

March 2017

Cyber Security & Insurance Solution Karachi, Pakistan

Ram Garg CFA, MBA
Financial & Casualty Line
J B Boda & Co (Singapore) Pte Ltd



Karachi Insurance Institute

Agenda

- Cyber Risk - Background
- Cyber Exposure
- Cyber Insurance Solution
- Claim Trend





“There are only two types of companies: those that have been hacked and those that will be”

Robert Mueller

Director, FBI

“We are in a day when a person can commit about 15,000 bank robberies sitting in their basement”

Robert Anderson

**Executive Assistance Director, FBI's Criminal
Cyber Response and Services Branch**

IF SOPHISTICATED ORGANIZATIONS SUCH AS THESE CAN HAVE A BREACH

- Amazon.com
- AT&T
- Bell Canada
- Cisco Systems
- Facebook
- Wells Fargo
- Research in Motion
- Nortel
- SONY
- IBM



**DO ANYONE
CLAIM THAT THEIR
IT SECURITY
PROTOCOLS MAKES
THEM
UNTOUCHABLE?**



Hackers steal



**\$100 Million
from Bangladesh**



Website blocked by Trend Micro Worry-Free Business Security Services

Lankan in Bangladesh cyber heist claims she was set up

2016-03-31 20:31:56

6849 5



Hagoda Gamage Shalika Perera, the Sri Lankan businesswoman who got a deposit of \$20 million in her account last month, claimed that the funds were anticipated but had no idea they were stolen from Bangladesh's Central Bank in one of the largest cyber heists in history.

Anonymous hackers breached Bangladesh Bank's systems between February 4, 5 and attempted to steal nearly \$1 billion from its account at the Federal Reserve Bank of New York.

Even though many of the payments were blocked, \$20 million made its way to Perera's Shalika Foundation before the transfer was reversed. Bangladesh Central Bank officials stated that they acted after a routing bank, Deutsche Bank, sought clarification on the transfer because hackers misspelled the company's name as "Fundation."

Another \$81 million was routed to accounts in the Philippines and diverted to casinos there, where the trail runs out, sources said.

The Philippines Senate is holding hearings in the case, but thus far, few details had emerged on the Sri Lanka link.

THE SIGNS OF AUTISM ARE SO SUBTLE THAT THEY CAN OFTEN GO UNNOTICED



LEARN MORE

A joint project by
CDB
Citizens Development Bank



THE SMART TRAVELLER'S CHOICE





What is Cyber Crime?

Wikipedia definition:

“Cybercrime, or computer crime, is crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target”



Cyber Environment

- Growing digital data and its connectivity with outside world
 - Mobile apps
 - Automated systems
 - Social media
 - Cloud computing
- Companies are collecting, storing and processing large amount of data of all kinds
- Increasing reliance on technology and connectivity leads to increasing Cyber exposure for all kinds of organisations



Source of Cyber Loss

State sponsored...



For Fun..



Criminals



Rogue employee...



Hacktivism..



Human error...



Types of Cyber Attacks

Malware...



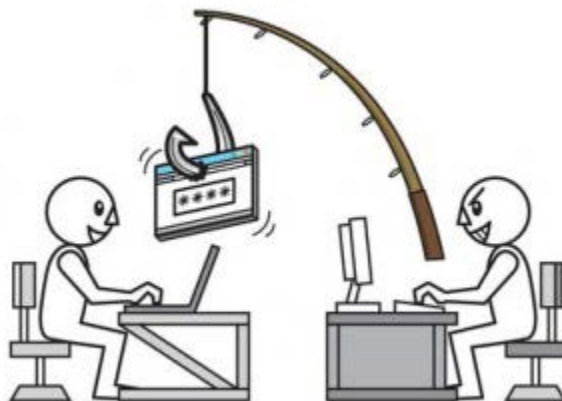
Code exploits..



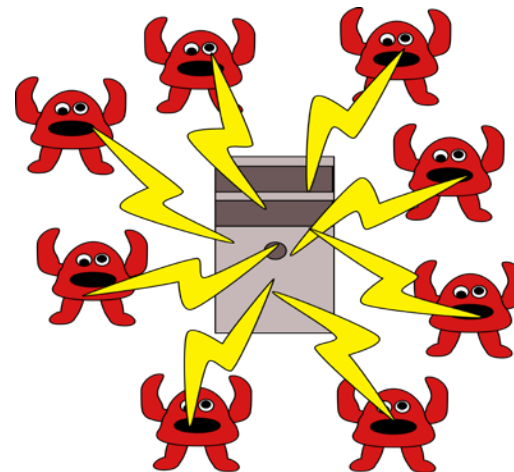
Ransomware..



Spear-phishing..



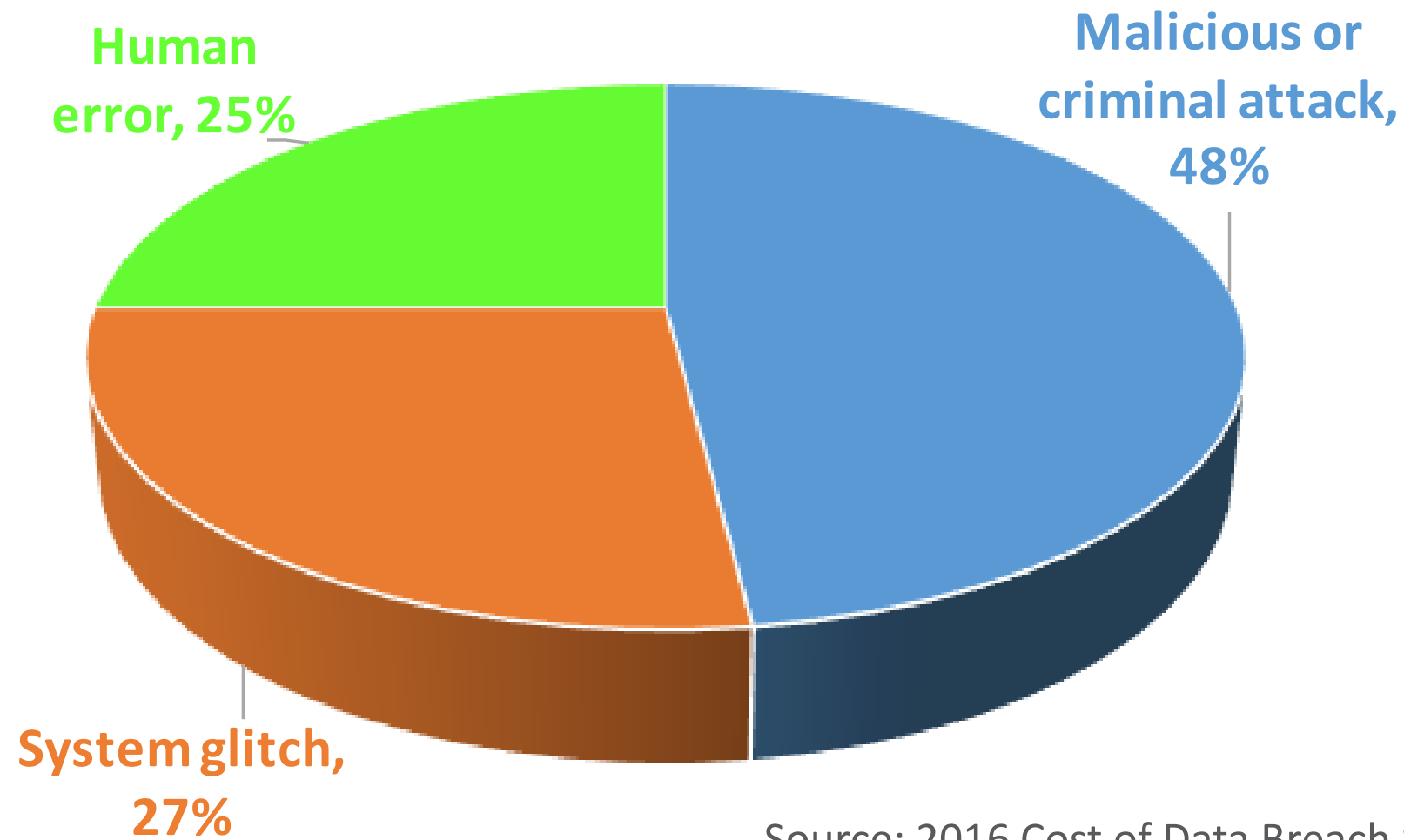
DOS attack...



Unauthorized access...



Cyber Risk – Root cause of Data Breach



Source: 2016 Cost of Data Breach Study: Global Analysis (IBM & Ponemon Institute LLC)



Cost of a Breach

Personnel Costs

- Staff time to research and collect information to measure the scope of the incident; executive time with legal counsel

Post incident Costs

- Media, investor relations, call centre, forensics, repairs, credit monitoring

Legal Costs

- Regulators, liability assessment, defence, damages

Lost Revenue

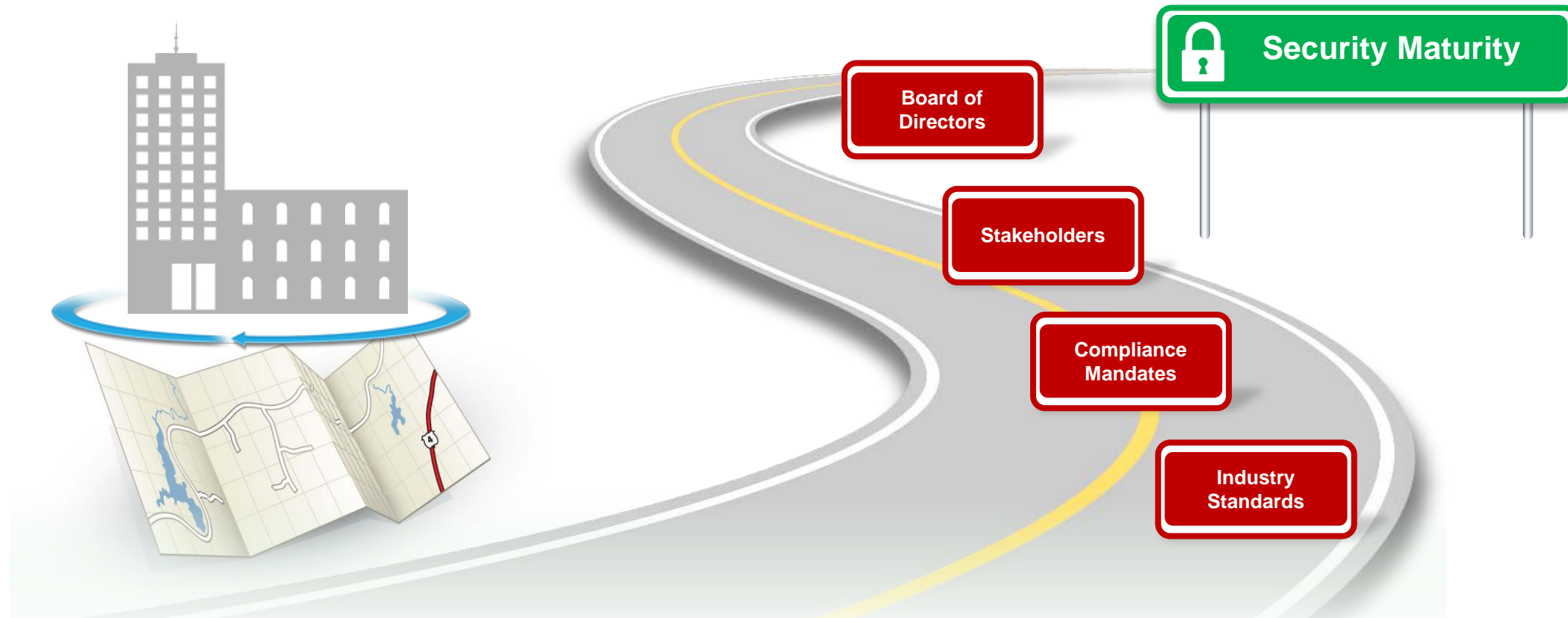
- Lost customers, lost opportunity costs



Malware Threats – Pakistan is 1st in position



CIOs face a shortage of skills, lack of metrics and strategy



49% 


of IT executives have **no measure of security effectiveness**

2012 Forrester Research Study

31% 

of IT professionals have **no risk strategy**

2013 Global Reputational Risk & IT Study, IBM

83% 

of enterprises have difficulty finding the **security skills** they need

2012 ESG Research

Pakistan – Emergency Readiness

FIA Established National Response Centre For Cyber Crime (NR3C-FIA) as a law enforcement agency in Pakistan

– <http://www.nr3c.gov.pk>

The National Assembly (NA) passed the Prevention of Electronic Crimes Bill (PECB) 2015

FEDERAL INVESTIGATION AGENCY
NATIONAL RESPONSE CENTRE FOR CYBER CRIME

HOME ABOUT US SERVICES CYBER CRIME REPORT CYBER CRIME FAQ CONTACT US

**STEALING DATA IS AN OFFENSE,
UPDATE ANTIVIRUS FOR DEFENSE**

STOP

Prevention of Electronic Crimes
ACT 2016

NATIONAL RESPONSE CENTRE FOR CYBER CRIME
CYBER RESCUE 9911

REPORT CYBER CRIME

INSURANCE



Cyber Insurance Market

- Cyber Insurance market is projected to be \$2.5b globally
- Cyber growing annually by more than 25%+
- Cyber market could be up to \$20b by 2020
- Most countries in Asia are developing their local data protection legislation



Cyber Insurance – First Party Loss

First Party	Network business interruption	Loss of income and extra expense resulting from a total or partial failure of by DOS, malicious code, unauthorized access/use to computer system
	Intangible property	Costs to restore or recreate data or software resulting from network security failure
	Loss of Digital Assets	Expenses & costs incurred resulting from damage, alteration, theft, digital assets caused by DOS, malicious code, unauthorized access/use to
	Crisis Management costs	Legal costs to comply with privacy regulations, credit monitoring, PR, costs, resulting from a security data breach, privacy breach or breach of
	Cyber Extortion	Extortion expenses and monies paid resulting from a threat to destroy or assets which are acquired by unauthorized access



Cyber Insurance – 3rd Party Loss

Third Party	Litigation and regulatory	Covers the costs associated with civil lawsuits, judgments, settlements or penalties resulting from a cyber event.
	Regulatory response	Covers the legal, technical or forensic services necessary to assist the policyholder in responding to governmental inquiries relating to a cyber attack, and provides coverage for fines, penalties, investigations or other regulatory actions
	Notification costs	Covers the costs to notify customers, employees or other victims affected by a cyber event, including notice required by law
	Crisis management	Covers crisis management and public relations expenses incurred to educate customers concerning a cyber event and the policyholder's response, including the cost of advertising for this purpose.

Continue..




Cyber Insurance – 3rd Party Loss

..Continue

Third Party	Credit monitoring	Covers the costs of credit monitoring, fraud monitoring or other related services to customers or employees affected by a cyber event.
	Media liability	Provides coverage for media liability, including coverage for copyright, trademark or service mark infringement resulting from online publication by the insured.
	Privacy liability	Provides coverage for liability to employees or customers for a breach of privacy

Covering Insurance Gaps with Cyber Insurance




	Property	General Liability	Crime	K&R	PI	Cyber
<i>1st Party Data Protection Privacy Risks</i>						
Network Interruption	Yellow	Red	Red	Red	Red	Green
Cyber Extortion	Red	Red	Red	Yellow	Red	Green
Data Restoration, Recollection, Recreation (Determination and Action)	Red	Red	Red	Red	Red	Green
Employee sabotage of Data	Red	Red	Yellow	Red	Yellow	Green
Virus/Hacker damage to Data	Red	Red	Red	Red	Red	Green
Denial of Service attack	Yellow	Yellow	Red	Red	Red	Green
Physical damage to Data Only	Yellow	Red	Red	Red	Red	Yellow

Coverage Provided 
 Coverage Possible 
 No Coverage 

For reference and discussion only: policy language and facts of claim will require further analysis

Covering Insurance Gaps with Cyber Insurance

	Property	General Liability	Crime	K&R	PI	Cyber
3rd Party Data Protection Privacy Risks						
Breach of Personal Information	Yellow	Yellow	Yellow	Red	Yellow	Green
Breach of Corporate Information	Red	Red	Red	Red	Yellow	Green
Outsourcing Liability/Vicarious Liability	Red	Red	Red	Red	Red	Green
Contamination of Third Party Data by any unauthorized software, computer code or virus	Red	Yellow	Red	Red	Yellow	Green
Denial of access to third party data	Red	Red	Red	Red	Yellow	Green
Theft of an access code from the Company's premises	Red	Red	Red	Red	Yellow	Green
Destruction, modification, corruption, damage or deletion of Data	Red	Red	Red	Red	Red	Green
Physical theft of the Company's hardware	Red	Red	Red	Red	Yellow	Green
Data disclosure due to a Breach of Data Security	Red	Red	Red	Red	Yellow	Green
Costs and expenses for legal advice and representation in connection with an Investigation	Red	Red	Red	Red	Yellow	Green
Data Administrative Fines	Red	Red	Red	Red	Yellow	Green
Repair of Company/Individuals Reputation	Red	Red	Red	Red	Yellow	Green
Media Content Liability (IP, Plagiarism, defamation, trespassing)	Red	Yellow	Red	Red	Yellow	Green
Notification Costs	Red	Yellow	Red	Red	Red	Green
Monitoring Costs (with identity theft education and credit file or identity monitoring)	Red	Yellow	Red	Red	Red	Green

Coverage Provided 
 Coverage Possible 
 No Coverage 

For reference and discussion only: policy language and facts of claim will require further analysis

Slide courtesy of AIG HK



Cyber Insurance – Typical Exclusions

- **Retroactive Date:** No cover for events/circumstances/viruses that happened before the retroactive date
- **Inception Date:** No cover for claim or any acts, facts, or circumstances that happened before the inception date, if the Insured knew or could have reasonably foreseen
- **Bodily Injury**
- **Property Damage:** No cover for hardware, but restorage expense for data and computer programs that exists in computer system is covered
- **Failure in power, telecommunications other infrastructure:** No cover for infrastructure failure unless under the Insured's operational control

Continue..

Cyber Insurance – Typical Exclusions

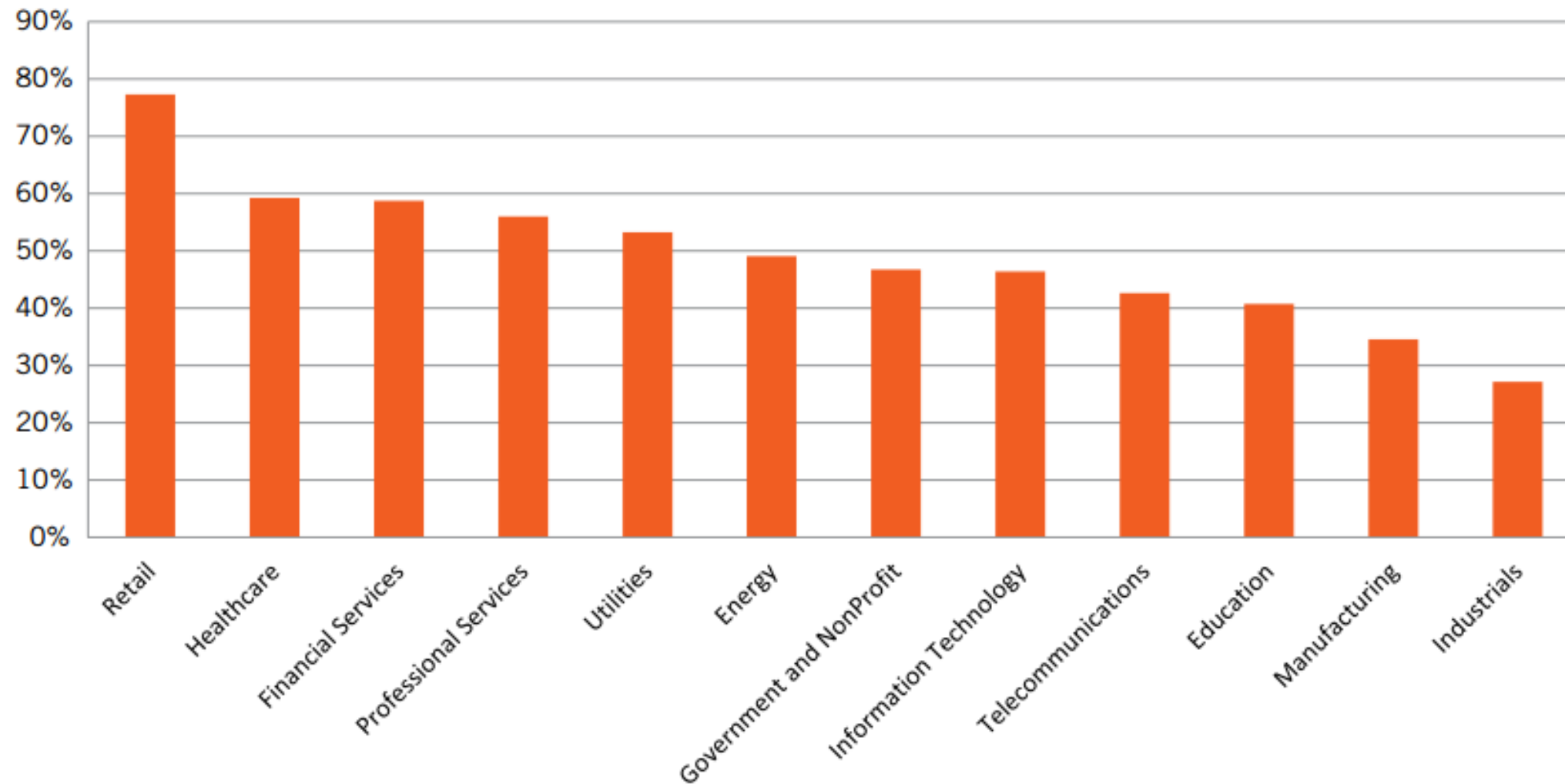
...Continue

- NAT CAT or any other physical event
- Act of Terrorism, war, invasion
- Fine or Penalty arising out of Payment Card Industry Standard/Payment Card Company Rules
- Infringement of any patent or trade secret by Insured, Insured former employee
- Unlawful collection of personally identifiable non public information by Insured
- Theft, Loss of unencrypted Lap tops and mobiles



Sector wise demand growth

Industry Sectors Underwriters Note Increase in Demand for Cyber Liability Policies/Endorsements



Source: CYBER LIABILITY INSURANCE MARKET TRENDS: SURVEY 2014

Sponsor by PartnerRe



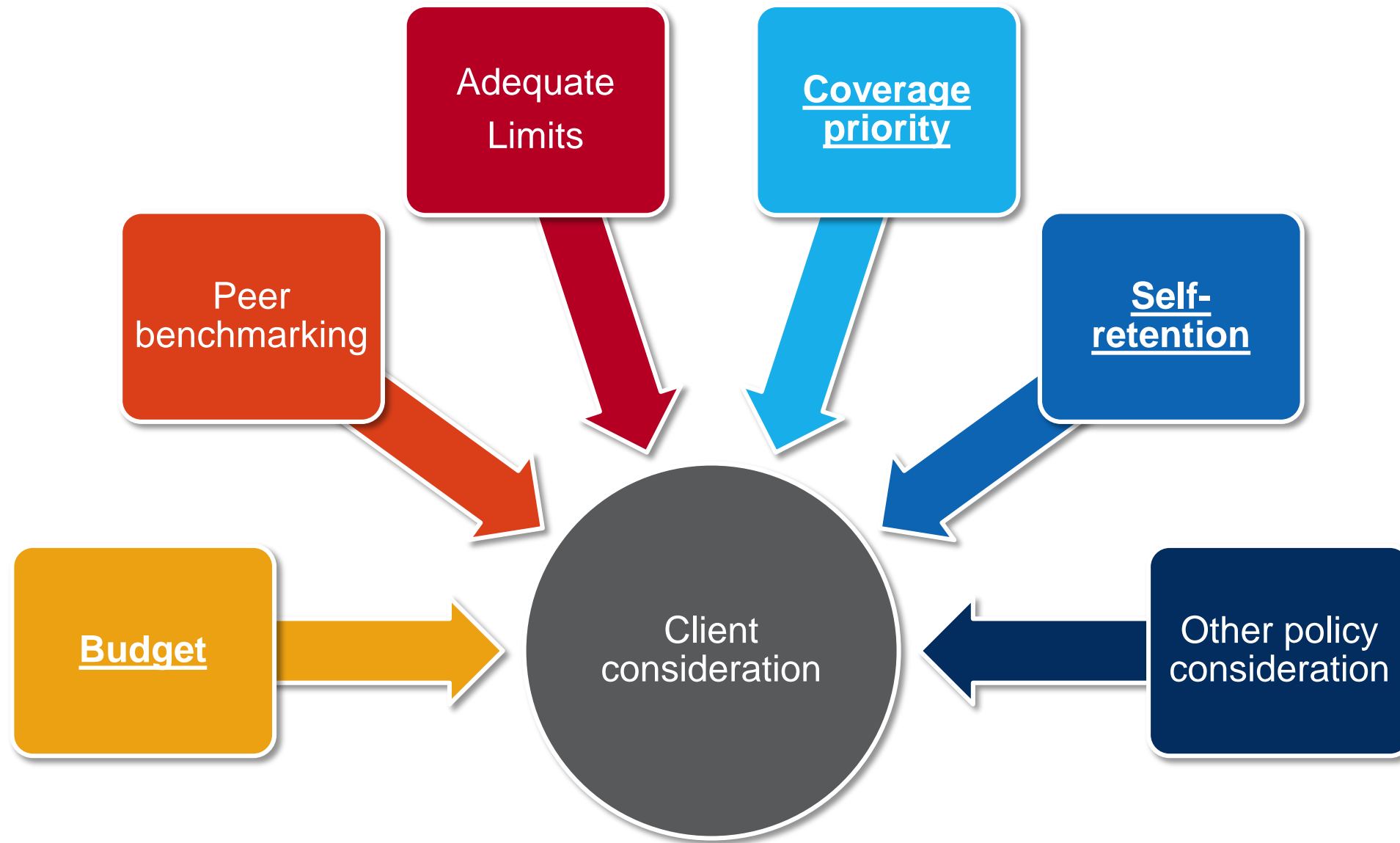
Most vulnerable industries in Asia

Within Asia, FireEye Labs identified the following industries as having experienced advanced persistent cyber-attacks during 2013, in order:

- Financial Services
- Government (Federal)
- High-Tech
- Chemicals / Manufacturing / Mining
- Services / Consulting
- Higher Education
- Telecom (Internet, Phone and Cable)
- Energy / Utilities / Petroleum
- Entertainment / Media
- State and Local Government



Client considerations



CYBER CLAIM TREND (Worldwide)



Loss Example

Third party fraud – Impersonation

Loss amount: US\$ 3,500,000

Insured's industry: Hotel

Country: Mauritius

Date: Mar 2016

Description: fraud was committed by persons whose identities are still unknown

- fraud was perpetrated through devious electronic means, impersonation resulting in two transfers to foreign bank



Loss Example

Third party fraud – Phishing attack

- Loss amount: US\$ 2,000,000
- Insured's industry: Banks
- Country: Taiwan
- Date: 2016
- Description: GIC of India became victim of 'phishing' attack and lost \$1.1 million
 - A fake email purportedly from the GIC Re Chief Managing Director (CMD) AK Roy was sent by the fraudsters to the company's Dubai office, directing it to make a payment of \$ 1.1 million to an American entity for reinsurance transaction. And the concerned official at Dubai branch made the payment.



Loss Example

Third party fraud – ATM malware heist

Loss amount: US\$ 2,000,000

Insured's industry: Banks

Country: Taiwan

Date: 2016

Description: Taiwan investigators suspect two Russian nationals hacked into a major domestic bank's ATMs last weekend, using malware to withdraw more than \$2 million from dozens of machines in the country's first recorded case of its kind.

- Combining cybercrime with daylight robbery after a typhoon battered greater Taipei, the suspects may have used a cellphone to trigger 41 First Bank ATMs to dispense fat wads of bills

Loss Example

Third party fraud – Hacking attack

Loss amount: NIL

Insured's industry: Banks

Country: Sri Lanka

Date: 2016

Description: Commercial Bank of Ceylon has released a statement admitting that a "hacking attack" on its website resulted in a successful intrusion - however, it maintained that no customer data has been compromised.

Loss Example

Third party fraud – Data breach

Loss amount: Not Known

Insured's industry: Banks

Country: India

Date: 2016

Description: The breach is thought to have been caused by malware on an ATM network

- A number of major Indian banks took safety measures amid fears that the security of more than 3.2 million debit cards has been compromised.

Loss Example

Third party fraud – Hacking

Loss amount: No

Insured's industry: Banks

Country: India

Date: Oct, 2016

Description: Axis Bank suffers cyber attack

- Upon information from an international network, Axis Bank team looked into the bank's servers, it found out that there was indeed an unauthorized login by an unnamed, offshore hacker.



Loss News in Asia

Singapore sees spike in number of cyberattack-for-ransom cases

By Sherwin Loh sherwinl@sph.com.sg @SherwinLohBT

MORE

Cyber defences need to be trustworthy, says ST Electronics boss

Cyber attacks of late underline need to remain ever vigilant

Hitting back at hackers: the debate heats up

Cyber threat needs urgent board level oversight

Attacks on network came from infected devices, says StarHub

Asean must develop regional strategy to fight cyber crime



news POST Purchase this article for republication.

newsminute Purchase this article as keepsake.



Security companies say ransomware attacks, where data is stolen or locked by hackers and released only when money is given, are fast becoming the most popular form of digital crime. PHOTO: BLOOMBERG

OCT 10, 2016 5:50 AM

Singapore

IT STARTED innocently enough, with a click on a third-party ad on an India news website by a staff member, back in 2014.

Soon, the data stored on that computer in a multinational logistics company in Singapore became inaccessible. The hard drive had been encrypted by a malware, triggered by the click on the ad.

A pop-up window offered to decrypt the data within the computer for the price of a bitcoin, a form of cryptocurrency then valued at about US\$500 per bitcoin.

StarHub: Cyber attacks that caused broadband came from customers' infected machines



1 of 2 Disruptions on StarHub's broadband network on Saturday (Oct 22) and Monday (Oct 24) were caused by bug-infested machines of the telco's own customers. ST PHOTO: ONG WEE JIN

PUBLISHED OCT 26, 2016, 6:17 PM SGT | UPDATED OCT 26, 2016, 9:47 PM



Irene Tham Tech Editor

SINGAPORE - The two waves of cyber attacks that brought down Internet surfing on StarHub's broadband network: last Saturday (Oct 22) and on Monday (Oct 24) came from the

Loss News in Asia

Security

Malaysians using South African cards pinch US\$12.7m in Japan

100 frothing fraudsters smash convenience stores in early morning raids



23 May 2016 at 07:32, Darren Pauli



Carders have made off with US\$12.7 million (£8.7 million, A\$17.5 million) ripping through 1400 ATMs in a mere two hours last week.

The attackers netted ¥1.4 billion in cash from ATMs located in convenience stores across the country using counterfeit credit cards.

Sources told local media the 1600 credit cards used in the attacks contained account information from an unnamed South African bank.

GOVINSIDER

SIGN UP FOR DAILY BRIEF

CONNECTED DIGITAL INCLUSIVE INNOVATION SECURITY SMART EVENTS ABOUT

Search GovInsider

550,000 Australians affected by records leak

Data breach described as the 'largest ever leak of personal data' in the country.



By Charlene Chin

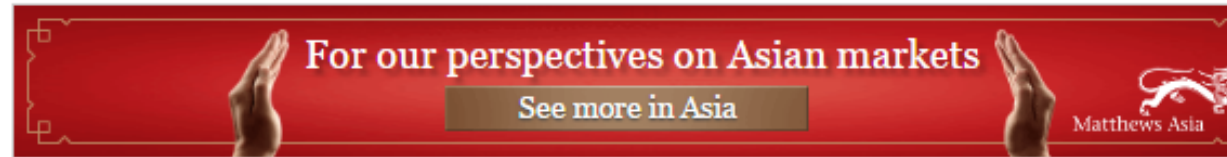
28 OCT 2016

CONNECTED GOV



550,000 Australian blood donors have had their medical records leaked due to a breach of data security at the Red Cross, it has been reported today.

Loss News in Asia



FINANCIALS | Fri Jul 22, 2016 | 11:44am EDT

UPDATE 2-India's Union Bank reports cyber breach on offshore account



(Adds chairman comment saying breach happened in New York)

Union Bank of India Ltd said on Friday one of the bank's offshore accounts was breached in a cyber attack, but the money trail was traced and the movement of funds was blocked.

"There is no loss caused to the bank," the state-run bank said in a statement, adding it had informed authorities about the breach.

Separately, Arun Tiwari, the bank's chairman, told Reuters that the breach of the "nostro" account - which a bank maintains with an overseas bank in foreign currency - took place in New York. A source familiar with the matter originally had said the breach occurred in Hong Kong.

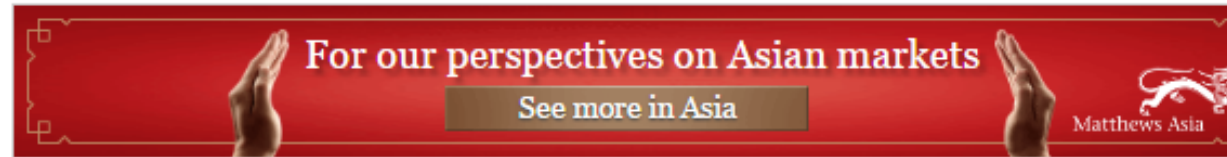
Tiwari declined to say how much money was transferred in the breach, but said the bank had



TRENDING

1 Immigrant team pre

Loss News in Asia



FINANCIALS | Fri Jul 22, 2016 | 11:44am EDT

UPDATE 2-India's Union Bank reports cyber breach on offshore account



(Adds chairman comment saying breach happened in New York)

Union Bank of India Ltd said on Friday one of the bank's offshore accounts was breached in a cyber attack, but the money trail was traced and the movement of funds was blocked.

"There is no loss caused to the bank," the state-run bank said in a statement, adding it had informed authorities about the breach.

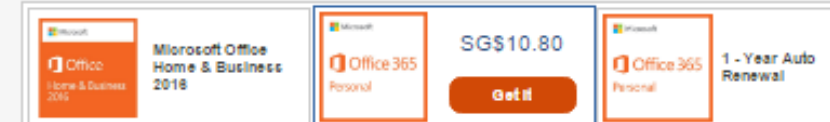
Separately, Arun Tiwari, the bank's chairman, told Reuters that the breach of the "nostro" account - which a bank maintains with an overseas bank in foreign currency - took place in New York. A source familiar with the matter originally had said the breach occurred in Hong Kong.

Tiwari declined to say how much money was transferred in the breach, but said the bank had



TRENDING

1 Immigrat team pre



North Korea hacked 140,000 South Korean computers in a huge campaign

Jack Kim, Reuters
© Jun. 14, 2016, 5:46 AM 1,828



SEOUL (Reuters) - North Korea hacked into more than 140,000 computers at 160 South Korean







Thanks

Ram Garg

DID: +65-6309 1158

Mobile: +65-8322 9962

E-mail: ram@jbboda.com.sg