2017 TRANSFORMATION SUMMIT

FitchLearning

Cybercrime:
Is it a Serious Threat to
the IT-BPM Industry?

Prepared by
Christopher J Pennington
Chartered MCSI
May 2017

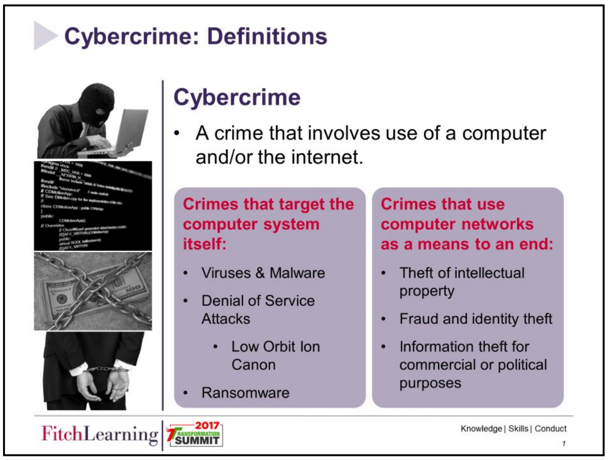
Knowledge | Skills | Conduct

Cybercrime: Is it a Serious Threat to the IT-BPM Industry?

Cybercrime has evolved as different markets and client sectors evolve, and as we all continue embrace new technologies. Yet do we truly understand this new risk? Is our lack of knowledge a reason why so many risk professionals globally now speak in hushed voices about it being when, not if cybercrime will bring down an institution? These are some of the questions that Chris Pennington *Chartered MCSI*, one of Fitch Learning's Senior Trainers will seek to explore with the audience.

As Chris explores the threat that cybercrime represents to both IT-BPM's and their clients with the audience, he will share his own views some of the things that IT-BPM's can do to help in the never-ending battle with Cybercrime and the important of education.

In the Philippines, the media reports that there's a dearth of IT experts on cybersecurity. Professionals are being lured to other Asian countries for more lucrative job opportunities. There are limited options for the development of the profession. CEdFIT is partnering with the Chartered Institute for Securities & Investment (CISI) and Fitch Learning to offer the globally-recognized Investment Operations Certificate (IOC). For any IT BPO company, in particular for those involved in financial services the IOC will enhance knowledge, understanding and credibility with a global clientele.



Cybercrime: Definitions

Cybercrime

- A crime that involves use of a computer and/or the internet.

Crimes that target the computer system itself:

- Viruses & Malware
- Denial of Service Attacks
  - Low Orbit Ion Canon
- Ransomware

Crimes that use computer networks as a means to an end:

- Theft of intellectual property
- Fraud and identity theft
- Information theft for commercial or political purposes

FitchLearning | 2017 TRANSFORMATION SUMMIT

Knowledge | Skills | Conduct

1

Cybercrime:

A crime that involves use of a computer and/or the internet. The object of cybercrime may be to misappropriate assets or confidential information or to deny the use of a computer system or network via the use of malicious software.

Cyber-dependent crimes can only be committed using computers, computer networks or other forms of information communication technology (ICT). They include the creation and spread of malware for financial gain, hacking to steal sensitive personal or industry data and denial of service attacks to cause reputational damage.

Cyber-enabled crimes, such as fraud, the purchasing of illegal drugs and child sexual exploitation, can be conducted on or offline, but online may take place at unprecedented scale and speed.

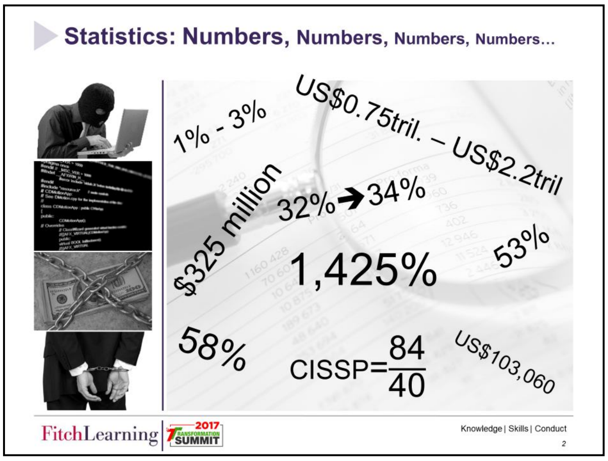
Over the last few years, cyber economic crime has evolved to a point where one could segment it into two distinct categories – the kind that steal money and bruise reputations; and the kind that steal IP and lays waste to an entire business.

Low Orbit Ion Canon:

Used by ordinary people, not your typical ‘cyber-criminal’

Randsomware:

Scary!



Statistics: Numbers, Numbers, Numbers, Numbers…

1% - 3%

US$0.75tril. – US$2.2tril

$325 million

32%➔34%

1,425%

53%

58%

CISSP=$\frac{84}{40}$

US$103,060

FitchLearning | 2017 Transformation Summit

Knowledge | Skills | Conduct

2

Statistics & Numbers:

1% to 3% of global GDP lost to cybercrime

US$0.75tril – US$2.2tril. GDP in US$ terms

(various sources)

53%: The UK Govt. (ONS) estimated that there were 2.46 million cyber incidents and 2.11 million victims of cyber crime in the UK in 2015 (53% of all crimes in UK)

32% of organisations affected*...and 34%* think they will be affected in the next two years

22% of respondents experienced losses of between $100,000 and $1 million, 14% of respondents suffered losses of more than $1 million, and 1% of respondents reported losses in excess of $100 million.

PwC Crime Survey 2016 (based on 6,000+ Organisations Globally)

One particular strain of Cryptowall ransomware was estimated to have cost victims over $325 million in 2015

Cyber Threat Alliance

1,425%: ROI on a simple Randsomware programme that cost $5,900 and generated $81,400

April 2016: “84 Certified Information Systems Security Professionals (CISSP) who are Filipinos. Out of this number, 40 are working overseas.”

Jan 2017: 94 (Malaysia: 283, Indonesia: 108, Singapore: 1,508)

http://www.philstar.com/banking/2016/04/12/1571843/lack-it-security-professionals-makes-philippines-prone-cyber-crime

US$103,060: what on average CISSP qualified professional is paid outside USA

58% of Philippine respondent to PWC Global Economic Crime survey do not believe the authorities are adequately trained/resourced. Rank 4th in a list you don’t want to top (Kenya at 79%)

Cybercrime

ELIMINATION

FitchLearning | 2017 Transformation Summit

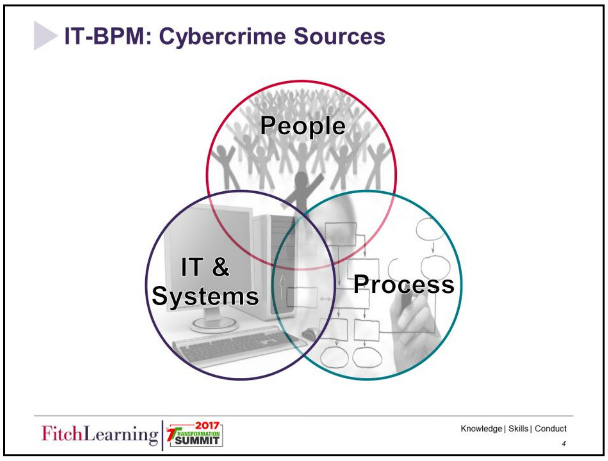
Knowledge | Skills | Conduct

3

Turn everything off – the ultimate DOS?

Isn’t going to happen!

It can not be eliminated.



IT-BPM: Cybercrime Sources

People

IT & Systems

Process

Knowledge | Skills | Conduct

4

IT-BPM: The paradox – technology enables and is a threat!

Vulnerability

Can be technical (eg, lack of a firewall) or human (eg, employees being tricked by phishing e-mails)

Malware: Any software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems

Virus: A form of malware which when executed, replicates itself and inserts copies into other software

DDoS Attacks T

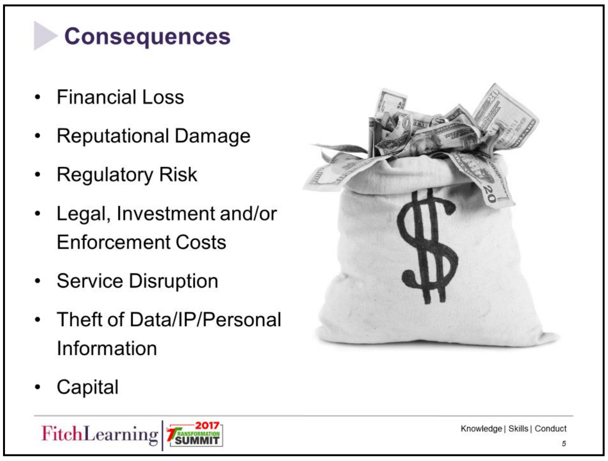
Trojans/Malware – placing malicious software on a customers computer

“Phishing” – sending fake email request to customers to obtain bank details or to get into system… Antwerp Port!

Theft of Information

Due to the intensity of compliance and regulations, the costs per breach to organizations in the health care and financial services sectors top all other industry groups, according to the Ponemon study.

41% of financial services respondents ranked assessment of security protocols and standards of third-party vendors as the top challenge to information security efforts. To address this issue, 41% said they will boost spending on monitoring and testing of third-party partner security (e.g.IT-BPM)



Consequences

- Financial Loss
- Reputational Damage
- Regulatory Risk
- Legal, Investment and/or Enforcement Costs
- Service Disruption
- Theft of Data/IP/Personal Information
- Capital

FitchLearning | 2017 TRANSFORMATION SUMMIT

Knowledge | Skills | Conduct

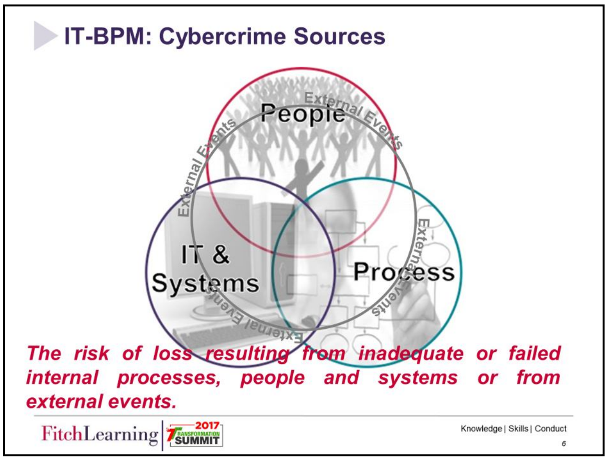
5

Stating the obvious, everything is money; directly or indirectly.

But how many people actually think about capital?

If 1%-3% of GDP is lost to cybercrime should you be making a provision of 1% to 3% in your accounts or at least a contingent liability?

ORX Operational Risk Report (a serious document for anyone involved in Operational Risk with Finance/Insurance industry) state that banks loss $3.47 of gross revenue to operational risk, and cybercrime is classed as an operational risk!



IT-BPM: Cybercrime Sources

The risk of loss resulting from inadequate or failed internal processes, people and systems or from external events.

FitchLearning | 2017 TRANSFORMATION SUMMIT

Knowledge | Skills | Conduct

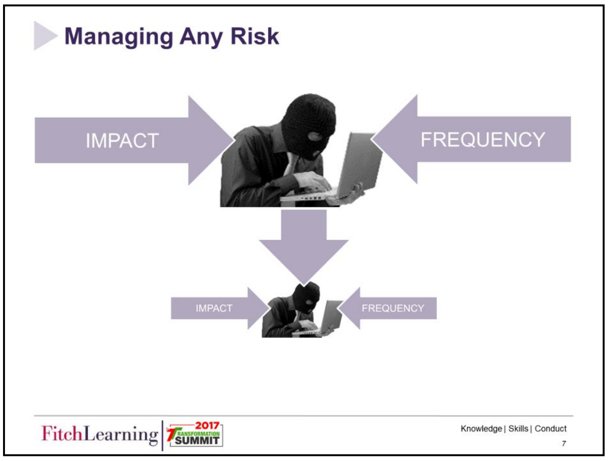
6

“…we must remember that cyber crime, cyber terrorism, cyber espionage, or cyber war are simply crime, terrorism, espionage or war by other means. Cyberspace adds a new dimension, but its use in warfare should be subject to the same strategic and tactical thought as existing means.”

Nick Harvey, Former UK armed forces minister (from 2010 to 2012)

Cybercrime is a type of operational risk!

If we can deal with operational risk, then we should be able to deal with cyber crime.



Managing Any Risk

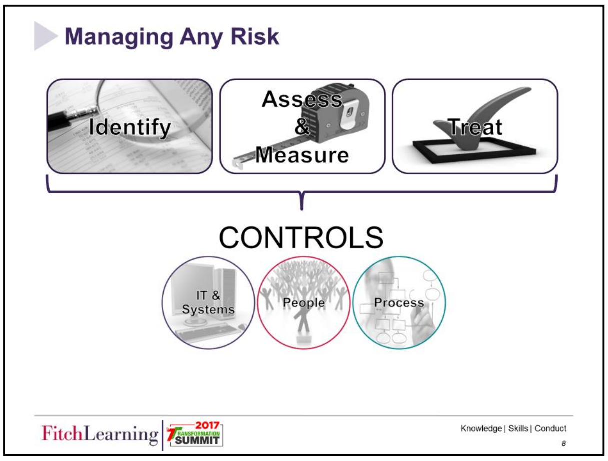
FitchLearning | 2017 TRANSFORMATION SUMMIT

Knowledge | Skills | Conduct

7

Cant beat!

Reduce Impact & Frequency



Managing Any Risk

Identify

Assess & Measure

Treat

CONTROLS

IT & Systems

People

Process

FitchLearning | 2017 TRANSFORMATION SUMMIT

Knowledge | Skills | Conduct

8

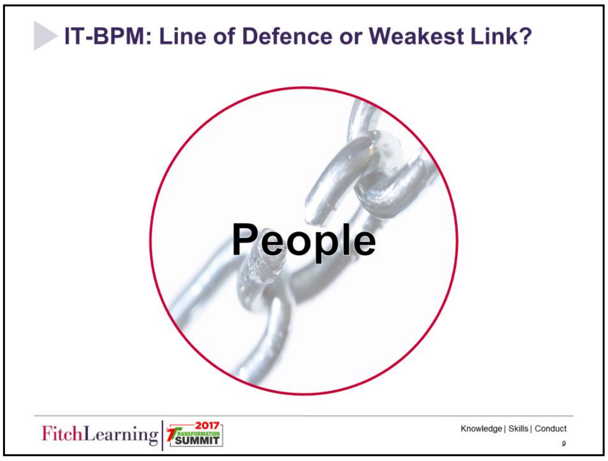
Controls: Physical controls, firewalls, anti-virus software, system scans

1. identify the assets— normally, the data and systems—that could be at risk from a cyberattack
2. conduct a risk assessment to gauge the impact and likelihood of attacks on each asset. The organization should estimate both financial and reputational impact using a relative scale
3. categorize assets according to value at risk. Often two categories will suffice: lower value-at-risk assets (such as informational Web sites), which existing best practice should cover, and higher value-at-risk assets (such as vital systems), which require additional measures.

Technology. Technology must be used to maximum advantage to counter cyberattacks. The organization must have the level of technical capabilities required and should prioritize technical spending in the areas of highest risk. Basic security best practices should be embedded within the architecture (for example, limiting administrator rights or conducting simulations of cyberattacks to test resilience).

Process and procedure. Procedures must be established to limit and mitigate the impact of attacks. Responsibility in this area includes ensuring that information about attacks is available to leaders within the business (for example, predictive threat analysis based on aggregating and analyzing e-mail headers) and that data assets are suitably categorized (for example, working with business owners to determine appropriate encryption levels).

People. Personnel policies must be in place to minimize risk. This includes providing training to support the policy and regularly testing compliance.



IT-BPM: Line of Defence or Weakest Link?

People

FitchLearning 2017 TRANSFORMATION SUMMIT

Knowledge | Skills | Conduct

9

Human Weakest Link

Moore’s Law (Computer Power x2 v User Linear)

Non-Malicious/Unintentional:

Poor induction/training/recruitment – your own fault!

Non-Malicious /Intentional:

Policies not fit for purpose; follow the process, but… your own fault!

Malicious/Intentional:

Exploit weakness

Work outsiders

Personal motivation (gambling debts!)

(The triangle)

Raise awareness, not just the what, but the why – if people understand wider consequences.

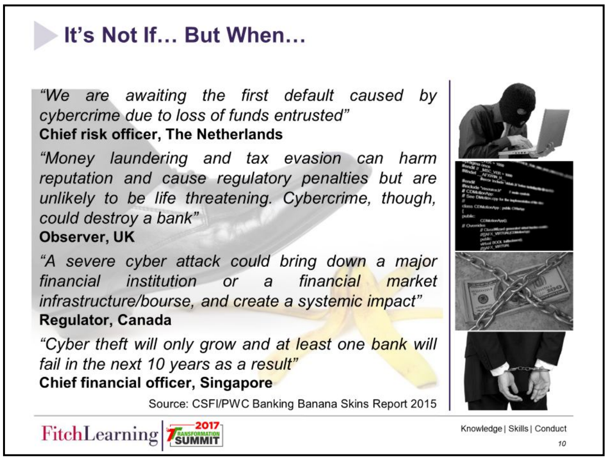
Turning PCs off (Fitch policy at least weekly)

USBs

Access to yahoo/gmail etc

BYOD

Training/qualifications/champions



It’s Not If… But When…

“We are awaiting the first default caused by cybercrime due to loss of funds entrusted”
Chief risk officer, The Netherlands

“Money laundering and tax evasion can harm reputation and cause regulatory penalties but are unlikely to be life threatening. Cybercrime, though, could destroy a bank”
Observer, UK

“A severe cyber attack could bring down a major financial institution or a financial market infrastructure/bourse, and create a systemic impact”
Regulator, Canada

“Cyber theft will only grow and at least one bank will fail in the next 10 years as a result”
Chief financial officer, Singapore

Source: CSFI/PWC Banking Banana Skins Report 2015

Expect
Us...