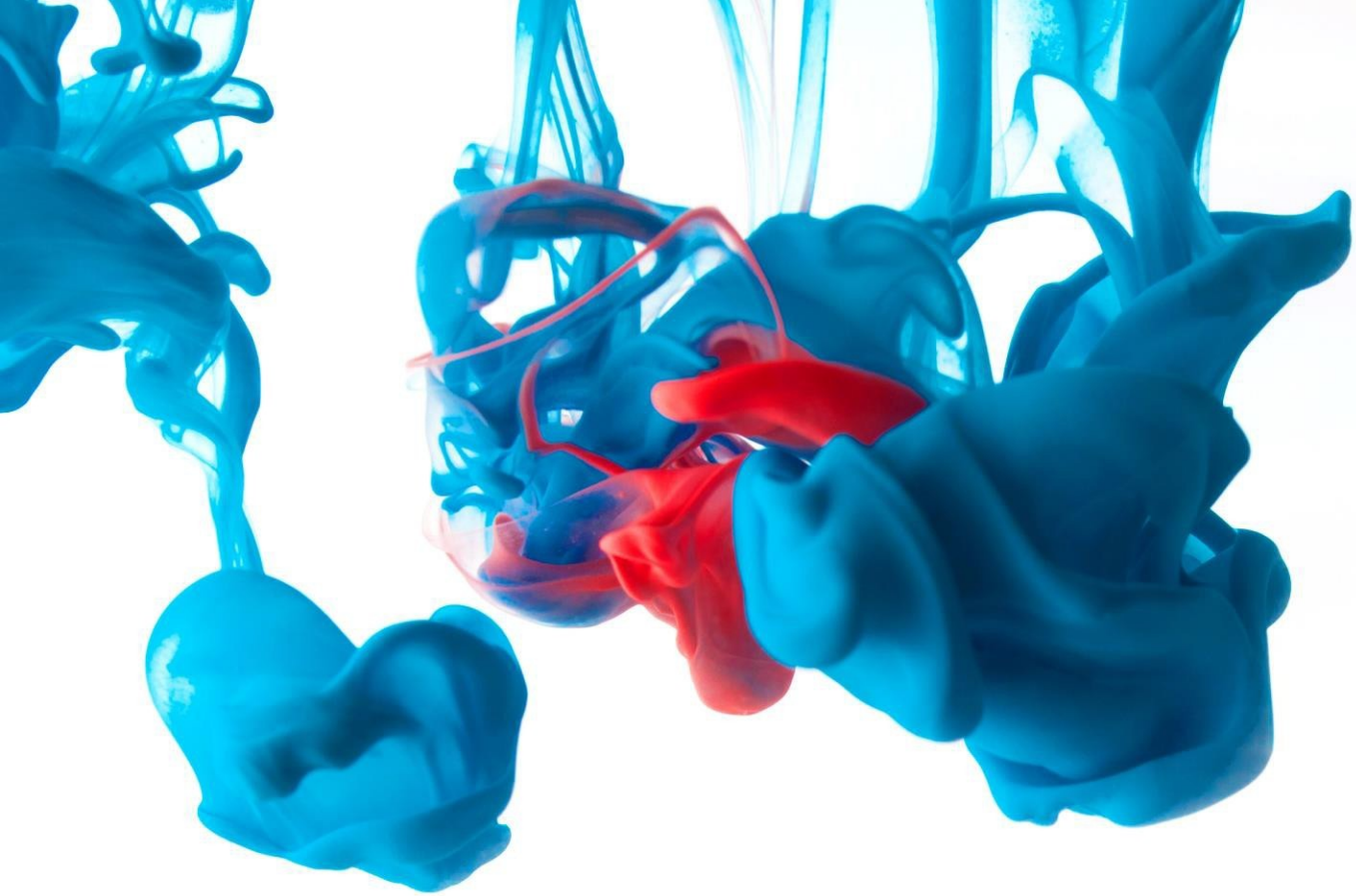


Dealing with Information Security, Risk Management & Cyber Resilience

ptl®

TODAY FOR TOMORROW

Introductions

- >19 years working in all areas of IT
- Former Associate Director, KPMG
- Former Lead Security Analyst & Architect for American-based CCBill
- Lecturer on Information Security & Computer Forensics, NCC
- >6 years PCI-DSS industry
- Information Security, Software Engineering, IT & Telecoms Law

ptl

Brief Agenda

[Information Security]

1. Why the need to think about it?
2. What exactly are we talking about?
3. How do we go about doing something about it?
4. Is there a one-size-fits-all framework?

ptl

Information Security?

[Information Security] is the preservation of confidentiality, integrity and availability of information.

But how do you *really* go about it within your business?

- After an incident occurs?
- If budget permits?
- Because you are mandated to comply?
- Who possesses the knowledge within your company to advise?
- Is it even a priority or a concern?
- Is there any structure to your approach?
- Are you really prepared / in control?

IT Governance..1/3

- IT is aligned with the business
- IT enables the business and maximizes benefits
- IT resources are used responsibly
- IT risks are managed appropriately

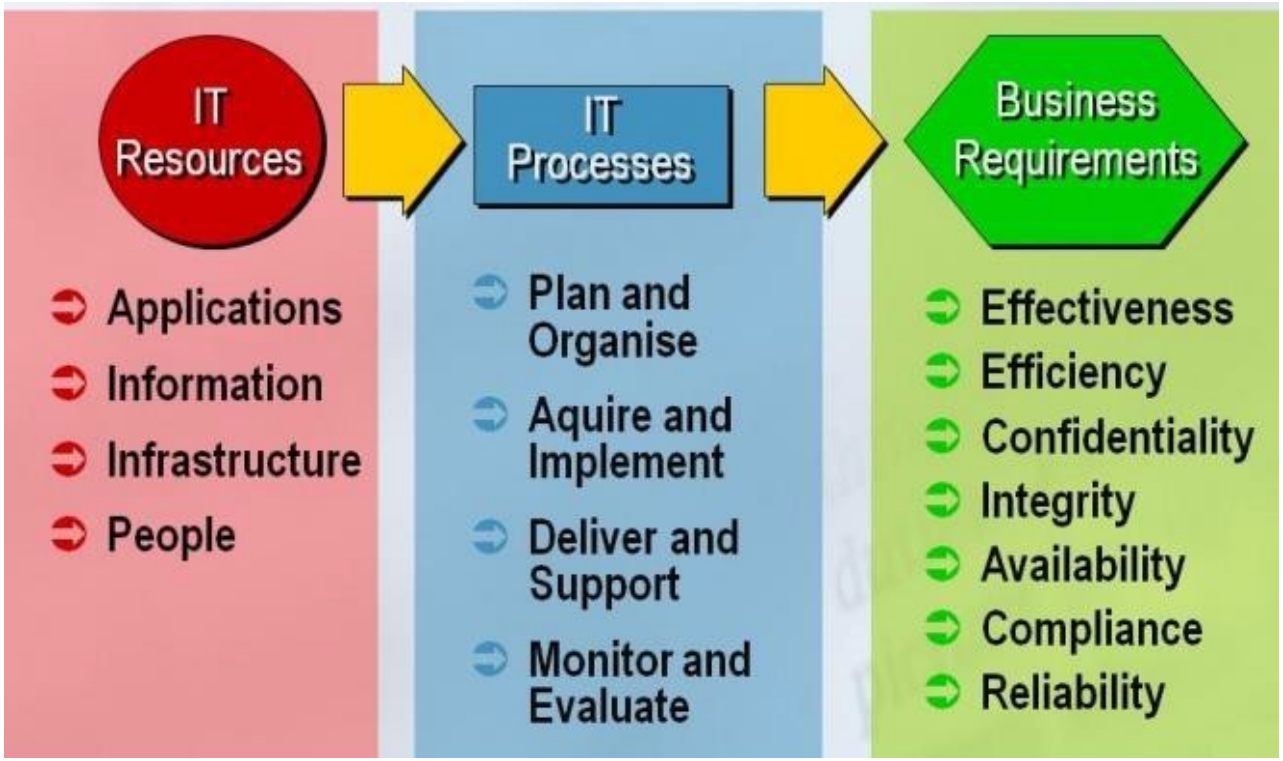
[COBIT (4.1) Framework]

COBIT
GOVERNANCE, CONTROL *and* ASSURANCE *for* INFORMATION *and* RELATED TECHNOLOGY

Source: http://www.isaca.org/Knowledge-Center/cobit/Documents/COBIT4.pdf

ptl

IT Governance..2/3



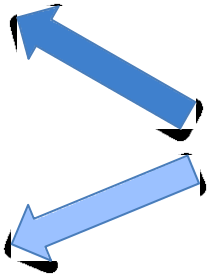
COBIT
GOVERNANCE, CONTROL *and* ASSURANCE *for* INFORMATION *and* RELATED TECHNOLOGY

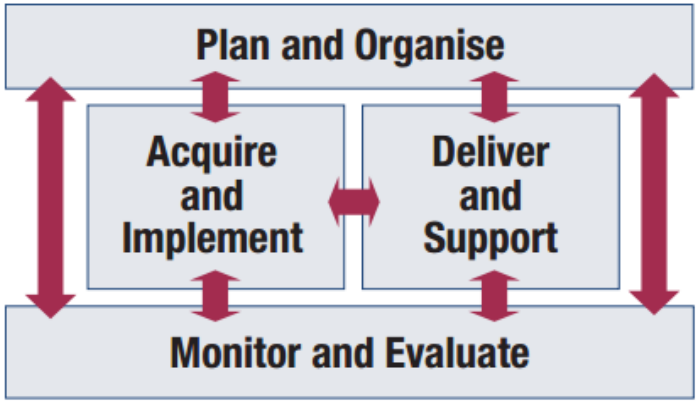
Source: http://www.isaca.org/Knowledge-Center/cobit/Documents/COBIT4.pdf

ptl

IT Governance..3/3

- Periodic assessments of IT processes for their quality and compliance
- Performance management
- Monitoring internal controls
- Regulatory compliance
- Provide IT governance





- Is IT's performance measured to detect problems before it is too late?
- Are internal controls effective and efficient?
- Are adequate confidentiality, integrity and availability controls in place for information Security?

COBIT
GOVERNANCE, CONTROL *and* ASSURANCE *for* INFORMATION *and* RELATED TECHNOLOGY

Source: http://www.isaca.org/Knowledge-Center/cobit/Documents/COBIT4.pdf

ptl

Incidents


Monday, March 30, 2009 by Kurt Sansone

Malta victim of international cyber spy network

Canadian researchers have uncovered an electronic spy network based in China which has infiltrated


Wednesday, May 22, 2013, 17:28

timesofmalta.com service returning to normal

The possible cyber-attack on the timesofmalta.com's servers yesterday evening has been reported to the Police Cyber Crimes Unit for investigation.

A company spokeswoman said:

"Our site and servers were never touched and our security was not breached. No data has been compro ised. We suffered what is referred to as a distri security prot nd due to

TIMESOF MALTA.COM


EDITION: INTERNATIONAL | U.S. | MÉXICO | ARABIC

Set edition preference

CNN

Home Video World U.S. Africa Asia Europe Latin America Middle East Business

Part of complete coverage on Digital Biz

digitalbiz

Sony: Hacker stole PlayStation users' personal info

By Mark Milian, CNN

April 27, 2011 -- Updated 1558 GMT (2358 HKT) | Filed under: Gaming & Gadgets


techradar pro

IT INSIGHTS FOR BUSINESS

HOME NEWS REVIEWS INSIGHTS NETWORKS AND SERVERS SECURITY

BUSINESS LAPTOPS/PC PRINTERS HARDWARE SOFTWARE MOBILE WORKING

TechRadar Pro › News › Dropbox confirms it was hacked, assures it's safe

Dropbox confirms it was hacked, assures it's safe

Some account names and passwords were stolen from the file transferring company


BBC News Sport Weather Travel Culture Autos

NEWS TECHNOLOGY

Home UK Africa Asia Europe Latin America Mid-East US & Canada Business Health Sci/Environ

7 June 2011 Last updated at 13:33 GMT

Share

Security firm RSA offers to replace SecurID tokens

Security firm RSA has offered to replace the SecurID tokens used by its customers to log into company systems and banks.

It follows a hack against the company in March where information related to the tokens was stolen.

RSA has now revealed that some of that information was used during the hack attack on

The targets?

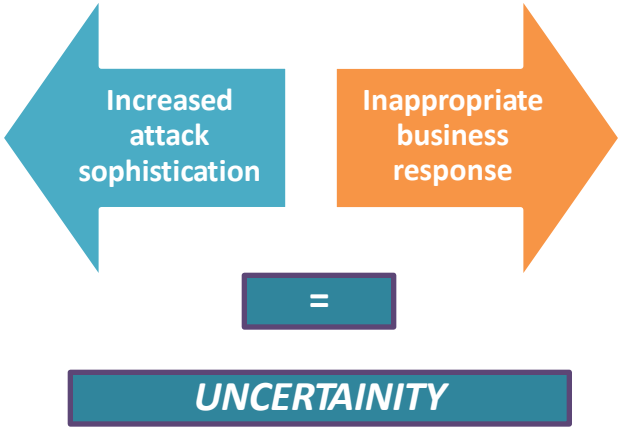
NEW YORK (CNNMoney)

Cybercriminals have picked their easiest prey: Small businesses.

A data breach investigations report from Verizon (VZ, Fortune 500), to be released Tuesday, will show that small businesses continue to be the most victimized of all companies.

The high level takeaways:

- 37 percent of breaches hit financial organizations;
- 24 percent of breaches happened in retail and restaurants;
- 20 percent of network intrusions involved manufacturing, transportation and utilities;
- 38 percent of breaches were aimed at large companies;
- 92 percent of breaches were perpetrated by outsiders;
- 19 percent were attributed to state-affiliated actors;
- And finally weak defenses make things a bit easy for the bad guys.



One study* conducted in the UK showed that small businesses suffer an estimated loss of **£800m** a year, averaging nearly £4000 per business

- **30%** of its members were victims of fraud as a result of virus infections
- **50%** hit by malware
- **8%** victims of hacking
- **5%** suffered security breaches

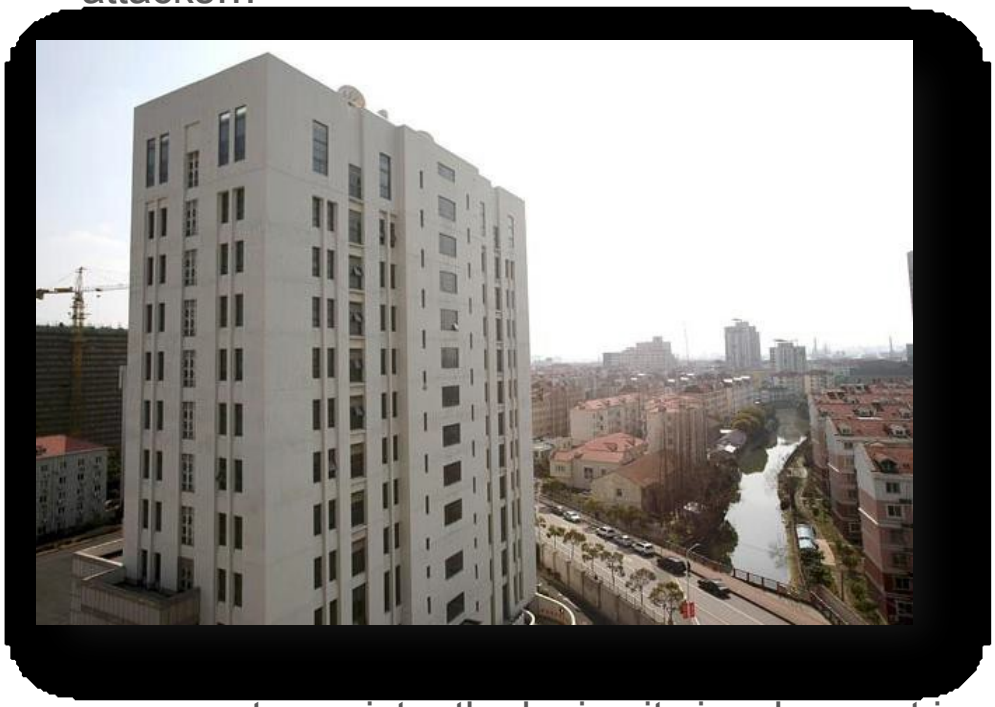
As a consequence, a second recent cybercrime study** revealed that

- **53%** of the British public is worried about the damage of cyber attacks
- **40%** feel more vulnerable to cyber attacks now than a year ago
- **38%** feel that their personal data exchanged with organisations they do business with may already have been compromised

* The study was carried out by the Federation of Small Businesses in the UK and is based on its 20000 members
** The study was conducted by PollOne in April 2013 for Tripwire on 1000 users

Meanwhile..

… just outside of Shanghai, “Unit 61398” of the Peoples Liberation Army is the alleged source of Chinese hacking attacks…



… although the Chinese government consistently denies its involvement in such activities claiming that such allegations are “irresponsible and unprofessional”

Should we be concerned?

Source: Hello, Unit 61398, The Economist

Threat horizon for 2015

- Reputation is a new target for cyber-attacks, from insider activists who leak information, and hacktivist collectives who vote on who they dislike this week.

- Criminals value your information, they're highly motivated to obtain it, or to use what leaks out of your organization.

- The changing pace of technology doesn't help; bring your own cloud (BYOC) and bring your own device (BYOD) also bring their own risks.

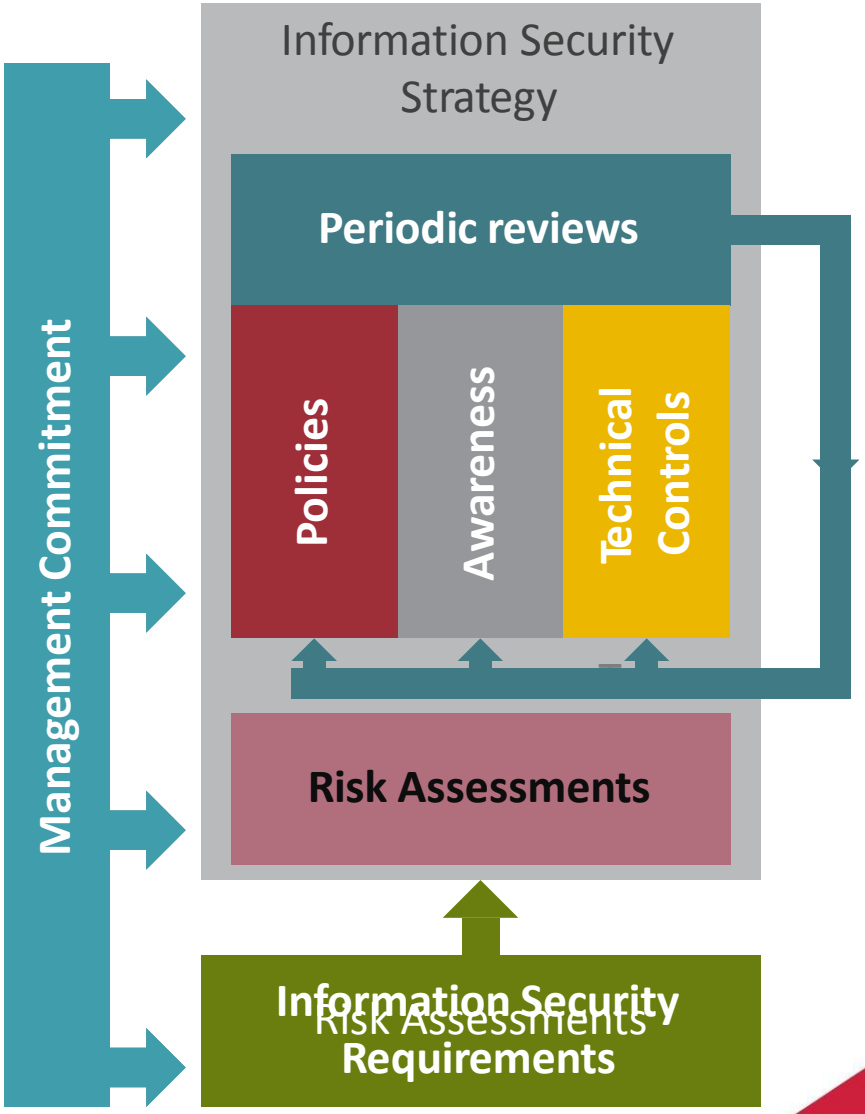
Source: Information Security Forum

Approach 1

ptl

Approach 2

- Identify critical information assets
- Obtain management buy-in
- Take a 3 pronged approach
- Conduct periodic reviews



m

Adopting a framework

"What does good cyber risk management look like?"

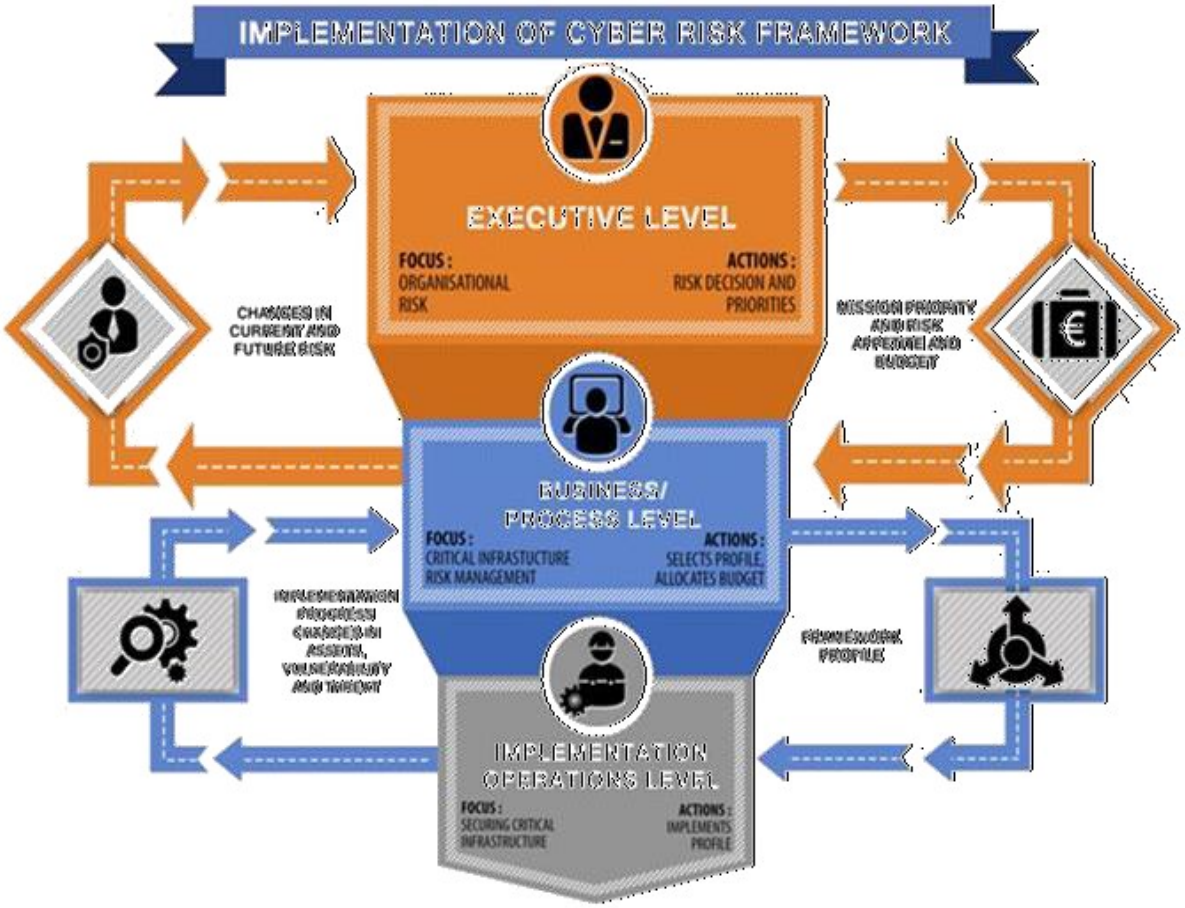
*By definition a framework is an **agreed structured approach** to dealing with a particular subject.*

- There is no such thing as a one-size-fits-all framework
- Use / implement the appropriate framework for your organisation's requirements
- i.e. access your requirements and design the appropriate framework for your needs
- Such that your organisation is not trying to 'fit' to a particular benchmark or rule book

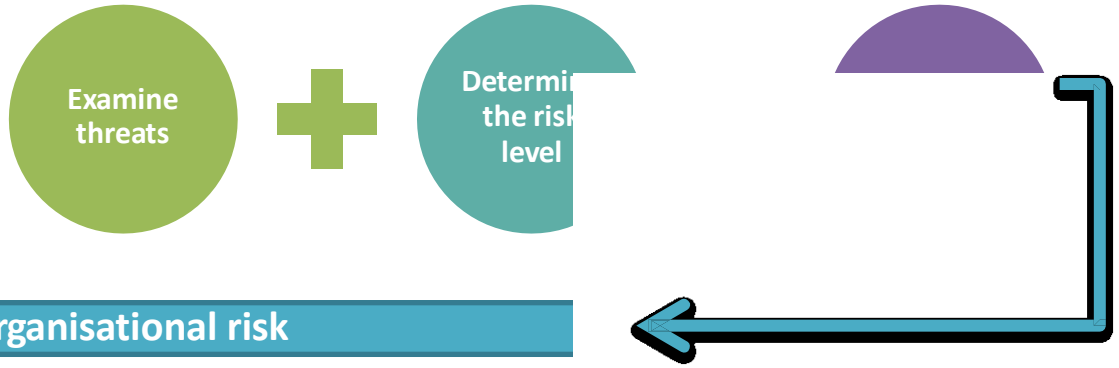
Implement what is appropriate to your business objectives, risk appetite and facilitates reporting to any third party against international generic cyber risk frameworks.

Source: Paul C Dwyer, Cyber Risk Expert

Adopting a framework



Juggling the risks



Risk Assumption	•With appropriate due diligence, management accept the potential risk and continue operating
Risk Alleviation	•Management approve the implementation of controls to lower risk to an acceptable level
Risk Avoidance	•Eliminate the process that could cause the risks
Risk Limitation	•Management limit the risk exposure by putting controls to limit the impact of a threat
Risk Planning	•A process to manage risk by developing an architecture that prioritises, implements and maintains controls
Risk Transference	•Management transfer the risk by using other options to compensate for a loss – e.g. Purchasing an insurance policy

ptl

Six Point action plan

Cyber Resilience

[redacted]

1. Organizational Readiness
2. Situational awareness
3. Detection
4. Cyber defence
5. Mitigation and containment
6. Recovery

#1 Organisational Readiness

Corporate awareness

Ownership at the C-level

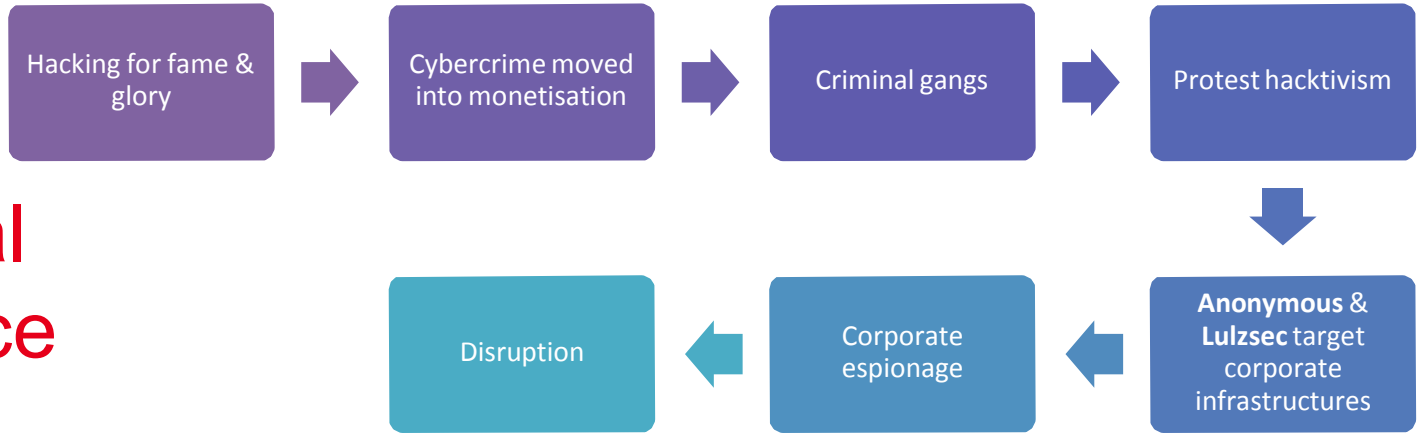
Assign the role and responsibility for information security oversight

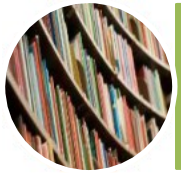
Understand your business risks

Focus on your information and reputation

Share intelligence and experiences

#2 Situational Intelligence





Specialist knowledge

Know your information assets

Keep abreast of the latest advanced threats

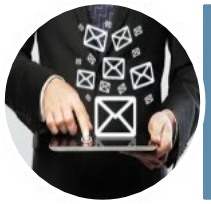
Classify your information assets

[redacted]

#3 - Detection

Develop the ability to detect attacks

Ensure you have an effective internal & external monitoring process



Scan outbound messages for ***abnormal volumes*** and ***patterns***

Early recognition of a compromise is key to early reaction

ptl

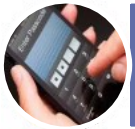
#4 – Cyber Defence

Get a grip on infrastructure and access security

Assert the levels of staff awareness

Define strict access control and remote access control

Ensure strong visitor procedures for key buildings



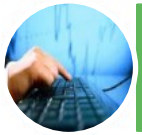
Keep your basic security controls in sight e.g. Password change policy

Infrastructure changes should trigger network configuration changes allowing you to move the shape of the target

ptl

#5 – Mitigation and containment

The aim is to limit the damage to your services and reputation

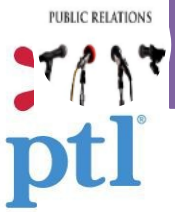


Limit the impact / shutdown the source

Being prepared is the key

Contingency planning – define and review your plans

Ensure adequate testing of business continuity plans



Prepared PR statements

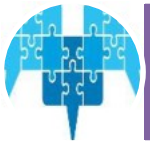
- Continuity of Operations Plan
- Disaster Recovery Plan
- IT / Network Contingency Plans
- Crisis Communication Plan
- ***Cyber Incident Plan***

#6 - Recovery

You need to develop the ability to re-establish normal service

☞ Your survival as a business depends on it

Apply the lessons learnt



Give feedback to senior executives

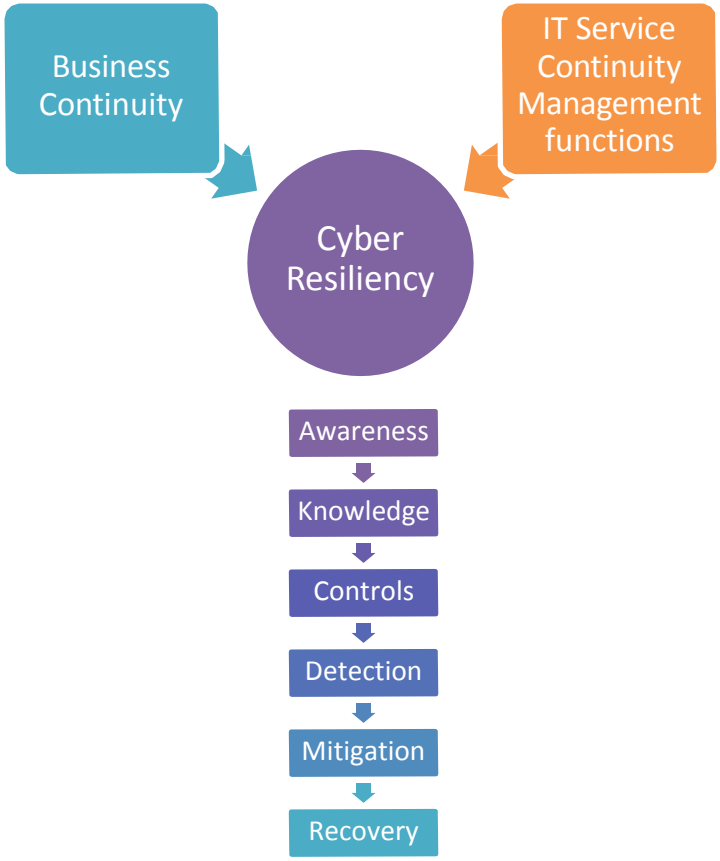
Here's what happened to us

This is how we reacted

This is what we've done to mitigate / prevent it

Conclusions

- Good IT governance by following a framework gives structure and business alignment
- Apply some form of strategy to the way you deal with information security
- Cyber threats are on the increase, so prevention and detection are always better than cure
- Becoming cyber resilient gives you the benefit of knowing how to tackle IT risks
- Take a pragmatic approach to investing in your defences



BEING PROACTIVE IS THE NAME OF THE GAME