RSA CONFERENCE ASIA PACIFIC 2013

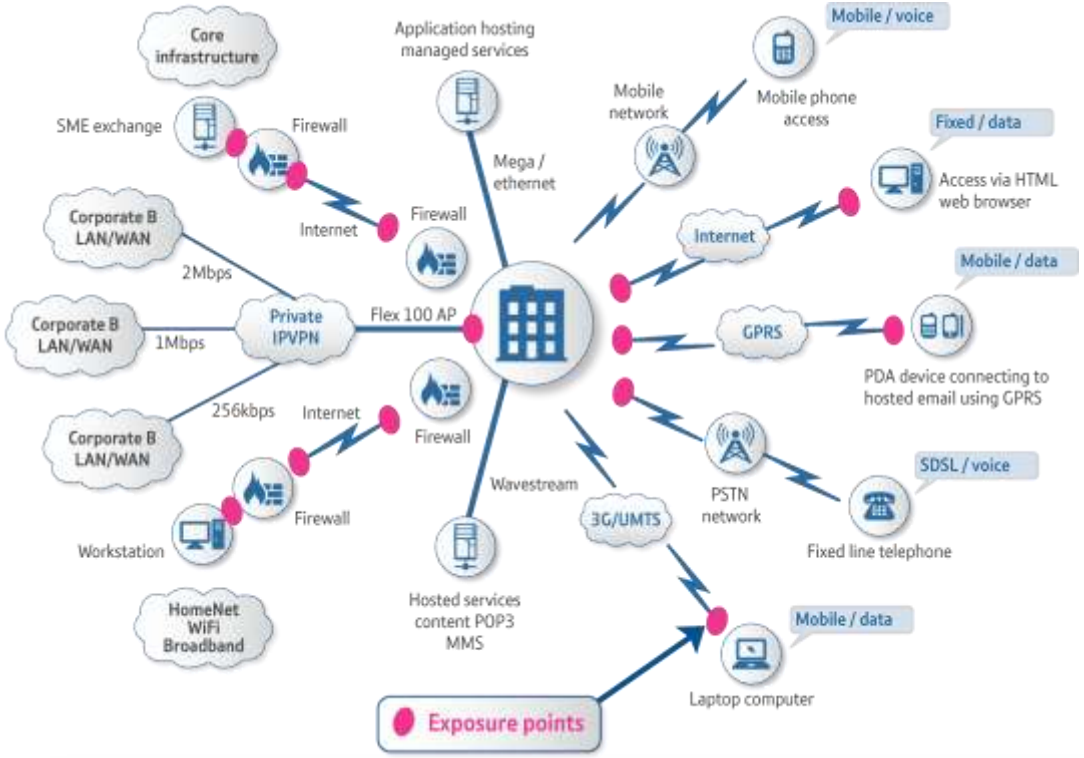
DOES BETTER SECURITY CONTRIBUTE TO YOUR BOTTOM LINE?

Hoo Chuan Wei BCCE, CFE, CISA, CISSP
BT Advise Assure / ISC2 Singapore Chapter

Session ID: ISC2

Session Classification: Intermediate

Today's networks are more exposed to threats



Cyberthreats continue to evolve, and businesses must evolve their defenses as well. Most new threats emerge as part of changes in technology or business processes, but a secondary wave occurs when complacency sets in."

Gartner, IT Security Threat Projection Timeline

The threat environment is constantly changing. Financially-motivated, targeted attacks are increasing – but most security processes and technologies are failing to keep up

US$136.5 Billion …wiped out in minutes

Hackers send fake market-moving AP tweet on White House explosions

Recommend | 554 people recommend this. Sign Up to see what your friends recommend.

Share 8 | Share this | +1 47 | Email | Print

Related News

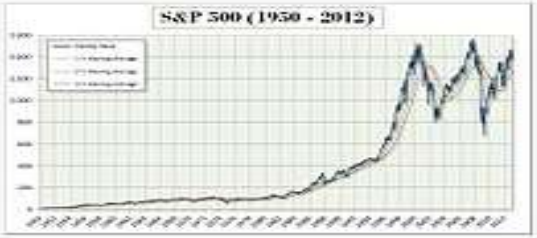
House passes cybersecurity bill as privacy concerns linger
Thu, Apr 18 2013

FBI says letter sent to Obama tested positive for poison ricin
Wed, Apr 17 2013

Obama, Putin set up two rounds of talks
Mon, Apr 15 2013

By Alina Selyukh
WASHINGTON | Tue Apr 23, 2013 7:01pm EDT

(Reuters) - Hackers took control of the Associated Press Twitter account on Tuesday and sent a false tweet about explosions in the White House that briefly sent U.S. financial markets reeling.



S&P 500 Index from 1950 to 2012

Foundation	1957[1]
Operator	Standard & Poor's[2]
Exchanges	NYSE, NASDAQ
Constituents	500[2]
Type	Large cap[2]
Market cap	US$ 13,274.65 billion *(as of January 18, 2013)*[1]

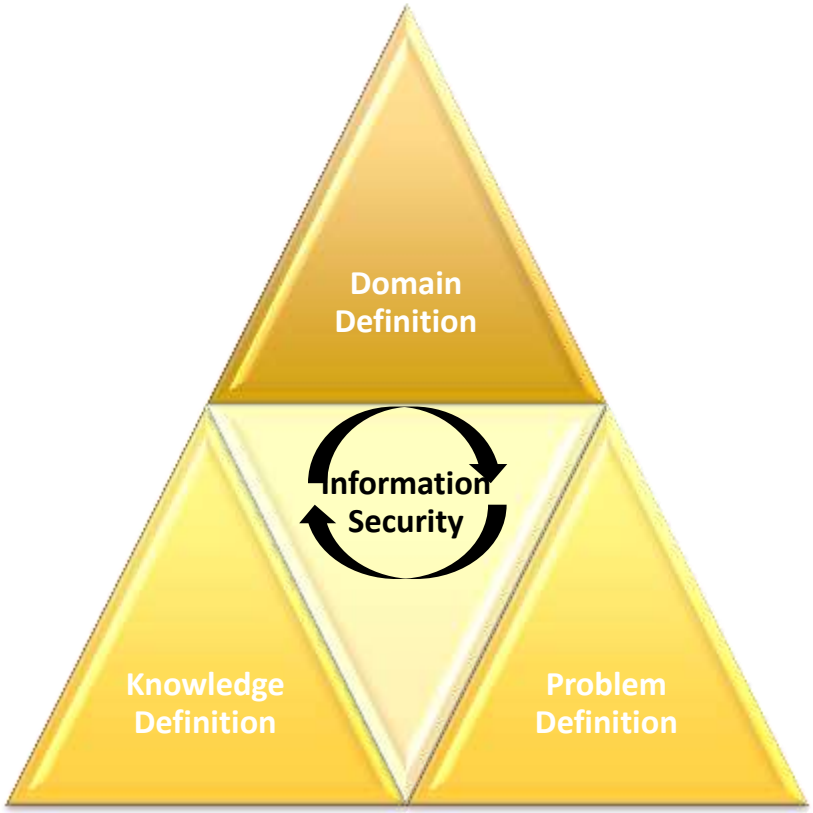
Root cause?

INSECURE PRACTICES

Resolution? …fix the root cause

Define before you invest…

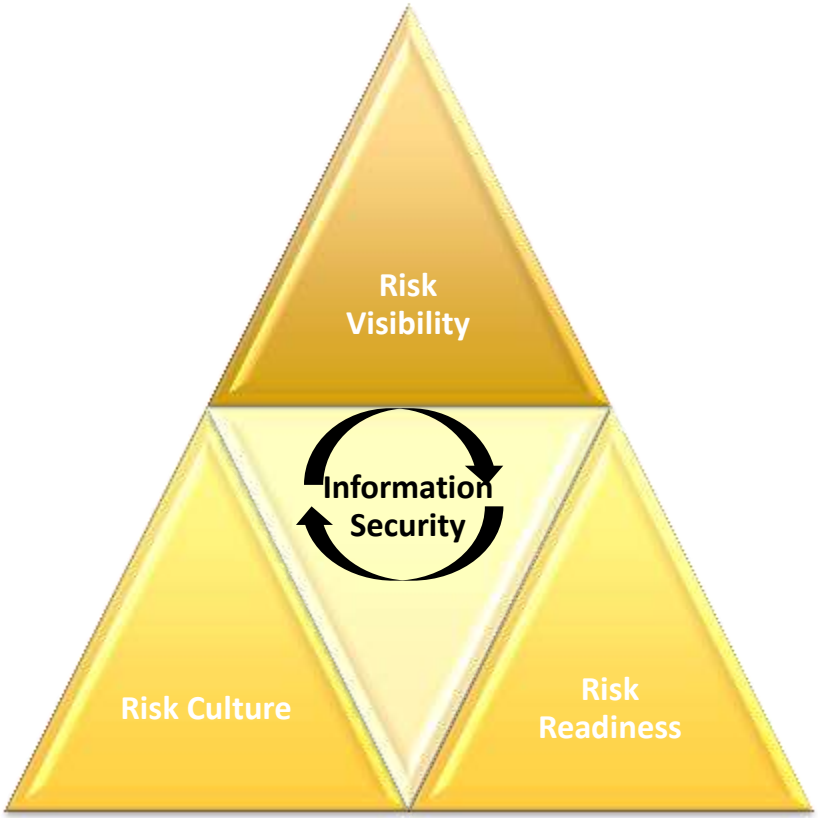
What are we covering?



We think we know everything

What is the problem?

Visibility



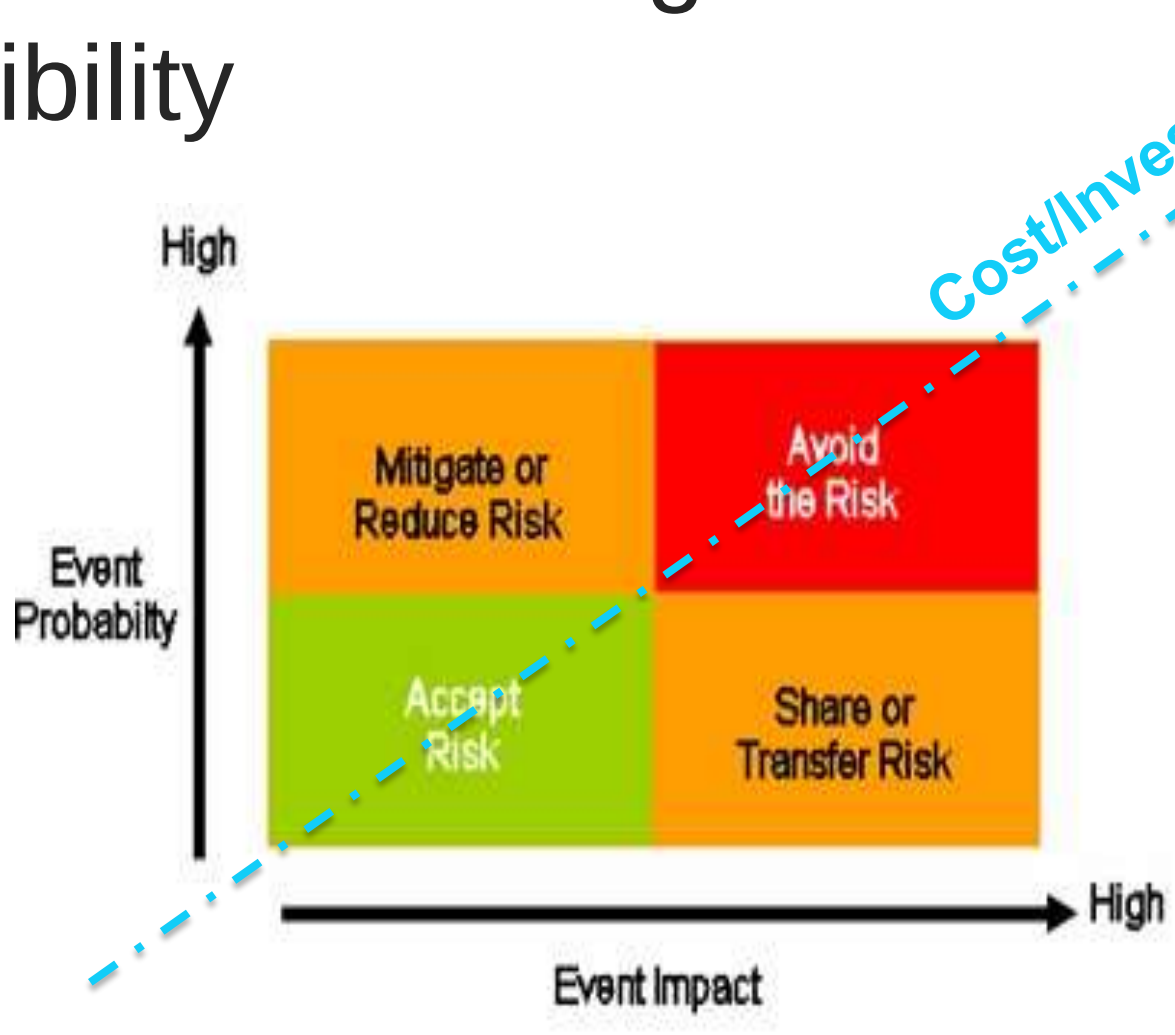
Culture

Response/ Readiness

Due diligence before you invest…

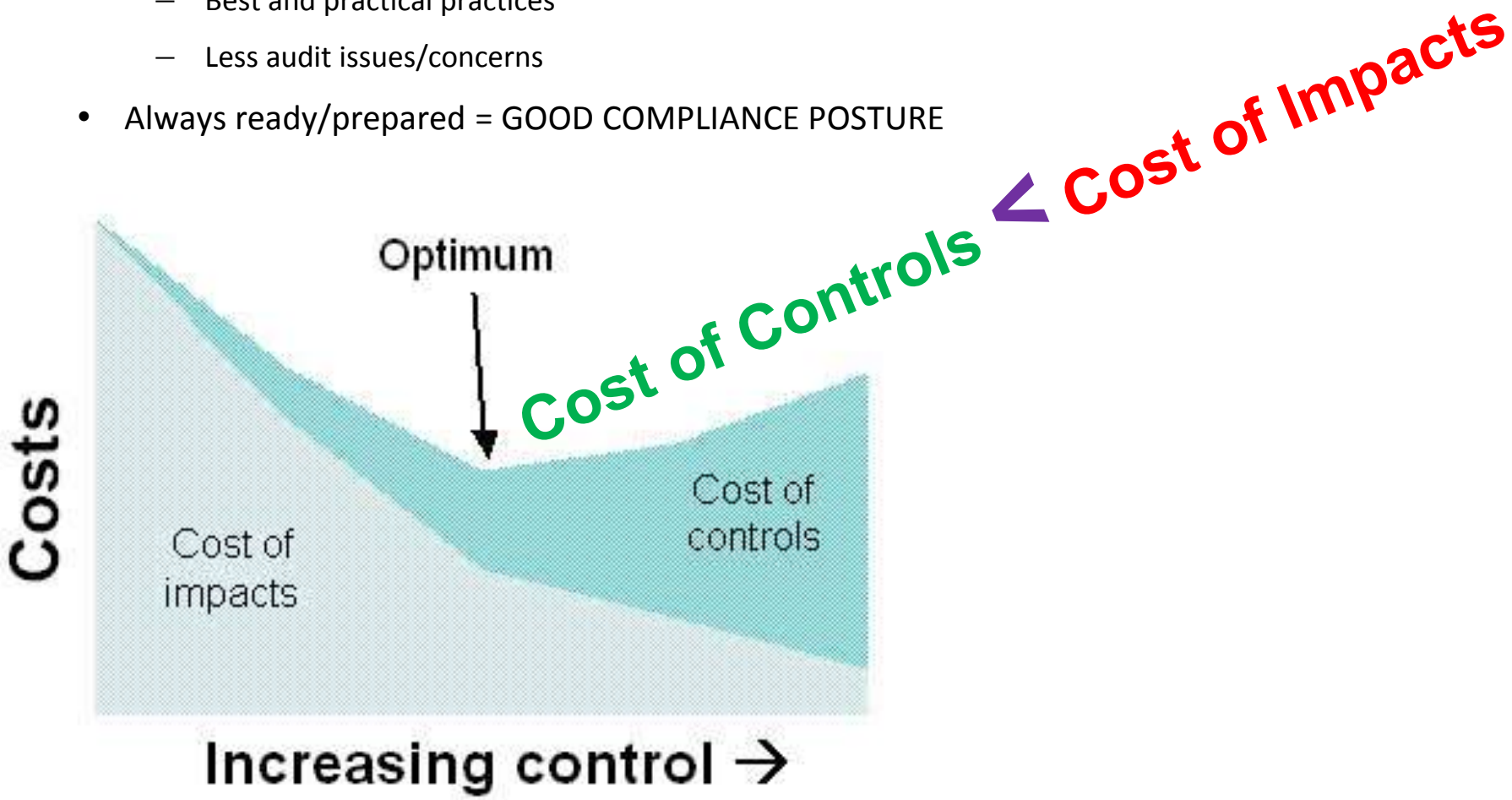
- Ask around for solution – ask your network for recommendations
- A good start is to look out for widely available references
  - ISO/IEC 27000 — Information security management systems
  - ISO/IEC 27001 — Information security management systems — Requirements
  - ISO/IEC 27002 — Code of practice for information security management
  - ISO/IEC 27003 — Information security management system implementation guidance
  - ISO/IEC 27004 — Information security management — Measurement
  - ISO/IEC 27005 — Information security risk management
  - ISO/IEC TR 27015 — Information security management guidelines for financial services
  - ISO/IEC 27032 — Guideline for CyberSecurity
  - ISO/IEC 27033-1 — Network security overview and concepts
  - ISO/IEC 27033-2 — Guidelines for the design and implementation of network security
  - ISO/IEC 27034 — Guideline for application security
  - ISO/IEC 27035 — Security incident management
  - ISO/IEC 27037 — Guidelines for identification, collection and/or acquisition and preservation of digital evidence
  - ISO/IEC 22301 — Business Continuity Management System (BCMS)

Immediate Management Benefit - Visibility

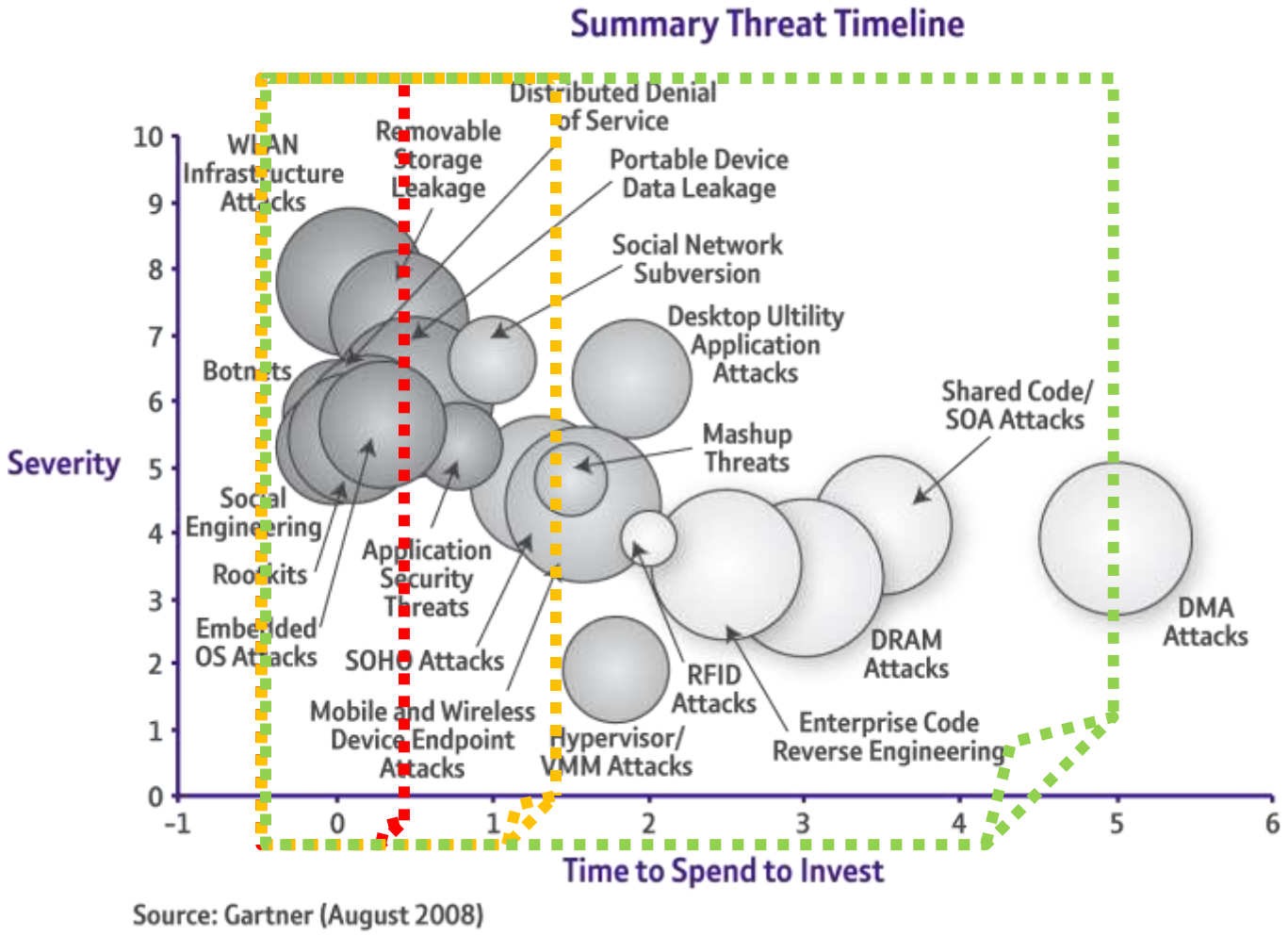


After investing

- Always in a complying mode = LESS REWORK, SAVING IN COSTS
  - Best and practical practices
  - Less audit issues/concerns
- Always ready/prepared = GOOD COMPLIANCE POSTURE



Typical severity vs cost timeline



Source: Gartner (August 2008)

Level of impact: Gartner rated the potential impact of threats on a common scale of 0-10, aka the "severity score," where 10 is the most severe.

Time to spend to prevent: Gartner analysed ideal conditions for a threat to be realised and cause significant damage to a typical business. Choices were limited to four time frames: now, within one year, within two to five years or more than five years.

In Information Security, no loss is already being profitable.

…very much like buying yourself an insurance package

Q & A