IT Governance and Risk Oversight of NGO Boards

Bernard Kan
Senior Consultant
HKCERT

Hong Kong Computer Emergency Response Team Coordination Centre

HKCERT

香港電腦保安事故協調中心

- Established in 2001
- Funded by the HKSAR Government
- Operated by **Hong Kong Productivity Council (香港生產力促進局)**

- Mission
  - –As the coordination of local cyber security incidents, serving Internet Users and SMEs in Hong Kong
  - –As the Point of Contact of cyber security incidents across the border

HKCERT Services

- Incident Report

24-hr Hotline: 8105-6060

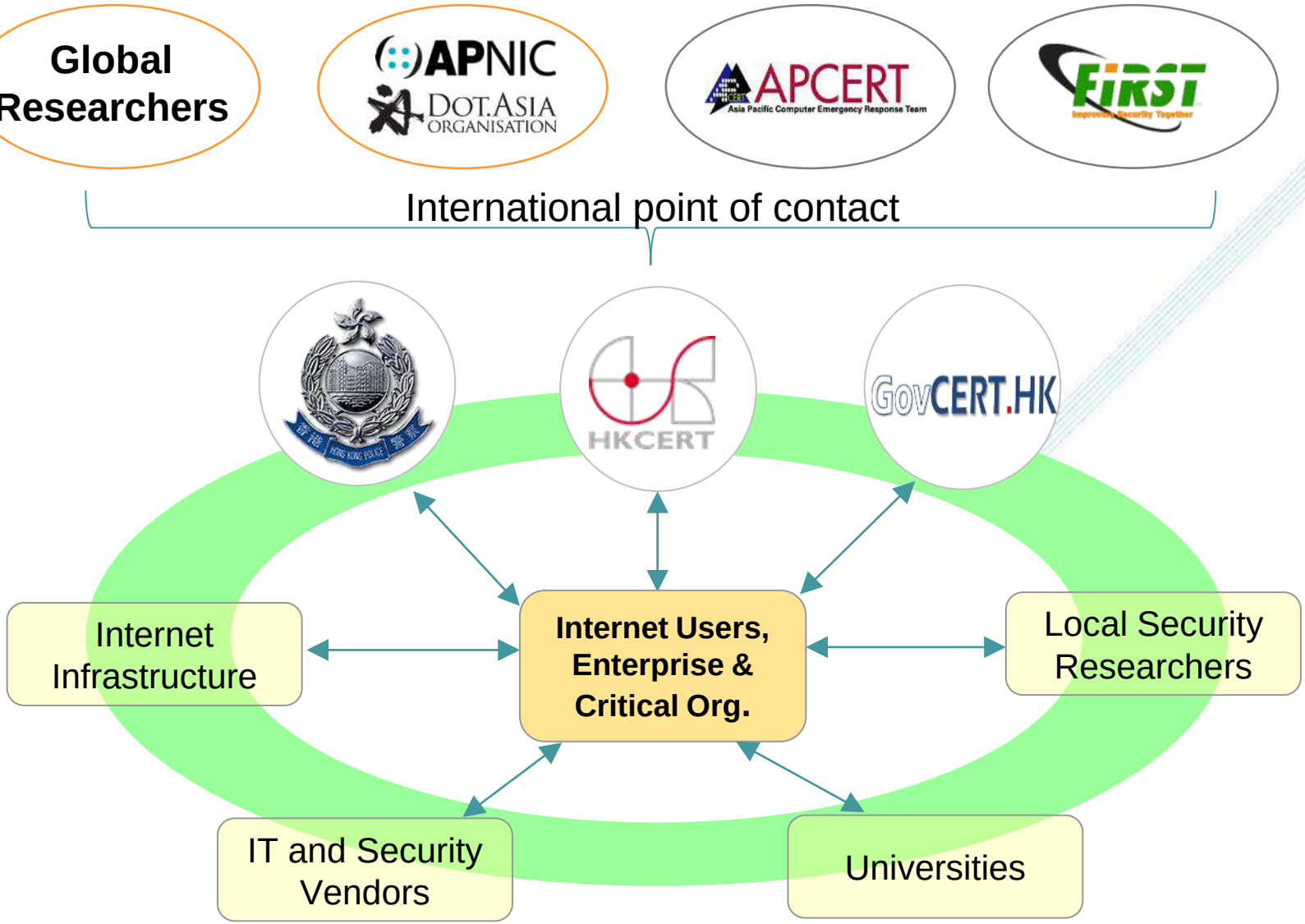
- Security Watch and Warning

Free subscription

- Cross-border collaboration

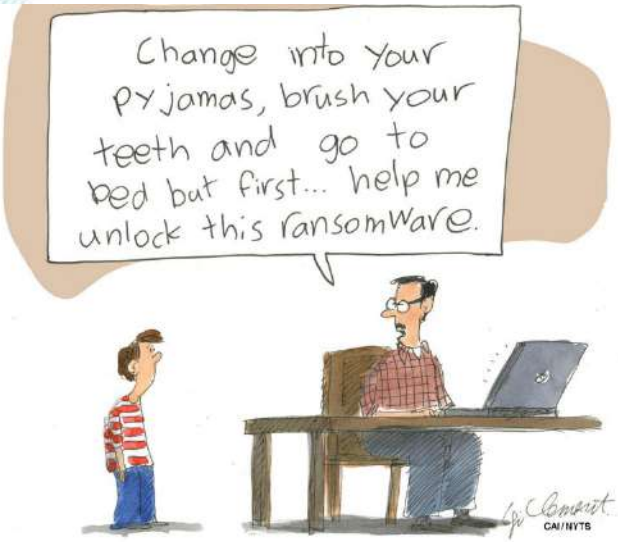
- Awareness education and guideline

As the Coordination Centre



Agenda

- Corporate Governance, IT Governance & IT Security Governance
- Recent Cyber Threats for Enterprises
- Cyber Security Concepts
- Best Cyber Security Practices
- Takeaway



Corporate Governance vs IT Governance

Corporate Governance: Leadership by corporate directors in creating and presenting value for all stakeholders

IT Governance: Ensure the alignment of IT with enterprise objectives

- Responsibility of the board of directors and executive management

IT Governance Objectives

- IT delivers value to the business
- IT risk is managed

Processes include:

- Equip IS functionality and address risk
- Measure performance of delivering value to the business
- Comply with legal and regulatory requirements

Information Security Importance

- Organizations are dependent upon and are driven by information
  - –Software = information on how to process
  - –Data, graphics retained in files
- Information & computer crime has escalated
- Therefore information security must be addressed and supported at **highest levels of the organization**

- Traditional term "**Information Security**" is now replaced by "**Cyber Security**".

Recent Cyber Threats for Enterprises

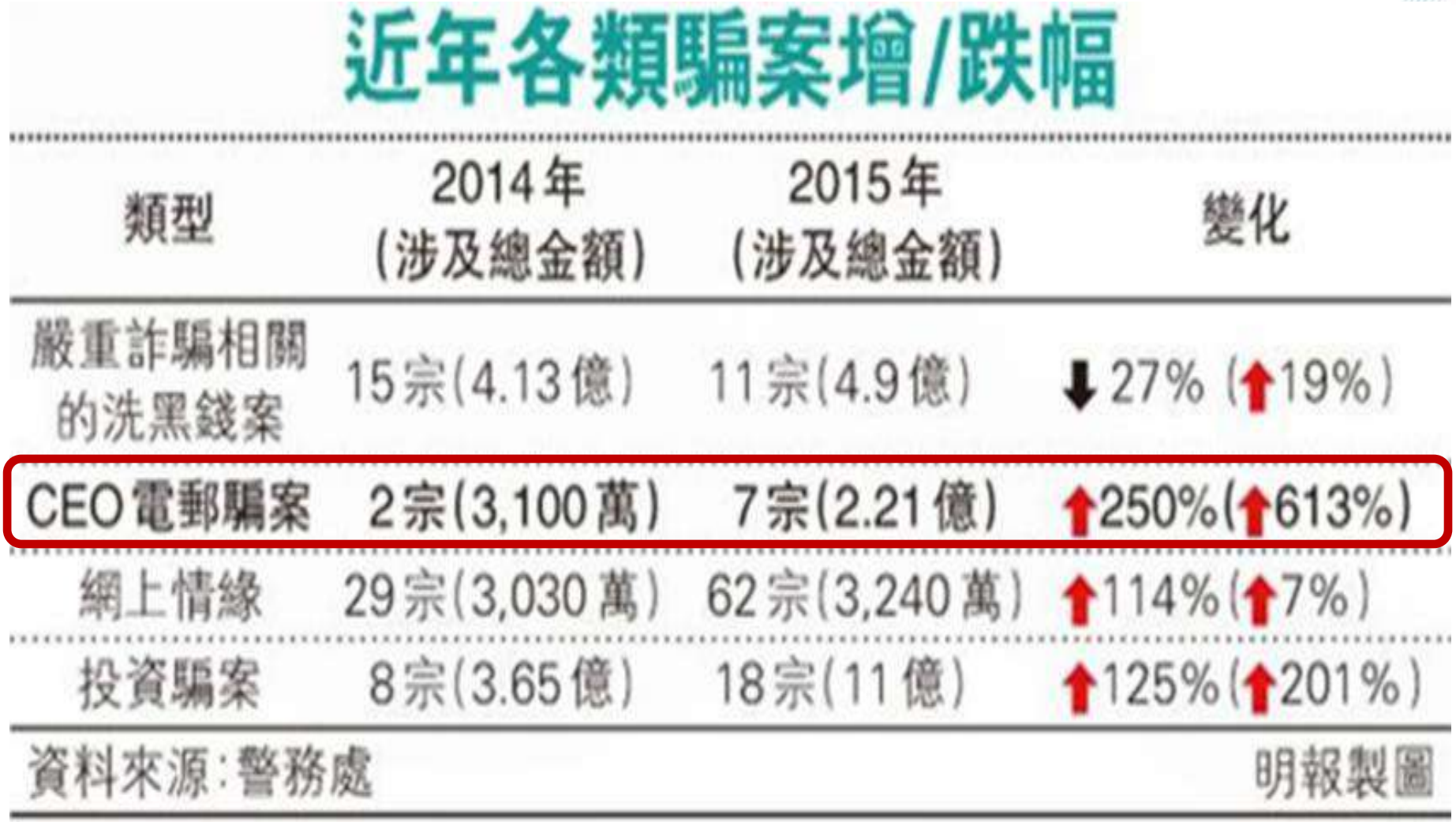
WannaCry Ransomware

WannaCry reports (May 2017)

- 500+ enquiries
- 30+ infection reports, cause of infection
  - no timely patching
  - direct connection to the Internet without firewall or router

- **Business attacks: Change of Bank Account**
- **Personal attacks: Overseas relative require urgent money**

Surge of CEO Email Scam



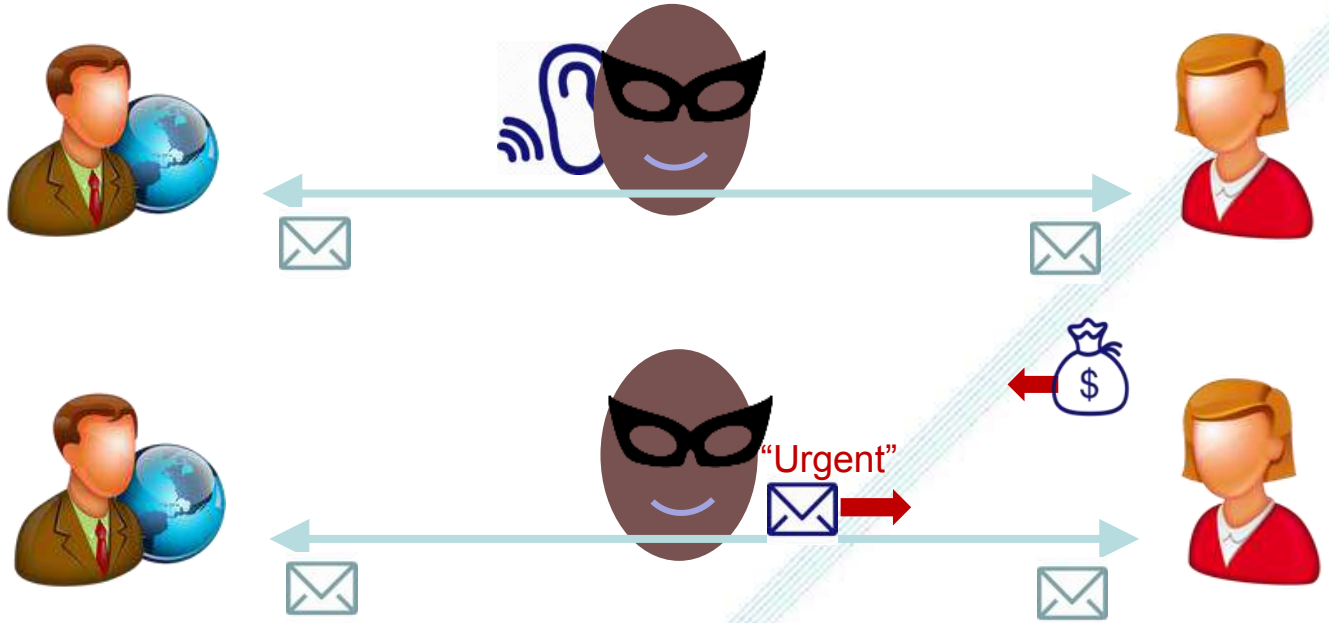
近年各類騙案增/跌幅

類型	2014年 (涉及總金額)	2015年 (涉及總金額)	變化
嚴重詐騙相關的洗黑錢案	15宗(4.13億)	11宗(4.9億)	⬇27% (⬆19%)
CEO電郵騙案	2宗(3,100萬)	7宗(2.21億)	⬆250%(⬆613%)
網上情緣	29宗(3,030萬)	62宗(3,240萬)	⬆114%(⬆7%)
投資騙案	8宗(3.65億)	18宗(11億)	⬆125%(⬆201%)

資料來源:警務處　　明報製圖

CEO Email Scam (with malware)

- **Step 1: Sniff and Learn** (via malware or hacked email account)



- **Step 2: Launch attack** when CEO is on business trip

Email scams compared

General phishing email

- Untargeted
- Spam email using spoofed sender
- Trick users to phishing website for credentials

CEO email scam

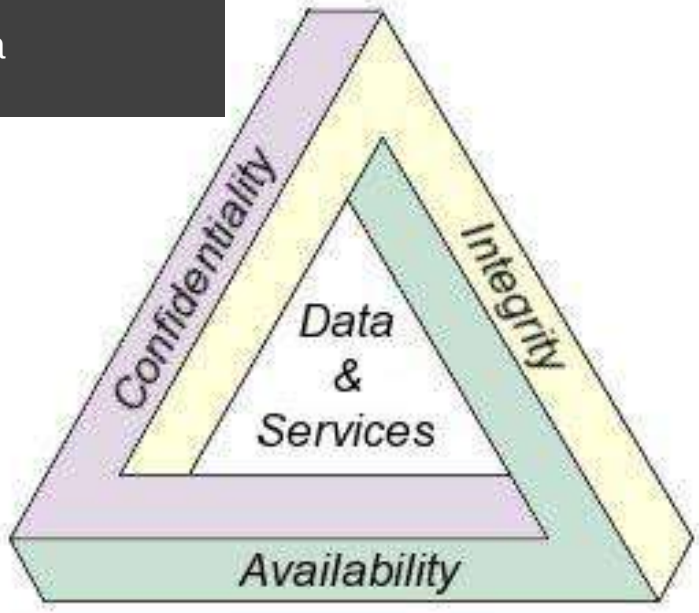
- Targeted
- Malware monitor email for a period silently
- Trick one side to transfer money / goods to scammer account

Cyber Security Concepts

CIA Triad of Information Security

Attack on Confidentiality (保密性)

- Leaking confidential data



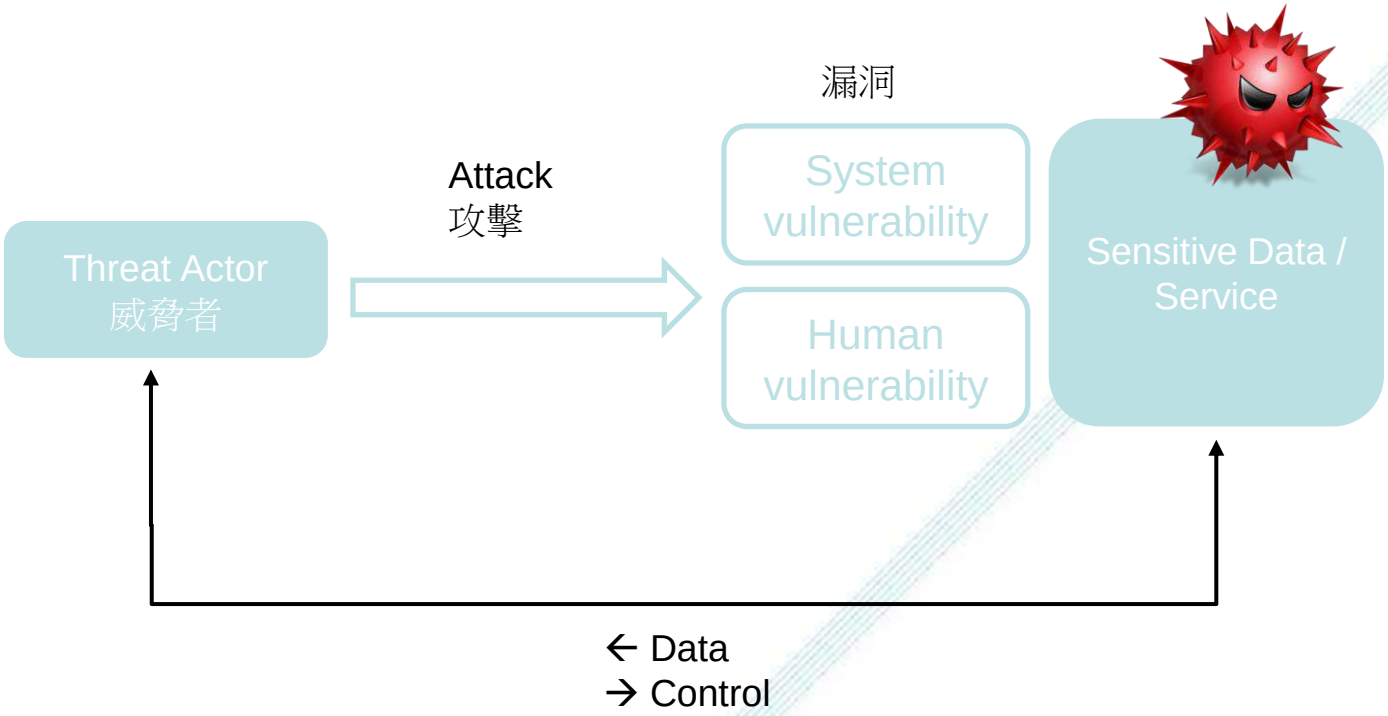
Attack on Integrity (完整性)

- Data contaminated
- Forged transaction
- System compromised
- Identity spoofed

Attack on Availability (可用性)

- System service not accessible (DDoS)
- Data destroyed or not accessible (ransomware)

Threat, Attack & Vulnerability



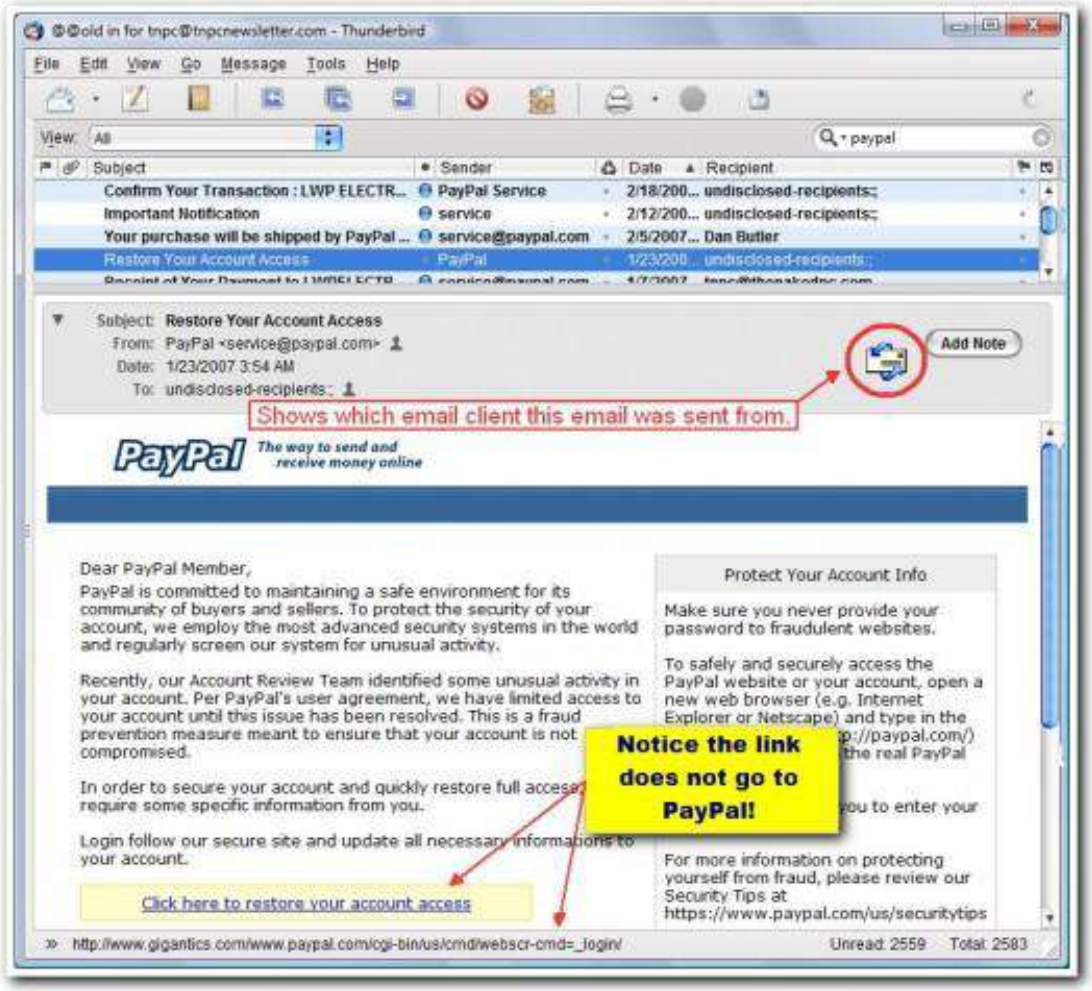
Attacks targeting Human

Who are you really talking to?

Social Engineering uses a lot of spoofing

Email: Identity spoofing

- Email protocol (SMTP) is open to spoof



Phishing attack

- Target general group
- Lure to enter credentials

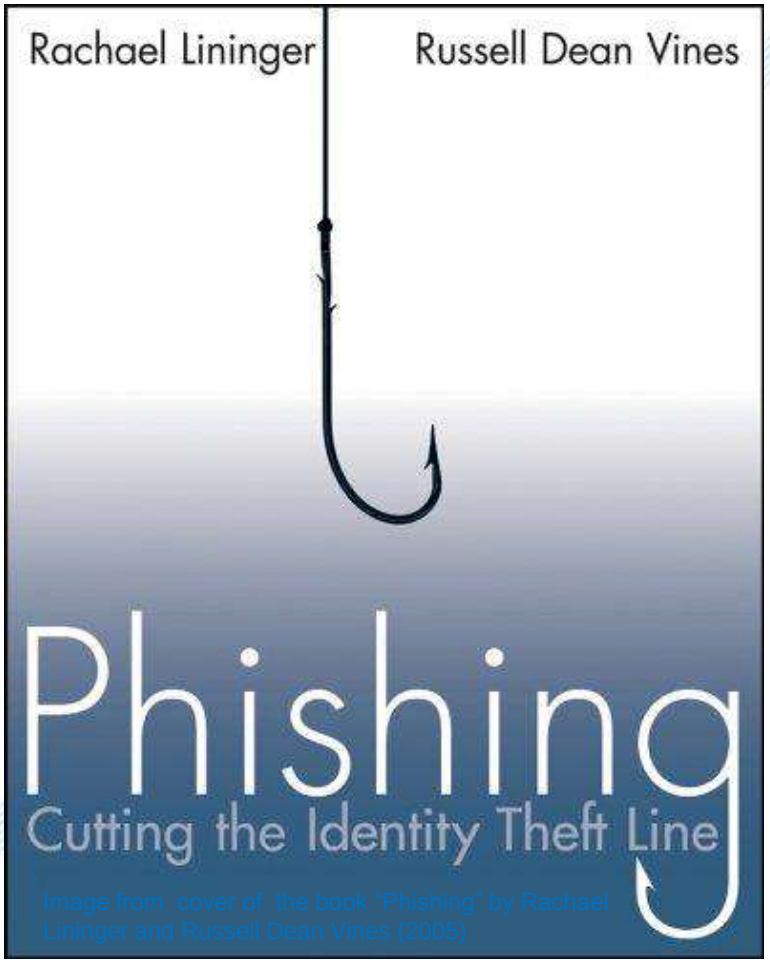


Image from cover of the book "Phishing" by Rachael Lininger and Russell Dean Vines (2005)

Social Network

- Malicious URL

Human vulnerabilities

95%

"95% of all attacks on enterprise networks are the result of successful spear phishing"

Source: Allan Paller, Director of Research - SANS Institute

AUTHORITY

URGENCY

FEAR

GREED

HELPFULNESS

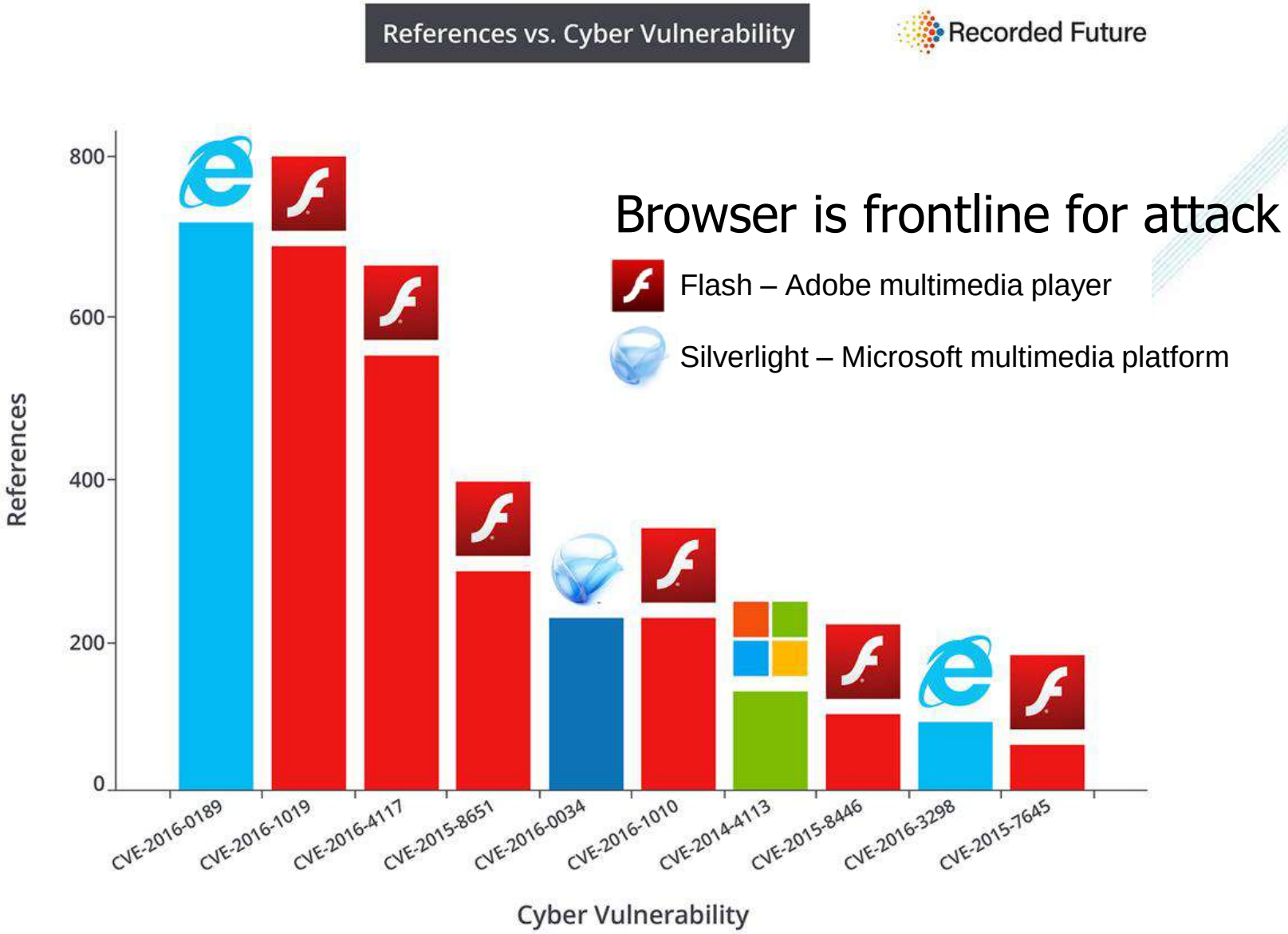
CARELESSNESS

SPOOFING

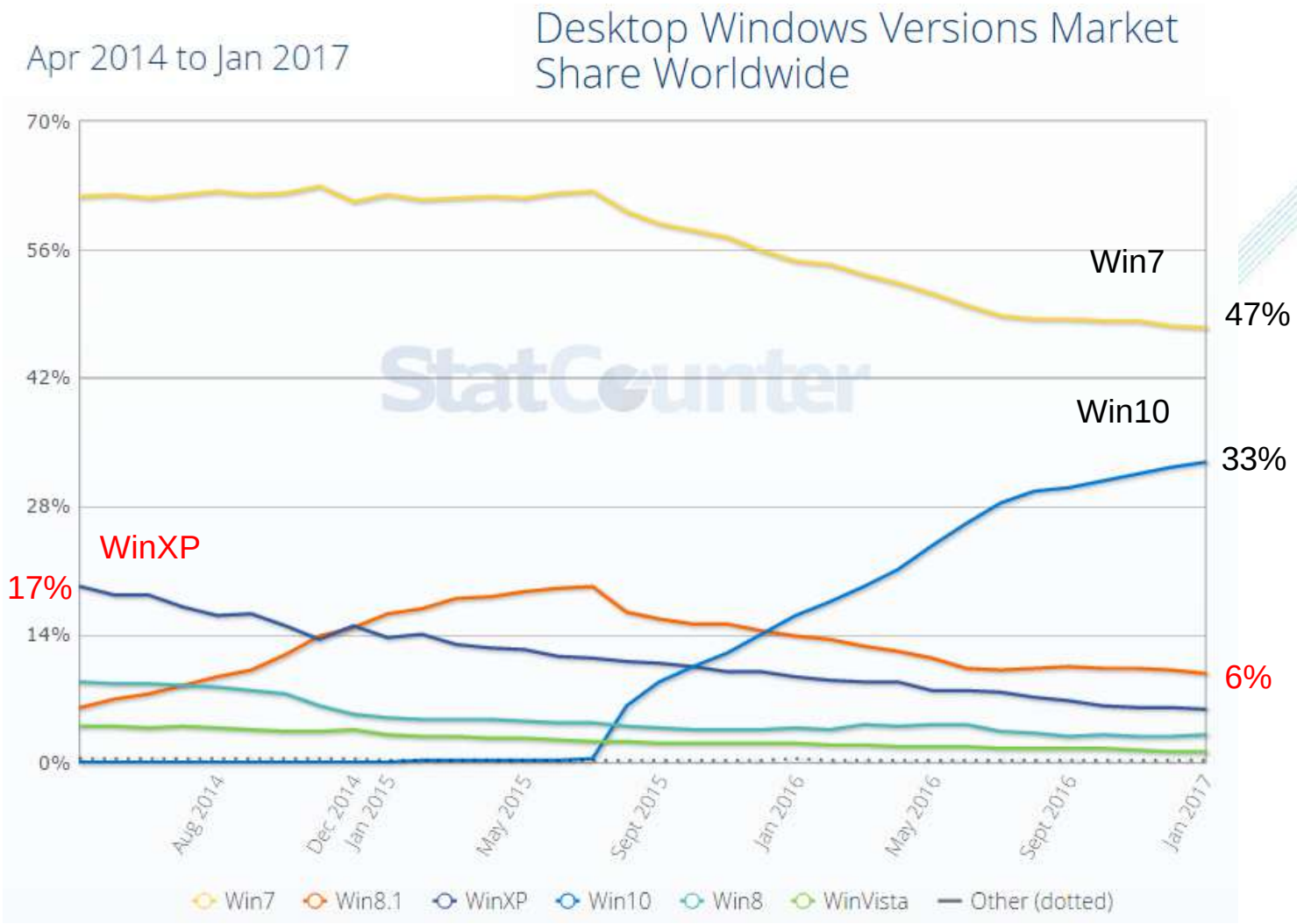
TRUST

Attack on Systems

Top system vulnerabilities in 2016



Unsupported software – Vulnerable systems



Malware Propagation channels

Executables

Document Malware

Website

- Fake security software
- Fake video player codec

Malware - Propagation channels

Executables

Document Malware ★

Website

Image by Websense

Malware - Propagation channels

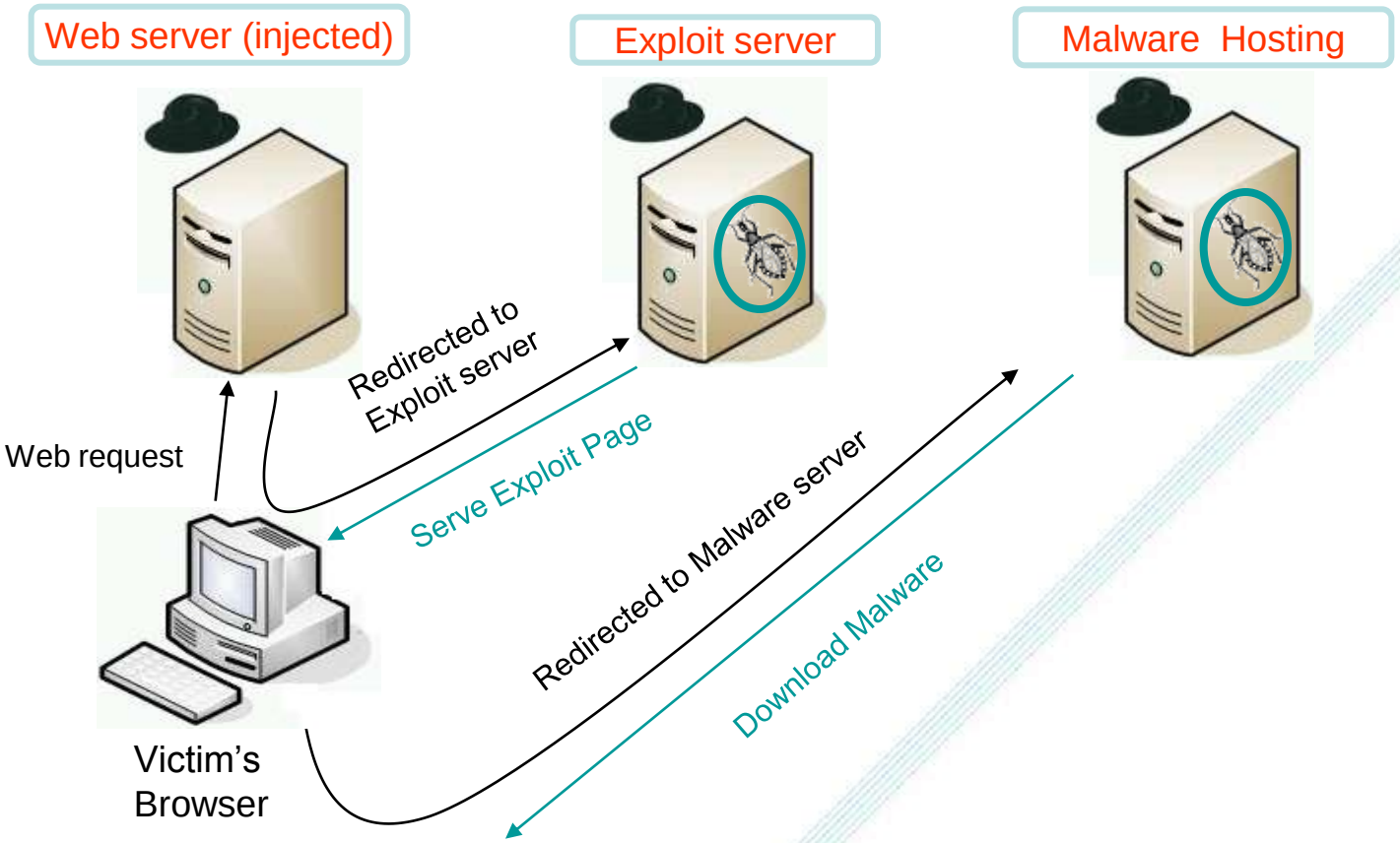
Executables

Document Malware

Website ★★

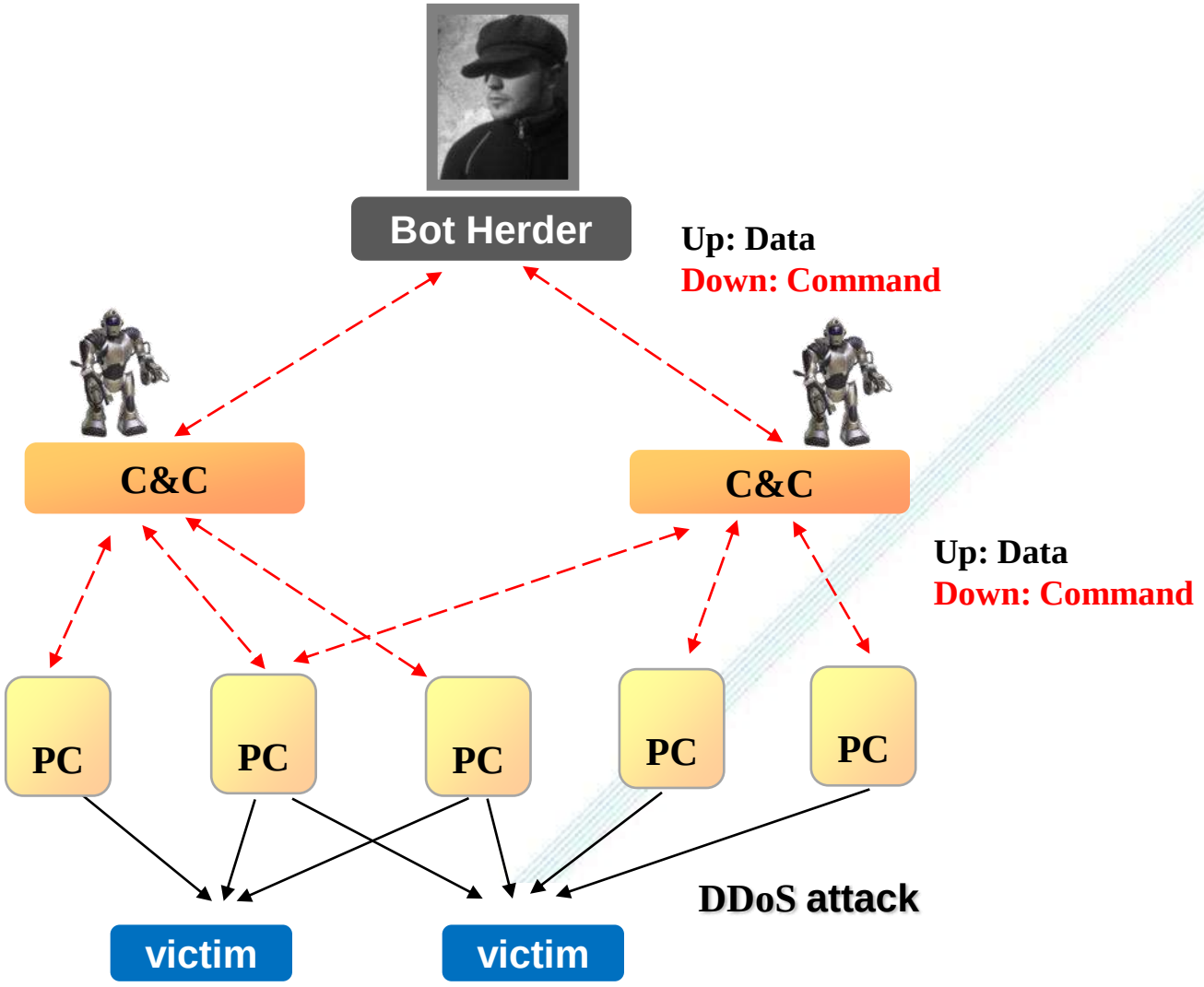
- **Legitimate and trusted websites compromised**
- **Web admin incapable to detect and mitigate the risks**

Attack via Visiting Websites



- Exploits imported from other servers via iframes, redirects
- When compromised, dropper download and install the actual bot malware

Botnet
Hacker's IT Infrastructure



Information Leakage

- Loss of
  - Disks / USB Thumb Drive
  - Mobile Devices
- Leakage on the Internet
  - Search Engine (Google)
  - Wi-Fi
  - Social networking website (Facebook)
  - Peer-to-peer sharing software (Foxy)

Loss of USB thumb drive

Leakage on the Internet (by Foxy)

警隊327份密件網上任睇

進擊之抵價! 立刻訂閱電子報

Recommend 19

警隊爆出歷來最大規模資料外洩事件，涉及屯門警區特別職務隊的機密文件。

警隊爆出最大宗資料外洩事件！多次踢爆警隊洩密的「FOXY天王」再出招，經分享軟件搜獲近三百三十份歷來最多的警隊內部文件，料全數來自屯門警區，部分註明「機密」，不單有多名被捕人士的姓名、身份證號碼、住址及手機號碼，更有八名線人的代號，其中一名線人曾多次向警方提供毒品情報，文件列出其銀行戶口號碼，令人擔憂會間接令其身份曝光置身險境；此外，文件亦披露了警區打擊各類黃賭毒案件的詳細案情及放蛇情節。

22 July 2013

Leakage on the Internet (hacking)

疑黑客入侵電腦 大昌行洩9000客戶資料

緊貼股市實況 Money18即秒報價

Recommend 0

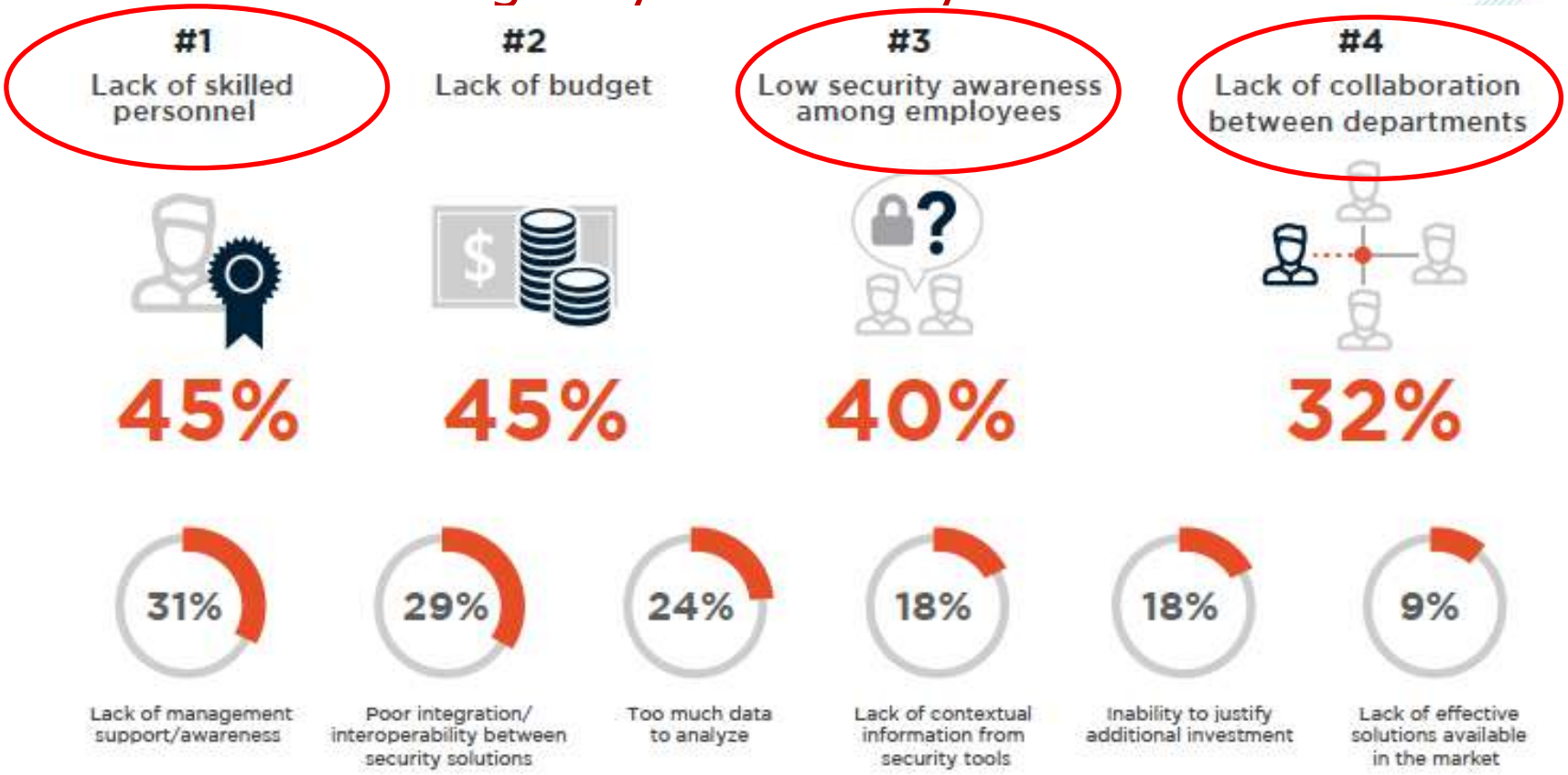
【本報訊】大昌行旗下經營租賃汽車服務的分公司疑洩漏九千客戶資料，有市民利用Google搜尋器時無意中發現，相關客戶的電話、地址等個人資料檔案可任人下載，當中包括養和醫院腫瘤科醫生、港鐵經理及商界高層的資料。大昌行指個人資料私隱專員公署已接觸該公司了解，公司技術部工程師初部了解，懷疑可能是公司網站被黑客入侵，前晚起已暫停網站運作及移除相關資料，截至工程部完成重新編寫網站後才重開。

26 Feb 2014

Best Cyber Security Practices

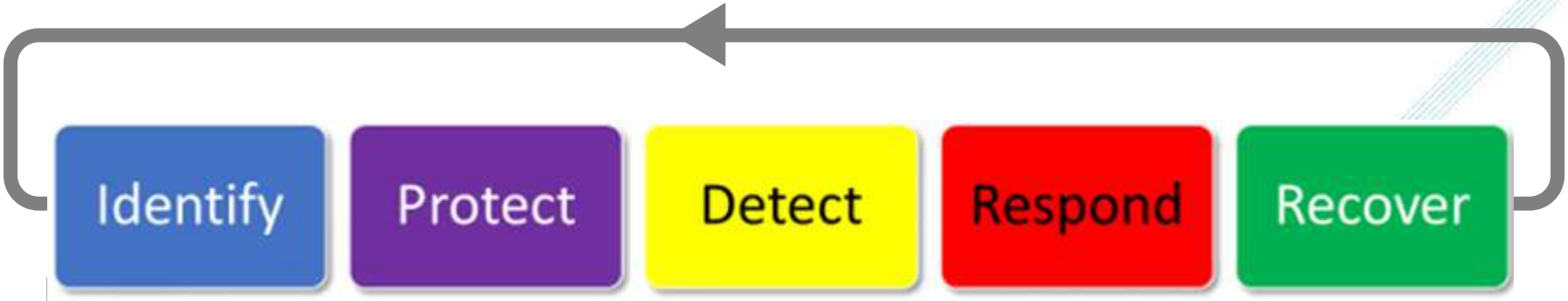
People – Key to Success in Cyber Security

Obstacles to Stronger Cyber Security



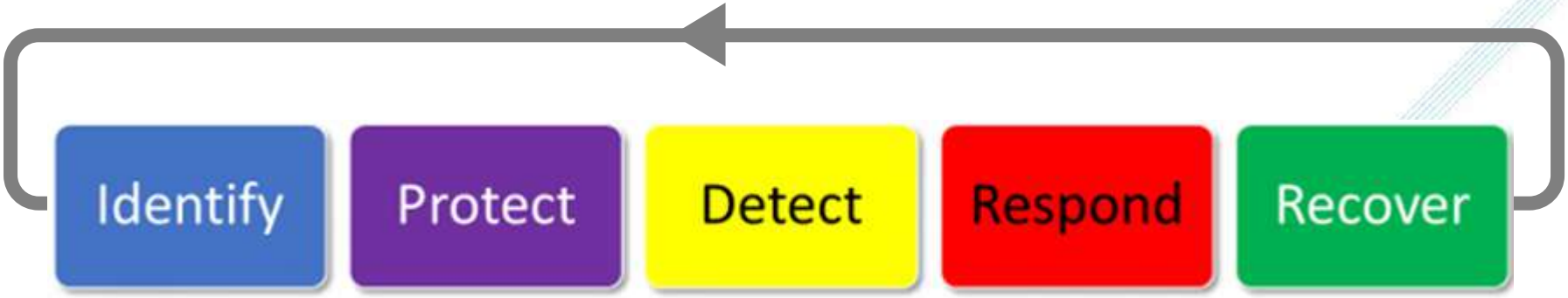
Source: 2017 Cybersecurity Trend Spotlight Report, (ISC)2

Steps to Tackle Cyber Threats



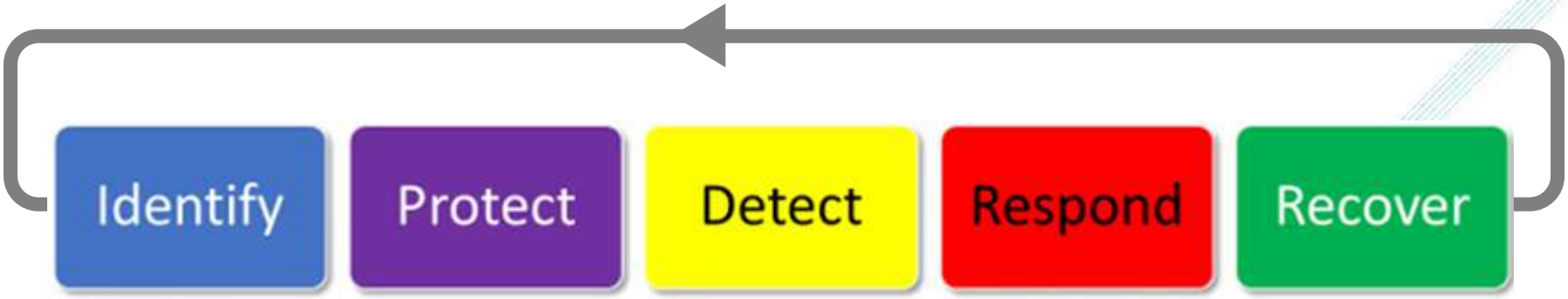
- Critical business data / services
  - Order routing system
  - Surveillance system
- Critical IT services
  - Remote Access
  - Privileged Access
- Data classification
- Risk Assessment

Steps to Tackle Cyber Threats



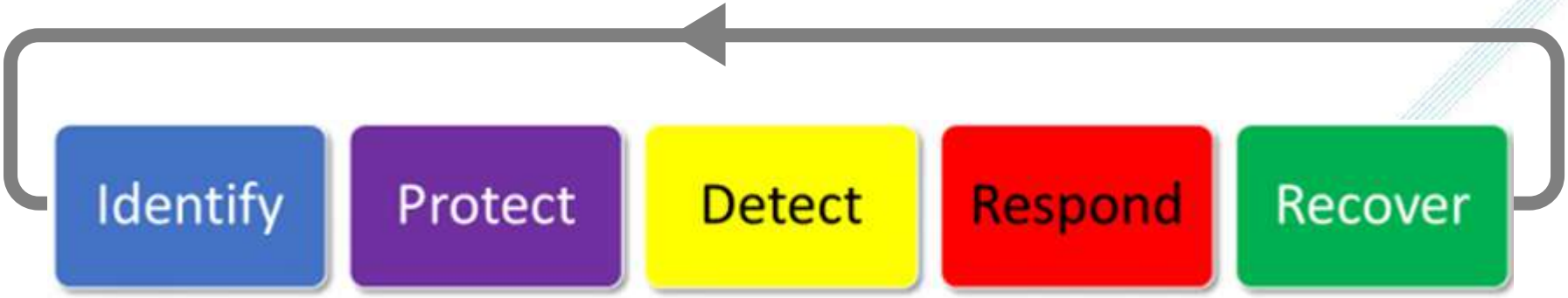
Access Control	• Firewall, Network segmentation • Remote access management • Privileged access management
Protective Technology	• Antivirus, (Client protection) • 2-factor authentication
Data Security	• Backup, Encryption
Info. protection and procedure	• Password policy
Maintenance	• Patch management
Awareness education	• Cyber security training

Steps to Tackle Cyber Threats



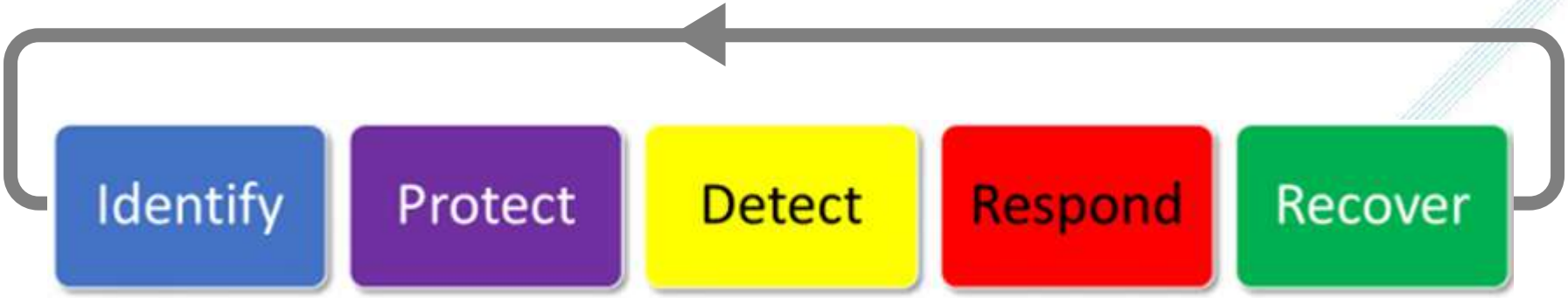
- Intrusion detection
  Suspicious trading location
  Suspicious trading pattern
- Centralized logging
- Security Information Event Management (SIEM)
- Situational awareness, Intelligence

Steps to Tackle Cyber Threats



• Build a Security incident response team & plan
• Contact List • Data breach notification • Account intrusion lockout
• Cyber Drill Exercise

Steps to Tackle Cyber Threats



- Disaster Recovery Plan
- Post-event review and improvement

Takeaway

- IT governance need to address Cyber security issues in order to achieve organization goals
- Senior management buy-in is crucial
- Success of cyber security is about PEOPLE
- General users awareness
- Systematic approach to handle cyber security threats

Q&A

Coming Event: Information Security Summit 15-16 August 2017

https://www.issummit.org

Free to participants

HKCERT Hotline: 81056060

www.hkcert.org