CyberDIVISION
FEDERAL BUREAU OF INVESTIGATION

Cybersecurity
Threats, Scene and Trends

The overall classification of this presentation is:
UNCLASSIFIED//FOR OFFICIAL USE ONLY

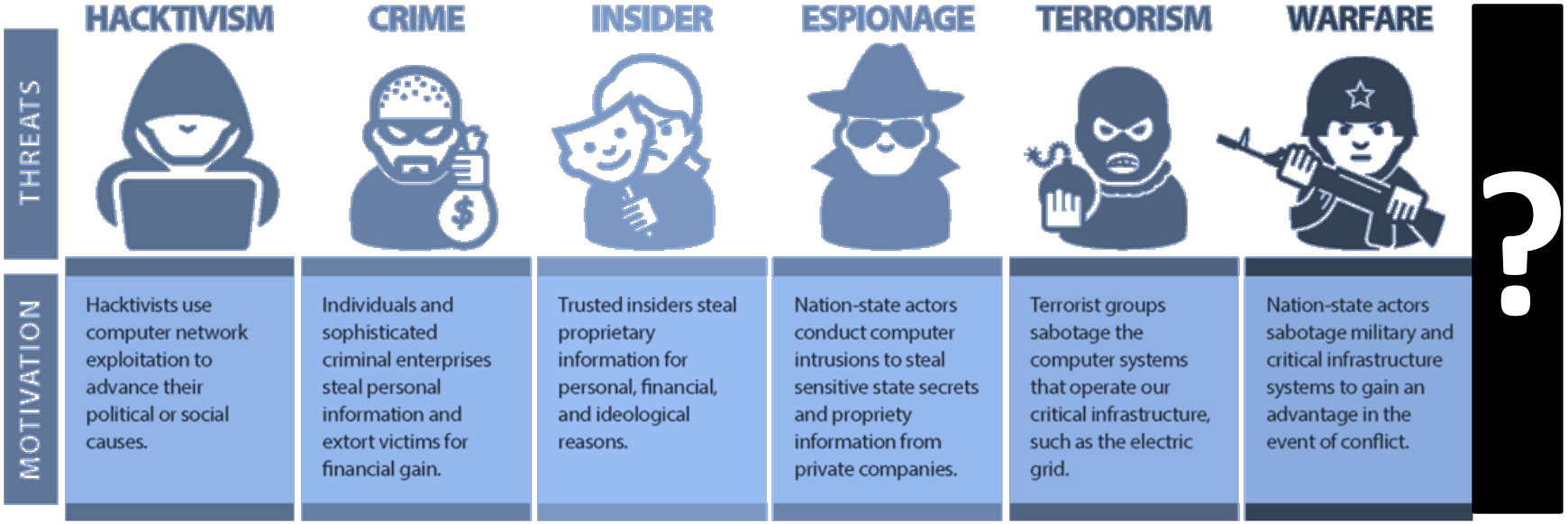
WHY IS IT IMPORTANT

OPM

THE ENVIRONMENT: STATISTICS

- **89%** of breaches have a financial or espionage motivation
- **>177 million** personal records stolen
- **$221** average per capita cost of stolen US record
- **>1 million** Web attacks each day
- **70%** targeted spearphishing open rate
- **35%** increase in ransomware
- **48%** of breaches are criminal

WHO'S DOING THE HACKING

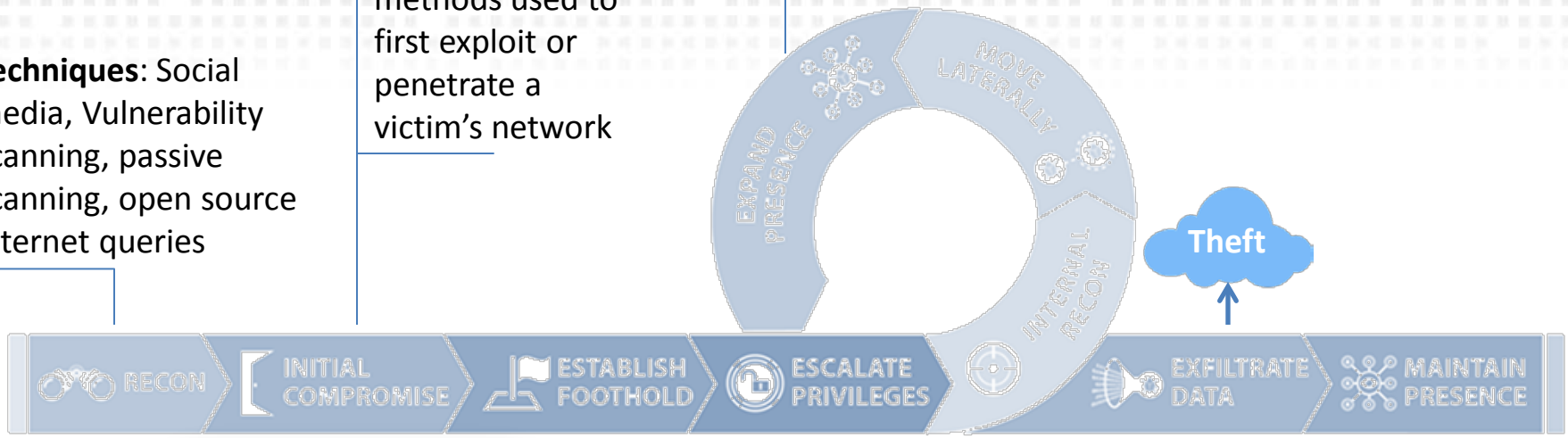


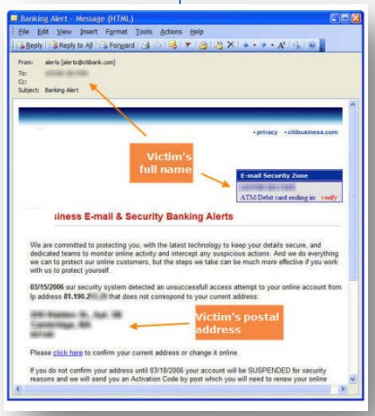
ANATOMY OF A HACK

Involves the methods used to first exploit or penetrate a victim's network

Establish backup communications channel

Techniques: Social media, Vulnerability scanning, passive scanning, open source internet queries





Obtaining additional access beyond the compromised credentials.

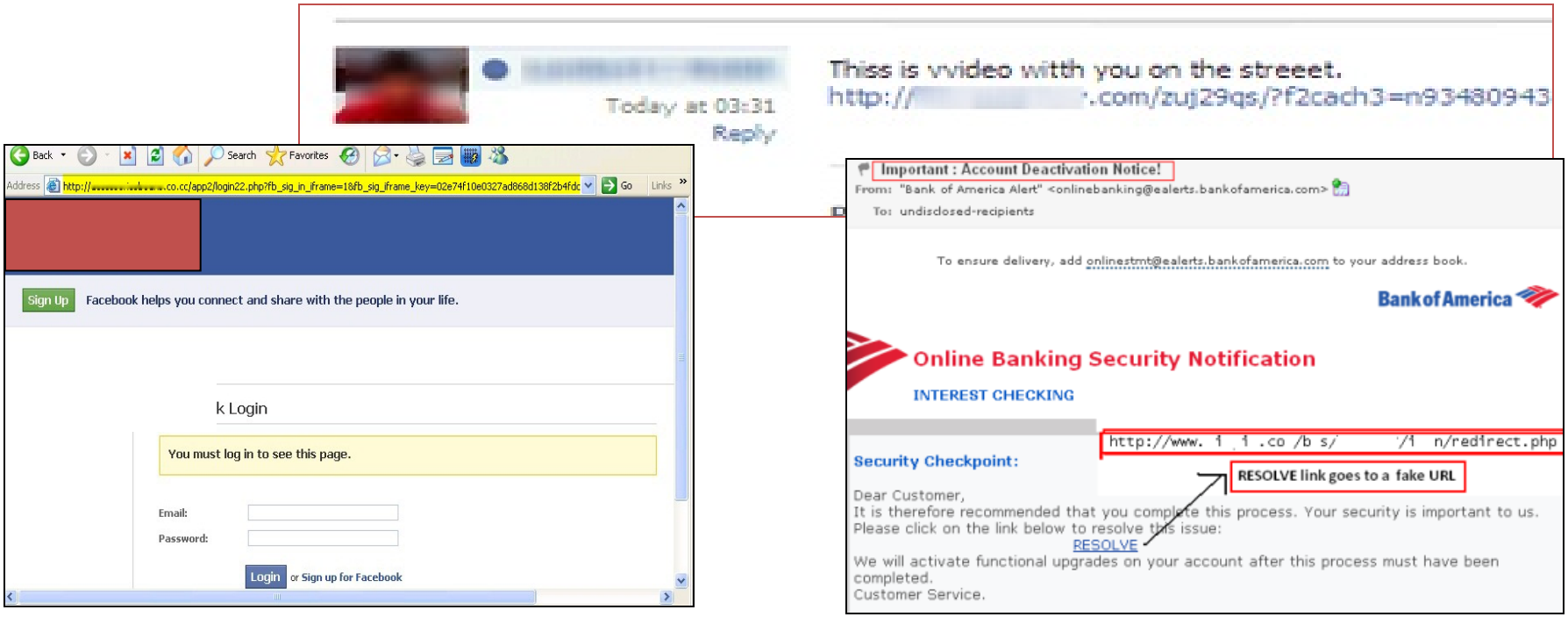
**Example Phishing Email Image. Could be from any apparent legitimate entity or person. Source: ICS SANS*

COMMON TECHNIQUES

- Self infection
- Brute Force/Social Engineering
- Spearphishing
- Wateringhole/Drive-by-Downloads
- Known vulnerabilities
- Man in the middle
- Zero Days

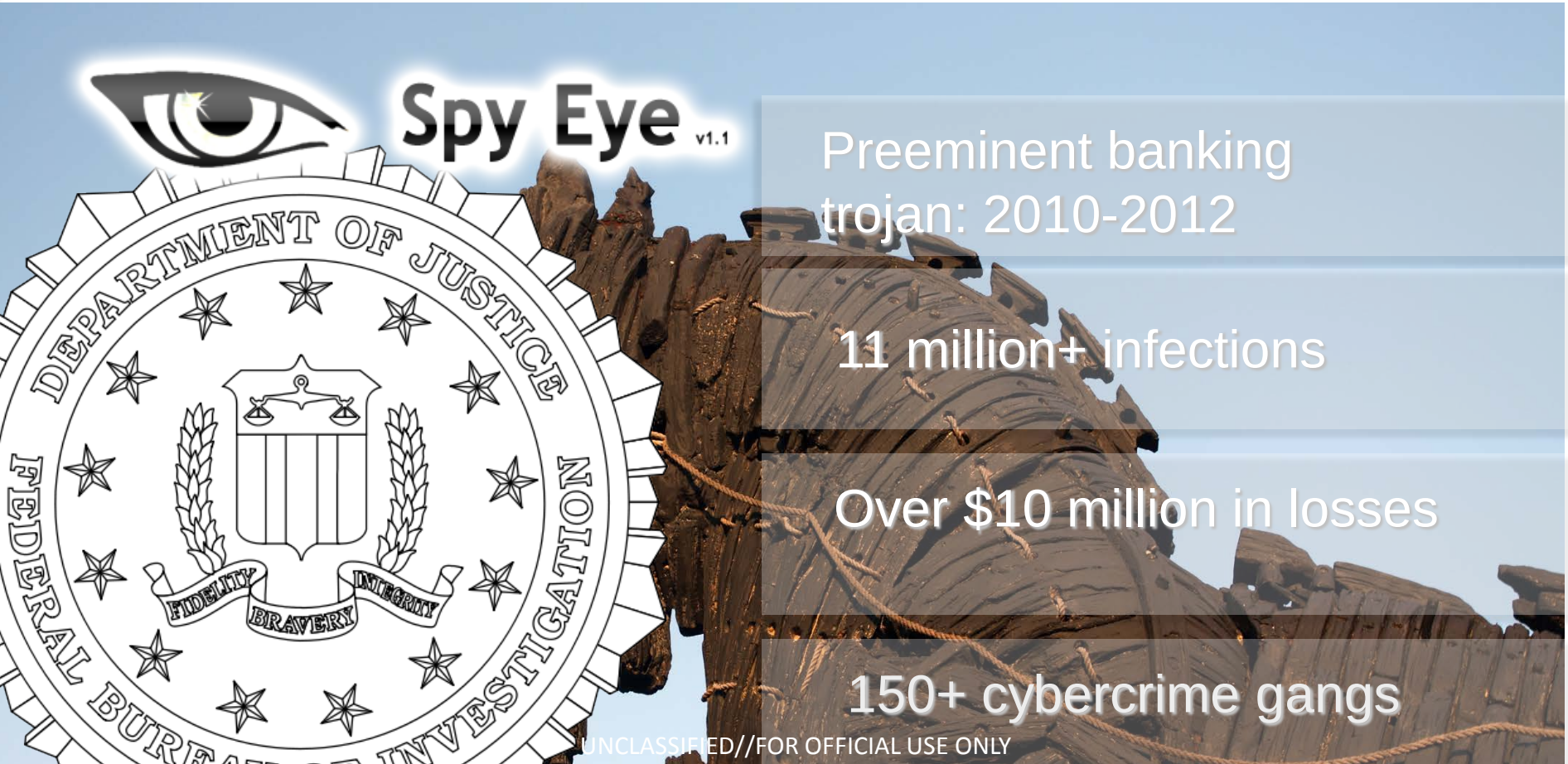
PHISHING

- E-mail Attachments with Malware
- E-mail with Links to Infected Web sites
- SNS messages with Links to Infected Web sites
- Request for banking login or credit card information



DRIVE-BY-DOWNLOAD

- By visiting a normal Web site, your computer gets infected with a Trojan, ransomware, keylogger, etc.

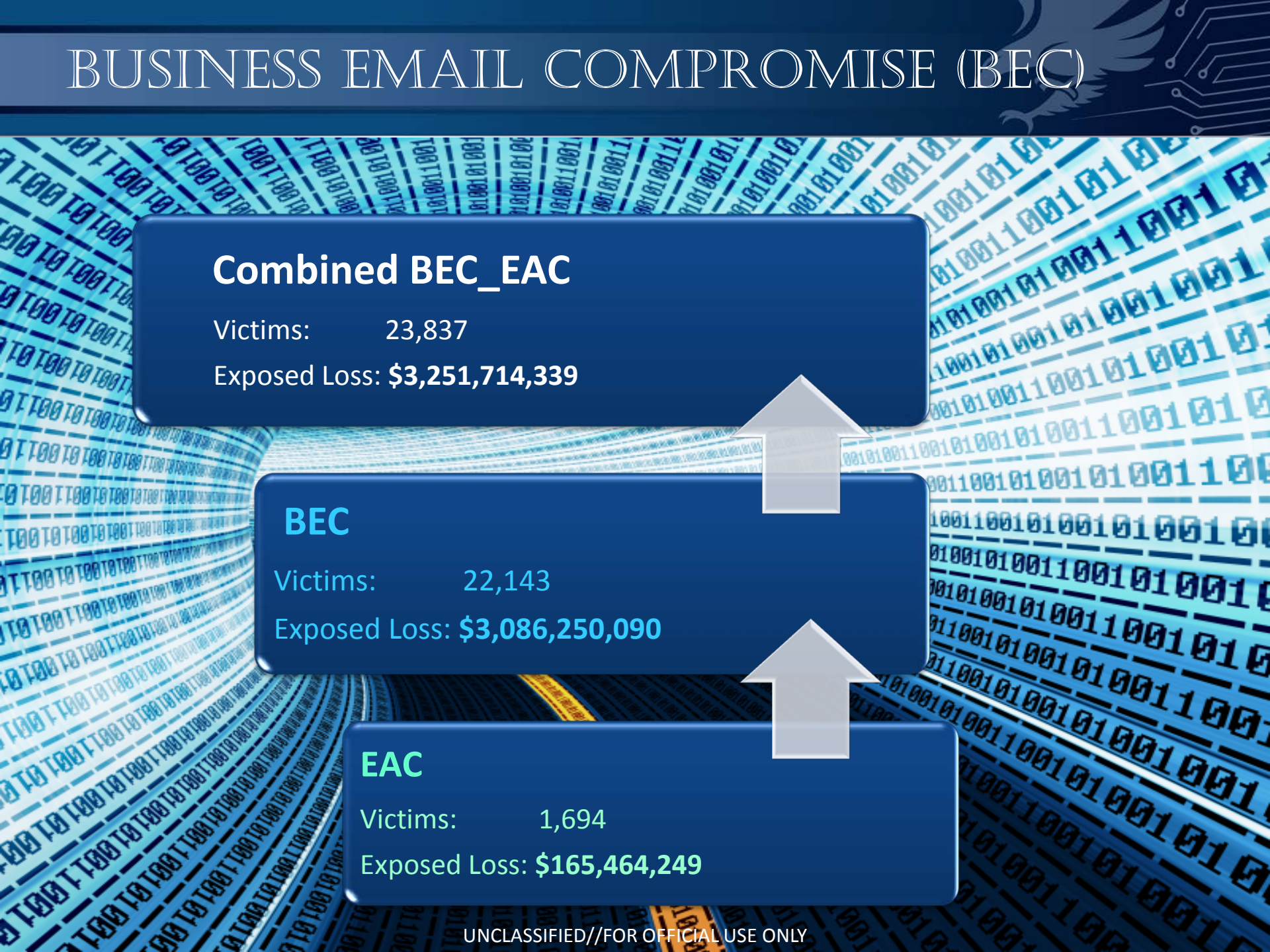


THE CYBER CRIME THREAT

Cyber criminals target victims for monetary gain using:

- Malware and botnets
  - Banking Trojans
  - Ransomware
  - Spyware
  - Keyloggers
  - Point-of-Sale
- Spearphishing and Spam
  - Business Email Compromise
- Extortion
- Identify theft
- Online fraud
- Unauthorized transactions

BUSINESS EMAIL COMPROMISE (BEC)



BEC ANATOMY

HACKER

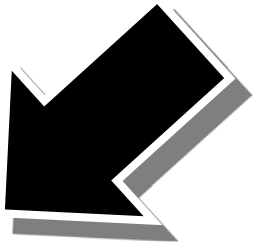
PHISHING
E-MAIL

"fakeinvoice.pdf**.exe**"

BEC ANATOMY

Data returned from 'keylogging' malware
Email will include e-mail addresses, Passwords, and IPs

Hacker has unfettered access to victim computer



Funds may be directed to fraudulent locations worldwide

RANSOMWARE

Infection Vectors:

- Highly Targeted Spearphishing
  - Malicious Attachments
  - Website Hyperlink
- Compromised Web site

Prevention:

- User Awareness & Training
- Patching
- Updated Anti-Malware
- Principle of Least Privilege
- Software Restriction Policies
- Disable Macro Scripts

Business Continuity:

- Secure Backups
- Network Segmentation

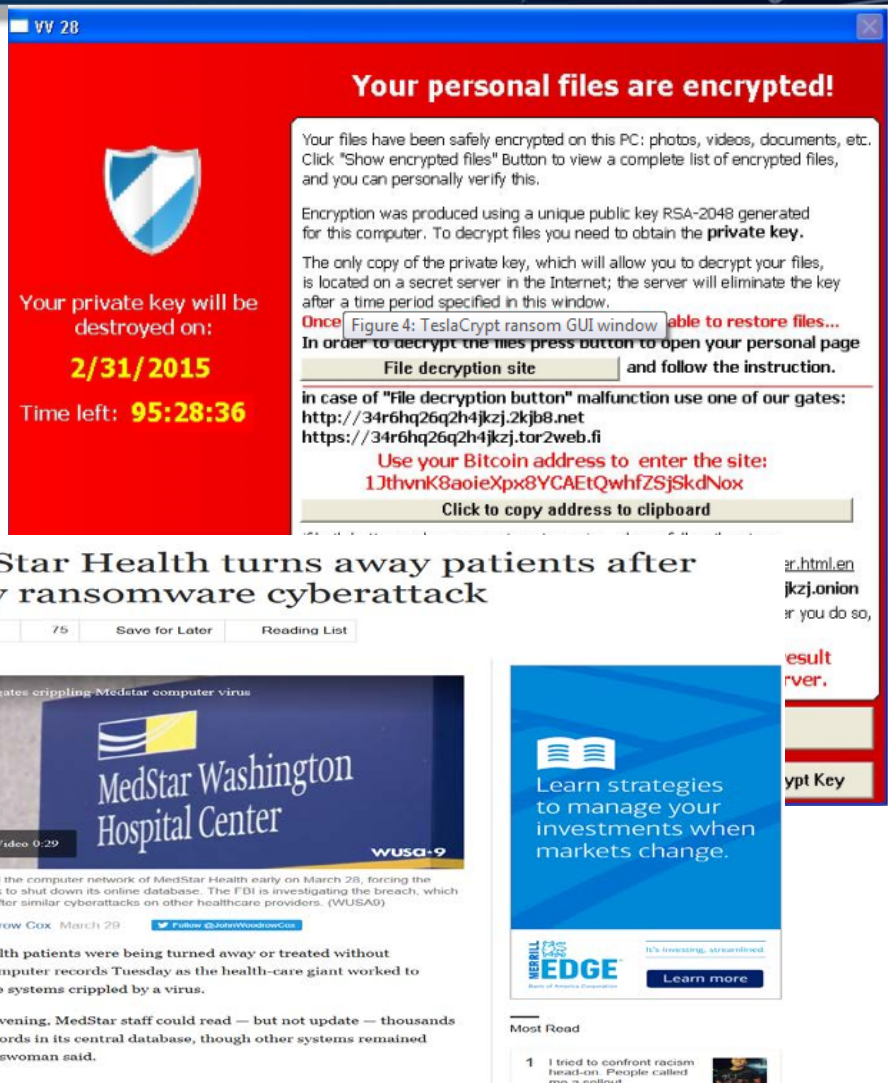


Figure 4: TeslaCrypt ransom GUI window

POINT-OF-SALE COMPROMISE

You are PCI compliant, but are you secure?

Target 2013 Breach:

- Approx. 98 million US-based consumers
- Nearly 1,797 Stores
- Cost of Breach: $368.4 million
- Records sold in underground for $18-$35.70
- Opportunity: Third-Party Vendor
- Motivation: Financial
- Means: spearphishing; multi-stage attack

Takeaways:

- Multi-stage attacks increasing
- Thus, need defense-in-depth
  - Human + Technical Controls

RECOMMENDATIONS

Ways to eliminate or reduce the effects of many malware campaigns:

- Antivirus/Firewall/Ad blocker software
- Patch, patch, patch
- Strong Passwords
- Two Factor Authentication
- Segregation of networks (use of Administrators/users and Virtual Machines)
- Use Virtual Private Networks
- Backup to external hard drive
- Limit digital footprint

QUESTIONS?

CONCLUSION

With enough time, money, and commitment, everyone is vulnerable.

Make yourself and your company a harder target by following safe practices.

Joshua Kim

Legal Attaché Hong Kong

646-438-2098

+852-2841-2348

Joshua.kim@ic.fbi.gov

Compromised?

Paul Black – Asia Pacific & Japan, Incident Response
Victor Law – Greater China Region, Enterprise Security

Compromise

It will happen

No longer an if - but when

Detection takes too long

229 - Average number of days to discover a breach

Not enough skills

70% of organizations lack staff to counter cyber security threats

Time is money

Big money

Key Themes

Targeted Attacks

Targeted Attacks Shifted from Economic Espionage to Politically Motivated Sabotage and Subversion

Cyber Bank Heists

Attackers Chase the Big Scores, Bigger Ambitions and is Targeting Banks

Internet of Things

Cyber Criminals Harnessed the Processing Power of IoT Devices to Fuel Zombie Army of Devices

Ransomware

Ransomware Squeezing Victims with Escalating Demands

Macros, IT tools & Malware

Attackers Weaponized Commonly Used Software

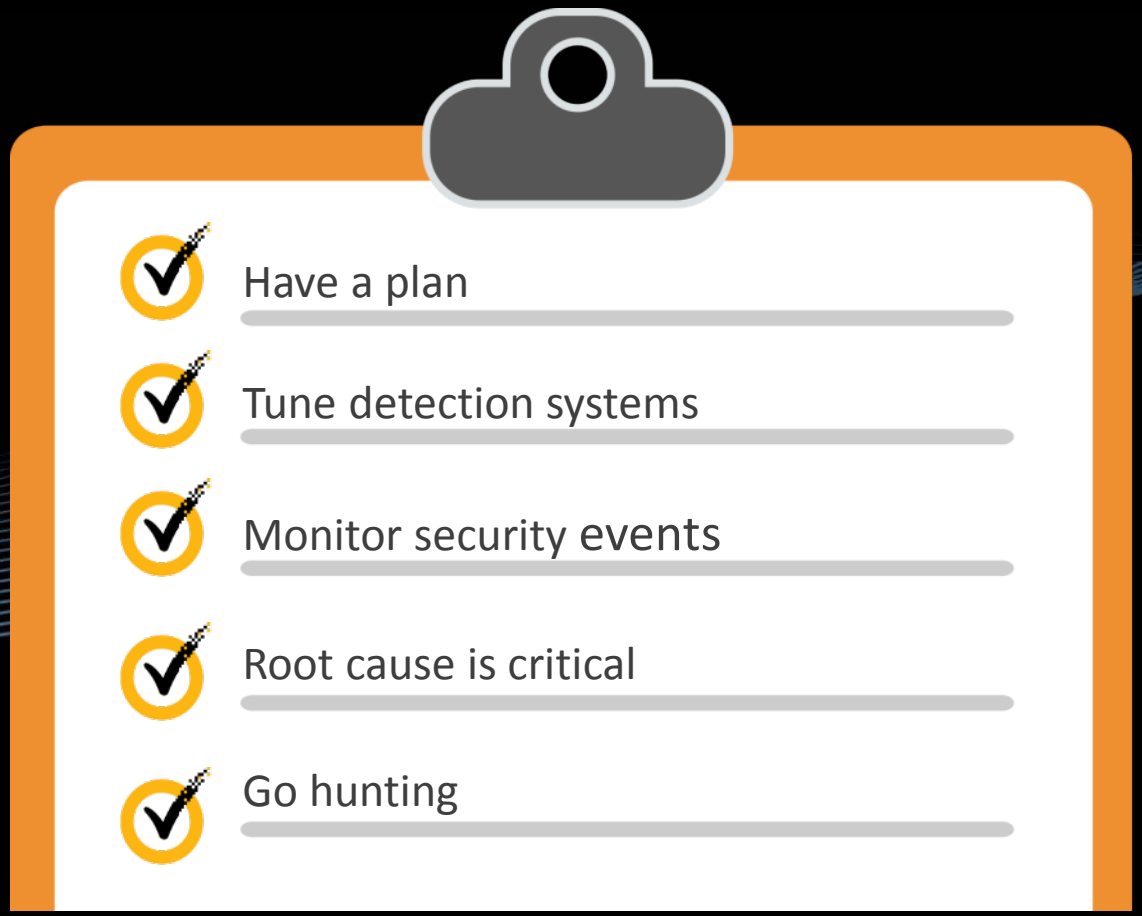
Email

Email Became the Weapon of Choice

Cloud

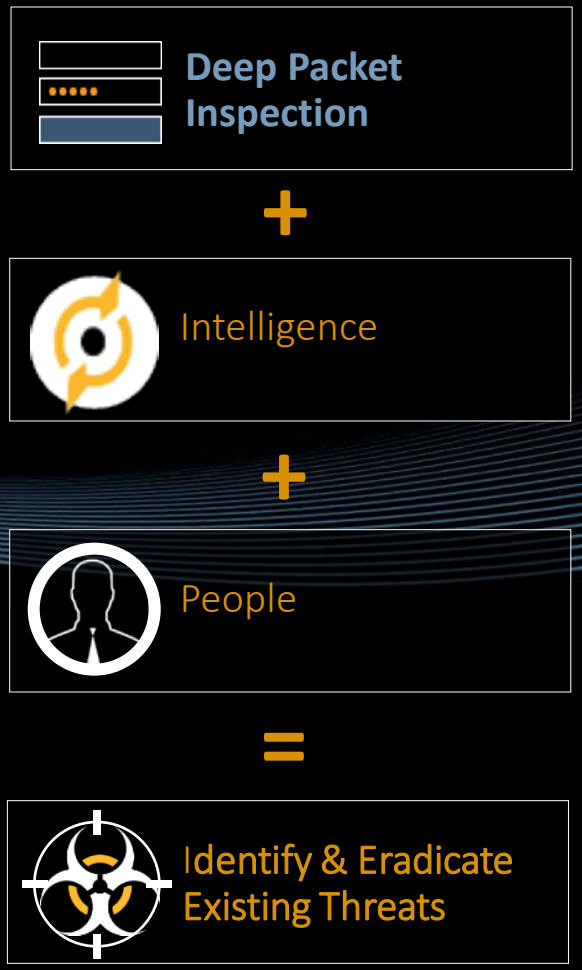
Cracks in the Cloud: The Next Frontier of Cybercrime is Upon Us

Quick Wins


Have a plan
Tune detection systems
Monitor security events
Root cause is critical
Go hunting

Go Hunting

Advanced Threat Hunting



Preventive Incident Response

Regularly hunting for threats helps to establish a consistent, known secure state for your network.

Don’t Wait For an Incident

Identify and **eradicate** existing compromises before they become a major data breach.

Reduce Breach Response Costs

Compromises are common and inexpensive to remediate.

Identify threats early to avoid high incident response costs.

Copyright © 2017 Symantec Corporation

The Importance of Root Cause

Infection vectors don’t change between commodity malware and targeted attacks

Know impact and intent, understand the risk and mitigate appropriately

Strengthen detection and prevention as an outcome of every qualified incident

Build trending and metrics into incident reporting

Use actual incident data to drive security awareness

Quick Wins


Educate users
Enforce complex passwords
Force password rotation
Implement 2 factor authentication
Practice incident response

Thank You!

MARSH

Network & Security Liability Insurance

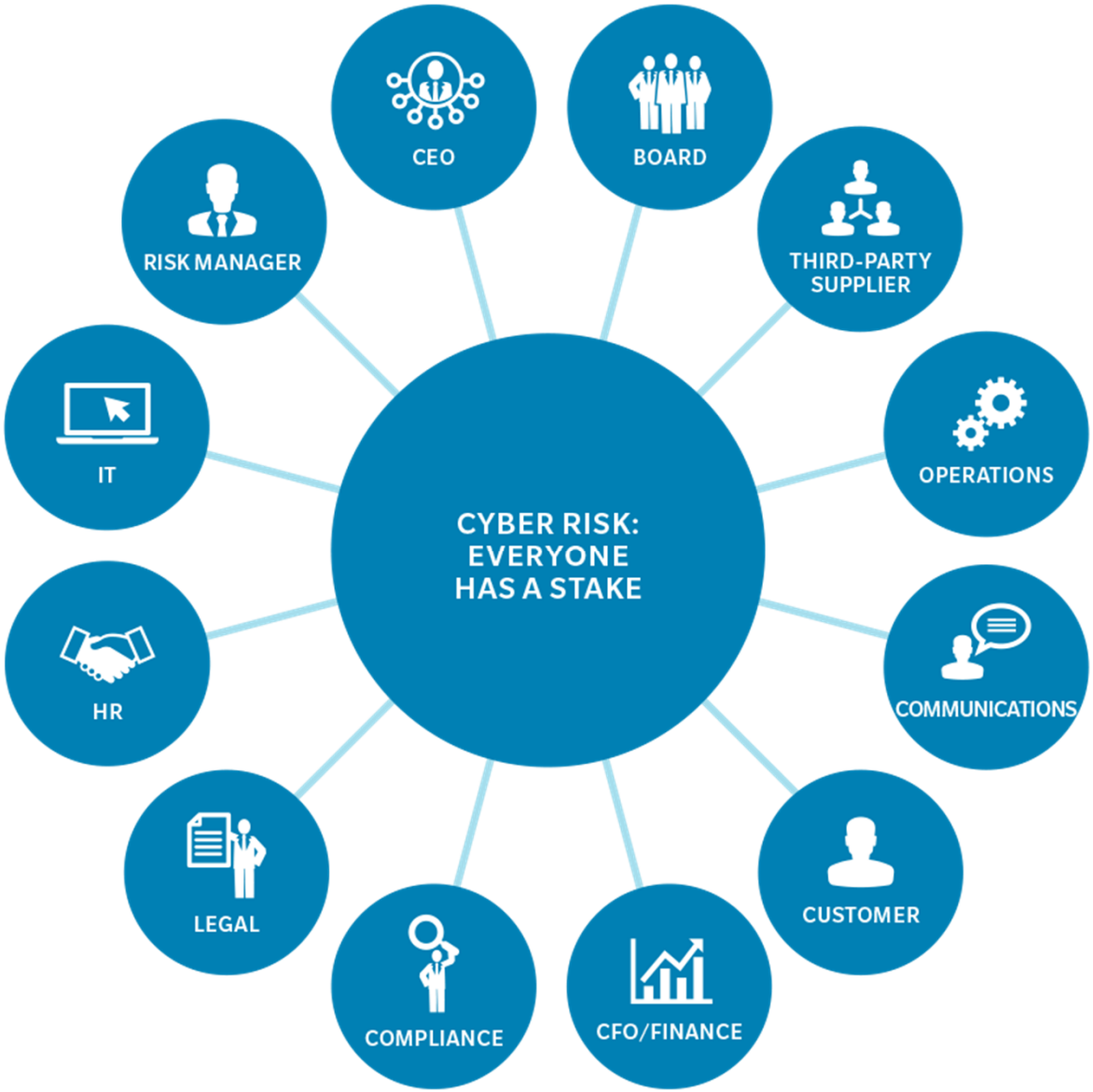
May 16th, 2017

Naureen Rasul, Regional Financial Institutions Industry Leader – Asia

Franky Mok, Financial and Professional Liability Practice – Hong Kong

Cybersecurity is no longer just an IT-department issue…

What Is The Impact Across An Organization?



What Is The Impact On An Organization?

Operational Disruption

Employee Exposures

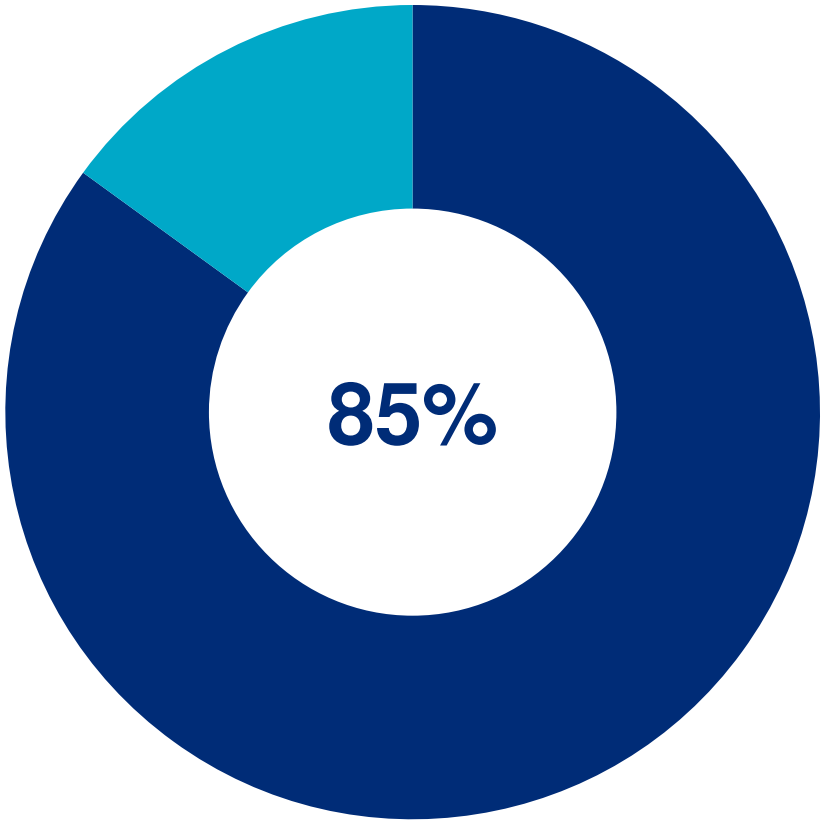
Lawsuits and Reputational Harm

Regulatory and Legal Implications

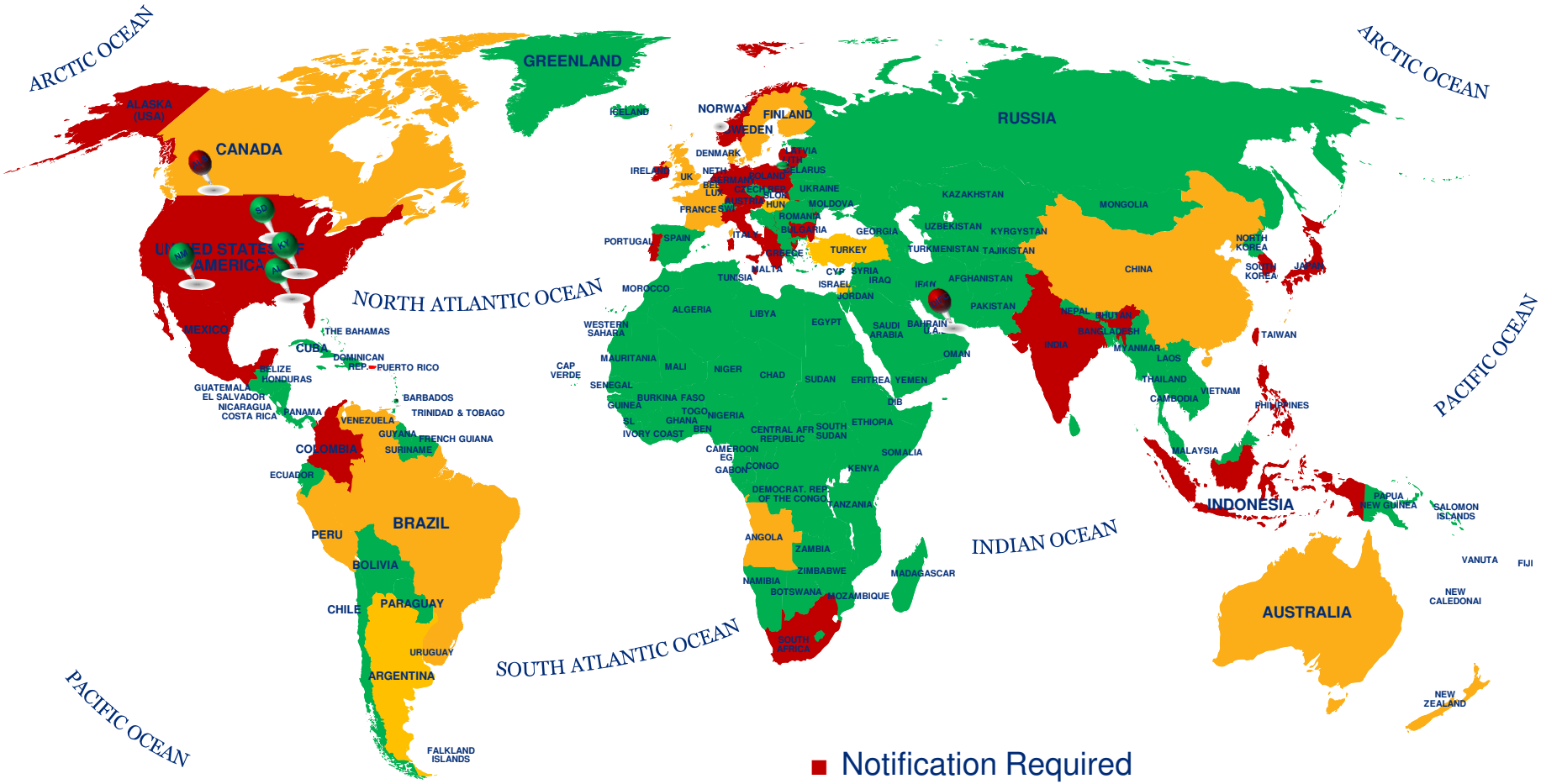
What Are The Cyber Statistics?

Source: 2016/2017 Global Fraud & Risk Report – Kroll

The number of executives who said that their company experienced a cyber attack, information theft, loss or attack in the last 12 months.



What Are The Breach Notification Requirements?



- Notification Required
- Notification Not Required but Certain Action Required or Recommended
- Notification Not Required

PCPD Actions Against Cyber Breaches in HK

Year	Nature of Business	Details	Fines (HKD)
2017	Bank	Failure to comply with customer's request to stop using his personal data for direct marketing.	$10,000
2016	Watch Company	Use of personal data in direct marketing without the subject's consent.	$16,000
2016	Marketing Company	Use of personal data in direct marketing without the subject's consent.	$16,000
2015	Individual	Release of personal data to third party for direct marketing without obtaining the subject's consent.	$5,000
2015	Telecommunications Service Provider	Failure to comply with customer's request to stop using his personal data for direct marketing.	$30,000
2015	Body Check Services Company	Failure to comply with an opt-out request.	$10,000
2015	Storage Services Provider	Use of personal data in direct marketing without the subject's consent.	$10,000

Types of Insurance Policies

Policies Terms and Conditions

First Party Costs and Other Expenses

Reimburses an organization for the costs it may incur to respond to a breach

1) Business / Network Interruption
2) Event Management
3) Cyber Extortion

- Forensic Investigations
- Legal & Regulatory Advice Costs
- Notification Costs
- Account & Credit Monitoring Costs
- Data Asset Restoration
- Public Relations Costs

Third Party Liability and Defense Costs

Covers an organization's liability to third parties from its failure to keep data secure

1) Privacy and Data Breach
2) Failure of Network Security
3) Regulatory Investigations
4) Media Content Infringement, Libel, Slander, Defamation

Insurance Markets in Asia

- **AIG**
- **Allianz**
- Allied World
- Antares
- Aspen
- AXA
- Axis
- Barbican
- Beazley
- Berkley
- Berkshire Hathaway
- Brit
- **Chubb**
- Dual
- Hiscox
- Kiln
- Liberty
- Markel
- Munich Re
- Novae
- QBE
- Scor Re
- Swiss Re
- Tokio Marine
- XL
- **Zurich**

Lead Primary Insurers

Questions & Answers

Appendix

Marsh Solutions and Proven Approach
Insuring Agreements: First Party Costs and Expenses

Insuring Agreements	Explanation
Business Interruption	Loss of income and / or extra expenses resulting from a business interruption or suspension of a computer system due to total / partial failure of technology.
Event Management	• Forensic Investigations – Fees and costs for an IT or other external expert to analyze an organization's computer system in order to (1) ascertain whether or not a cyber breach has occurred, (2) determine the cause and extent of such a breach, and (3) how it can be mitigated in the future. • Legal and Regulatory Advice Costs – Fees and costs to advise an organization on its legal and regulatory duties to report the cyber breach to any affected subjects, third parties and regulators. • Notification Costs – Fees and costs to notify affected subjects, third parties and regulators of the cyber breach. This includes the operation of a call center. • Account and Credit Monitoring Costs – Fees and costs to establish and procure new account numbers and credit monitoring services for a period of time following the cyber breach. • Data Asset Restoration – Fees and costs an organization incur to restore, recreate or recollect its data and other intangible assets (i.e. databases, software, applications, etc.) that are corrupted or destroyed by a cyber breach. • Public Relations Costs – Fees and costs incurred in retaining a consultant or other crisis communications consultant to prevent or reduce the effects of negative publicity.
Cyber Extortion	Fees and costs by a credible and probable threat to cause a cyber breach, and monies payable by an organization in order to resolve or terminate the extortion threat.

Marsh Solutions and Proven Approach

Insuring Agreements: Third Party Liability and Defense Costs

Insuring Agreements	Explanation
Privacy and Data Breach Liability	Defense and liability costs for failure to prevent unauthorized access, disclosure or collection of confidential information, or for failure of others to whom the organization have entrusted such information (e.g., data storage facility, credit card processor, etc.). It includes liability for not properly notifying of a privacy breach.
Network Security Liability	Defense and liability costs for failure of system security to prevent or mitigate a cyber breach, including but not limited to, the spread of virus or a denial of service. This includes failure of written policies and procedures addressing technology use.
Privacy Regulatory Defense Costs	Costs to defend an action or investigation by regulators due to a cyber breach, including indemnification for any fines or penalties assessed.
Media Liability	In the context of an organization's publication or broadcast of any digital media content, any defense and liability costs for online libel, slander, defamation, disparagement, misappropriation of name or likeness, plagiarism, copyright infringement, and negligence in content to those that relied on content.

Marsh Solutions and Proven Approach
Common Exclusions

Exclusions	Explanation
Antitrust	Any actual or alleged antitrust violation, restraint of trade or unfair competition.
Bodily Injury and Property Damage	Any actual or alleged bodily injury, sickness, mental anguish or emotional distress, disease or death of any person causing damage to or destruction of any tangible property.
Contractual Liability	Any liability under any contract, agreement, guarantee or warranty assumed or accepted by the organization.
Dishonest, Improper or Intentionally Act	Any deliberate, criminal, fraudulent, dishonest, intentional or malicious act or omission, breach or violations. Not applicable to Data Security Liability.
Prior Claims and Circumstances	Any claim, breach, threat, event, wrongful act or circumstance that is likely to give rise to a claim, breach, threat, or wrongful act (a) notified to a prior insurance policy; or (b) which an Insured Person was aware of or should have been aware of prior to the policy inception.
Pollution and Natural Perils	Any discharge, dispersal, seepage, migration, release or escape of any solid, liquid, gaseous, biological or thermal irritant or contaminant, including smoke, vapor, soot, fumes, acids, alkalis, chemicals, radiation and waste.
Securities Claims	Any actual or alleged violation of law, regulation or rule relating to the ownership, purchase, sale, offer or solicitation of an offer to purchase or sell securities.
Terrorism / War	Any form of war, terrorism or riot.
Trade Secrets and Intellectual Property	Any actual or alleged plagiarism of or infringement of copyright, patent, trademark, trade secret, service mark, trade name, or misappropriation of ideas or trade secrets or other intellectual property rights.
Trading Losses	Any losses or liabilities connected with any types of purchase or sale of securities, commodities, derivatives, currencies, foreign exchange, and the like.

Marsh Solutions and Proven Approach

Step 1: Privacy and Information Security Assessment

How to assess cyber risk?

A thorough understanding of your risk profile is critical, and that means more than the typical compliance audit. You need to inventory cyber-vulnerable assets, identify new and emerging threats – internal and external – and model an event's potential impact.

The evolving nature of cyber risk requires you to continuously monitor changes in their risk profile – then adapt.

How to manage cyber risk?

Cyber risk management typically requires a balanced approached of:

- *Prevention* – to stop cyber-attacks from succeeding
- *Preparation* – to make sure you are ready when an event happens
- *Risk Transfer* – to transfer the exposure off your balance sheet

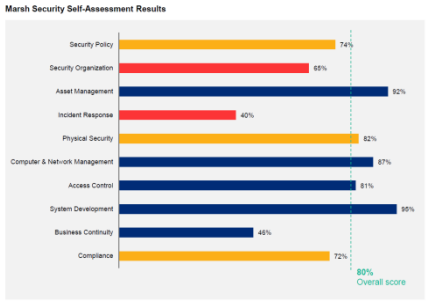
How to respond to a threat, breach or attack?

You cannot stop a cyber-attack from occurring, but you can control how you respond to it. A quick, effective reaction is essential, and the decisions you make after an event can have lasting implications.

Marsh Solutions and Proven Approach (continued)

Step 1: Privacy and Information Security Assessment

Assets	Threats	Control	Impact
What are your cyber assets?	**What are your threats?**	**What security controls do you have in place?**	**What is the impact of a breach?**
Begin by identifying, categorizing and ranking your cyber-related assets. Assets form the motivations for threats against the organization.	Understand the cyber threats that correspond to the identified assets. Since cyber-attacks are perpetrated by people – understanding how your organization look to the world is paramount to understanding the likelihood of an attack.	How mature are your defenses to protect against cyber-attacks? *Understand* processes, procedures, protocols, technical solutions and other measures that have been instituted. Compare those to your peers and industry best practices to understand how ready you are for a cyber event.	Data breaches are one of the most common cyber risks faced by organizations today. You should better understand the potential impact of a breach to your organization's assets, both qualitative and quantitatively, so that you can prioritize your efforts to transfer or mitigate the risk of a breach.



Data Breach Event Total Costs

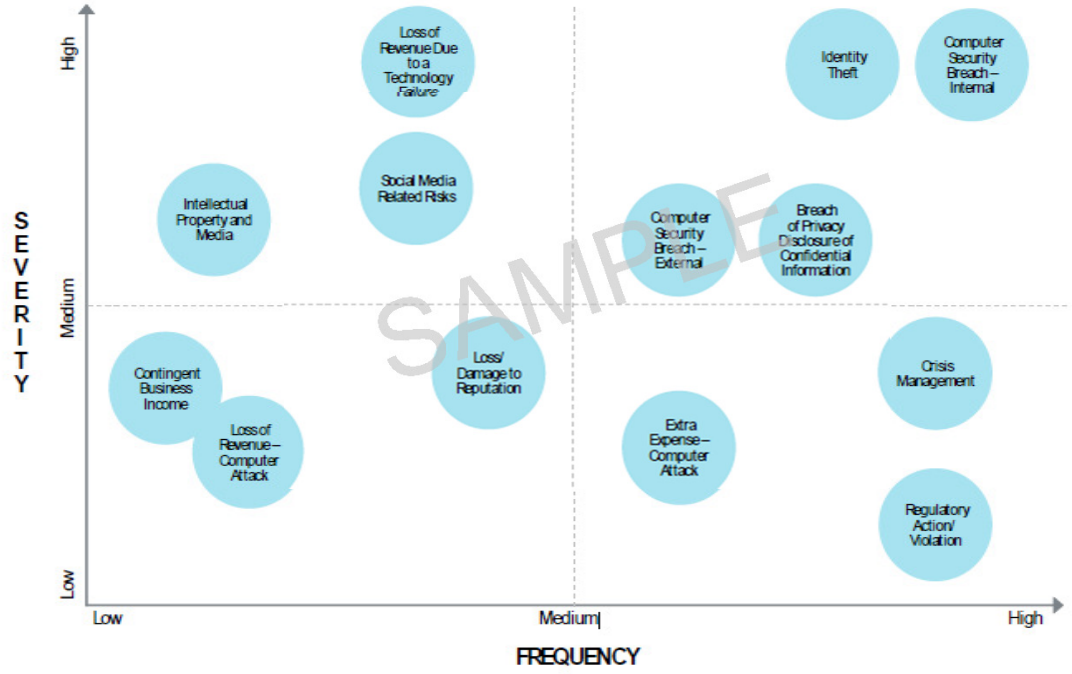
Event Type	Percentile	Number of Affected Records	Total Cost per Event
Mean	–	293,897	$2,034,491
1 in 2 Events	50%	5,176	$232,319
1 in 4 Events	75%	73,499	$495,939
1 in 5 Events	80%	142,851	$816,888
1 in 10 Events	90%	574,609	$3,746,131
1 in 20 Events	95%	1,570,302	$9,177,485
1 in 100 Events	99%	6,124,874	$38,061,069

Marsh Solutions and Proven Approach

Step 2: Risk Mapping

Taking what we learned from the privacy and information security assessment, we can then align risk management with your objectives.

We will also prioritize the likelihood and severity of risks and identify any interrelationships among them.



Marsh Solutions and Proven Approach

Step 3: Benchmarking and Modeling

Privacy IDEAL Model (Identify Damages, Examine and Assess Limits)

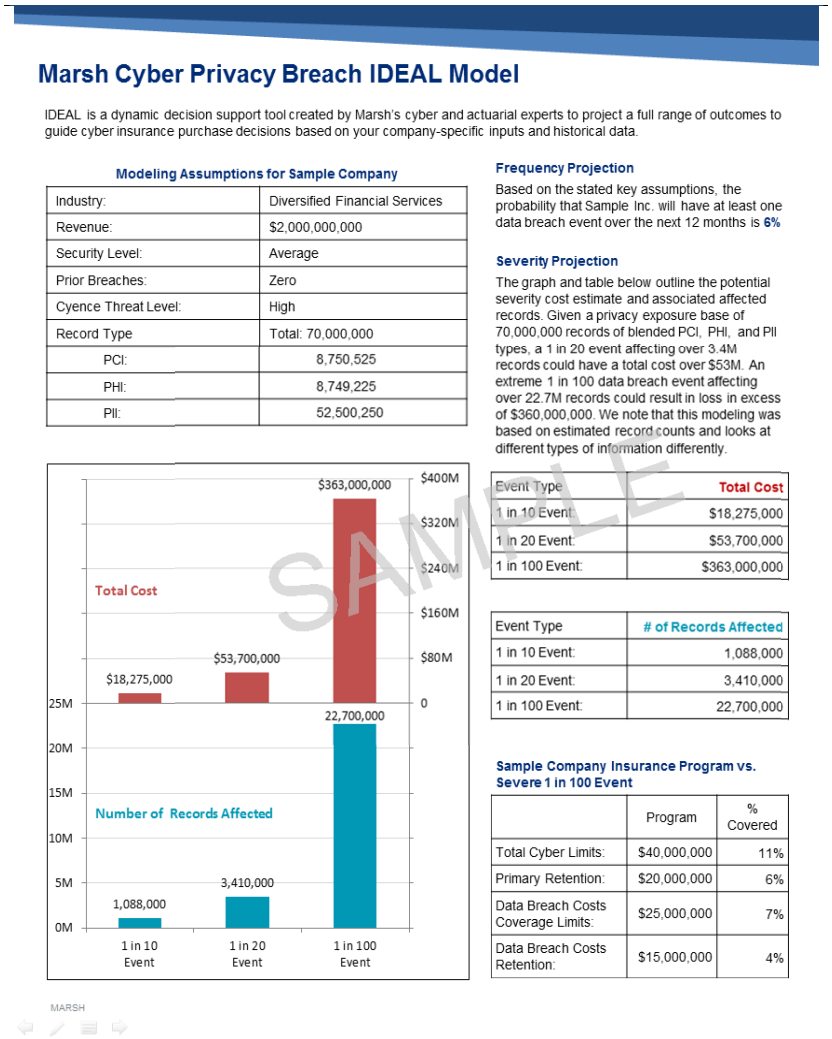
- Developed by Marsh Global Analytics to harmonize analytics offerings globally, aggregate data, and provide industry-leading analytics through cutting-edge technology.

Privacy IDEAL is built upon the following data sources

- Marsh proprietary Cyber Database
- Privacy Rights Clearinghouse Chronology of Data Breaches
- Advisen MSCAd Large Loss Database

Privacy IDEAL has two parts

- Frequency Model – predicts the likelihood of unauthorized disclosure.
- Severity Model – estimates the likely cost per breach.



Marsh Cyber Privacy Breach IDEAL Model

IDEAL is a dynamic decision support tool created by Marsh's cyber and actuarial experts to project a full range of outcomes to guide cyber insurance purchase decisions based on your company-specific inputs and historical data.

Modeling Assumptions for Sample Company

Industry:	Diversified Financial Services
Revenue:	$2,000,000,000
Security Level:	Average
Prior Breaches:	Zero
Cyence Threat Level:	High
Record Type	Total: 70,000,000
PCI:	8,750,525
PHI:	8,749,225
PII:	52,500,250

Frequency Projection

Based on the stated key assumptions, the probability that Sample Inc. will have at least one data breach event over the next 12 months is **6%**

Severity Projection

The graph and table below outline the potential severity cost estimate and associated affected records. Given a privacy exposure base of 70,000,000 records of blended PCI, PHI, and PII types, a 1 in 20 event affecting over 3.4M records could have a total cost over $53M. An extreme 1 in 100 data breach event affecting over 22.7M records could result in loss in excess of $360,000,000. We note that this modeling was based on estimated record counts and looks at different types of information differently.

Event Type	Total Cost
1 in 10 Event:	$18,275,000
1 in 20 Event:	$53,700,000
1 in 100 Event:	$363,000,000

Event Type	# of Records Affected
1 in 10 Event:	1,088,000
1 in 20 Event:	3,410,000
1 in 100 Event:	22,700,000

Sample Company Insurance Program vs. Severe 1 in 100 Event

	Program	% Covered
Total Cyber Limits:	$40,000,000	11%
Primary Retention:	$20,000,000	6%
Data Breach Costs Coverage Limits:	$25,000,000	7%
Data Breach Costs Retention:	$15,000,000	4%

MARSH

Marsh Solutions and Proven Approach

Step 4: Coverage Gap Analysis

Once we understand your risk profile, we will conduct a comprehensive gap analysis across all insurance product lines.

This will help determine what coverage is available to respond to claims and losses in the event of cyber attack, breach of privacy, or loss of confidential information.

Covered | Dependent upon specifics of claims and policy, may not be covered | Not covered

CATEGORY	LOSS ITEM	PROPERTY	TERRORISM	GENERAL LIABILITY	PROFESSIONAL INDEMNITY	FIDELITY (CRIME)	CYBER/PRIVACY POLICY
Assets	Destruction, corruption or theft of your electronic information assets/data due to a breach of computer or network security.						Information asset protection
Business interruption	Business interruption loss caused by a material interruption to your computer system due to a breach of computer or network security.						Network business interruption
	Business interruption loss caused by a material interruption to your computer system due to operational error of your staff.						Network business interruption
Privacy liability	Liability arising from the unauthorised release of personally identifiable information.						Privacy liability
	Costs incurred to notify affected individuals following the release of personally identifiable information where you are compelled to do so by law.						Privacy liability
	Defence costs incurred and penalties imposed (where insurable) in connection with a regulatory action brought as a result of the unauthorised release of personal information.						Privacy liability
	Payment Card Industry fines incurred as a result of the unauthorised release of credit/debit card information.						Privacy liability
Network liability	Liability arising from the failure of computer or network security to prevent a breach that damages a third party's data.						Network liability
	Liability arising from the negligent transmission of a computer virus caused by the failure of computer or network security to prevent a breach.						Network liability
	Liability arising from the prevention of authorised access to a computer system caused by the failure of computer or network security to prevent a breach.						Network liability
	Liability arising from the use by a hacker of your IT assets in a denial-of-service attack caused by the failure of computer or network security to prevent a breach.						Network liability
Electronic media liability	Liability arising from the content of your website(s) that is defamatory.						Electronic media liability
	Liability arising from the content of your website(s) that infringes another's intellectual property rights with exception of patent and trade secret.						Electronic media liability
	Liability arising from negligent publication or misrepresentation within the content of your website(s).						Electronic media liability
Extortion	Cost of a ransom paid as a result of a valid threat to release or destroy data assets including confidential commercial information or personally identifiable information.						Cyber extortion

Marsh Solutions and Proven Approach

Post Incident – Crisis Management and Business Continuity

1 DETERMINE RESILIENCE

Determine how resilient you are to a cyber-attack

Determine risk profile and complete a cyber stress test

Review compliance with regulatory environment

Review risk assessment and business interruption threats

Validate technology requirements and recovery time objectives

2 DEVELOP STRATEGY

Determine the most effective response strategy to deal with your cyber risk exposures

Identify / validate critical business functions

Develop recovery strategies with those functions exposed and critical to the company response

Determine technology requirements

3 PLANNING

Plan writing

Creation of appropriate business continuity and crisis management plans

Create framework documentation

Develop policy and roles and responsibilities to manage risk and improve awareness

4 IMPLEMENTATION

On-site training, consultation and exercising

Preparation of desktop exercise and creation of credible cyber scenario(s)

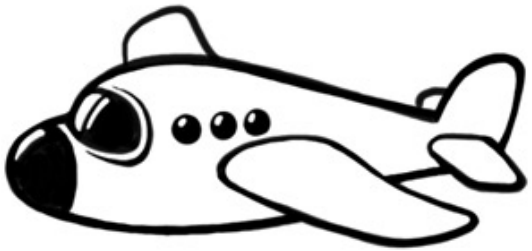
Desktop simulation exercise

Present observations and recommendations

Actual Cyber Incidents in Asia

Airlines

- 2016 – hackers attacked the website of a Vietnamese airline and posted political messages. Airport operators had to temporarily halt all electronic check-ins.
- 2016 – an estimated 47,000 scanned personal documents were left unsecured on the website of a major Korean airline. Victims were Koreans and foreigners who travelled using the airline, including its affiliated international airlines.
- 2015 – the domain name system of a Malaysian airlines was compromised and users were redirected to a hacker website.
- 2015 – theft of 4.7M miles and gifts worth HKD100K from 121 mileage group members.
- 2014 – personal information of 750K loyalty program members were stolen when hackers installed a malware in the customer information management system. Data included names, birthdates, gender, home and addresses, phone and fax numbers, mileage program membership numbers and enrolment dates.



Actual Cyber Incidents in Asia (continued)

Educators

- 2014 – an IT engineer on a temporary contract stole 22.6M customer files using his smartphone. About 1/3 of Japan's total population was affected. Data included names, addresses and email addresses. Approximately 6.2M customer files were sold to a name-list trader. The company had to book a USD210M loss for expenses to mail apologies and for strengthening its data management capabilities. Over 1,700 people filed a lawsuit demanding damages for each plaintiff.

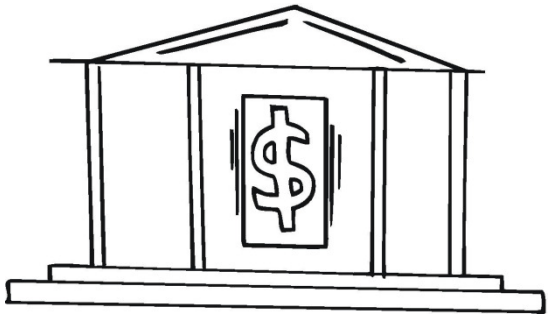
Food & Beverages

- Data of over 108K customers who signed up for a bonus point scheme was leaked to an outside party when the file was accidentally attached to an email. The company offered a small token of appreciation to all affected customers amounting to USD1.4M.

Actual Cyber Incidents in Asia (continued)

Financial Institutions

- 2016 – ATM heists in Bangladesh, Japan, Malaysia, Thailand and Vietnam.
- 2016 – 3.2M debit cards were compromised; the leak may have originated in the use of ATM where the backend system was hacked.
- 2015 – two banks were hacked leading to unstable service. Both bank received emails demanding bitcoin payments or another round of attacks would occurs.
- 2014 – a computer contractor stole 106M customer information files from three credit card companies and sold the information to marketing firms. Each of the three companies was fined 6M won and was banned from issuing new cards for three months.
- 2014 – Bitcoin's leading exchange suffered a security breach and filed for bankruptcy; account data included usernames, email addresses and an encrypted passwords. The company already had class action lawsuits filed alleging the lack of adequate security.



Actual Cyber Incidents in Asia (continued)

Hospitality

- 2015 – a hotel operator discovered signs of unauthorized access to payment card data. Malware was installed on computers that operate its payment process system. Over 100 hotels in the US and in 54 countries, including Asia, were affected.
- 2015 – a luxury hotel was attacked by malware on its credit card system. Ten hotels within the group's operation in the US, Europe and Asia were affected.

Leisure

- 2014 – prosecutors alleged that an employee of a third party contractor used a portable hard drive device to steal credit card data. The regulator suspended the operations of the three credit card firms for three months. About 20M customers were affected by the firms' data breach.
- 2014 – a karaoke entertainment company suffered a security breach where personal data of 300K customers in its database was leaked. This was part of a threat by some hacktivists protesting against new toll charges.

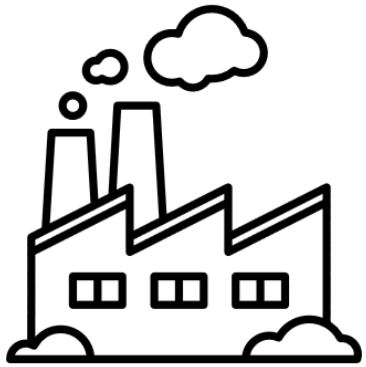
Actual Cyber Incidents in Asia (continued)

Manufacturers

- 2015 – a toy manufacturer detected irregular activity on their website. Nearly 5M customers in 16 countries and 6.3M children profiles worldwide were affected. Parent information included names, mailing and email addresses, secret questions and answers for password retrieval, IP addresses, download histories and encrypted passwords. Kid profiles included names, gender and birth dates.

- 2015 – a class action suit was filed against a PC manufacturer alleging fraudulent business practices and that a pre-loaded adware made the PCs vulnerable to malware and malicious attacks. The plaintiff accused the manufacturer of both invasion of privacy and profited by internet browsing habit studies. The software plugs product recommendations into search results which can caused connections hijacks and open security holes.

- 2014 – computer systems at a nuclear plant operator was hacked raising concerns about safeguarding nuclear facilities in the country.



Actual Cyber Incidents in Asia (continued)

Telecommunications

- 2014 – account information of 12M customers were stolen; data included names, registration numbers and bank account information. Two hackers and the CEO of a telemarketing firm infiltrated the telco's servers and stole up to 300K records a day.
- 2014 – a telecoms service provider started taking online pre-orders of the Apple iPhone 6; a postgraduate student used a cookie modifier plug-in to access forms showing data from customers, including personal data, prompting the company to shut down the pre-order web page for 12 hours.
- 2012 – internal employees sold customer data to telemarketers; hackers stolen 8.7M punters and sold them after breaching a customer sales system.
- 2011 – hackers broke into two popular social networks and stole 35M user information. Names, email addresses, phone numbers and resident registration numbers were compromised. Multiple class action lawsuits were filed alleging improper security measures.

Marsh Solutions and Proven Approach
Cyber Risk Management Framework

Marsh Risk Consulting (MRC) helps clients assess, manage and respond to current or future cyber threats in an efficient and cost effective manner, using all available means to reduce the risk exposure.

- **Privacy and Information Security Assessment**
- **Risk Mapping**
- **Benchmarking and Modeling**
- **Coverage Gap Analysis**

Why Marsh?
Trusted Advisor, Innovator and Market Maker

Cyber risk is evolving so rapidly that only a trusted advisor, innovator and market maker can help a prospect surmount the largest cybersecurity threats today and those of tomorrow.

Marsh can evaluate every prospect according to our Cyber Risk Management Framework so that they can assess, manage and respond to risks with the right mixture of risk transfer and advisory solutions.

- **ADVISOR:** Our approach to managing cyber risk is multidimensional, comprehensive and inclusive. We consider the perspective of all stakeholders in the organization.
- **INNOVATOR:** A recognized leader in cyber innovation – beginning with the creation of the first cloud-computing coverage, first stochastic model of a data breach (Marsh Cyber IDEAL) and first cyber catastrophe program (Marsh Cyber CAT) designed for large risks capable of taking $100 million+ self-insured retentions. We also have strategic partnerships to develop proprietary cyber solutions that help to quantify and manage a prospect cyber risk.
- **MARKET MAKER:** Having shaped the direction of some of the earliest forms of cyber insurance, we continually look to bridge gaps that exist in traditional coverage when it comes to cyber risk. As the leader in cyber risk placement, Marsh has placed more than $250 million into the global market annually.

MARSH BY THE NUMBERS

25+
Global experts in network security, privacy, PI and media liability

$250M+
Cyber premiums placed globally

90%+
Client retention rate

1,400+
Network security, privacy and PI clients

1,300+
Cyber IDEAL models run annually


MARSH