Cyber Security Perspectives

OPTUS

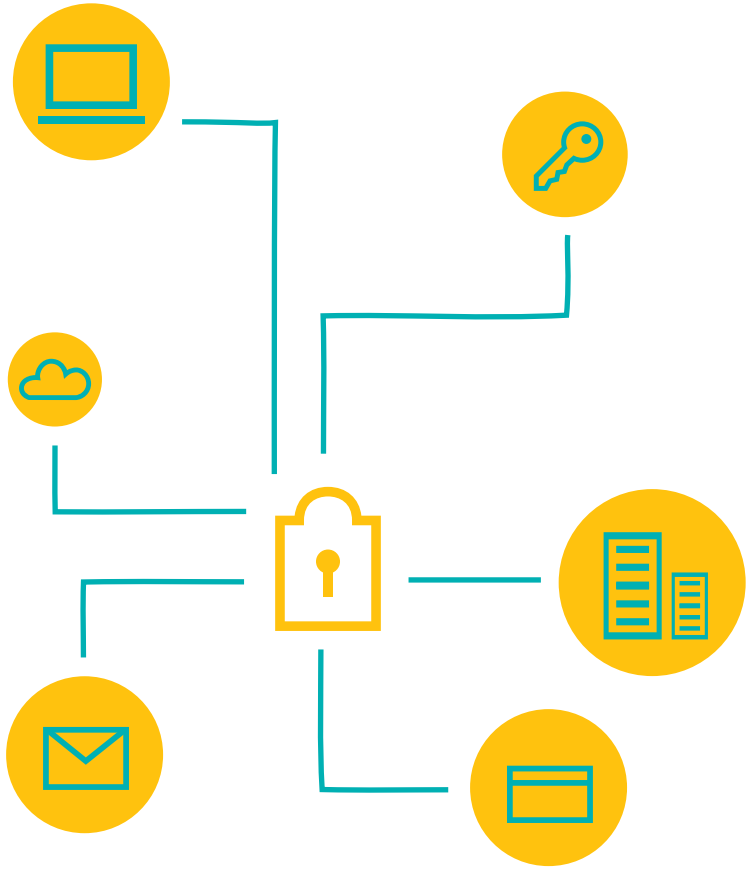
Contents

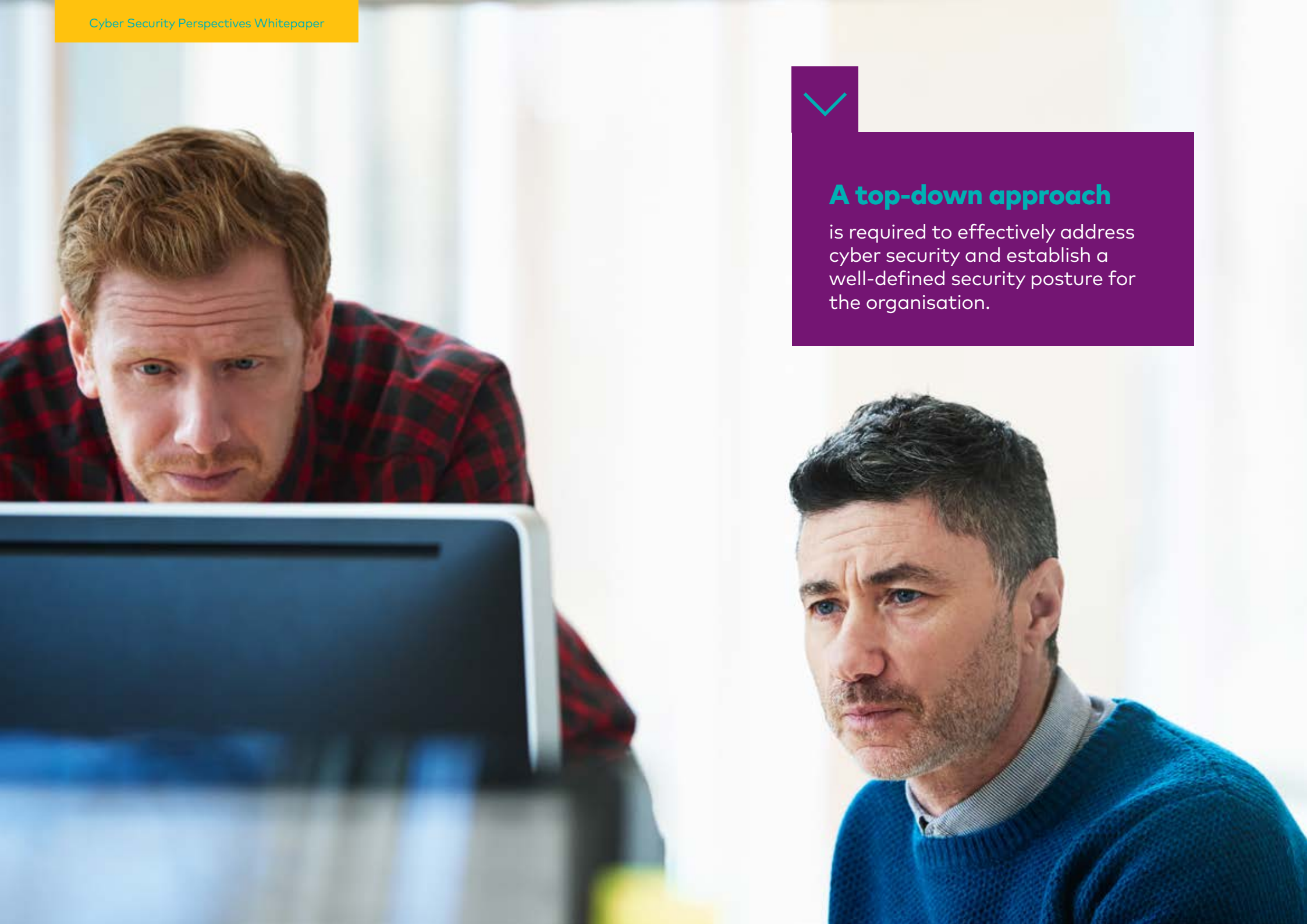
Executive Summary

Data thefts, cyber crimes and malicious attacks are wreaking devastating damage on businesses. Cyber criminals and hackers are increasingly stealthier and more sophisticated, and are infiltrating networks without being detected. As a result, the real cost of a cyber attack increases exponentially with delays in detection and time taken to respond to breaches; costs range from both direct financial losses and regulatory impact to less quantifiable, but no less long-ranging, damage to reputation, credibility and brand perception among customers and shareholders.

With cyber security morphing from a niche IT issue to an enterprise risk, the Board, with its responsibility to shareholders, has an important role to play.

Board members need to take proactive steps to increase their cyber security awareness, equip themselves to sift through technical jargon to appreciate and assess strategic and business implications, and shift from a position of acknowledgement to leadership and ownership over cyber security decisions.





A top-down approach

is required to effectively address cyber security and establish a well-defined security posture for the organisation.

Cyber Security in the Boardroom: From Acknowledgement to Ownership

As recently as a few years ago, cyber security was not a topic often discussed in the boardroom.

With cyber crime costs projected to reach $2 Trillion by 2019[1] it is increasingly becoming a critical concern for businesses of all sizes, industry and location.

Although boards have acknowledged its importance in today's digital economy, most still perceive it as an IT risk and therefore delegate such issues to the Chief Information Officer (CIO) or Chief Technology Officer (CTO).

Over the last two years alone, many high-profile cyber attacks on JP Morgan, Target, Home Depot, Sony, Ashley Madison, Anthem, Bangladesh Bank and more have driven investors, governments and regulators to press boards to account for their diligence in this area, as part of their fiduciary duties.

To effectively address and oversee decisions relating to cyber security, a top-down approach is required to establish a well-defined security posture for the organisation. The board needs to:

- **Proactively acknowledge the impact of cyber risks;**
- **Prioritise cyber security conversations in the boardroom; and,**
- **Be equipped to ask the right questions and engage in meaningful conversations with management.**

Understanding the Global Threat Landscape

From nuisance-causing incidents and data theft for economic or political gains, covert cyber crimes for financial gains, to high-visibility hacks and destructive attacks, cyber threat actors have diverse motivations and will manifest themselves differently.

Across the Cyber Threat Landscape

Cyber threat actors are exploiting networks for an ever-widening array of economic and political objectives.

	Nuisance	Data Theft	Cyber Crime	Hacktivism	Destructive Attack
Objective	Access & propagation	Economic, espionage & political advantage	Financial gain	Defamation, press & policy	Disrupt operations
Example	Botnets & spam	Advanced Persistent Threat (APT) groups	Credit card theft	Website defacements	Delete data
Targeted	✗	✓	✓	✓	✓
Character	Often automated	Persistent	Frequent opportunistic	Conspicuous	Conflict driven

Ease in Purchasing or Renting Hacking Products and Services

Cyber vulnerabilities can be easily purchased via cleverly-camouflaged commercial entities or brokerages.

Zero-day vulnerabilities sell easily starting from[2]

US$5K < US$250K

For an Adobe Reader exploit

For an iOS exploit

Lizard squad, a hacker collective's service[3]

"LizardStresser"

Enables anyone to launch a Distributed Denial of Service (DDoS) attack on servers to take websites down

"Harvested" data is available for sale[4]

- Credit card details - from the widely reported December 2013 breach of retail giant Target's 40 million credit cards and 70 million user accounts – were available in the black market within days of the attack.
- They are priced at US$23 to US$135 each - depending on the card type, expiration and credit limit.

Easy access to both tools and monetisation avenues has fanned the scale and profile of fast evolving cyber attacks. The threats posed to businesses are as varied as the criminals sitting behind their computers.

Distributed Denial of Service (DDoS) Attacks

Cyber threat actors are exploiting networks for an ever-widening array of economic and political objectives.

What is a DDoS attack?[5]

A Distributed Denial of Service (DDoS) attack aims to interrupt or suspend the online services of a web-connected system, such as banks, credit card payment gateways and more. A common method used by malicious hackers is to command a fleet of remotely-controlled machines to generate a flood of traffic or communication requests to a server. This uses up the target's bandwidth, paralysing the system and denying users access to essential online services.

What is its purpose?

Organisations and nations are targets for financial extortion, protests against certain humanitarian or government policies, for political espionage or to cause a nuisance.

Who are its targets?

According to Akamai, the top 2 most attacked verticals by DDoS are: Financial Services and Retail[6].

What are the damages?

Companies reported an average of US$1.5 million in DDoS related costs over the average of 4 DDoS attacks they suffered in the last 12 months[7].

Hard Truths[8]

8 out of 10 were mega DDoS at or above 100Gbps in 2014

Largest **DDoS attack** reported in 2014 was 400Gbps (compared to 8Gbps reported as largest attack 10 years ago)

90 hours is the average duration of each attack campaign

90% of respondents reported application-layer attacks, with 42% experiencing multi vector DDoS attacks.

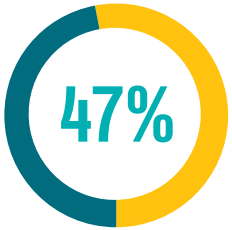
Zero-Day Attacks: New Enemies That Require New Defence Strategies

Traditional Defence Not Sufficient

Traditional firewalls, intrusion detection systems and anti-malware programmes as defence mechanisms have been proven ineffective in the face of a new generation of zero-day attacks. These exploit previously unknown vulnerabilities in a computer application or operating system, and infiltrate networks without triggering intruder alerts.

How compromises are being detected[9]

Victims discovered the breach internally



Victims notified by an external entity

Time Magnifies Impact of Breaches

One critical factor magnifies the impact of such breaches exponentially as compared to traditional threats: Time. This is significant especially when there are delays in breach detection, and when organisations experience a period of downtime while recovering from a breach.

Time from earliest evidence of compromise to discovery of compromise[9]

Median number of days that threat groups were present on a victim's network before detection

59 days less than 2014

Longest presence: 2,982 days

Breaches Do Not Stop at Detection

Detection is not the end of the story. Once breached organisations often need many hours of incident response support to recover from the breach. Consider the repercussions equivalent delays in remittance to a bank or a disruption in supply chain may have on your business.

Zero-Day Attacks By Sophisticated Cyber Criminals

Zero-day attacks are perpetuated by technically advanced actors that help cyber crimes go undetected or un-remedied for an extended period of time They are often associated with Advanced Persistent Threat (APT) groups who launch sophisticated attacks to evade traditional defences.

Advanced Persistent Threat (APT) Attacks

What are APTs?

Advanced Persistent Threats (APTs) are stealthy and continuous hacks orchestrated across a long period of time, targeted at a specific business or individual within an organisation. System vulnerabilities are often exploited using sophisticated techniques, months before an actual attack is launched. These initial intrusions are backed by highly-organised and persistent efforts to extract data off a specific target from an external command and control.

What is its purpose?

Organisations, individuals and/or nations are targeted for data theft, economic gains or political advantage.

Who are its targets?

More than 50% of APT attacks in Southeast Asia are targeted at these industries: Government (27%), Telecommunication (24%), Financial Services (16%), High-Tech (10%) and more[10].

What are the damages?

The loss arising from diminished brand and reputation is the most costly consequence of APT attacks. Amounting to three times that of other factors, it is estimated to average US$9.4 million, according to a US-based survey[11].

Hard Truths

US$9.4 million

US$9.4 million was the estimated average cost to restore reputation after an APT attack [11].

>3X other cost

This was 3x greater than other cost categories: technical support (US$ 2.5 million), revenue and business disruption (US$3 million) and productivity loss (US$3.1 million)[11].

78%

78% of APT phishing email often impersonate the targeted company's IT or security department, or an anti-virus vendor[12].

47%

47% of victims did not detect attacks on their own, but learnt from a third party, such as supplier, customer, or law enforcement[12].

In a breach, internal and confidential data as well as customers' data **could be leaked, modified or stolen.**

Sizing It Up: What Do All These Mean to Your Organisation?

Costs of Data Breaches[13]

Data is one of the most valuable assets of enterprises. In a breach, internal and confidential data, as well as customers' data could be leaked, modified or stolen. According to an independent study sponsored by IBM and conducted by Ponemon Institute, the average total cost of a data breach in 2014 is US$3.5 million, a 15% increase from 2013[13].

The study revealed the following[13]:

42%

Malicious or criminal attacks are most often the root cause of data breaches globally (42%); other causes are employee negligence (30%) or system glitches (29%)

US$145

Average cost paid for each lost or stolen record containing sensitive and confidential informaion.

Industries that registered the highest per capita data breach costs are:

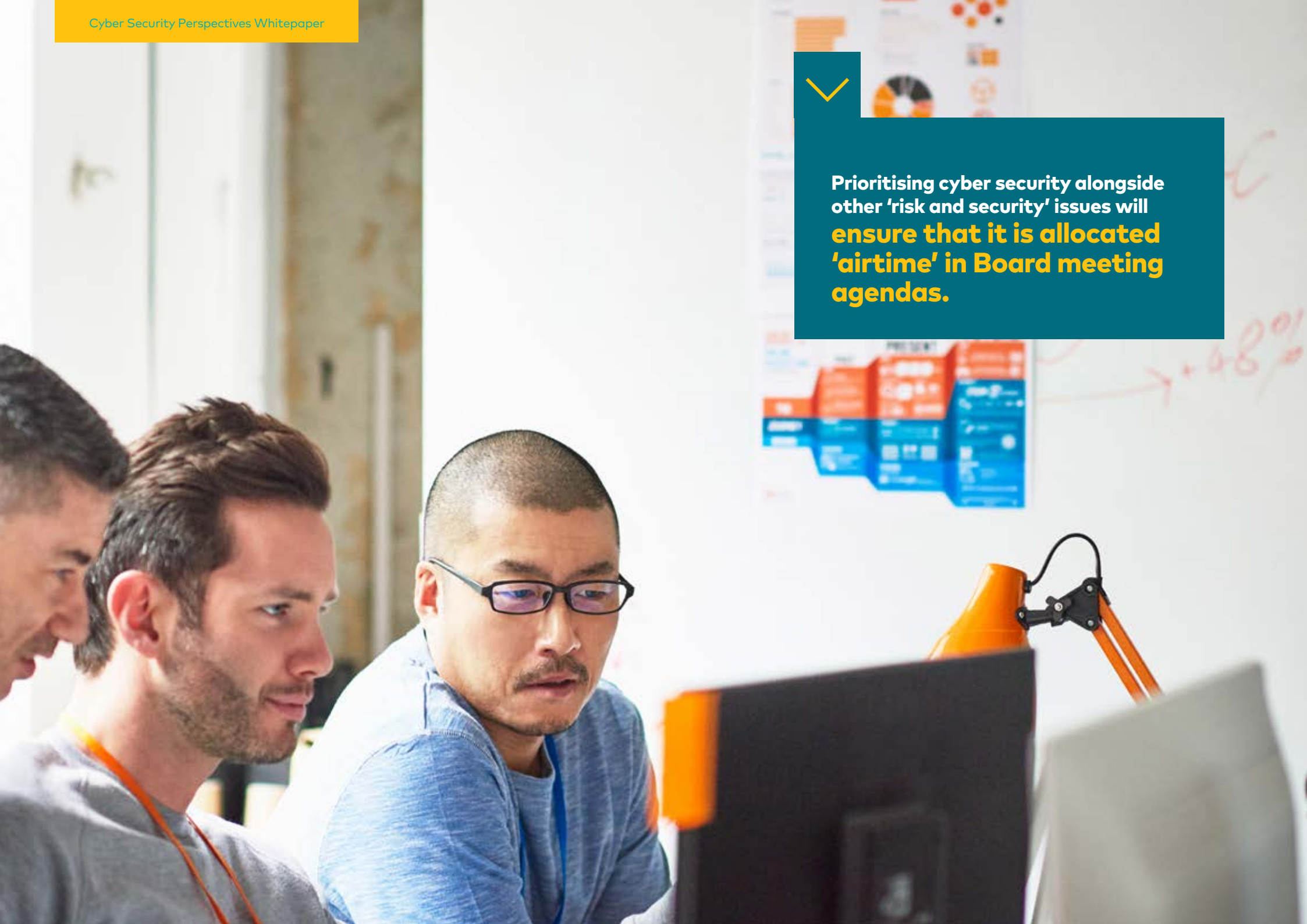
- **Healthcare**
- **Education**
- **Pharmaceutical**
- **Financial**
- **Communications (largely due to their heavily regulated nature)**

Factors that would decrease the cost of a data breach are:

- **Having a strong security posture;**
- **Engaging in business continuity management;**
- **Putting in place an incident response plan; and**
- **Appointing a Chief Information Security Officer.**

US$3.5 MIL

Average total cost of data breach in 2014



Prioritising cyber security alongside other 'risk and security' issues will ensure that it is allocated 'airtime' in Board meeting agendas.

Increasing Cyber Security Literacy in the Boardroom

Costs of Data Breaches[13]

Prioritising cyber security alongside other 'risk and security' issues will ensure that it is allocated 'airtime' in Board meeting agendas.

Many Board members may grapple with IT knowledge and deem this a limitation to gaining a good understanding of cyber security issues. Yet, board members often do not require prior accounting or auditing knowledge to peruse financial statements. The same applies to understanding cyber security risks.

Take steps to increase cyber security literacy in the boardroom:

1: Arrange for periodic deep-dive discussions with your CIO, CTO and/or Chief Information Security Officer (CISO) to identify business-critical assets and review and assess current security policies, processes and budgets to protect them.

2: Define and assign roles and responsibilities for cyber security within the organisation and track security risks on the company's risk register.

3: Invite industry experts periodically to provide up-to-date technology and industry trends briefing, and to keep current with knowledge of the threat landscape.

The statements in Table 1 represent the essentials of cyber risk management for Board members. As a useful sign-post, it points you to where potential gaps are, and provide ideas on how to engage management or industry experts on cyber security.

Cyber Security Self-Assessment Tool

Check your cyber security readiness:

I know my organisation's most critical assets and the key cyber threats to them.	Y N
I understand my organisation's risk profile and am confident that our critical assets are being protected adequately.	Y N
I have an accurate and up-to-date picture of the potential business, financial and reputational impacts on our company if: • **Sensitive internal or customer information were lost or stolen.** • **Our online services were disrupted.**	Y N
In the event of a cyber security breach, my organisation has stipulated procedures and protocols to promptly respond and contain the business, financial and reputational impacts.	Y N

Proactive Defence and Sustained Vigilance

Boards will also need to assess how adequate the defences of their organisations are, the relative merits of managing security in-house and with external partners, and to balance trade-offs between risk and mitigation costs. A report by PandaLabs[14] released the following alarming statistics:

>75mil

malware strains

More than 75 million new malware strains were recorded in 2014 (2.5x of those detected in 2013).

200,000

new samples every day

200,000 new malware samples were spotted every day.

73mil

samples coded in 2014

A third of the 220 million malware samples recorded in PandaLabs were coded in 2014.

Businesses can look to Managed Security Service Providers (MSSPs) as trusted partners to meet their cyber security needs.

All these point to the need for a proactive and comprehensive strategy to protect against rapidly evolving threats as well as ensure sustained vigilance. This entails building capabilities in these 3 areas:

People

Nurture a pool of deep and specialised security expertise that is constantly plugged into the latest threats and technologies.

Intelligence

Engage in continuous global visibility and intelligence that is shared and analysed across vendors and businesses to better predict and defend against new threats.

Technology

Leverage technologies to offer integrated, multi-layered protection against multi-vector cyber threats via Internet, corporate network and mobile devices.

Building such capabilities requires significant and recurring investment in costly and resource intensive platforms. For many enterprises, there are limited resources to do this entirely in-house.

Businesses can look to Managed Security Service Providers (MSSPs) as trusted partners to meet their cyber security needs.

Some potential benefits of outsourcing cyber defence to a MSSP:

Capability	Benefits
Scale	Enjoy the ability to scale your cyber defence capabilities with access to centralised platforms and infrastructure, including Security Operations Centres, for round-the-clock vigilance.
Global visibility	Increase security insights by plugging into global intelligence, with up-to-date visibility into latest threat data, trends, technologies and more.
Expertise	Gain access to a critical mass of security expertise, competencies and skill.
Comprehensiveness	MSSPs typically offer a comprehensive service offering portfolio-from device monitoring and management, to expert services such as threat intelligence, to managed identity, mobile security, forensics and remediation.
Platform independence	Enjoy the flexibility of leveraging best-of-breed technology and solutions on a common platform, with the assurance of seamless integration to address specific security needs.
End-to-end visibility across security and network	Enhance visibility via a single point of view across network management, traffic visibility, and security incident alert monitoring, with full integration between security, network management and network traffic.

In this digital age where everything and everyone is online and connected, cyber security can cripple a business, undermine a brand built up over many years, or shake the confidence that customers and investors have in it. A cyber-first mentality should permeate all levels of the organisation in its day-to-day business activities and growth plans. Studies have shown that the ability of organisations to effectively deal with cyber threats - where the lines between known and unknown, insider and outsider adversaries are increasingly blurred - depends fundamentally on leadership and commitment.

We assert that cyber security cannot be delegated to IT teams to manage and that the Board has a critical role to play to ensure there is a sustainable, holistic and risk-based approach to putting in place capabilities, processes and technology to protect the organisation's most critical assets. Gaps in in-house capabilities should be identified and potentially plugged through partnerships with external security providers.

The Board has a critical role to play to ensure there is a sustainable, holistic and risk-based approach to putting in place capabilities.

At-a-Glance: High Profile Cyber Attacks

Type of Impact	Consequences	Example
Impact on customer privacy	Theft of customers' personal information (name, email, home addresses, financial information and more) exposes customers to: • Risk of identity theft • Danger of potential physical harm • Becoming a victim of financial scams, credit card fraud and embezzlement	**eBay (February - March 2014)** What happened: • More than 230 million eBay users' account information compromised[15] • Data theft included bank account details, eBay account details, phone numbers and addresses Impact on Customer Privacy: • Put eBay customers in danger of identity theft and financial loss • Resulted in loss of US$18 billion to US$18.3 billion with obstruction of operations[16] **JP Morgan (July 2014)** What happened: • More than 75 million households affected[17] Impact on Customer Privacy: • Customers' personal information including names, email addresses and home addresses were stolen over duration of a month • Pledged US$ 250 million annually to increase investments in cyber security measures[18]
Impact on financial loss	Severe disruption of business operations and breach-induced costs can cause significant financial losses, including: • Fall in stock value • Compensation or complimentary provision of solutions for affected customers (eg. provision of free credit monitoring service) • Investigation, hardware repair and replacement • Implementing new security preventive measures • Hiring new, dedicated staff to manage security • Loss in potential business, trade secrets, intellectual property, contracts and more • Devising new marketing plans and sales promotions to rebuild customers' confidence	**Target (December 2013)** What happened: • More than 40 million credit card accounts and 70 million customers' personal information were stolen[19] Impact on Financial Loss: • Stock price fell 11% immediately after breach was reported • US$61M in breach-related losses **Sony Pictures (November 2014)** What happened: • Exposed customer information • Immobilised Sony's gaming network around the world from 25 to 26 December 2014 • Prolonged delay in mitigation of attacks due to immobilisation Impact on Financial Loss: • Sony said in an earnings report that the hack would cost $15 million "in investigation and remediation costs" for the quarter to Dec. 31[20]. The figure would be $35 million for the full fiscal year through March 31.
Impact on business and / or brand credibility	Severely dented customer confidence and brand credibility built across years of marketing efforts after just one cyber attack, affecting customers' perception on: • Product quality • What the business or brand stand for • Trustworthiness of the business behind the brand • How well the business is managed	**Sony Pictures (November 2014)** Impact on Business/Brand Credibility: • Suffered lowest customer confidence in 6 years following the attack based on YouGov's assessment of customer perception levels[21] **Snapchat (January 2014)** What happened: • Released an app that exposed 4.6 million customers' phone numbers and usernames Impact on Business/Brand Credibility: • Led to the publishing of an official apology on Snapchat's blog[22]

At-a-Glance: High Profile Cyber Attacks (continued)

Type of Impact	Consequences	Example
Impact on Leadership	Harsh criticism and close scrutiny of top management by other senior executives in the organisation, the media and regulatory bodies, after a cyber attack. Impact includes: • Executives were pressured to take personal responsibility for the inability to circumvent the attack • Potential leadership void when executives are pressured into early retirement or resignation	**Target (December 2013)** Impact on Leadership: • Resignation of CEO, Gregg Steinhafel, with 35-year tenure[23] • Resignation of CIO, Beth Jacob[24]
Regulatory and Legal Risks	Failure in circumventing devastating cyber attacks often hint at inadequate security policies and measures, thus exposing the business to: • Heavy criticism by regulators and Internet watchdogs • Investigations into the organisation's security practices and protocols • Mandatory "security" services stipulated by law enforcement agencies	**Home Depot (September 2014)** What happened: • Approximately 56 million customers' payment/debit and credit card information were stolen over a five month period[25]. • Approximately 53 million email addresses were extracted[26] Impact on Regulatory Compliance: • Close monitoring by financial institutions. Compromised customer debit/credit cards were deactivated by financial regulators, with new ones immediately reissued after disclosure of attack **JP Morgan (July 2014)** Impact on regulation: • JP Morgan was subject to probes by federal authorities in several states in the US[27] • This incident occurred following the passing of legislation that required immediate disclosure of security breaches that resulted in data loss • JP Morgan's delayed acknowledgement and disclosure of the breach led to extended probes and investigations.

Glossary

APT (Advanced Persistent Threats)

A set of targeted attacks that gain unauthorised and undetected access to a system for an extended period of time.

Botnet

A network of private computers infected with malicious software and controlled as a group without the owners' knowledge.

DDoS (Distributed Denial of Service)

An attack where multiple compromised systems are used to overwhelm a single system - usually temporarily interrupting or suspending the services of a host connected to the internet.

Firewall

A network security system designed to prevent unauthorised access.

Intrusion Detection System

A system that inspects all inbound and outbound network activity for suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system.

Malware

Software designed to disrupt/damage or gain access to a computer system.

Multi-vector attack

A cyber attack that employs a range of technologies, deployed in numerous stages, to penetrate the defences of the target organisation.

Political espionage

The use of spies by governments to discover the military and political secrets of other nations.

Trojans

A malicious/harmful programme hidden in apparently harmless programming/data. It is often used to obtain control and wreak havoc.

Worms

A standalone malware computer programme that replicates itself in order to spread to other computers.

Zero-day attack

An attack that exploits previously unknown vulnerabilities in computer systems.

Footnotes

1. www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#15160e4a3bb0
2. www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits
3. http://www.businessinsider.com.au/hacker-gang-lizard-squad-is-now-selling-ddos-attacks-as-a-service-2014-12
4. Krebs, Brian, "Non-U.S. Cards Used at Target Fetch Premium," krebsonsecurity.com, December 22, 2013h. As of February 4, 2014: http://krebsonsecurity.com/2013/12/non-us-cards-used-at-target-fetch-premium/
5. www.digitalattackmap.com/understanding-ddos
6. Akamai, State of the Internet [Security] Q2 2015
7. Ponemon Insitute © Research Report, 2015, "The Cost of Denial-of-Services Attacks (March 2015)"
8. Arbor Networks 10th Annual Worldwide Infrastructure Security Report
9. Mandiant M-Trends 2014 – 2016 Reports
10. FireEye, 2015, "Southeast Asia: An Evolving Cyber Threat Landscape"
11. Ponemon Institute© Research Report, 2014, "The Economic Impact of Advanced Persistent Threats (May 2014)"
12. M-Trends 2014 – 2016 reports.
13. Ponemon Insitute© Research Report, 2014, "Cost of Data Breach Study: Global Analysis (May 2014)". These costs comprise both direct costs relating to breach detection/discovery, escalation and notification, as well as post breach costs such as extrapolated value of business loss due to losses in turnover, loss of goodwill and customer churn.
14. PandaLabs Annual Report 2014
15. http://www.forbes.com/sites/jaymcgregor/2014/07/28/the-top-5-most-brutal-cyber-attacks-of-2014-so-far
16. http://www.forbes.com/sites/ryanmac/2014/07/16/ebay-ceo-sales-earnings-affected-by-cyberattack-body-blow-in-challenging-second-quarter
17. http://www.wsj.com/articles/j-p-morgan-says-about-76-million-households-affected-by-cyber-breach-1412283372
18. http://www.ibtimes.com/jp-morgan-chase-cyberattack-more-80-million-accounts-compromised-says-new-report-bank-hack-1698834
19. http://blogs.marketwatch.com/behindthestorefront/2014/02/26/two-months-after-damaging-data-breach-target-stock-has-its-best-day-in-5-years
20. http://www.networkworld.com/article/2879814/data-center/sony-hack-cost-15-million-but-earnings-unaffected.html
21. http://www.brandindex.com/article/hacking-crisis-brings-sony-new-perception-lows
22. http://www.theverge.com/2014/1/9/5291526/snapchat-updates-app-to-let-users-opt-out-of-contentious-find-friends
23. http://www.bloomberg.com/bw/articles/2014-05-05/as-data-breach-woes-continue-targets-ceo-resigns
24. http://www.nytimes.com/2014/03/06/business/targets-chief-information-officer-resigns.html?_r=0
25. http://www.wsj.com/articles/home-depot-breach-bigger-than-targets-1411073571
26. http://www.wsj.com/articles/home-depot-hackers-used-password-stolen-from-vendor-1415309282
27. http://www.bloomberg.com/news/articles/2015-01-14/jpmorgan-asked-by-states-for-more-detail-on-2014-data-breach

Give us a call

To discuss how Optus can help you navigate through advanced security solutions, **contact your Optus Account Manager or call the Optus Business hotline on 1800 555 937**

Join the conversation

1800 555 937 optus.com.au/business

@optusbusiness yesopt.us/blog

SS00530 0516KD