heard

“This is one of the best conferences that I have attended globally. With its superb and flawless execution, it sets a new benchmark for digital related conferences. We are pleased to have been associated with it.”

Mr Stephen Raj, Director of Enterprise Sales, Asia Pacific, Dimension Data

“I found the conference scintillating. It brought home the crucial importance of digital disruption to boards, and does so in a very digital way too.”

Mr Hsieh Fu Hua, Chairman, UOB Bank and Stewardship Asia Centre

“The conference was an experience and an eye opener for me. I was impressed with the range and diversity of speakers. The content was very relevant to what is happening today. It clearly is important for boards to face front the megatrend of digital disruption.”

Ms Pauline Goh, CEO, CBRE

“After last year’s event, I was not going to miss this year’s. I flew from Australia to attend this and it was great. The techno tsunami theme came through very aptly and strongly. The event was great networking and great knowledge too.”

Mr Robert Gordon, Director, Board Accord

“This year’s conference provided plenty of mental stimulus and new insights, a good platform to get new ideas.”

Mr Remko Wessels, Vice President Finance, Unilever South East Asia & Australasia

“I flew back from Hong Kong for this conference and was not disappointed. The digital format and presentations were totally in line with the theme of digital disruption and blew me away at times.”

Mr Tee Fong Seng, Vice Chairman Private Banking, Asia Pacific, Credit Suisse AG

The secrets & art of cyber security

On 29 July 2016, SID held a cyber security forum in partnership with PwC and Quann, a leading managed security service provider in Asia. The event, attended by over 80 directors and professionals,

brought together a group of information security experts and users to share their insights on cyber security threats and trends. We provide here key points made by the respective speakers at the event.



Left to right: Tan Yen Yen, Foo Siang-Tse, Vincent Loy, Ben Gerber, Low Huan Ping.

It's bad already, and will get worse

"While it is no longer about 'if' but 'when' a cyber attack will happen, we should not just wait for it to happen."

Joyce Koh, Executive Director, SID

"The sophisticated state-sponsored attacks will eventually and soon come to the average corporation because the sophisticated tools being used by these state-sponsored actors will become cheaper and more accessible, especially through the Dark Web."

Mr Ben Gerber, Head of Data Governance & Strategy, DBS Bank

"There is no silver bullet with cyber security. Organisations need a combination of robust technology, proven tools, the right skillsets, and real-time cyber intelligence, in other words, cyber security requires both art and science."

Mr Paul Chong, Chairman, Quann



Preparing for an attack



"You need to balance the cost, flexibility desired and the level of security."

Mr Low Huan Ping,
Chief Information Officer,
Singapore Press Holdings

"The biggest risk for DBS is not within the bank, but with customers who use handphones and other devices which are subject to hacking. By protecting these customers, we protect ourselves."

Mr Ben Gerber, Head of Data Governance & Strategy,
DBS Bank

When there is an attack

“Speedy response is critical. There should be an incident response team in place, and the team must be vested with the appropriate authority. Apart from the technical response, you must manage both the key internal stakeholders - the CEO, the Board and business users as well as the external stakeholders – customers and the media.”

Mr Low Huan Ping, Chief Information Officer, Singapore Press Holdings

“Some perpetrators have proper business model and they understand human psychology. For instance, some cyber criminals are making the ransom in ransomware cases affordable. But companies should not pay. Apart from it being illegal to pay a ransom, there is no guarantee that your data will be released or that the attacker will not come back in the future.”

Mr Vincent Loy, Partner, PwC



Do boards care enough?

“The silence of many boards is worrying. More education is needed.”

Mr Foo Siang-tse, Managing Director, Quann

“Cyber security is not a top priority on most board agendas. It tends to be relegated to the IT department. Instead, the board should ask for and review the cyber security plan.”

Ms Tan Yen Yen, Regional Vice President, SAS Institute

“Boards have other priorities. Cyber security should be a standing item on the board agenda, not only when there is an incident.”

Mr Vincent Loy, Partner, PwC



Business futures for directors



By **TAN YEN YEN**
Council member, SID

To be an effective director requires deep understanding and appropriate application of two types of knowledge: directorship and the company's business.

Directorship knowledge and competency include a slew of matters from board composition, diversity and dynamics, to senior executive compensation and regulatory compliance. These are mostly covered in the over 100 professional development sessions that SID conducts every year.

However, the fundamental role of a board and directors is to steer the company while taking risks that still grow the business and ensure the long term success of a company. To do so, directors need a deep appreciation of the company's business context: the macro-economic environment, products and services, competitive positioning, revenue and cost levers, and so on.

Much of this knowledge is formally provided to most directors as part of orientation when they join a company's board, and during the subsequent board meetings or retreats in briefings by management and external advisors.

There is usually an expectation that training matters relating to the company's business would not be provided by external parties. However, the external business context and issues are common across many companies and industries, and external briefings and forums can be found on such matters. Directors and executives can and have benefitted by attending such sessions. On its part, SID has also organised some of these



EXPANDING HORIZONS

sessions under the "Current Topics" (formerly "Hot Topics") category of our professional development framework. In the last two years, we have held sessions on emerging markets, China, intellectual property, cyber security, tax evasion and sustainability. However, much of these are short two-hour sharing sessions by experts.

My view is that directors would find greater value in a deeper dive into critical business topics that are pitched exclusively at the director level. The fact is that the role and duties of directors are different from that of management, and having a session on common business issues explained from a director standpoint and discussed with and among other directors would be more effective.

To this end, the "Business Future Series" for directors (BFS) is born. It is a series of courses that will be conducted to provide deeper understanding of common and complex business issues that boards and directors commonly face.

The future is digital

The question was what area shall we start with?

The answer became more obvious when we looked at the theme of this year's SID Directors' Conference which is "digital disruption". As our chairman, Mr Willie Cheng, noted in the last issue of the Bulletin, digital is the defining megatrend of our time.

This message was brought home by Prime Minister Lee Hsien Loong in the National Day



Rally 2016 where he highlighted disruption as the “defining challenge for Singapore’s businesses”.

It also ties in with the emerging trend of ensuring that each board should have one or more “digital directors”. In the last issue of the Bulletin, Audrey Tan of Russel Reynolds Associates defined a digital director as “someone who plays a significant role in a digital company”.

However, beyond having digital directors, it is important for all members of a board to be digitally literate. As directors, we should at least have an appreciation for technology trends and the opportunities and threats they represent to the companies that they have a stewardship responsibility for.

Towards this end, we thought we would start with two BFS courses for this year.

BFS 1: Disruptive Technologies for Directors

The first course aims to provide directors with an overview of the current trends in technologies, focusing on the major disruptive technologies such as the Internet of Things (IoT), data analytics, mobility and social media, using case studies and examples.

We are fortunate that Accenture, a global technology and management consulting firm has agreed to partner us to conduct this session, and make available its IoT Centre of Excellence. The Centre is Accenture’s first in the world and is purpose-built to show how these technologies can be harnessed

in a hands-on experiential manner, and most importantly, how they can be applied to business.

The six-hour session will be held on 4 October 2016. The faculty includes Accenture’s senior partners who lead their advanced technology practice. SID Chairman and I will also participate in a panel on digital directorship and digital literacy.

BFS 2: Cyber Security for Directors

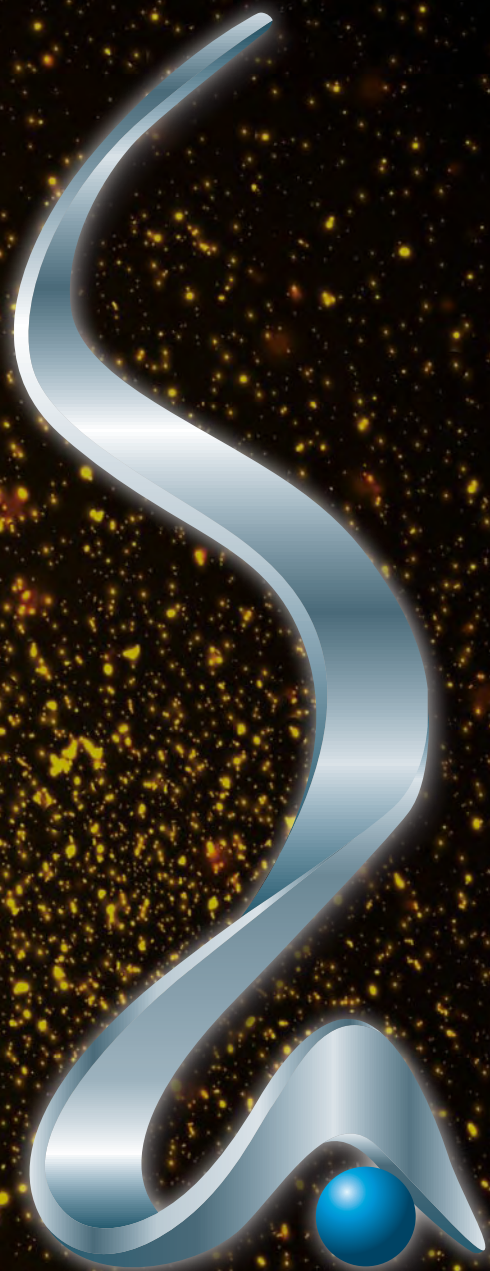
Although the topic of cyber security has been covered in previous forums organised by SID and other parties, its importance has not diminished. What most directors have not experienced in such forums is the experiential learning of dealing with cyber attacks hands on.

We have partnered with Booz Allen Hamilton, Dimension Data and PwC to put together an extended half-day programme on cyber security especially for directors on 14 October 2016.

The session will include a cyber security wargame to simulate a cyber crisis. In addition, we are fortunate that Booz Allen Hamilton is bringing in Mike McConnel who was formerly the Director of the National Security Agency of the US. Other speakers will include experts from PwC, Dimension Data and Booz Allen.

The future is?

These two courses kick off the BFS for 2016. We are currently planning for 2017, and look forward to your feedback and suggestions for other topics to cover in the future. ■



2016 SINGAPORE CORPORATE AWARDS

CELEBRATING THE BEST IN CORPORATE GOVERNANCE, “OSCAR” STYLE

The Singapore Corporate Awards celebrated its 11th year with a gala dinner that was held on 19 July 2016 at the Resorts World Convention Centre. Mr Gan Kim Yong, Minister for Health was the guest-of-honour. The black tie event is one of the most prestigious in Singapore’s corporate social calendar and was well attended by over 800 corporate leaders.

The Awards is co-organised by SID, the Institute of Singapore Chartered Accountants, and the Business Times. It is supported by the Accounting and Corporate Regulatory Authority and the Singapore Exchange, and sponsored by Bank Julius Baer.

The “Oscar” style Awards evening started with a fun-fact quiz by the emcees for the night, Ms Rachel Eng, Deputy Chairman of Wong Partnership and Mr Philip Forrest, SID Council Member. A surprise performance by the three co-chairs of the awards steering committee who displayed some cool hip-hop dance moves after their speech, warmed the crowd and promised a dazzling evening of fun and entertainment.

Later that evening, Kenneth Yap, CEO of ACRA surprised many by shedding his regulator’s hat as he impressively belted out two songs in Mandarin and English.

There was a series of presentations of the award winners, announced by six pair of hosts, done in the tradition of the Academy Awards.



The night of glitz and glamour concluded with an inaugural Special Recognition Award to recognise organisations and/or individuals that have demonstrated outstanding and exemplary corporate governance in the conduct of the affairs of boards and





organisations. It went to City Developments Limited (CDL) as a testament to its outstanding leadership and as a role model in pioneering sustainability practices in the building industry. Mr Sherman Kwek, Deputy CEO of CDL received the award. He paid special tribute to CDL's late Deputy Chairman, Mr Kwek Leng Joo for his conviction that besides doing well financially, a company should also do good for the community and the environment, which laid the foundation of CDL's Corporate Social Responsibility efforts.

The evening ended with a big bang as all winners and presenters gathered on stage for a confetti cannon send-off. ■



SINGAPORE CORPORATE AWARDS 2016

SPECIAL RECOGNITION AWARD

City Developments Limited

BEST MANAGED BOARD AWARD

Market Cap of \$1b and above

Gold
Singapore Telecommunications Limited

Gold
Oversea-Chinese Banking Corporation Limited

Bronze
Global Logistic Properties Limited

Market Cap of \$300m and less than \$1b

Gold
Yoma Strategic Holdings Limited

Silver
Keppel Telecommunications & Transportation Limited

Bronze
Riverstone Holdings Limited

Market Cap of less than \$300m

Gold
Sing Investments & Finance Limited

Silver
Micro-Mechanics (Holdings) Limited

Bronze
Global Investments Limited

BEST CHIEF EXECUTIVE OFFICER AWARD

Market Cap of \$1b and above

Mr Lim Eo Seng
Group Chief Executive Officer
Fraser's Centrepoint Limited

Market Cap of \$300m and less than \$1b

Mr William Liem
Chief Executive Officer
Tuan Sing Holdings Limited

Market Cap of less than \$300m

Mr Kong Chee Min
Group Chief Executive Officer
Centurion Corporation Limited

BEST CHIEF FINANCIAL OFFICER AWARD

Market Cap of \$1b and above

Mr Tony Mallek
Chief Financial Officer
Singapore Press Holdings

Market Cap of \$300m and less than \$1b

Mr Loh Kai Keong
Group Chief Financial Officer
Boustead Singapore Limited

Market Cap of less than \$300m

Mr Tan Kah Ghee
Chief Financial Officer
Keong Hong Holdings Limited

BEST INVESTOR RELATIONS AWARD

Market Cap of \$1b and above

Gold
StarHub Limited

Silver
Wilmar International Limited

Bronze
Capitaland Limited

Market Cap of \$300m and less than \$1b

Gold
Keppel Telecommunications & Transportation Limited

Silver
Tuan Sing Holdings Limited

Bronze
Riverstone Holdings Limited

Market Cap of less than \$300m

Gold
MegaChem Limited

Silver
Nam Cheong Limited

Bronze
Frencken Group Limited

REITS & Business Trusts

Gold
CapitaLand Retail China Trust

Silver
Ascendas Real Estate Investment Trust

Bronze
Cache Logistics Trust

First-Year Listed Companies

Merit
JUMBO Group Limited

BEST ANNUAL REPORT AWARD

Market Cap of \$1b and above

Gold
Singapore Telecommunications Limited

Silver
DBS Group Holdings Limited

Bronze
Keppel Corporation Limited

Market Cap of \$300m and less than \$1b

Gold
Keppel Telecommunications & Transportation Limited

Silver
Banyan Tree Holdings Limited

Bronze
Del Monte Pacific Limited

Market Cap of less than \$300m

Gold
OKP Holdings Limited

Silver
MegaChem Limited

Bronze
TEE International Limited

REITS & Business Trusts

Gold
Keppel REIT

Silver
Mapletree Greater China Commercial Trust

Bronze
Ascott Residence Trust

First-Year Listed Companies

Merit
Singapore O&G Limited

Merit
Fraser's Hospitality Trust

Singapore corporate governance and directorship (Chinese) seminar

新加坡企业治理准则与董事职责（中文）研讨会

2016年8月2日上午，新加坡董事协会在新加坡滨海大酒店举办首次新加坡企业治理准则与董事职责（中文）研讨会。会议由新加坡中华总商会支持，联合早报为媒体伙伴。与150与会者包括本地华商众多熟悉的面孔；不少代表主要经营地在中国的公司的董事也前来出席。

研讨会开幕，主宾--文化、社区及青年部兼财政部高级政务部长沈颖女士致辞。政务部长强调优良的企业治理及新加坡的经济增长携手迈进，尤其是在当前经济不稳定的状况有助于恢复投资者信心。



接下来，新加坡交易所首席监管官陈文仁在“监管条例的变更与考量”的话题发表主题演讲。首席监管官敦促主要经营地在中国的公司支持随即加强的监



管、改进治理实践与有关披露，并且更全面、及时披露重大信息，以让投资者对类似公司的股票有所信心。

这次会议邀请了两位曾经在新加坡与大陆演说董事职责的主讲。

首先是依莱雅斯大律师楼的许廷芳律师。许律师描述了诚信义务的概念，并抽出近期法案最要紧的见解和教训。

其次，普华永道新加坡企业治理主管--吴绍均先生阐释董事局对治理准则的集体责任。吴先生时断提





起他往年跟董事连往的轶事，并指明如何纠正独立及执行董事之间比较常见的误解。

与会者用膳过后，便是针对“董事须知”这项课题的研讨会。参与研讨的嘉宾包括：

- 许廷芳律师，依莱雅斯大律师楼顾问（主持人）
- 萧韵梅女士，新加坡交易所上市持续监管部副总裁
- 吴绍均先生，普华永道新加坡企业治理主管
- 孟繁秋先生，中国航油（新加坡）股份有限公司首席执行官
- 邓昌桂先生，新加坡股票交易所前执行副总裁及多家上市公司独立董事

研讨嘉宾各个分享他们的经验，观众也踊跃参加问答。辩论的事件包括董事局怎么保护少数股东的利益、怎样与兼大股东的总裁保持适当的联系、还有内部控制以及风险管理的新趋势与实践。

研讨会的终果：董事局必需注重“上梁不正下梁歪”的思想，努力培植公司间的道德文化。■



The Singapore Governance & Transparency Index

Launch of a new benchmark for corporate governance and accountability



On 3 August 2016, SID together with CPA Australia and the Centre for Governance, Institutions and Organisations (CGIO) of the NUS Business School launched the results of the inaugural Singapore Governance and Transparency Index (SGTI). More than 180 directors and senior management of companies came to the forum at Mandarin Orchard Hotel to find out more about the SGTI.

Mr Philip Yuen, Divisional President Singapore of CPA Australia in his opening address explained how the SGTI has evolved from the previous seven-year Governance and Transparency Index (GTI) which was used to assess and rank listed companies in Singapore based on the Singapore Code of Corporate Governance. The SGTI has strengthened these measurements by additionally drawing upon the G20/OECD Principles of Corporate Governance to develop a refined index with a sharper and more focused consideration of the company's stakeholders and shareholders.



The 2016 SGTI assesses the corporate governance performance of all the listed companies. Mr Yuen announced that the index will be extended to cover Business Trusts and REITS in the following year.

Guest-of-honour, Mr Chew Choon Seng, Chairman of Singapore Exchange (SGX) observed that the case for a holistic approach is where the SGTI brings value. The index provides a rounded, balanced perspective on how well governed the listed companies are, and how they treat minority shareholders as well as other stakeholders, and goes beyond any singular dimension of a company's score.



Associate Professor Lawrence Loh, Director of CGIO then presented the findings and interpretations of the SGTI.

With the unveiling of the results, Mr Chew Choon Seng presented awards to the top five companies overall, as well as the top company in the Mid-Cap category (S\$300 million to less than S\$1 billion market capitalisation) and Small-Cap category (less than S\$300 million market capitalisation).

A lively and robust panel discussion followed as a panel of experts shared their views and observations of the results and trends.

Mr Willie Cheng, Chairman, SID, closed the event with a sound reminder to companies to be innovative in their approach to improving corporate governance, taking into account some of the more unique characteristics of companies in Singapore.

SGTI Panel Discussion

A panel of corporate governance practitioners and experts took place after the unveiling of the results of the SGTI. It was moderated by Mr Melvin Yong, Country Head of Singapore, CPA Australia.

Mr John Lim, Chairman of Boustead Projects noted that while the SGTI shows improvements made by companies locally, there is a need to see how our local companies compare to companies from our neighbouring countries.

Mr William Liem, CEO, Tuan Sing Holdings, expressed his sentiments that there is a need to balance costs and compliance for smaller companies, in particular the SMEs, who have less resources to manage compliance.

Mr Tan Boon Gin, Chief Regulatory Officer of SGX, noted that companies tended to perform better in the scores when guidelines are followed. He advised companies to look at the rationale for corporate governance, and not focused solely on the costs involved in

ensuring compliance. Companies that follow the “comply or explain” route diligently would have achieved the necessary market discipline to good corporate governance, and gained the trust of investors.

Managing director of Aberdeen Asset Management Asia, Mr Hugh Young added that the SGTI scores revealed that the government-linked companies tend to perform better, but, in general, areas such as diversity of boards, disclosures of remuneration of top executives, and the renewal of boards still need improvement. He shared that while CG indices such as SGTI helps, investors must still do their part to analyse and assess companies.

Associate Professor Mak Yuen Teen from the audience observed that while a lot of companies have whistle-blowing policies, he did not think that they have proven to be very useful. He added that for interested person transactions, as long as an independent director has an interest in a transaction whether the transaction is ongoing or not, it should be disclosed.

GUEST OF HONOUR
MR CHEW CHOON SENG
CHAIRMAN, SINGAPORE EXCHANGE



Left to right: Melvin Yong, William Liem, Tan Boon Gin, John Lim, Hugh Young.

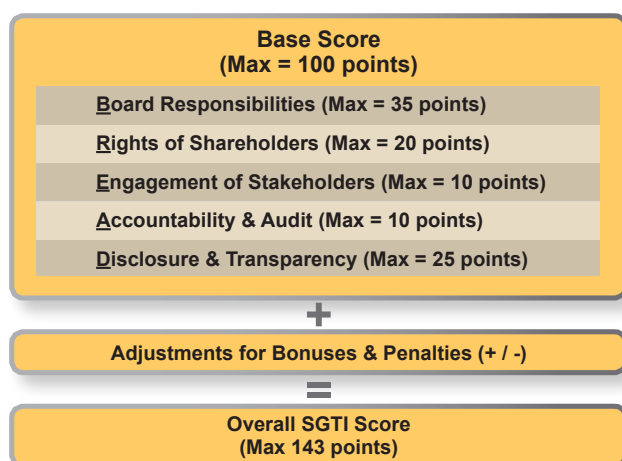
SGTI Findings

Summarised here are some key takeaways from Associate Professor Lawrence Loh's presentation on the results of the 2016 SGTI.



Methodology

- SGTI looks at five assessment areas using the following structure:



- SGTI studied 631 companies that released 2015 annual reports by 31 May 2016. In addition to annual reports, website information, company announcements, media coverage and companies' investor relations responses were used in the assessment.
- 143 companies were excluded including newly listed companies without a full year's financial reports, secondary listings, REITs, Business Trusts and Funds, and companies suspended from trading.

Trend

- Compared to the GTI in the last two years, the mean is at an all-time high of 49.7. The top scoring company has a record high of 124 points.
- The score distribution trend over three years shows that the majority of companies are improving.

Improvements

- The following improvements and areas for further improvements were noted:

Assessment Area	Improvements Made	Further Improvements Needed
Board Responsibilities	<ul style="list-style-type: none"> • Director appraisal • Selection of new directors • Board chairman independence 	<ul style="list-style-type: none"> • Time commitments of directors • Board chairman independence • Disclosure of exact remuneration of executive directors
Rights of Shareholders	<ul style="list-style-type: none"> • Voting by poll • Disclosure of detailed voting results 	<ul style="list-style-type: none"> • Disclosure of policy on payment of dividends • Directors to refrain from participation in board discussions and decision making process when they have conflicts of interest • Companies to ensure IPTs are conducted fairly and on arm's length basis
Engagement of Stakeholders	<ul style="list-style-type: none"> • Having a whistle-blowing policy • Disclosing details of whistle-blowing policy 	<ul style="list-style-type: none"> • Disclosure of policies regarding employees' health, safety and welfare, and training and development • Disclosure of customers' health and safety efforts • Disclosure of supplier and contractor selection practice • Disclosures on anti-corruption
Accountability & Audit	<ul style="list-style-type: none"> • Disclosure of risk management process and framework • Internal audit function 	<ul style="list-style-type: none"> • Having a fully independent board-level risk committee
Disclosure & Transparency	<ul style="list-style-type: none"> • Disclosure of directorships / chairmanships • Email responsiveness 	<ul style="list-style-type: none"> • Disclosure of IPT policies

SGTI Awards

Singapore Governance and Transparency Index 2016 Awards

SGT2016 Rank	SGT2015 Rank	Company Name	SGT2016 Total Score	SGT2015 Total Score	Market Cap as of 31 Dec 2016 (\$ million)	Market Cap as of 31 Dec 2015 (\$ million)
Top 5 Companies Award						
1	1	SINGAPORE TELECOMMUNICATIONS LTD	124	118	\$65,847	\$58,513
2	4	DBS GROUP HLDGS LTD	121	111	\$39,745	\$41,755
3	2	SINGAPORE EXCHANGE LTD	117	113	\$8,152	\$8,251
4	4	CAPITALAND LTD	115	111	\$13,009	\$14,231
5	3	KEPPEL CORP LTD	113	112	\$9,984	\$11,790
Mid-Cap Award						
7	10	TUAN SING HLDGS LTD	102	95	\$349	\$383
Small-Cap Award						
13	22	SING INVESTMENTS & FINANCE LTD	94	83	\$178	\$192

Note:

1. Small-Caps are companies with market capitalisation of less than \$300 million.
2. Mid-Caps are companies with market capitalisation from \$300 million to below \$1 billion.
3. Large-Caps are companies with market capitalisation \$1 billion and higher.



Left to right: Mr William Liem (Chief Executive Officer, Tuan Sing Holdings Limited), Mr Harold Woo (Senior Advisor for Investor and Partner Relations, CapitaLand Limited), Ms Khuza Suparto (Assistant Group Company Secretary, DBS Group Holdings), Mr Chew Choon Seng (Guest of honour, Chairman, Singapore Exchange), Ms Jeanne Low (Group Chief Corporate Officer, Singapore Telecommunications Limited), Mr Chng Lay Chew (Chief Financial Officer, Singapore Exchange), Mr Lee Sze Siang (Deputy Managing Director, Sing Investments and Finance), Mr Paul Tan (Group Controller, Keppel Corporation Limited).

SGTI Ranking of Companies 2016

RANK 2016	COMPANY NAME	OVERALL SGTI2016 SCORE
1	SINGAPORE TELECOMMUNICATIONS LTD	124
2	DBS GROUP HLDGS LTD	121
3	SINGAPORE EXCHANGE LTD	117
4	CAPITALAND LTD	115
5	KEPPEL CORP LTD	113
6	SEBACORP INDUSTRIES LTD	107
7	SMRT CORP LTD	102
7	TUAN SING HLDGS LTD	102
9	OVERSEA-CHINESE BANKING CORP LTD	101
10	CITY DEVELOPMENTS LTD	99
11	GLOBAL LOGISTIC PROPERTIES LTD	98
11	SINGAPORE PRESS HLDGS LTD	98
13	SING INVESTMENTS & FINANCE LTD	94
14	GREAT EASTERN HLDGS LTD	93
14	UNITED OVERSEAS BANK LTD	93
16	STARHUB LTD	92
17	WILMAR INTERNATIONAL LTD	91
18	KEPPEL TELECOMMUNICATIONS & TRANSPORTATION LTD	90
18	SEBACORP MARINE LTD	90
20	NEPTUNE ORIENT LINES LTD	88
20	SINGAPORE AIRLINES LTD	88
20	VICOM LTD	88
23	BAKER TECHNOLOGY LTD	87
23	BANYAN TREE HLDGS LTD	87
23	M1 LTD	87
26	SATS LTD	86
27	MICRO-MECHANICS (HLDGS) LTD	85
28	ARA ASSET MANAGEMENT LTD	84
28	FRASERS CENTREPOINT LTD	84
28	SIA ENGINEERING COMPANY LTD	84
32	CHINA AVIATION OIL (S) CORP LTD	84
32	COMFORTDELGRO CORP LTD	83
32	DEL MONTE PACIFIC LTD	83
32	HOTEL ROYAL LTD	83
36	OLAM INTERNATIONAL LTD	83
37	FIRST RESOURCES LTD	82
37	MEGACHEM LTD	80
37	OKP HLDGS LTD	80
37	SOILBUILD CONSTRUCTION GROUP LTD	79
41	INDOFOOD AGRI RESOURCES LTD	79
41	SBS TRANSIT LTD	78
43	BEST WORLD INTERNATIONAL LTD	78
43	YOMA STRATEGIC HLDGS LTD	77
45	AURIC PACIFIC GROUP LTD	77
45	COSMOSSTEEL HLDGS LTD	77
45	HTL INTERNATIONAL HLDGS LTD	77
48	ASL MARINE HLDGS LTD	76
48	IFAST CORP LTD	76
48	WHEELLOCK PROPERTIES (S) LTD	76
51	AZTECH GROUP LTD	75
51	GLOBAL INVESTMENTS LTD	75
51	HONG LEONG ASIA LTD	75
51	SINGAPORE TECHNOLOGIES ENGINEERING LTD	75
51	TELECHOICE INTERNATIONAL LTD	75
51	UOL GROUP LTD	75

RANK 2016	COMPANY NAME	OVERALL SGTI2016 SCORE
57	BREADTALK GROUP LTD	74
57	HALCYON AGRI CORP LTD	74
57	OVERSEAS EDUCATION LTD	74
57	VENTURE CORP LTD	74
61	CHINA SUNSINE CHEMICAL HLDGS LTD	73
61	DYNAMIC COLOURS LTD	73
61	LIBRA GROUP LTD	73
64	BIOSENSORS INTERNATIONAL GROUP LTD	72
64	CNMC GOLDMINE HLDGS LTD	72
64	JAPAN FOODS HLDG LTD	72
64	MTQ CORP LTD	72
64	PERENNIAL REAL ESTATE HLDGS LTD (FORMERLY ST. JAMES HLDGS LTD)	72
64	TEE LAND LTD	72
70	FRASER AND NEAVE LTD	71
70	NERA TELECOMMUNICATIONS LTD	71
70	YEO HIAP SENG LTD	71
73	UNITED INDUSTRIAL CORP LTD	70
74	BBR HLDGS (S) LTD	69
74	CORDLIFE GROUP LTD	69
74	FIGTREE HLDGS LTD	69
74	HONG LEONG FINANCE LTD	69
74	NORDIC GROUP LTD	69
74	RAFFLES UNITED HLDGS LTD (FORMERLY KIAN HO BEARINGS LTD)	69
74	SINGAPURA FINANCE LTD	69
74	UNITED ENGINEERS LTD	69
82	CENTURION CORP LTD	68
82	MEWAH INTERNATIONAL INC.	68
82	SHENG SIONG GROUP LTD	68
82	UNI-ASIA HLDGS LTD	68
86	AVIC INTERNATIONAL MARITIME HLDGS LTD	67
86	ES GROUP (HLDGS) LTD	67
86	NAM CHEONG LTD	67
86	REX INTERNATIONAL HLDG LTD	67
86	VASHION GROUP LTD	67
91	HUATONG GLOBAL LTD	66
91	KEONG HONG HLDGS LTD	66
91	METRO HLDGS LTD	66
91	NET PACIFIC FINANCIAL HLDGS LTD	66
91	Q & M DENTAL GROUP (S) LTD	66
96	GRAND BANKS YACHTS LTD	65
96	HAW PAR CORP LTD	65
96	HWA HONG CORP LTD	65
96	INTRACO LTD	65
96	K1 VENTURES LTD	65
96	MARCO POLO MARINE LTD	65
96	OUE LTD	65
96	PACC OFFSHORE SERVICES HLDGS LTD	65
96	RIVERSTONE HLDGS LTD	65
96	SINGAPORE EDEVELOPMENT LTD (FORMERLY CCM GROUP LTD)	65
96	SINO GRANDNESS FOOD INDUSTRY GROUP LTD	65
96	SPACKMAN ENTERTAINMENT GROUP LTD	65
96	STARBURST HLDGS LTD	65
96	TIH LTD (FORMERLY TRANSPAC INDUSTRIAL HLDGS LTD)	65
96	TIONG SENG HLDGS LTD	65

The State of Corporate Governance Disclosures Forum

In July 2016, SGX released a report on the *Review Of Mainboard Companies' Code Of Corporate Governance Disclosures* that was conducted by KPMG. On 16 August 2016, SID organised a forum with SGX and KPMG to discuss the findings of the report.

Some 160 directors and senior corporate executives turned up at the Marina Mandarin Singapore for the State of Corporate Governance Disclosures Forum.

In his opening remarks, SID Chairman Willie Cheng said all the players in the corporate ecosystem including the board, regulators, investors and industry associations have a role to play in ensuring compliance with the Code.

In his keynote address, Mr Tan Boon Gin, Chief Regulatory Officer of SGX, remarked that though the results of the review were generally good, there were areas for improvement. He added that, good scores notwithstanding, there must be an urgency in the pursuit of better standards and compliance because of recent developments. He pointed out that it is not just about

making disclosures but also ensuring material information is announced via SGX Net in a timely and clear manner, as completely as possible.

As regards determinant of materiality of whether the information will be useful to investors, he reminded the audience of the cardinal rule: "when in doubt, disclose". He further pointed out that, an issuer must announce any information which is necessary to avoid the establishment of a false market in its securities or would likely materially affect the price or value of its securities.

Mr Irving Low, KPMG Head of Risk Consulting then presented the results of the review, followed by a panel discussion on various aspects of corporate governance and the "comply or explain" regime in particular.



Insights from the Study

Summarised below are the key observations made by Mr Irving Low, KPMG Head of Risk Consulting on the study.



Methodology

- Reviewed 545 SGX Mainboard companies, excluding Catalist-listed companies, Funds, secondary listings, and those with no annual report, suspended or change in financial years.
- Focused on compliance with Code of Corporate Governance 2012, SGX Disclosure guidance Document 2015, and SGX Listing Rule 1207 (10).
- Review of 16 principles and 85 guidelines, on the following basis:
 - Presence: extent of positive or negative statement in place
 - Quality: extent of forthcoming and meaningful information

Performance

- The state of disclosures is good with room for improvement.
- Large Cap companies outperformed Small Cap and Mid Cap companies, and Government-linked corporations (GLCs) outperformed other companies.
- Scores by focus areas:



- Strongest performing guidelines:
 - Audit, Nominating and Remuneration Committees
 - Board's opinion on internal controls
 - Appointment of proxies
 - Board meetings
 - Director's key information
 - One-third independence
- Weakest performing guidelines:
 - Director, CEO and KMP full disclosure of remuneration
 - Long-term incentive schemes and reclaiming incentives
 - Executive performance criteria and conditions
 - Sustainability
 - Board diversity
- Poor disclosures happened when companies lacked awareness, frequently used boilerplate statements, have inherent process gaps, as well as when there were new requirements to track.

Tips to improve disclosures

- Corporate Governance disclosure review. Conduct a detailed gap analysis of corporate governance disclosures to ensure presence and quality. At a minimum, address the missing guidelines. Consider benchmarking based on company size and sector.
- Board practices review. Conduct a gap analysis of underlying board and corporate governance practices to substantiate the adequacy and effectiveness of such processes. Develop or enhance practices as required and reflect updates in the disclosures.
- Sustainability reporting. Review and develop processes to prepare for the effective start date of the new SGX Sustainability Reporting Guidelines.
- Corporate Governance training. Develop awareness and capabilities relating to corporate governance requirements, practices and disclosures. Attend upcoming training sessions.

Panel Discussion on Corporate Governance Disclosures

The panel at the Forum discussed a wide range of issues related to corporate governance compliance and disclosures.

Moderator Mr Daniel Ee, independent director of Keppel Infrastructure Trust, started by seeking clarification from SGX on the extent of the “comply” needed in the “Comply or Explain” regime as there was still some lack of understanding of it.

Ms June Sim, SGX Head of Listing Compliance said that the regulator had taken a progressive approach with the introduction of the 2012 Code and has decided not to take a prescriptive stance.

Following the clarification, panellists were asked if there were any results in the study that surprised them. Ms Veronica Eng, independent director of Keppel Corporation shared that “although most large private companies have no compliance regime to follow, they voluntarily set up strict framework for disclosures as it adds value to the companies”. She also observed that key investors gave more merit to companies that are transparent, and for large companies with a diverse spread of investors, this is usually demanded.

Mr John Lim, Chairman of Boustead Projects Ltd emphasised that a lot of companies still do not believe in the value of good governance. He said that “boards are too focused on shareholders who ask mostly about company performance”. Mr Lim, advised that even though shareholders may not focus on compliance with the Code, the board should still play a part in ensuring that it is closely adhered to.

Ms June Sim commented that the lowest ranked score was on remuneration, which although not surprising, was disappointing. She highlighted that in the US, companies are required to disclose

the package paid to the CEO, CFO and the top three executives. It was similarly so in Hong Kong and the UK. Ms Sim said that it is important to recognise that capital funds flow to companies and Singapore at large if investors are convinced that there is a culture of good governance and transparency. Mr Irving Low agreed that corporate governance is a journey which all companies must embark on.

During the Q&A from the floor, Mr Paul Ma, Chairman of Mapletree Greater China Commercial Trust highlighted that 99 per cent of companies in the review have said that they have adequate internal control.



He asked if this is correct and if the controls are really effective. Mr Low said that it could be an issue of understanding the definition of “effective”. Ms Eng added that it is unlikely for a company to declare that their internal controls are “ineffective” and she also questioned if all companies fully understood what “effective controls” meant.

Mr Ma also sought clarification on the need and basis for SGX requiring the Board Undertaking to be signed annually. It was clarified that only new directors appointed mid-way need to sign the individual Board Undertaking. The Undertaking is to ensure directors understand their obligations to comply with the listing rules.

Ms Yvonne Goh, SID member, highlighted that the Corporate Governance Disclosure Report is a massive one and asked who should take responsibility to draw it up and if boards





Left to right: Mr Irving Low, Mr John Lim, Ms June Sim, Ms Veronica Eng, Mr Daniel Ee.

do really review it. Ms Sim replied that some companies delegate this to a Corporate Governance Committee, but emphasised that the board is ultimately responsible for disclosures and the information should be reflective of actual company practices. Ms Sim suggested that smaller companies who are unfamiliar with CG disclosures, could approach SID for relevant training courses.

Mr John Lim added that “having processes is what results in good corporate governance. For some areas, there is no cost impact”. Ms Veronica Eng said “it is a cost only when it is deemed of no benefit. Companies who comply with corporate governance can attract and enhance company value which in turn attract investors”. Ms Sim recommended that “there is a need to ensure that the board has diversity of experience so

that they can advise the Board and hence reduce compliance-related costs”.

Mr Andy Tan, SID Council member, enquired if Singapore regulators are adopting all the regulations implemented in other countries lock, stock and barrel. Ms Sim clarified that the focus for SGX is to work with companies with the lowest scores in the review. These companies need to engage using a bottom-up approach to identify areas where they can improve and address these issues in a progressive manner.

In ending the session, Ms Sim reiterated that SGX will not be prescriptive as the US and other jurisdictions but will work and engage with companies to improve the overall level of corporate governance disclosures. ■

Building a high impact board



Twenty corporate directors and senior management attended an enlightening talk on “Building a High Impact Board” on 9 June 2016.

Mr Bob Arciniaga, Founder and Managing Partner of US-based consultancy, Advisory Board Architects, shared the trends of boardroom interactions and dynamics in the US and around the world, which he observed to be evolving at an unprecedented rate, owing to the increasing demand from stakeholders for greater effectiveness.

He kicked off the session by asking the audience on the amount of time that their boards spent on conformance versus value creation activities. It was evident that most boards spent the bulk of their time on conformance and risk management, and far too little time on value creation. He showed how companies with a high impact board performed better than those where boards were conformance focused.

Mr Arciniaga emphasised how building a high impact board, engaging and holding each board member accountable, is crucial. He outlined a four-step process, “Design-Build-Leverage-Evaluate”, highlighting only board members with the relevant knowledge and skill sets,



as well as connections that could be leveraged, should be on the board.

These board members must also be “speaking” on strategy in the boardroom 90 per cent of the time versus merely updating what already happened. He also asked the audience to explore the idea of having a dedicated team comprising relevant experts to assist them in developing, articulating, executing and evaluating strategic initiatives for the growth of the company. He shared that this strategy works especially well for family-owned or tightly-held businesses as it allows greater engagement of independents and subject matter experts on board matters.

In closing his session, he remarked that a good board should seek to be evaluated regularly as it would be immensely beneficial for the health of the company they direct. ■

Fair process leadership in the boardroom

A key challenge most boards consistently face is the process of coming to a consensus which is agreeable to all board members and management, and one which is seen to be derived through a fair process.

Fair Process Leadership (FPL), a difficult but important topic, was covered by Prof Ludo Van der Heyden, Chaired Professor in Corporate Governance & Professor of Technology and Operations Management at INSEAD. Prof Ludo articulated that in the concept of kaizen (philosophy of continuous improvement), boards should leverage FPL to build positive dynamics.

He shared that FPL is an alternate way of leading that invites stakeholders to discuss in an open and disciplined manner so that decisions made can be well executed and supported by all stakeholders.

Prof Ludo outlined the essential “5 Es of FPL” to help leaders build a robust and disciplined process for boards and management.



Prof Ludo also emphasised that a key part of FPL is communication. Leaders should ASK 80 per cent of the time, and only TELL only 20 per cent, and it is essential to know when to ask and when to tell to ensure a fair process.

In summary, the participants learnt that a FPL leader gets a good viewpoint and understanding of the situation, thinks through various key positions and functions in the organisation, and then fully supports those that execute the decisions and strategy. ■

FPL

5E & 5C OF FAIR PROCESS LEADERSHIP



Board Chairmen's Conversation Beyond the hype of IoT



On 23 June 2016, 15 board chairmen attended a session on the “Internet of Things: Beyond the Hype” at Accenture’s Internet of Things (IoT) Centre of Excellence.

Ms Teo Lay Lim, Senior Managing Director Accenture, took participants on a journey of the future of technology and its impact on businesses. She shared how, among these, IoT is changing the landscape, empowering employees to monitor operations, and boosting the productivity of companies. Accenture estimates that the IoT market will be worth about US\$14.2 trillion by 2022.

Participants were led on a tour of six different set-ups at the IoT Centre where they had hands-on experience on how drones, sensors, and augmented reality can play an increasingly important role in the natural resource and other industries.

After the tour, Ms Alison Kennedy, Managing Director of Accenture Strategy, described how IoT can change businesses. For example, by 2022, in healthcare, the US aims to use IoT extensively to keep consumers healthy without these same consumers coming face-to-face with doctors.



Participants discussed how data analytics, cloud technology and better user interface design enhance the use of IoT. They also discussed the challenges such as data privacy and cyber risk with the greater interoperability of devices.

The session raised many thought-provoking points. Board chairmen left with an appreciation for the power of this technology, how it could be applied, as well as the measures and challenges needed to ensure that the IoT delivers its value. ■

AC Chairmen: IA at the speed of business with data analytics



Fifteen audit committee (AC) chairmen attended a lunch session hosted by EY on 18 August 2016. Mr Benjamin Chiang, Partner, EY, led the discussion on the impact of technology on the internal audit (IA) function.

He said that the approach of sampling a small number of transactions out of thousands, if not millions, of transactions to evaluate control effectiveness, is no longer effective nor adequate. In addition, with the speed of businesses today, focusing on historical transactions and “yesterday’s risk”, do not provide meaningful insights on emerging risks. He shared how the use of data analytics can move IA’s focus from hindsight, towards insight (what is happening today, why things are happening) and foresight (ability to predict what will happen).

The AC chairmen engaged in a lively discussion on how IA can embark on the data analytics journey. At the same time, several felt that data analytics can also be of much value beyond IA. ■

RC Chairmen: Bridging the gap with shareholders on pay

Fourteen RC Chairmen came together on 15 July 2016 for a breakfast discussion on the worldwide pay debate.

Mr Jon Robinson, Remuneration Practice Leader, Mercer, who led the discussion, highlighted the global trend of increasing wealth and income divide and disconnect, and how this is leading to push for greater remuneration disclosure requirements through measures such as Say-on-Pay, pay ratios, direct dialogue between RCs and investors, and explicit limits on remuneration outcomes raised.



Participants discussed how these global trends could be applicable to Singapore and the local factors impacting disclosure. In summarising, Ms Wong Su-Yen, who curated the discussion, shared that global trends in remuneration will affect Singapore, but the local context will continue to steer the needs of Singapore companies. ■

Black Swans: Predicting the unpredictable



On 24 June 2016, the “Greenhouse” in Deloitte was the site for 18 directors who gathered to learn about “Black Swans”.

Mr David Chew, Executive Director of Risk Advisory at Deloitte Southeast Asia, described how Black Swans are typically outliers that come as surprises to

businesses and have major, sometimes catastrophic impacts, but when rationalised on hindsight, could have been expected. He also shared how businesses have to overcome cognitive biases comprising confirmation bias, herd mentality and ambiguity bias, and conceded that there are always threats.

Participants were then divided into four groups to review and discuss case studies provided by the Deloitte team.

How Black Swans are hard to define in businesses, yet they are real threats, and that doing away with biasness is key to recognising these Black Swans are some of the key thrusts participants derived from the session. ■

CG experts come together to enhance the ASEAN Corporate Governance Scorecard

SID hosted a two-day review meeting for 18 corporate governance experts and support staff from the various ASEAN Countries who are the respective appointed Domestic Ranking Bodies (DRBs) for the ASEAN Corporate Governance Scorecard (Scorecard).

Conducted on 20 and 21 July, the review meeting was part of the continuing discussion focused on improving the Scorecard template and strengthening the evaluation process by subjecting the company reviews by an external independent validator.

Chaired by Ms Carmela Rosario from the Philippines and who is part of the secretariat for the Scorecard initiative, the review meeting saw



active and constructive views exchanged on the current methodology. SID and CGIO of the NUS Business School, the appointed DRB in Singapore, also provided their inputs on streamlining segments of the questionnaire.

After a productive first day, participants were treated to dinner at Gattoprado, hosted by SID.

“I benefited greatly from the meeting not only from the usual exchange of ideas and best practices among CG experts, but it gave me a chance to see SID’s activities up close and how much hard work and thought go into the production of great domestic CG programmes,” said Ricardo Nicanor Jacinto, CEO of the Institute of Directors of Philippines.

With the Scorecard review in progress, there will be a gap year between official assessments. But the DRBs are not unwinding as yet as conversations will continue over the next few months on enhancing the template. ■

Director Appointments

SID members appointed to listed companies during the period 1 June 2016 to 31 August 2016.

Company	Person	Designation
Advancer Global Limited	Loy Soo Chew	Director
AF Global Limited	Woo Peng Kong	Independent Director
Asian Micro Holdings Limited	Lee Teck Meng Stanley	Non-Executive Director
Bonvests Holdings Limited	Andy Xie Guoyuan	Executive Director
Bonvests Holdings Limited	Yee Lat Shing Tom	Independent Director
CFM Holdings Limited	Er Kwong Wah	Independent Director
Edition Ltd.	Lui Seng Fatt	Independent Director
Elec & Eltek International Company Limited	Jeffrey Ong Shen Chieh	Independent Director
Elektromotive Group Limited	Ricky Ang Gee Hing	Non-Executive Chairman
Epicentre Holdings Limited	Giang Sovann	Independent Director
GKE Corporation Limited	Er Kwong Wah	Independent Director
GS Holdings Limited	Lee Dah Khang	Independent Director
Healthway Medical Corporation Limited	Ho Sun Yee	Independent Director
Hiap Tong Corporation Ltd.	Tan Eng Ann	Independent Director
Imperium Crown Limited	Alex Yong Chor Ken	Director
ISDN Holdings Limited	Tan Soon Liang	Independent Director
JES International Holdings Limited	Aloysius Wee Meng Seng	Independent Director
Jubilee Industries Holdings Ltd.	Ng Siew Hoong Linus	Independent Director
Katrina Group Ltd.	Ang Miah Khiang	Director
Koh Brothers Group Limited	Er. Lee Bee Wah	Independent Director
Koh Brothers Group Limited	Ow Yong Thian Soo	Independent Director
Koyo International Limited	Francis Wong Loke Tan	Independent Director
Loyz Energy Limited	Richard Ong Beng Chye	Independent Director
Company	Person	Designation
Pharmesis International Ltd.	Chew Heng Ching David	Non-Executive Chairman
Shanghai Turbo Enterprises Ltd	Kelvin Tan Wee Peng	Independent Director
Tai Sin Electric Limited	Bobby Lim Chye Huat	Non-Executive Director
Transcorp Holdings Limited	Kelvin Tan Wee Peng	Independent Director
United Global Limited	Leong Koon Weng	Director
Wong Fong Industries Limited	Pao Kiew Tee	Director
Wong Fong Industries Limited	Tan Soon Liang	Director



NATIONAL DAY AWARDS 2016

Congratulations to the following SID fellows and members on their National Day Awards.

The Meritorious Service Medal

Chew Gek Khim

The Public Service Star (BAR)

Kua Hong Pak

David Wong Cheong Fook

The Public Service Star

Desmond Teo Bee Chiong

Edwin Lee Yong Chuan

Sajjad Ahmad Akhtar

Goh Geok Khim

Lee Kwok Cheong

Tan Pheng Hock

The Public Service Medal

Wu Hsioh Kwang

Chew Choon Seng

The Long Service Medal

Png Cheong Boon

The Long Service Medal (Military)

LTC Khoong Hock Tai

Walk a mile in my shoes



By **SOH GIM TEIK**
Vice-chairman, SID



AFTER HOURS

I have never been much of a hiker. But for quite a number of years now, I will include hikes in my itinerary, especially when the scenery promises to be inspiring. Hikes during holidays mean I get some exercise that helps burn the extra calories I tend to take in during vacation. The four most memorable walks I have had are:

Perito Moreno Glacier, Argentina

Located within Los Glaciares National Park, which is a UNESCO World Heritage Centre, Perito Moreno is said to be one of only three glaciers in the world today that is not receding. Walking sticks, gloves, sunglasses and crampons attached to your walking shoes to grip the ice are essentials for the two-hour trek along the path around the glacier, which can get pretty icy and slick at certain junctures and the park is only accessible via the town of El Calafate. Of course, Los Glaciares is only a “tip of the iceberg” of Argentina, a beautiful country blessed with numerous natural reserves and parks.



Paro, Bhutan

This particular three-hour trek uphill to see the renowned Taktshang (Tiger's Nest) Monastery, situated about 10km outside Paro, is uplifting to say the least. I especially enjoyed the walk through the trek along

the padi fields and as you go through the countryside; you will be greeted by school children who are always eager to flash their million dollar smiles – a sight befitting of a country which tops the world's Gross Happiness Index. I also learnt that their teachers are among the highest paid among Bhutanese civil servants, and smoking and the sale of cigarettes are forbidden in the country.



Lamma Island, Hong Kong

Excellent trails are plenty in Hong Kong, like Shek O and Dragon's Back. But my favourite from last year's trip was the walk around Lamma Island. Getting there involved a ferry ride from the main island. Not only is it a hiker's haven, Lamma is also a photographer's paradise, so remember to bring along a good camera if you intend to hike there. What was interesting for me was meeting villagers who were going about their daily routines far from the madding crowd of Kowloon and Hong Kong Island. The trail ends where many seafood restaurants are congregated—an apt reward for all that hard walking!



Machu Picchu, Peru

Our hike was up Huayna Picchu, the sharp hill rising above the famous Machu Picchu ruins commonly seen in many postcards. It was my most memorable one because in spite of being ill prepared for the climb, I actually made it to the top. A good 2,700m above sea level (360m higher than Machu Picchu), Huayna Picchu peak is only open to maximum of 400 visitors over two sessions daily. My travelling group stumbled upon the entrance to the trail and a passing guide managed to convince us by saying it was “an easy walk” and we would be rewarded with a bird's eye view of the Incan citadel. It was anything but easy: the slopes were steeped and raw, steps were uneven and broken, and add to that thin air and very little safety precautions taken, the two-hour journey up was a real trudge. Apart from the magnificent view, the image of two English girls we bumped into weeping at the peak (because they were too scared to descend the steep steps) is forever etched in my mind. ■



SID's Q3 Events (July 2016 – September 2016)

DATE	TYPE	EVENT DETAILS
6 – 8 Jul 2016	PD	Governance, Risk Management and Compliance Professional Training Course
12 Jul 2016	PD	LCD Module 1: Listed Company Director Essentials
13 Jul 2016	PD	LCD Module 2: Audit Committee Essentials
13 Jul 2016	PD	LCD Module 3: Risk Management Essentials
14 Jul 2016	PD	LCD Module 4: Nominating Committee Essentials
14 Jul 2016	PD	LCD Module 6: Investor and Media Relations Essentials
15 Jul 2016	PD	LCD Module 5: Remuneration Committee Essentials
15 Jul 2016	PD	Remuneration Committee Chairmen's Conversation
19 Jul 2016	Event	SCA Gala Dinner
28 Jul 2016	PD	Nonprofit Directors (NPD) Programme Preview
29 Jul 2016	PD	The Secrets and Art of Cyber Security
1 Aug 2016	PD	FRSP Feedback with ACRA
2 Aug 2016	Event	Corporate Governance Chinese Forum
3 Aug 2016	Event	Launch of Singapore Governance and Transparency Index
4 Aug 2016	PD	So, You Want to be a Director?
5 Aug 2016	PD	FRSP Feedback with ACRA
11 – 12 Aug 2016	PD	SID-SMU Directorship Programme Module 4: Risk and Crisis Management
16 Aug 2016	Event	The State of Corporate Governance Disclosures in Singapore
18 Aug 2016	PD	Audit Committee Chairmen's Conversation
25 Aug 2016	PD	Directors Compliance Programme
5 Sep 2016	Event	SID Directors' Conference
6 – 7 Sep 2016	PD	SID-SMU Directorship Programme Module 6: Effective Succession Planning and Compensation Decisions
7 Sep 2016	PD	Masterclass for Directors Module 4: Board Evaluation
21 Sep 2016	PD	GVG Module 1: Effective Board for Growth Companies
21 Sep 2016	PD	GVG Module 2: Fund Raising for Growth Companies
22 Sep 2016	PD	GVG Module 3: The Paradox of Risk for Growth Companies
22 Sep 2016	PD	GVG Module 4: Improving Financial Savviness for Directors
22 Sep 2016	Socials	Fellows' Evening
23 Sep 2016	PD	GVG Module 5: Family Business Governance and Succession
26 – 28 Sep 2016	PD	Governance, Risk Management and Compliance Professional Training Course
26 – 28 Sep 2016	PD	IDP Module 2: Board Decision Making and Oversight
28 Sep 2016	PD	Board and Director Fundamentals
28 Sep 2016	PD	Directors Compliance Programme
30 Sep 2016	PD	Directors Financial Reporting Essentials

Sponsors Appreciation Evening • 24 June 2016



Members Networking – Laughter Yoga • 31 June 2016



Listed Company Directors (LCD) Modules 1 - 6 • 12 - 15 July 2016



Nonprofit Directors (NPD) Programme Preview • 28 July 2016



So, You Want to be a Director? • 4 August 2016



FRSP Feedback with ACRA • 1 and 5 August 2016



Upcoming events

Core Professional Development Programmes

PROGRAMME	DATE	TIME	VENUE
BFS 1 – Disruptive Technologies for Directors	4 Oct 2016	0900 – 1500	MBFC Tower 3
SID-SMU Directorship Programme Module 3: Finance for Directors	5 – 7 Oct 2016	0900 – 1700	SMU Campus
LCD Module 1: Listed Company Director Essentials	6 Oct 2016	0900 – 1730	Marina Mandarin Singapore
Directors' Compliance Programme	10 Oct 2016	1300 – 1730	Capital Tower
LCD Module 2: Audit Committee Essentials	11 Oct 2016	0900 – 1230	Marina Mandarin Singapore
LCD Module 3: Risk Management Essentials	13 Oct 2016	0900 – 1230	Marina Mandarin Singapore
NPD Module 1: The Nonprofit Environment	13 Oct 2016	1700 – 2030	SSI Training Hub
BFS 2 – Cyber Security for Directors	14 Oct 2016	0900 – 1300	Aperia Tower 1
LCD Module 4: Nominating Committee Essentials	19 Oct 2016	0900 – 1230	Marina Mandarin Singapore
So, You Want to be a Non-Profit Director?	20 Oct 2016	1730 – 2030	Crossings Café
LCD Module 5: Remuneration Committee Essentials	25 Oct 2016	0900 – 1230	Marina Mandarin Singapore
LCD Module 6: Investor and Media Relations Essentials	27 Oct 2016	0900 – 1230	Marina Mandarin Singapore
LCD Mandarin in China	3 – 4 Nov 2016	0900 – 1700	TBA
Directors' Compliance Programme	3 Nov 2016	1300 – 1730	MND Annex D
NPD Module 2: Board & Management Relationship	10 Nov 2016	1700 – 2030	SPD
SID-SMU Directorship Programme Module 2: Assessing Strategic Performance: The Board Level View	14 – 16 Nov 2016	0900 – 1700	SMU Campus
Directors Financial Reporting Essentials	25 Nov 2016	0900 – 1700	Capital Tower
Directors' Compliance Programme	2 Dec 2016	1300 – 1730	MND Annex D
NPD Module 3: Board Dynamics & Evaluation	8 Dec 2016	1700 – 2030	SATA CommHealth
IDP Module 3: Director Effectiveness and Development	13 – 15 Dec 2016	0900 – 1700	INSEAD Campus
NPD Module 4: Strategic Decision Making	12 Jan 2017	1700 – 2030	HCA Hospice Care
LCD Module 1: Listed Company Director Essentials	18 Jan 2017	0900 – 1730	Marina Mandarin Singapore
Board and Directors Fundamentals	1 Feb 2017	0900 – 1730	Marina Mandarin Singapore
NPD Module 5: Financial Management and Accountability	9 Feb 2017	1700 – 2030	SID
So, You Want to be a Non-Profit Director?	15 Feb 2017	1730 – 2030	Capital Tower
Director's Financial Reporting Essentials	21 Feb 2017	0900 – 1730	Capital Tower
So, You Want to be a Director?	2 Mar 2017	1000 – 1230	Capital Tower
LCD Module 1: Listed Company Director Essentials	8 Mar 2017	0900 – 1730	Marina Mandarin Singapore
NPD Module 6: Fundraising and Outreach	9 Mar 2017	1700 – 2030	Children's Cancer Foundation
LCD Module 2: Audit Committee Essentials	14 Mar 2017	0900 – 1230	Marina Mandarin Singapore
LCD Module 3: Risk Management Essentials	16 Mar 2017	0900 – 1230	Marina Mandarin Singapore

Core Professional Development Programmes

PROGRAMME	DATE	TIME	VENUE
LCD Module 4: Nominating Committee Essentials	21 Mar 2017	0900 – 1230	Marina Mandarin Singapore
LCD Module 5: Remuneration Committee Essentials	23 Mar 2017	0900 – 1230	Marina Mandarin Singapore
LCD Module 6: Investor and Media Relations Essentials	23 Mar 2017	1400 – 1730	Marina Mandarin Singapore
LCD Module 7: Sustainability	29 Mar 2017	0900 – 1230	Marina Mandarin Singapore
NPD Module 7: Social Trends	13 Apr 2017	1700 – 2030	Crossings Social Ventures
Director's Financial Reporting Essentials	26 Apr 2017	0900 – 1730	Capital Tower
LCD Module 1: Listed Company Director Essentials	17 May 2017	0900 – 1730	Marina Mandarin Singapore
BFS 1: Disruptive Technology	25 May 2017	0900 – 1500	TBA
IDP Module 1: Creating and Safeguarding Value	18 – 21 Jun 2016	0900 – 1700	INSEAD Campus
Director's Financial Reporting Essentials	29 Jun 2016	0900 – 1700	Capital Tower

Other Professional Development Programmes

PROGRAMME	DATE	TIME	VENUE
Board Risk Committee Chairmen's Conversation	8 Nov 2016	1100 – 1300	Alkaff Mansion Ristorante
Nominating Committee Chairmen's Conversation	25 Nov 2016	1100 – 1300	The Pan Pacific Singapore
COSO ERM Workshop	22 Mar 2017	0900 – 1100	TBA
Audit Committee Chairmen's Conversation	19 Apr 2017	1100 – 1300	TBA
Board Chairmen's Conversation	23 Apr 2017	1100 – 1300	TBA

Major Events

EVENT	DATE	TIME	VENUE
Launch of Singapore Directorship Report 2016	18 Oct 2016	0900 – 1100	Marina Mandarin Singapore
Launch of Board Guide	11 Nov 2016	0900 – 1100	Marina Mandarin Singapore
SID Annual Corporate Roundup	24 Nov 2016	1000 – 1300	Orchard Parade Hotel
SID AGM 2016	24 Nov 2016	1330 – 1500	Orchard Parade Hotel
SID-ACRA Audit Seminar	13 Jan 2017	0900 – 1100	Marina Mandarin Singapore

Socials

EVENT	DATE	TIME	VENUE
Wine Appreciate Workshop	24 Nov 2016	1800 – 1930	Club Meatballs Singapore

Course dates are subject to change. Please refer to www.sid.org.sg for the latest updates.

Welcome to the family

May 2016

Ang Jonathan
 Ang Jo-hua, Joshua
 Aw Hui Mien
 Boh Thai See
 Chan Wai Men, Andrew
 Chew Kok Chor
 Chia Wah Kum
 Choo Kok Wei, Eric
 Da Silva William
 Gallegos Dean
 Hendro Grace
 Hession Michael Anthony Ignatius
 Hew TzeYee
 Hutchinson Gerard Patrick
 Khong Choun Mun
 Koh Chai Nyuk
 Lau Kay Heng
 Lim Chiu Hsia, Celeste
 Lim Choo Leng
 Lin Ruiwen
 Long Yann Yann, Carina
 Low Wai Peng
 Lye Kevin
 Mackay Donald Stanley
 MCGowan Michael John
 Nagel Willem Frederik
 Neo Chia Reei
 Ng Charles
 Ng Shin Ein
 Okorochenko Elena
 Quek Patricia
 Shah Arif
 Shankar Narayanan
 Shepherdson Kevin Linus
 Sugiono Gabriel Giovanni
 Tan Yuh Woei
 Tan Pek Tong
 Tan Cheng Hye, Johnny
 Tan Hwee Yong
 Tan Kay Yong
 Tan Lay Koon
 Tan Yuh Cherng
 Tee Swee Siang
 Teng Soo Hai
 Tomlin Robert
 Ujioka Yasushi
 Wee Reginald
 Wong Chin Sing
 Wong Meng Yun
 Wong Wei Teck
 Yuen Pei Lur, Perry

June 2016

Bai Liguo
 Betteridge Adam Gordon Edward
 Brochet Dave
 Chan Lie Leng
 Chew Wai Yin, Doreen
 Chia Boon Leong, Richard
 Chia Yau Leong
 Chong Khee Chung
 Chua Adrian
 Chuang Tiong Kie

Daniels Aaron
 Davies Keith
 Dev Sateesh Kumar
 Ewen Jeffrey
 Goh Soo Jin
 Goh Peng Wah
 Hatton Alan Ian
 Hi Cheong Leong
 Hong Chok Hane, Jennie
 Januschka Yvonne
 Khoong Hock Tai
 Kok Peet Leong
 Kong Wai Fun, Patricia
 Kypraios George
 Lai Hing Nam
 Lim Leong Peck, Margaret
 Lim Fang Liang, Daniel
 Lim Hua Ming, Andre
 Lung Sing Wei
 Menon Dayanand
 Ng Chee Soon
 Ng Eng Kiong
 Ng Siew Choo
 Nooy Allard
 Norton de Matos Tomas A.
 Oo Cheong Kwan, Kelvyn
 Ooi Sang Kuang
 Phua Cher Chew
 Po Chee Chow, Kavin
 Ramsey Niall
 Saw Jeremy
 Seah Kim Ming, Glenn
 Selvamalar P Arul
 Siah Yang Wen, Oliver
 Siah Hung Wee
 Sim Chng Yong, Winnie
 Sim Juat Quee, Michael Gabriel
 Sincharoenkul Viyavood
 Soo Wei-Chieh
 Syn Hsien-Min, Michael
 Tan Yam Ngee, Marcus
 Tan Hooi Bin
 Tan Ly-Ru, Dawn
 Tan Teck Liang, William
 Tang Kok Fai
 Tee Fong Seng
 Teo Randy
 Toh Jin Chiang, Brian
 Wan Kin Choy, Francis

July 2016

Agrawal Vinay
 Ang Soon Leong, Nicholas
 Carl Johan Pontus Sonnerstedt
 Chan Jwee Heng
 Chee Soon Cheng, Arthur
 Chia Nam Toon
 Chua Serene
 Clements Scott
 Eu Yee Fong, Clifford
 Fagan Kenneth
 Goel Divay
 Goonetilleke Aruni
 Hashizume Toshifumi
 Koay Bee Fong

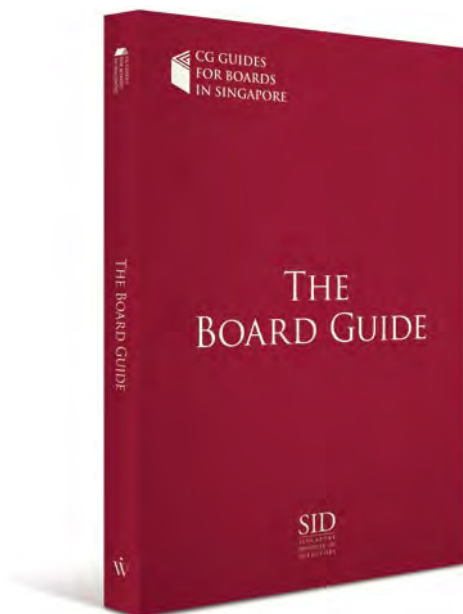
Koh Ching Hong
 Koh Kok Tian
 Lai Keng Wei
 Lau Kenneth
 Lee Andrew
 Lee Lai Who, David
 Lim Albert
 Lim Michelle
 Lim Simon
 Lim Swee Lee
 Lim Yit Keong
 Lin Nigel
 McKinley Brian
 Naismith Murray Paul
 Ng Siew Hoong
 Ng Wei Joo
 Padmanabhan Abhayakumar
 Poh Jing Shan, Josiah
 Sau Ean Nee
 Schmidt Stefan
 Shegar Brian B
 Tan Alvin
 Tan Eng Heong, Jeffery
 Tay Yu-Jin
 Venkataraman Raju
 Yap May Ling, Merleen

August 2016

Boo Hui Yun
 Chung Lai Hoon
 Chung Richard
 Jeffrey Ting Tshung
 Detmold Pippa
 Finlayson David
 Fong Mervyn
 Goh Siew Lian
 Goh Heng Heng Benny
 Heerasing Bobby Ashick
 Heng Tong Bwee
 Khan Yahiya
 Lam Raymond
 Law Kim Lam
 Lee Kief
 Lee Geok Ing
 Lee Seck Hwee
 Lee Ka Shao
 Lieu Chin Leong
 Liew Yun Chong Agnes
 Liow Chang Lee
 Morgan Rona
 Nejade Henri
 Ng Koon Keng
 Ng Wilson
 Pong Siew Inn
 Ryan Francis Benedict
 Soh Chee Hwee, Alex
 Steiner Bernhard
 Tan Kay Yan
 Tan Kok Heng
 Teh Chun Sem
 Thio Tse Gan
 Thye Kim Meng
 Toh Seng Hong
 Unsworth Gregory Andrew
 Wong Kok Hoe



LAUNCH OF BOARD GUIDE



Date: Friday, 11 November 2016

Time: 9.00 am to 11.00 am

Venue: Ballroom, Level 1, Marina Mandarin Hotel

Guest of Honor

Ms Indranee Rajah

Senior Minister of State for Law and Finance

Keynote Address

Mr JY Pillay

Chairman, Securities Industry Council

Board Guide Presentation

Mr Ng Siew Quan

Partner, PwC Singapore

Panel Discussion

Mr Yeoh Oon Jin

Executive Chairman, PwC Singapore

Mr Robert Gordon

Director of Programs, Board Accord

Mr Piyush Gupta

CEO, DBS Group

Professor Walter Woon

SC, David Marshall Professor,

National University of Singapore Faculty of Law

Closing Remarks

Mr Ng Yao Loong

Executive Director, MAS

Cost: \$60 for SID members \$90 for non-members

Register for the event at www.sid.org.sg

Boardvantage

Going paperless with your board has never been easier



Organisations around the globe are experiencing the benefits of the Boardvantage board portal called MeetX. You can too.



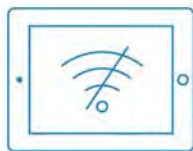
Automate the board meeting process

With dedicated workflows and support for last-minute updates, MeetX automates boardbook creation and distribution. Board members view the particulars of the current meeting or quickly reference relevant items from previous meetings. Any updates are flagged with visual cues.



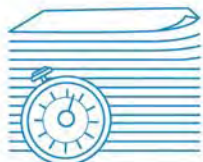
Go beyond boardbook access

When it comes to eSigning consents, voting on resolutions, or filling out self-assessments, MeetX makes all board process paperless.



Make online-to-offline transparent

MeetX auto-syncs its content so board members have ready access to their documents, private notes, approvals, and surveys, whether online or offline. Even annotations made offline sync back to the server when the board member is back online.



Cut cost, time and paper

With MeetX, you no longer have to print, ship and track board materials, and no one has to lug them around.

In 50 countries and half the Fortune 500

Request a free demo at boardvantage.com/demo.

boardvantage.com/sg

1 Raffles Place #20-61, Tower 2, Singapore 048616
6808 5672 | sales@boardvantage.com