Information Security Reality in the Enterprise

Tim Mather, VP of Technology Strategy
(formerly CISO)

Agenda

- Insider threats
- Privacy considerations
- Changing threat environment

Information security Jeopardy

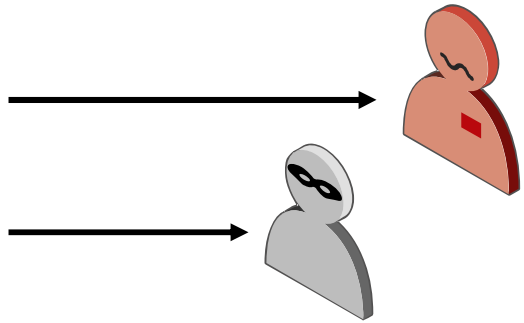
For your PhD Martin, define "**CIA**" – and be sure that your answer is in the form of a question.

I'll take information security for $200 please Alex.

What is:
- Confidentiality
- Integrity, and
- Availability

Definitional issue with “insider threats”

- Most statistics and surveys refer to “hackers” and “insider threats” – which presupposes that “hackers” are external
  - *CSO* magazine E-Crime Watch survey (conducted in cooperation with the U.S. Secret Service) does not
- What is the definition of “inside” an enterprise today**?**
  - Are non-employees “inside”**?**
  - Are partners and suppliers with persistent connections “inside”**?**
- Threat graphics used in section:
  - “Insider”
  - “Outsider”



Insider threats:

- Physical versus electronic crime
- Is this a problem for enterprises**?** Yes!
- Incomplete information security architecture
- Necessary components

Physical versus electronic crime

- Relevant quotations:

"**The difference between genius and stupidity is that genius has limits.**" Gerhard Casper, former President of Stanford University (1992-2000)

"**Only two things are infinite, the universe and human stupidity, and I'm not sure about the former.**" Albert Einstein

Example of the latter – stupidity

Bank robbery of SunTrust Bank in Manatee County, Florida.

Average take in a physical bank robbery

- Less than $5,000.00
  - “A computation of UCR [Uniform Crime Results] Summary data showed that a bank robbery occurred just under every 52 minutes in 2001, accounting for 2.4 percent of all robbery in the United States.[4] This represented a total loss of approximately $70 million. While this seems like a large amount of money taken, the average amount of money taken in a bank robbery over the period 1996 through 2000, according to NIBRS [National Instant-Based Reporting System] data is **less than $5,000**.”

Chances of getting caught (physical bank robbery)

- 57% of bank robbers are arrested
- 2nd highest “clearance rate” for all crimes
  - 2nd only to murder – 64%
  - (Which makes you wonder about that other 36%)

As “Deep Throat” famously said:

“Follow the money”

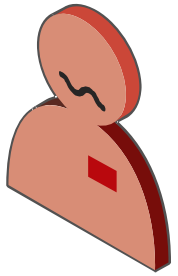
More lucrative target: electronic crime

More lucrative target: electronic crime

The Federal Reserve Board

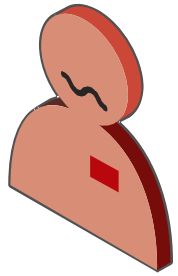
Fedwire Funds Service

In 2000, Fedwire moved more than $1.5 trillion per day. (Today, Fedwire moves more than $2 trillion per day.)



More lucrative target: electronic crime

- 0.0001% of $1.5 trillion (i.e., 1 / 1,000,000)
- = $150 million
- 30,000**x** average take in physical bank robbery



Is this a problem for enterprises? Yes!

Symantec's Cupertino headquarters

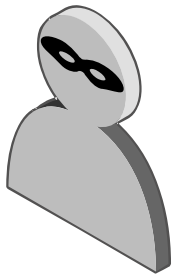
Is this a problem for enterprises? Yes!

- **2006 E-Crime Watch Survey from *CSO Magazine***
  - Conducted in cooperation with the U.S. Secret Service, Carnegie Mellon University Software Engineering Institute's CERT® Coordination Center and Microsoft Corp.

Crime:	**Affected:**
Theft of intellectual property	30%
Theft of other (proprietary) informa-tion, including customer records, financial records, etc.	36%
Intentional exposure of private or sensitive information	11%

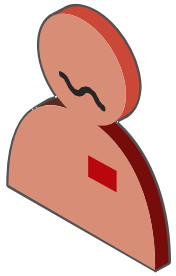
High technology target – physical crime

- Lenovo ThinkPad T60p base bundle with Symantec's standard image
- $2,508.25



High technology target – electronic crime

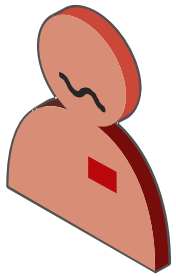
- According to Gartner, the cost of a privacy breach is $90 / record
- 50,000 records = $4.5 million
- Or 1,794**x** cost of laptop itself



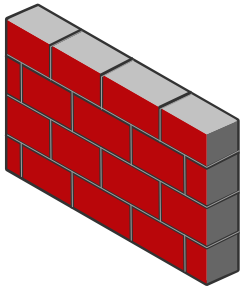
Is this a problem for enterprises? Yes!

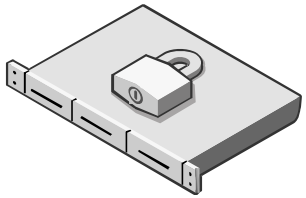
Privacy Rights Clearinghouse
Nonprofit Consumer Information and Advocacy Organization

- According to the Privacy Rights Clearinghouse, a non-profit consumer information and advocacy organization, there have been 115 such privacy breaches reported in the first six months of 2006
- 47 of those privacy breaches involved laptops being lost/stolen, or data going or being sent to an unauthorized location
- In those 47 incidents, privacy information of more than 32 million persons in the United States was compromised - and that number does not include the number of people in 8 (of those 47) incidents in which the compromised enterprise could not even determine whose, or the number of people whose, information was compromised



Incomplete information security architecture



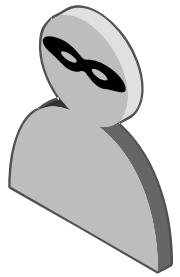


Access control based on exclusion

- Information security formerly relied on: **infrastructure security**
  - Network
  - Host
  - Application
- Goal was to prevent: **intrusions**

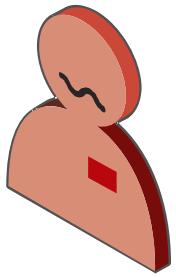
Access control based on exclusion

- Sales were based on: **transactions**
- Personnel were almost entirely: **employees**
- Perimeter protection was a viable strategy
  - Limited or even no external connectivity



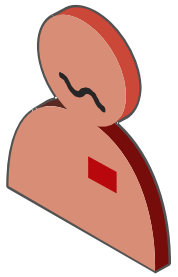
Access control based on inclusion

- Information security now needs to include: **data security**
- Goal now needs to include prevention of: **extrusions**



Access control based on inclusion

- Sales are based on: **relationships**
- Personnel are significantly: **non-employees**
- Perimeter protection alone is no longer a viable strategy
  - Extensive external connectivity to Internet and 3rd parties

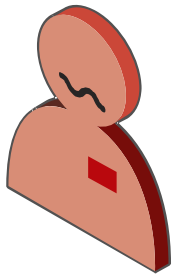


Access control based on inclusion

- Perimeter protection alone is no longer a viable strategy
  - Extensive external connectivity to Internet and 3rd parties

The Jericho Forum

- Jericho Forum is not about elimination of perimeter security; their real message is nothing new – it is defense in depth



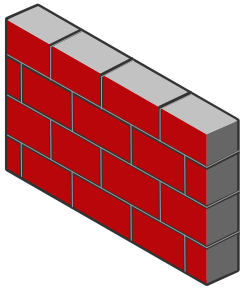
Information security architectures

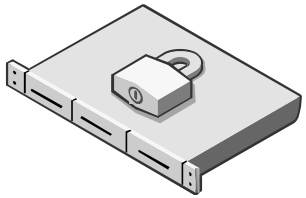
Designed to prevent:

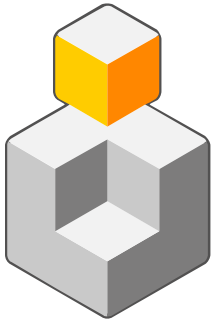
Access control based on:

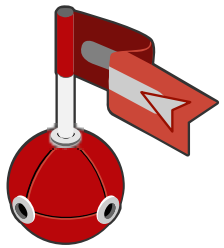
Exclusion	Intrusions
Inclusion	Extrusions

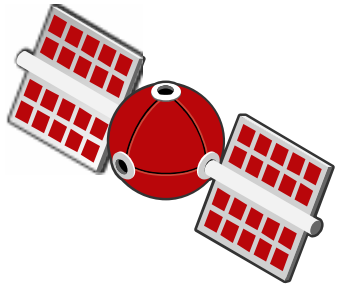
Necessary components – data leakage











Necessary components – data leakage

- Have a **policy**
  - If you want people to follow the rules, then they have to know what the rules are
  - Ensure that the policy explains why the rules are what they are – understanding greatly aids compliance
- Consider use of **enterprise DRM** (digital rights management)
- **Encryption of data at rest**
  - Encryption of data at rest on non-mobile assets, particularly database servers, should already be in use today
  - Encryption of data at rest on mobile devices with policy enforcement set and enforced by the enterprise is also required – as is data elimination (remote wiping)
  - Ignore this ridiculous talk (e.g., with regard to HR 4127, Data Account-ability and Trust Act) of redaction, alteration, editing, or coding in such a way that PII data is not "in usable form"

Necessary components – data leakage

- **Encryption of data in transit** – already standard practice (e.g., use of SSL in file transfers)
  - 'In transit' needs to include not only transmission security, but encryption of stored data that is physically moved – back-up media
  - Compliment to this measure should be physical asset tracking through use of RFID tags attached to storage media (How many companies' back-up media has gone missing recently?)
- Consider use of **data leakage prevention products**
  - Oakley Networks, Reconnex, Tablus, Vericept, Vontu

Great, but….problems remain

- While all of these components exist today, they are stand alone
  - There is little or insufficient cross-platform support
  - No unified management
  - No unified reporting
- Additionally, implied assumptions are faulty
  - Network-based solutions *assume* no permitted use of peripherals (e.g., CD-ROM or DVD burners, memory sticks)
  - Host-based solutions (agents) *assume* that I can control all of my hosts, am knowledgeable about the presence of them, that all are under enterprise management – probably that all are enterprise assets (not personal); and that end-users do not have administrative control of systems

What is really needed….location

- GIS (Geographic Information System) for (or about) enterprise data itself
  - While RFID (Radio Frequency IDentification) provides location data for physical assets, unfortunately, there is no logical equivalent for data – yet
- Closest thing that exists today is relative simple tracking provided of Web site and e-mail reading through the use of Web bugs
- Research being conducted on electronic file bulletins – essentially 'RFID' for data
- Goal: electronic file bulletins coupled with E-DRM capabilities (with interoperability standards)

What is really needed….protection

- Goal: electronic file bulletins coupled with E-DRM capabilities (with interoperability standards)
- Holy Grail of E-DRM:
  - "Agentless" on the host for all data, where the agent is appended to / encapsulated with the data itself so that no "stand-alone" agent must be installed on a host
  - Appended or encapsulated agent would have to quite "thin" to not "hog" available bandwidth – which could be quite limited (e.g., wireless connectivity, or even wired connectivity in less developed regions of the world)
  - Goal is about two years away

Agenda

- Insider threats
- **Privacy considerations**
- Changing threat environment

What do these companies have in common?

ChoicePoint

Feb 22, 2005

140,000 customer records

Bank of America Higher Standards

Feb. 26, 2005

1.2 million customer records

LexisNexis™

March 9, 2005

332,000 customer records

citi financial℠

June 6, 2005

3.9 million customer records

How many (Symantec) personnel?

≈ 17,000

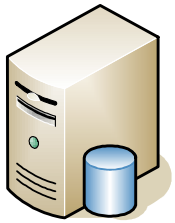
How many suppliers with access to PII?

≈ 100

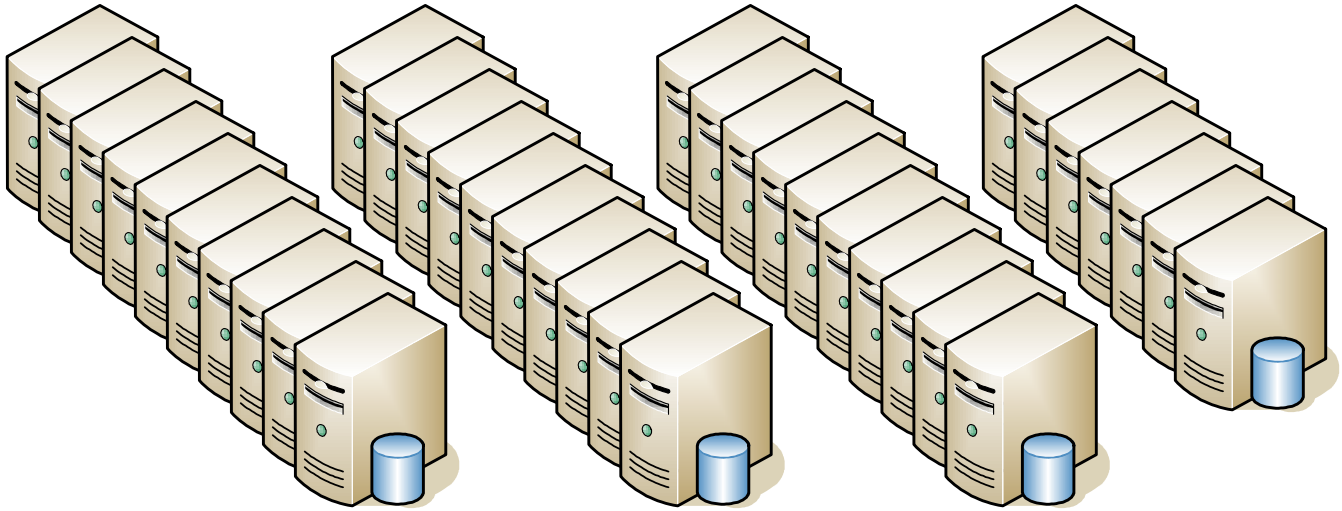
How many (Symantec) customers?

> 100 million

How many (Symantec) databases store PII?



How many (Symantec) databases store PII?



37 – that I am aware of.

How many laptops?

≈ 10,000

Where did this customer list come from?

- When using e-mail lists be sure it's been scrubbed with a marketing suppression lists
  - Understand what the customers in the list have consented to receiving
  - "Unsubscribe" lists must be incorporated with marketing suppression lists
  - When in doubt, don't use the list

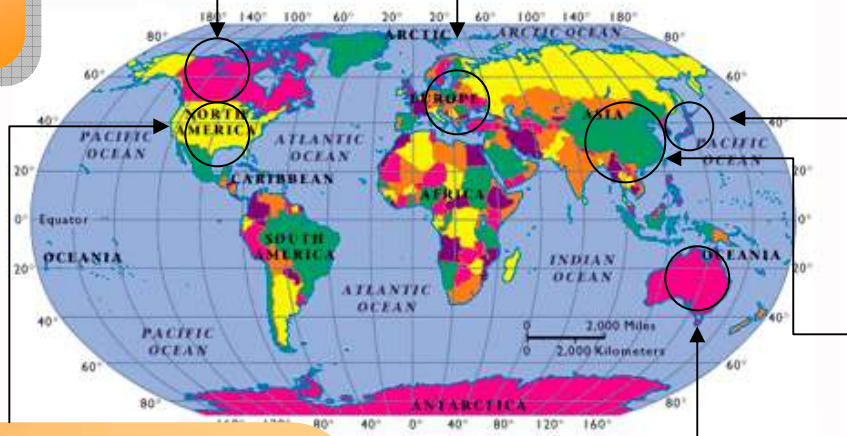
Liability is not transferable

- E-mail and direct marketing vendors must be as vigilant as we are.
  - Symantec will be held liable for their privacy violations
  - Contract process must include a privacy audit and agreement stipulating that vendor will adhere to Symantec's privacy practices

Where the rules apply

1. European Union (EU)
- EU Data Protection Directive (1995)
- EU Privacy & Electronic Comm's Directive (2002)

4. Canada
- PIPEDA – Personal Information Protection & Electronic Documents Act (2004)



5. Japan
- Personal Data Protection Law (effective April 2005)

6. China
- Forthcoming Privacy Law (2006?)

3. U.S.
- Sector-Specific Federal Laws – HIPAA & GLBA
- Anti-Spam Federal Law – CAN-SPAM (2003)
- California State Law:
  (1) Online Privacy Protection Act (July 2004)
  (2) Security Breaches Disclosure (July 2003)

2. Australia
- Trade & Privacy Law (2002)

Agenda

- Insider threats
- Privacy considerations
- **Changing threat environment**

Changing threats – problems

- Formerly random
  - Viruses & worms
  - Port scans
  - Phishing
- Increasingly targeted
  - Worms that target information or even specific businesses
  - Port “knocking”
  - Spear phishing
- Shift in attack “direction”
  - Was overwhelmingly outside in (e.g., attacks from Internet)
  - Increasingly inside out (e.g., insider threat; interconnected 3rd parties)

Changing threats – characteristics

- Increasingly sophisticated
- Increasing persistence
- Increasing control
- Demographics and intent
- Threatened environments

Increasingly sophisticated

- Malware capabilities
  - Viruses → worms → blended threats → **advanced blended threats (worms spreading rootkits)**
- Social engineering
  - Phone calls → Unsophisticated (spam) → **sophisticated ("spear" phishing)**
  - Why even bother now with social engineering? Just "bypass" humans altogether with keystroke logging Trojans

Increasing persistence

- "One time" compromise or crash (e.g., due to worm)
- Unacceptable activity – until found and deleted (e.g., spyware)

- **Stealth "ownership" (e.g., rootkits)**

Increasing control

- "Dumb" worms
- Targeted worms (e.g., Witty Worm)
- **Botnets with real-time control (e.g., real-time changes to attacks to counter target's responses)**

Demographics and intent

- Young, with challenged social skills, seeking thrills
- **Mature, with experience & resources, for financial gain**

Threatened environments

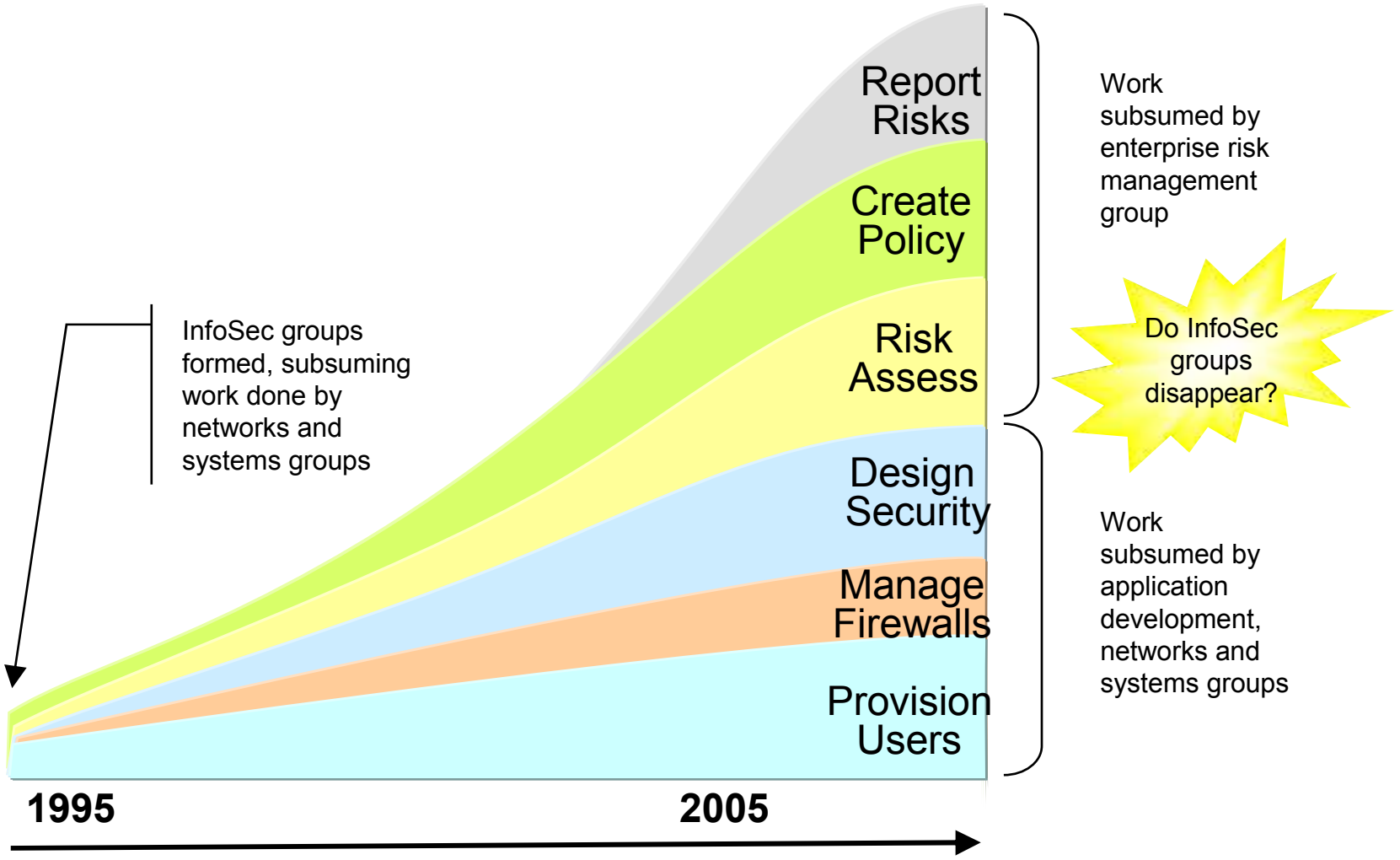
- Desktops → laptops → **mobile devices (e.g., PDAs, smart phones, game consoles)**

- Traditional (separate) voice network → **VoIP**

All that – and important business changes too

1. Network is no longer “an IT-thing”
   Network is the business!
2. “Perimeter” – what perimeter?
   Increasing interconnectedness
   Increasingly transient data with increased BPO
3. Changing nature of personnel within an enterprise
   # of employees: ↓ **# of non-employees: ↑**
4. Increasing regulation – especially with regard to privacy
   Impact on information security:
   - You can have security, and not have privacy
   - The converse is not true

Changing role for information security



Changing role for CISOs

 or  or  or 

 Continue on path to CRO?

 Make a “left turn” and return to business unit?

 Make a “right turn” to research director?

Questions?