โครงการสัมมนา

เสริมความคิด ติดปีกวิชาชีพ กับคณะพาณิชย์ฯ ธรรมศาสตร์ (ฟรี)

เรื่อง "แนวทางการจัดการความเสี่ยงจากการทุจริต"

วันจันทร์ที่ 10 กันยายน 2561 เวลา 13.15 – 16.30 น.

ณ ห้องประชุมบุญประกอบ หุตะสิงห์

อาคารอเนกประสงค์ 1 ชั้น 3 มหาวิทยาลัยธรรมศาสตร์ ท่าพระจันทร์

จัดโดย ภาควิชาการบัญชี คณะพาณิชยศาสตร์และการบัญชี มหาวิทยาลัยธรรมศาสตร์

ภายใต้การสนับสนุนจากมูลนิธิบุญชู โรจนเสถียร, บริษัท ดีลอยท์ ทู้ช โธมัทสุ ไชยยศ สอบบัญชี จำกัด,
บริษัทสำนักงาน อี วาย จำกัด, บริษัท เคพีเอ็มจี ภูมิไชย สอบบัญชี จำกัด
และ บริษัท ไพร้ซวอเตอร์เฮาส์คูเปอร์ส เอบีเอเอส จำกัด

การบริหารความเสี่ยงการทุจริตอาชญากรรมไซเบอร์

๑๐ กันยายน ๒๕๖๑

สมชาย ศุภธาดา

(เนื้อหาส่วนหนึ่งนำมาจากการนำเสนอของ Chris Keesing หน่วยงานตำรวจกรุงลอนดอน ประเทศอังกฤษ)

Agenda:

- **Cybercrime/ Cybersecurity** สิ่งพึงระวัง
- การบริหารความเสี่ยงจากอาชญากรรมไซเบอร์
- ทีมทำงาน การจัดการเชิงรุก
- ทำอะไรได้บ้าง จะทำอะไรต่อไปดี

เรา อยู่ ใน ยุคดิจิตอล

- *คุณลักษณะของยุคดิจิตอล*
  - เราดำรงชีพทั้งในโลกเสมือนและโลกทางกายภาพ
  - เราหาความรู้ได้แค่ปลายนิ้ว แต่ขาดความสามารถในการคิดอย่างลึกซึ้ง
  - เรายอมแลกความเป็นส่วนตัวกับความสบาย ทำให้ข้อมูลส่วนบุคคลถูกเปิดเผยโจมตีได้โดยง่าย
  - เพื่อให้ยอมรับว่าเป็นสังคมที่พัฒนา เราอาจต้องยอมให้มีการสอดแนมสอดส่องความเคลื่อนไหวของผู้คน

Cybercrime/ Cybersecurity?

อาชญากรรมไซเบอร์

การประกอบอาชญากรรมโดยใช้คอมพิวเตอร์และinternet.

Cybersecurity

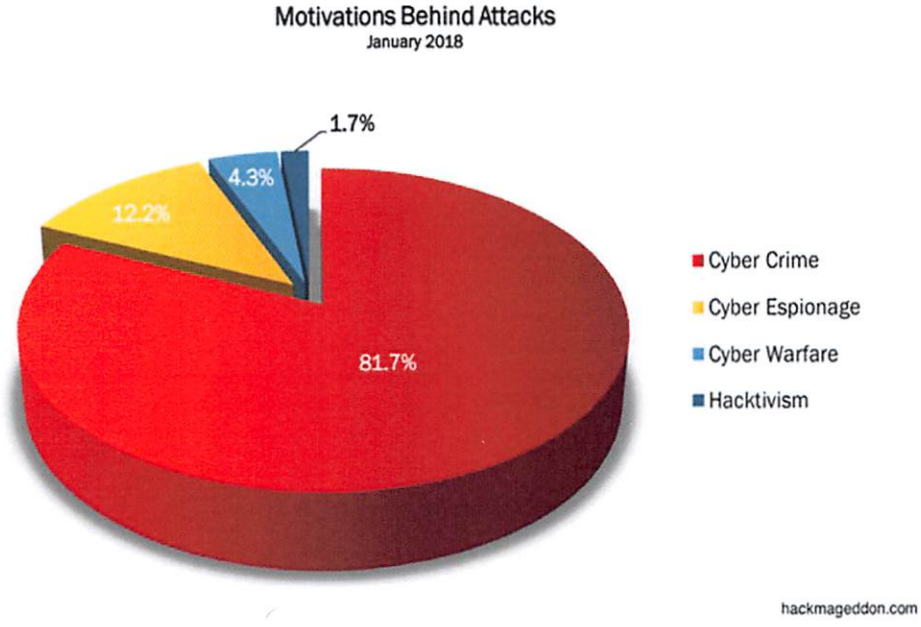
การปกป้องตนเอง องค์กร และลูกค้า ในโลกยุคดิจิตอลผ่านทางผู้คน กระบวนการ และ เทคโนโลยี

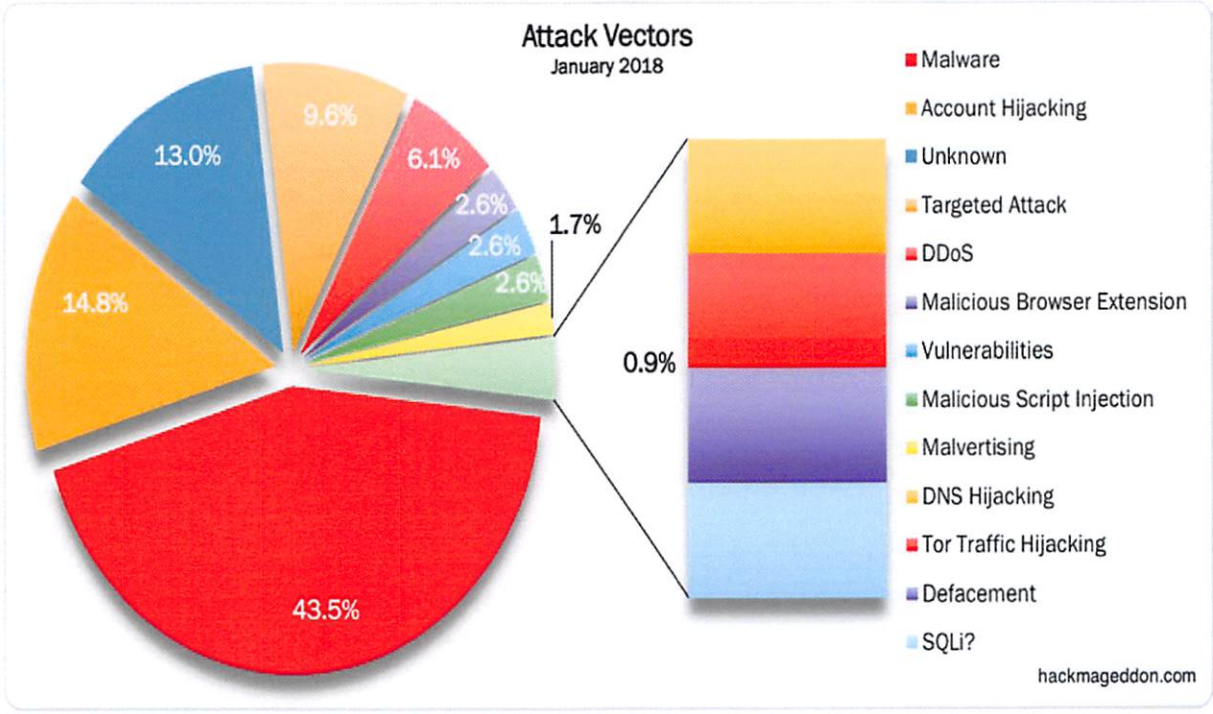
"Computer and Internet Fraud"

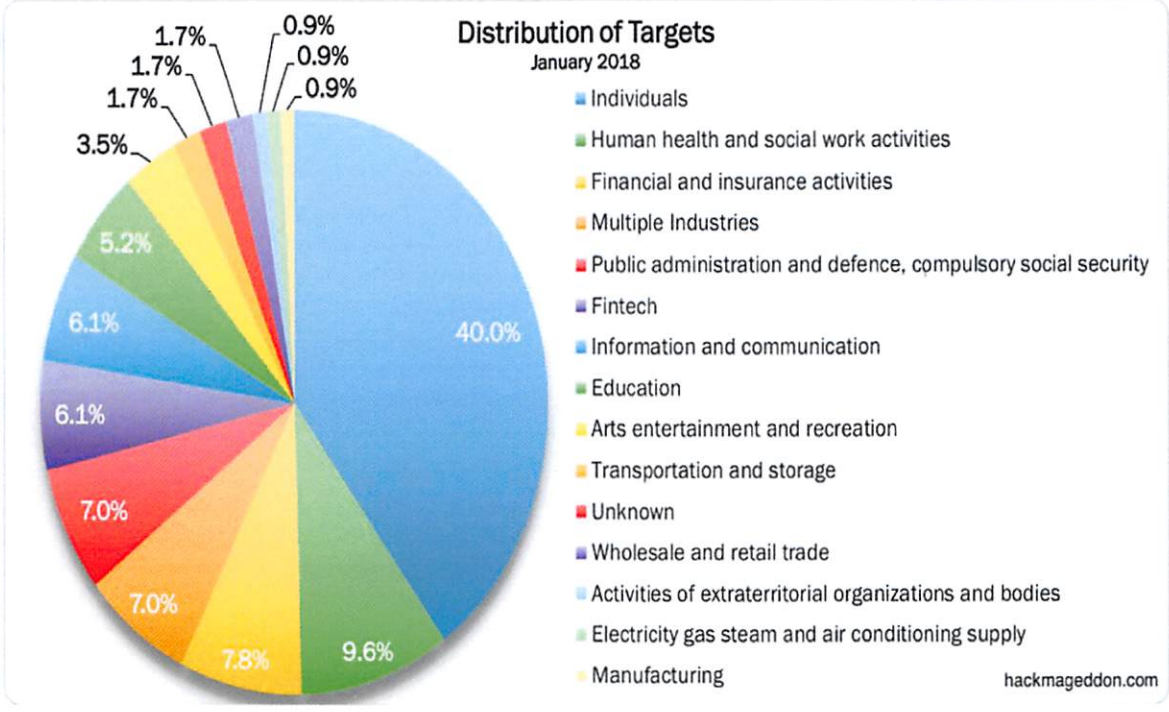
ปัญหาสำหรับนักบัญชีนิติวิทยา

- *ไม่มีร่อยรอยให้ตรวจสอบที่เป็นลักษณะกระดาษ*
- ต้องมีความเข้าใจเทคโนโลยีที่ใช้ในการก่ออาชญากรรม
- *ต้องเข้าใจเทคโนโลยีของคอมพิวเตอร์/เครือข่ายที่เหยื่อใช้*
- จำเป็นต้องมีผู้เชี่ยวชาญมากกว่า 1 แขนงมาช่วยงาน

Motivations Behind Cyber Attacks




Attack Vectors
January 2018
13.0%
9.6%
6.1%
2.6%
2.6%
2.6%
1.7%
14.8%
0.9%
43.5%
Malware
Account Hijacking
Unknown
Targeted Attack
DDoS
Malicious Browser Extension
Vulnerabilities
Malicious Script Injection
Malvertising
DNS Hijacking
Tor Traffic Hijacking
Defacement
SQLi?
hackmageddon.com


Distribution of Targets
January 2018
1.7%
0.9%
1.7%
0.9%
1.7%
0.9%
3.5%
5.2%
6.1%
40.0%
6.1%
7.0%
7.0%
7.8%
9.6%
Individuals
Human health and social work activities
Financial and insurance activities
Multiple Industries
Public administration and defence, compulsory social security
Fintech
Information and communication
Education
Arts entertainment and recreation
Transportation and storage
Unknown
Wholesale and retail trade
Activities of extraterritorial organizations and bodies
Electricity gas steam and air conditioning supply
Manufacturing
hackmageddon.com

ประเภทของ Cybercrime

- PBX/dial-through fraud
- Phishing
- Ransomware - 'Locky'
- Hacking
- Denial of service attacks – DoS DDoS
- Social engineering
- Insider risk

What is PBX/dial-through fraud?

- PBX (Private Branch Exchanges) are systems which enable organisations improved communication
- PBX/dial-through fraud occurs when hackers target PBX's from the outside and use them to make a high volume of calls to premium rate or overseas numbers.
- Since the end of June 2013 there have been nearly 500 Action Fraud reports relating to this - costing victims over £6m.

What is Phishing?

- It's a con !
- Using email or websites with malicious code in links or attachments that can install malware into your system.
- Often very convincing emails.
- Or telephone calls from IT service desk asking for passwords or to click on a link or attachment.
- Examples in everyday life are banking scams.

"The spear phisher thrives on familiarity. He knows your name, your email address, and at least a little about you."

What is 'Locky' Ransomware

- "Locky" is the nickname of a new strain of ransomware, so-called because it renames all your important files so that they have the extension .locky.
- It doesn't just rename your files, it scrambles them first.
- Only the crooks have the decryption key which can be brought from the crooks over the dark web using bitcoin (BTC).
- Prices seen vary from BTC 0.5 to BTC 1.00 (BTC is short for "bitcoin," where one bitcoin is currently worth about £295).

What is Hacking?

- A hacker is someone who seeks and exploits weaknesses in a computer system or computer network.
- Hackers may be motivated by a multitude of reasons - profit, protest, challenge, enjoyment, identify weaknesses.
- There are different types of hackers:

  - White Hat Hacker

  - Black Hat Hacker

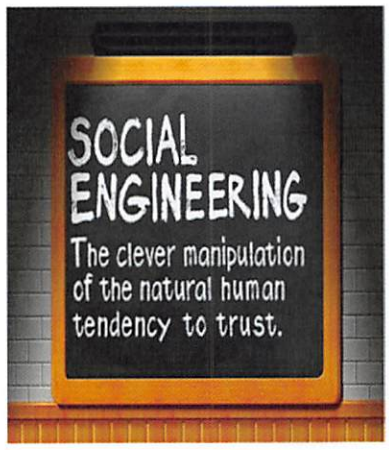
  - Grey Hat Hacker

What are Denial of Service attacks?

- Also known as Dos or DDos attacks.
- Exploit emails, information access requests and network timings to interrupt or shutdown an entire IT system - for example sending multiple emails or flooding a website with useless traffic so the system can no longer cope.
- Aim is to cause disruption to legitimate business or to expose vulnerabilities.

What is social engineering?

- A social engineer runs what used to be called a "con game."
- Many social engineering exploits simply rely on people's willingness to be helpful and they are therefore tricked into breaking normal security procedures.
- For example, the attacker might pretend to be a co-worker who has some kind of urgent problem that requires access to additional network resources.



What is insider risk?

- The person sitting next to you....
- Often regarded as the highest risk for data loss.
- Sensitive information is lost when someone makes a genuine mistake such as sending an email with a confidential attachment to the wrong addressee.
- Motivation can be financial, personal or political .
- Stolen data can be used for fraudulent purposes and criminal gain when in the wrong hands.

- คุณมีข้อมูลอะไรบ้าง มีใครอยากได้ข้อมูลนี้ไหม
- ถ้าข้อมูลตกไปในมืออาชญากร เขาจะนำไปใช้ประโยชน์อะไร ดูแรงจูงใจ
- ผลเสียหายอะไรที่จะตามมา ชื่อเสียง เงินทอง ฯลฯ
- มีการจัดตั้งทีมงานต่อต้านการทุจริตในองค์กรหรือยัง
- ดูแลตรวจตราสอดส่องข้อมูลและสารสนเทศเป็นประจำวันหรือไม่
- การแชร์ข้อมูลระหว่าง หน่วยตรวจสอบภายใน ผู้สอบบัญชี หน่วยงานกำกับดูแล (ความสัมพันธ์ระหว่างกันดีไหม)

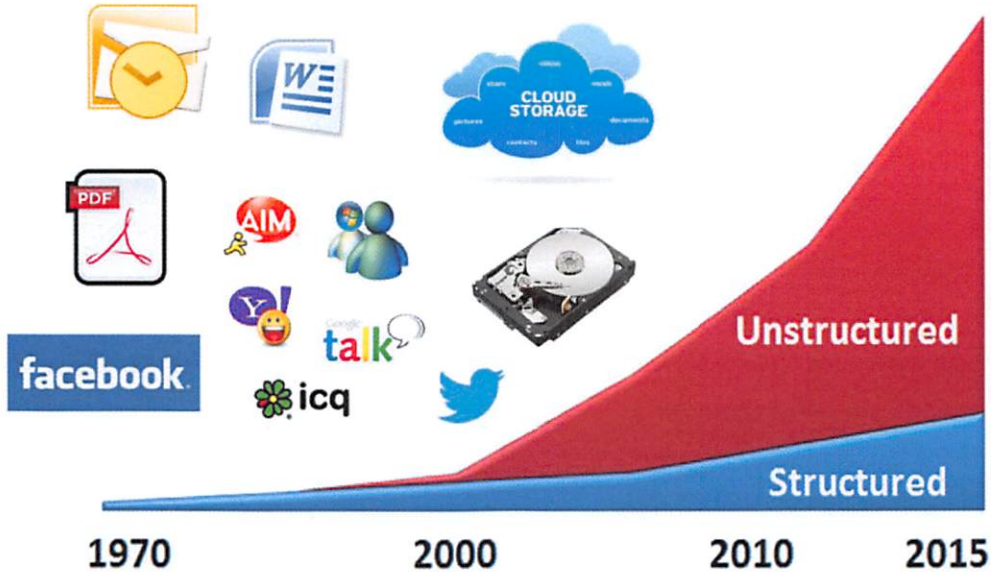
ต้องทำอะไรบ้างเพื่อการบริหารความเสี่ยง

- ให้รวม **cyber fraud risk** ไว้ในแผนการต่อต้านการทุจริตเชิงรุก
- รายงานและปรึกษาหารือ กับ คณะกรรมการตรวจสอบ คณะกรรมการบริหารความเสี่ยง
- ทำงานร่วมกับผู้ตรวจสอบ **IT** อาวุโส
- ปฏิสัมพันธ์กับ เพื่อนร่วมงานด้าน **IT** และ ผู้ดูแลความปลอดภัยทาง **IT**
- ทบทวนกลยุทธ์ จุดยืนในการดูแล **Cyber security**
- **Information Security Policy and Procedure.**
- **Information Security training – Responsible for Information.**

ต้องทำอะไรบ้างเพื่อการบริหารความเสี่ยง

- สอบทานผลจากการทดสอบการบุกรุกระบบ **IT**
- พิจารณากำหนดแผนและนโยบายสำหรับการตรวจสอบภายใน
- สอบทานแนวทางการบริหารตาม **ISO 27001**
- ร่วมมือกับ ทีม **IT Information security** เพื่อกำหนด **roadmap** เชิงรุกในการติดตามและปรับแก้ระบบ **IT** อย่างต่อเนื่อง
- ทำความเข้าใจ **BIG DATA , DATA ANALYTICS,** เทคนิคการขุดเหมืองข้อมูล **(data mining)**

Growth of Unstructured Data



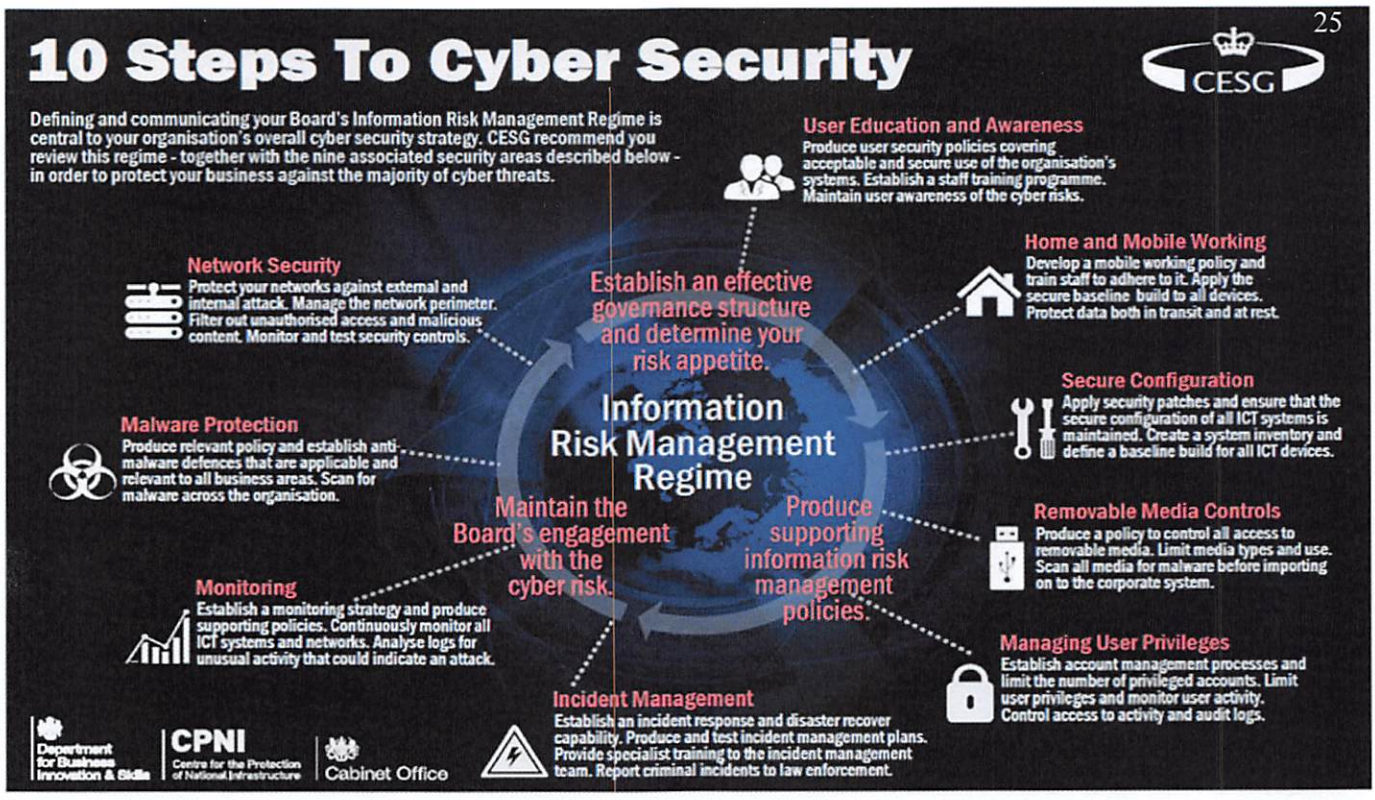
- เนื่องจากสารสนเทศทางการเงินปัจจุบันมีมากมายมหาศาล โดยเฉพาะอย่างยิ่งการฟอกเงินและการฉ้อฉล จึงจำเป็นอย่างยิ่งที่กลยุทธ์ของสถาบันการเงินสมัยใหม่ต้องพึ่งพิง **Data Mining and Digital Forensic** เข้ามาช่วยในการปฏิบัติงาน

Financial Crime : The 'Crack Team'

10 Steps To Cyber Security

CESG

Defining and communicating your Board's Information Risk Management Regime is central to your organisation's overall cyber security strategy. CESG recommend you review this regime - together with the nine associated security areas described below - in order to protect your business against the majority of cyber threats.



User Education and Awareness

Produce user security policies covering acceptable and secure use of the organisation's systems. Establish a staff training programme. Maintain user awareness of the cyber risks.

Network Security

Protect your networks against external and internal attack. Manage the network perimeter. Filter out unauthorised access and malicious content. Monitor and test security controls.

Home and Mobile Working

Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline build to all devices. Protect data both in transit and at rest.

Secure Configuration

Apply security patches and ensure that the secure configuration of all ICT systems is maintained. Create a system inventory and define a baseline build for all ICT devices.

Malware Protection

Produce relevant policy and establish anti-malware defences that are applicable and relevant to all business areas. Scan for malware across the organisation.

Removable Media Controls

Produce a policy to control all access to removable media. Limit media types and use. Scan all media for malware before importing on to the corporate system.

Monitoring

Establish a monitoring strategy and produce supporting policies. Continuously monitor all ICT systems and networks. Analyse logs for unusual activity that could indicate an attack.

Managing User Privileges

Establish account management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs.

Incident Management

Establish an incident response and disaster recover capability. Produce and test incident management plans. Provide specialist training to the incident management team. Report criminal incidents to law enforcement.

Department for Business Innovation & Skills | CPNI Centre for the Protection of National Infrastructure | Cabinet Office