

An Approach to Assessing Information Security in Complex Environments

Dave McComb

Simon Hoare

Semantic Arts

Semantic Arts

We are a consulting company dedicated to reducing information system complexity.

Focus: Enterprise Architecture

The Security challenge: track the impact of increased complexity on security.

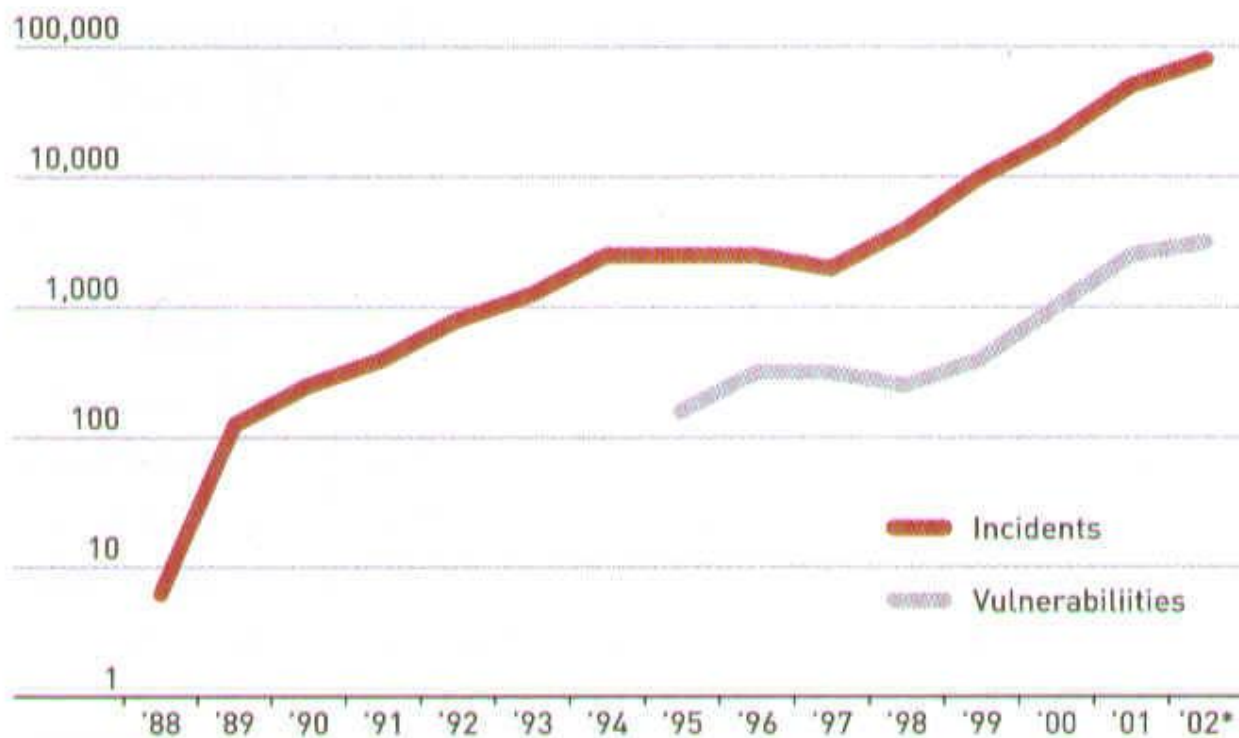
Information Systems Security

Whistling past the graveyard?



Attacks are up

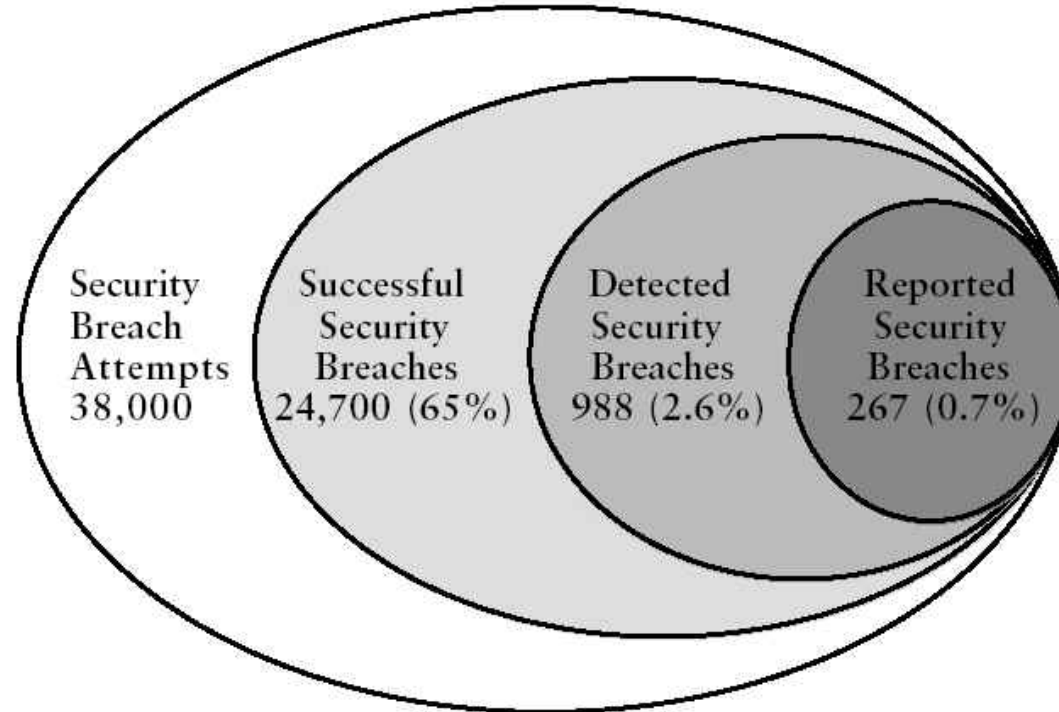
Computer security vulnerabilities and incidents



*Q1-Q3. An incident is a specific type of attack, and may involve one site or even thousands of them; some incidents may involve ongoing activity for long periods of time. A vulnerability is a specific aspect of devices, networks, or software that can be exploited for malicious purposes. SOURCE: Carnegie Mellon's CERT Coordination Center

Breaches are up

Figure 8. Vulnerability Analysis & Assessment Program Results, 1996



Losses are up

- CSI/FBI survey (1997 v. 2002)
 - Average financial loss
 - \$954,000 (1997)
 - \$6,571,000 (2002) seven fold increase
 - Total loss from respondents
 - \$20 million (1997)
 - \$170 million (2002) eight fold increase

It's one of our few remaining growth industries



Growth on a small base?

- CERT estimates computer security price tag at \$100 billion per year
- Identity theft (a small part of security loss in total) is currently a \$73.8 billion industry
- Software piracy is a \$12 billion industry

Recent News

- Microsoft's Passport Vulnerability
 - url to reset passwords
 - FTC fines could hypothetically reach \$2.2 trillion (“experts doubt that the actual amount would be this high”)

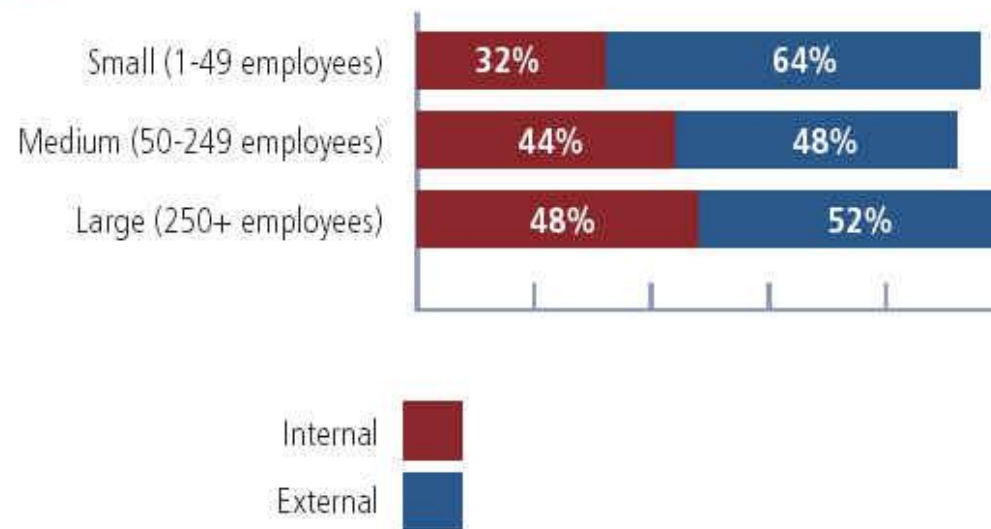
Nobody is safe

- It's not “if” but “when”
- Attacks are as likely to come from within as without

Inside/outside

Was the cause of the worst security incident internal or external?

Figure 22



Information Technology

- Is no different than non information intensive activities, except,
 - It is more complicated

No company relies on one security technique

- Banks
 - Vaults
 - Separation of duties
 - Video cameras
 - Insurance
- Jewelry stores
 - Electric eyes
 - Cameras
 - Bonding

All companies rely on a balance

- Prevention
- Detection
- Correction

Prevention

- Clearly, it is best to prevent problems.
Techniques include
 - Locking things up
 - Requiring special clearance
 - Only allowing access to “copies”

Detection

- Some breaches may not be obvious, and some resources need to be devoted to detecting that something has happened
 - Audits
 - Reviews

Correction

- Given that not all problems can be prevented, what are the appropriate means to have in place to restore things to the pre-problem state
 - Backup
 - Insurance (cyber-risk insurance is now available and priced based on exposure and countermeasures)

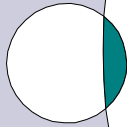
How does complexity make security
difficult?

Then and Now

- How security used to work in the days of the “glass house” versus now

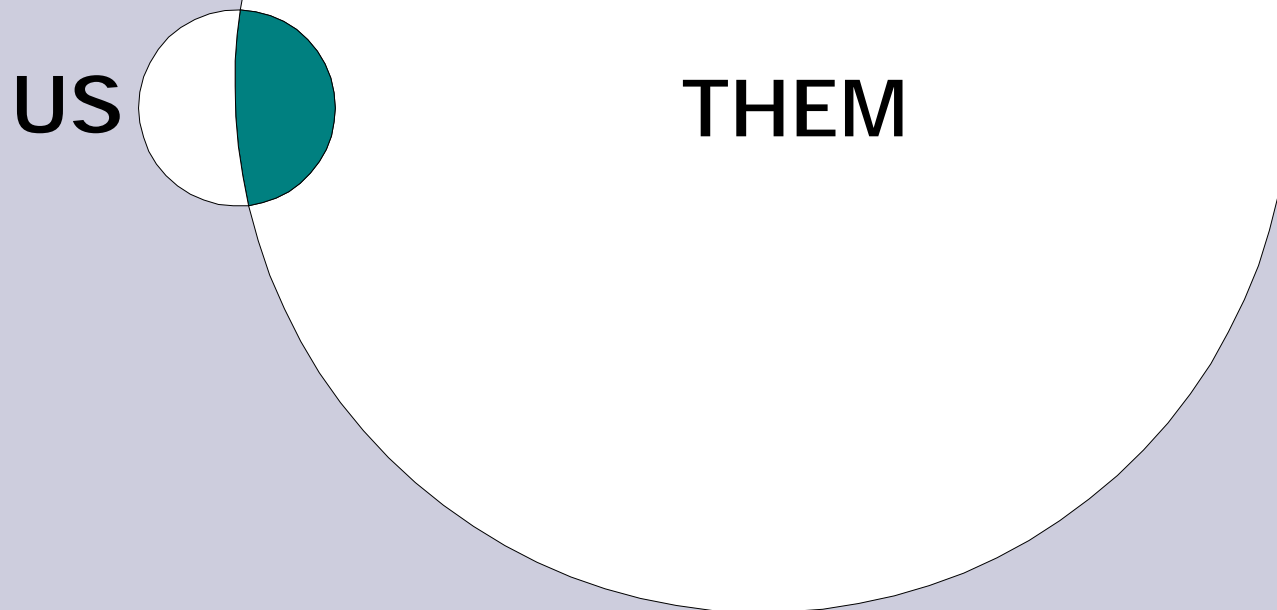
Us and Them

US



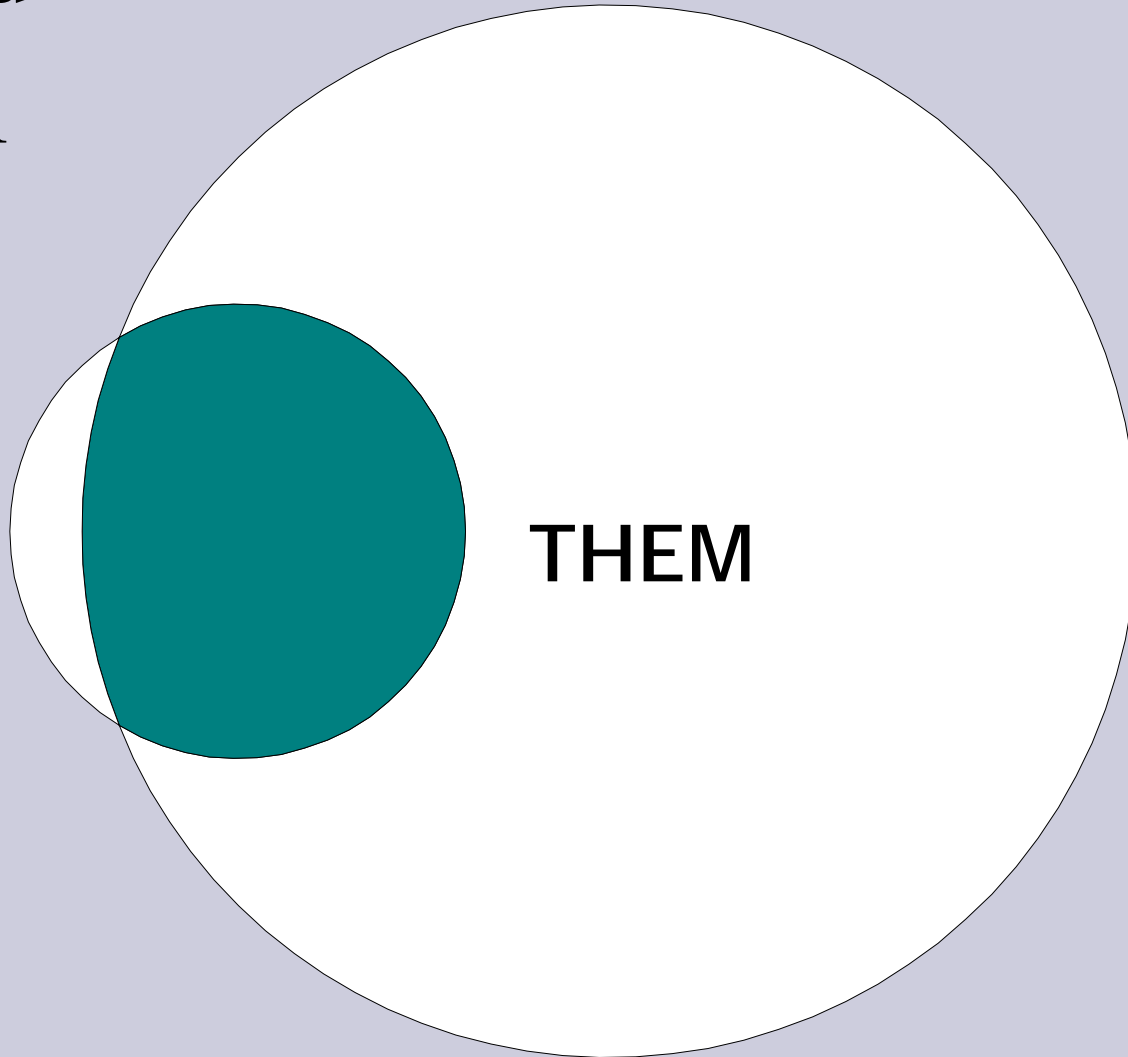
THEM

Us and Them



Us and Them

US



THEM

Analogies that don't work any more

- Theft and removal
- Keys and passwords
- Firewalls and, well firewalls

Theft and removal



In normal theft you
detect crime
because the assets
are missing

That isn't always
the case with
information systems

Asset status after a potential breach

Company

Invader

	Has	Doesn't
Has	Copied	Converted
Doesn't	Secured	Denied

Keys and passwords



Keys are typically one per lock, it's assumed you only need a handful of them to get around, you'll know when its time to change the locks.

Basic assumption is that ownership of a key/password is equivalent to permission to open the lock.

↑
SPARE KEY
TO GARAGE

↑
SECURITY
PASSWORD

← SPARE
CAR KEY

ALARM
CODE →

← C.O.D.
CASH

WELCOME

Diurnal Organizer®

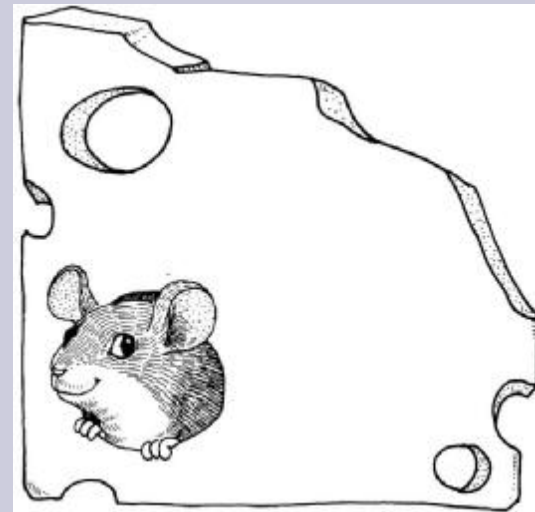
← BANK
CHECK

KEY TO
GUEST
HOUSE →

SPARE
HOUSE KEY
↓

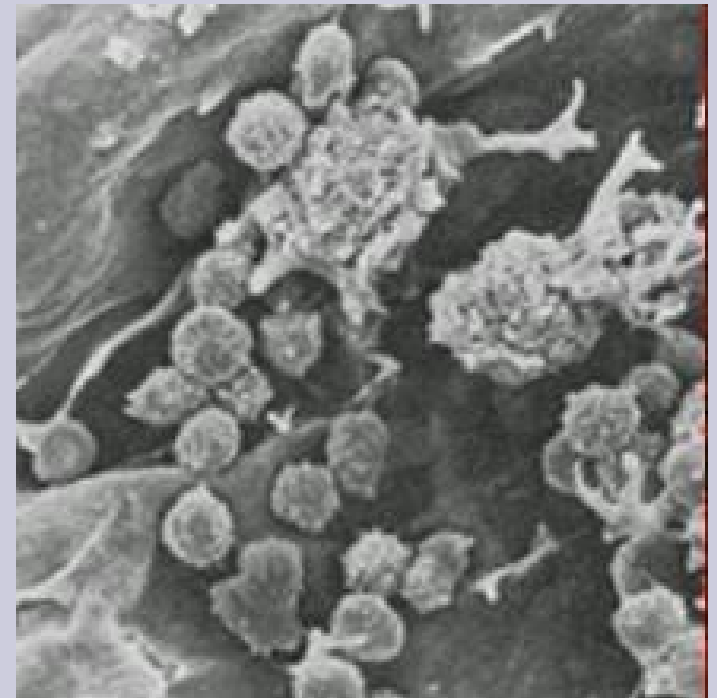
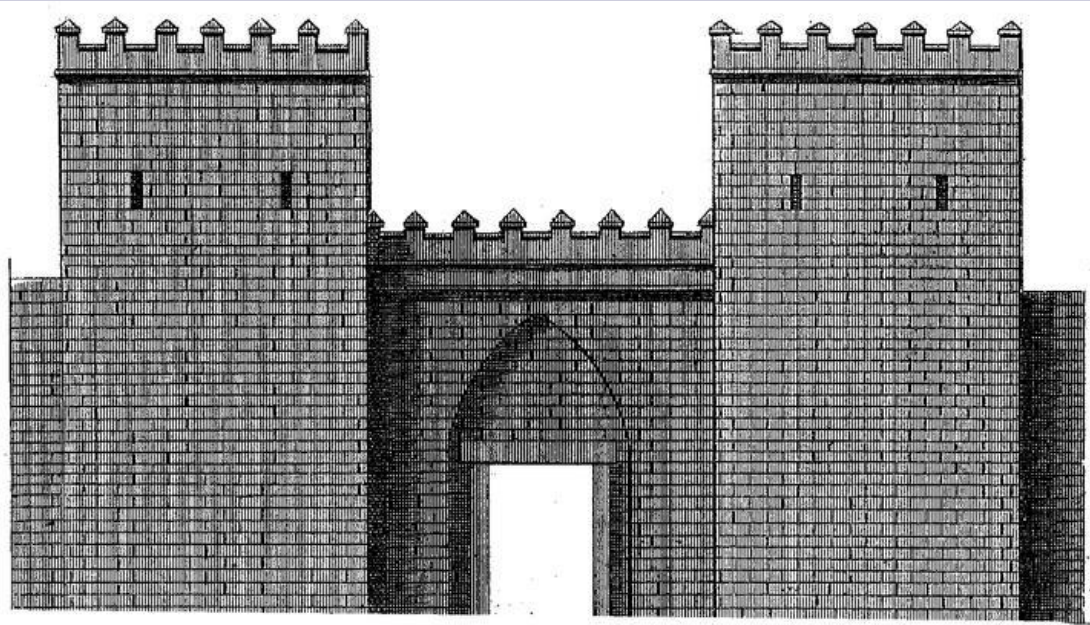
KEY TO
NEIGHBOR'S HOUSE
↓

Firewalls and...

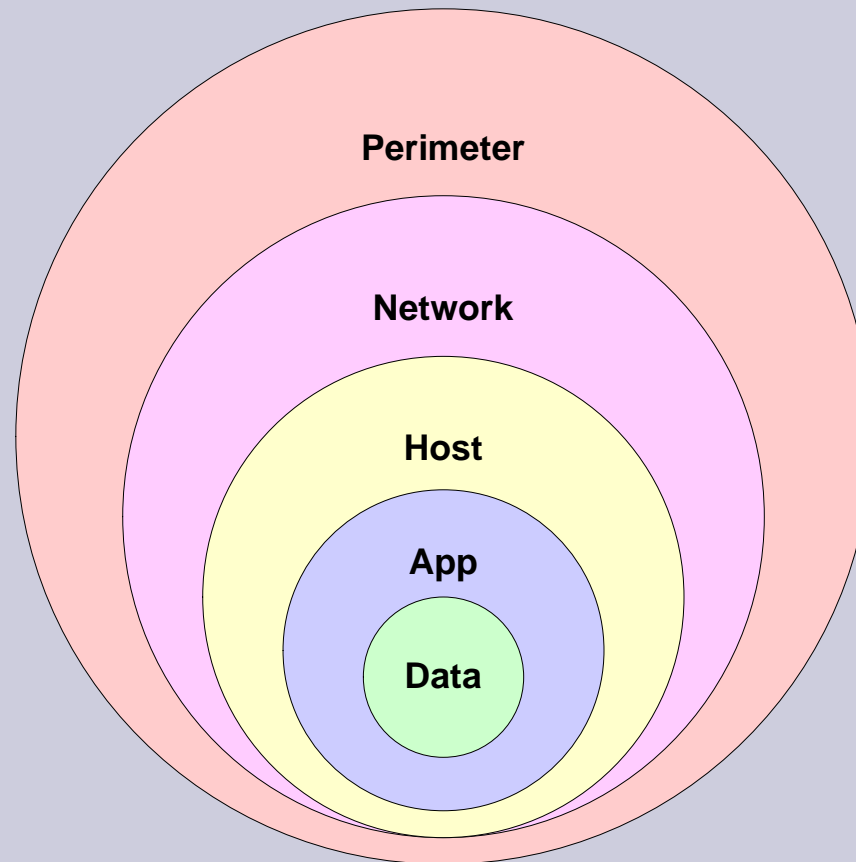


Analogy is that of a protective wall that will keep bad stuff out. Reality is that the firewall has to be full of holes to work

Fortress v. Immune system



The Information Security “Onion”



Traditional Risk Assessments

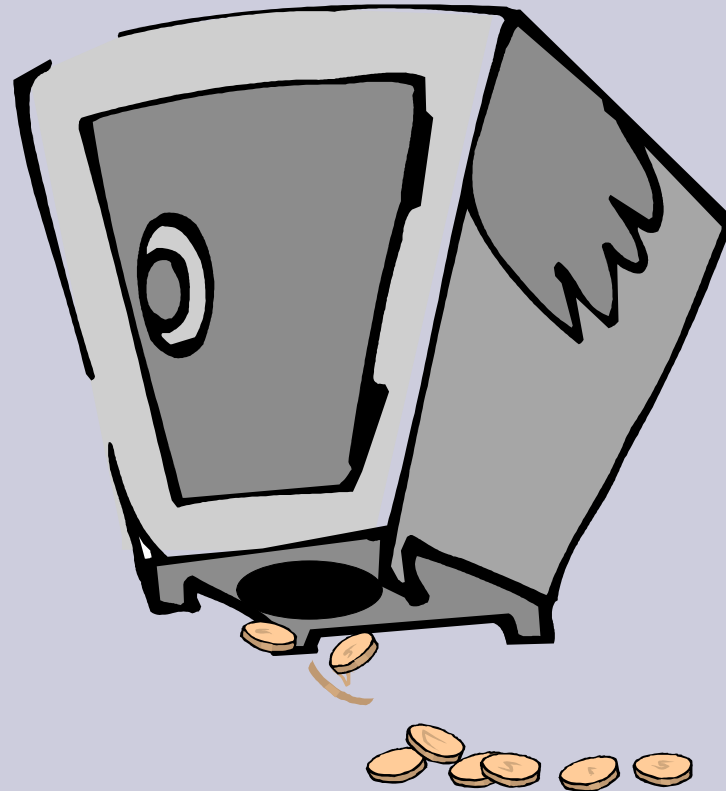
- Typically subjective
- Checklist style

Problems with traditional approach

- No confidence that you found even most of the risks, and at the same time
- It easily generates more risks than can be dealt with
- And there is no way of structuring and organizing what you have found.

Which leads to

- Not all risks considered



And/or

- “More” security
- Belts and suspenders



A suggested approach

- In order to make an assessment manageable we've developed an approach that organizes the information you discover and keeps it current as things change
- This is not a technological solution to the problem— we don't believe there is a technological solution to the problem

Method to the Madness

methodology

- A structured approach to comprehending the security environment
- A strategy for quantifying risk

Catalog Assets

- Cash
- Physical Assets
 - Vehicles
 - Laptops
- Data assets

Catalog
Assets

Data Assets

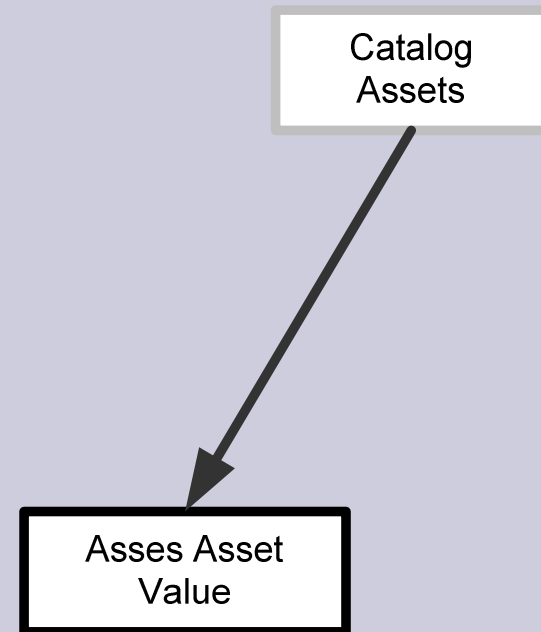
- Data convertible to cash
 - Bank Accounts
 - Vendor file/AP name and address
- Mission critical data
 - Can't continue operations
- Sensitive/private data
 - Legal liability

Categorize assets

- Don't want too many categories
- Security analysis at this level of detail
- Some things are attractive
 - Hand tools vs appliances
 - Narcotics vs diuretics
 - Credit card numbers vs regulations

Assess the value for each asset category

- Value to us
 - Monetary value
 - Embarrassment value
 - liability
- Value to others
 - Credit card numbers
 - Convertible to cash
- Threats are a function of value to others
 - Family photos vs. family silver
- Risk is a function of value to us

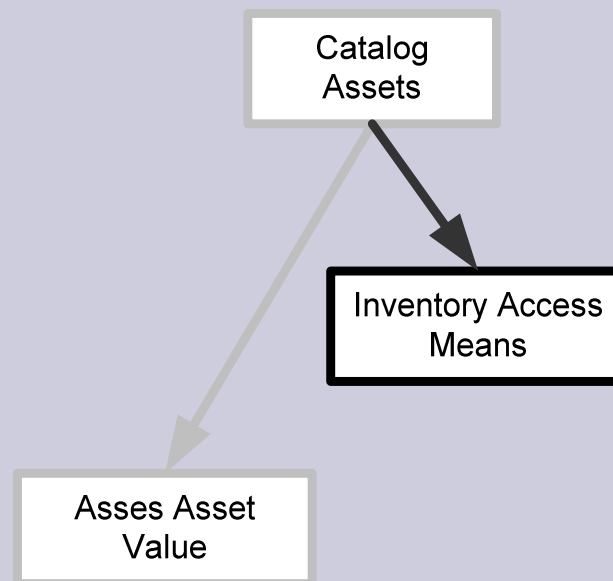


If there were no means of access

- The asset would be secure

Inventory Means of Access for each asset

- Physical access
 - doors
- Electronic access
 - Programs
 - networks
- Assets of the same type reside on different technologies..

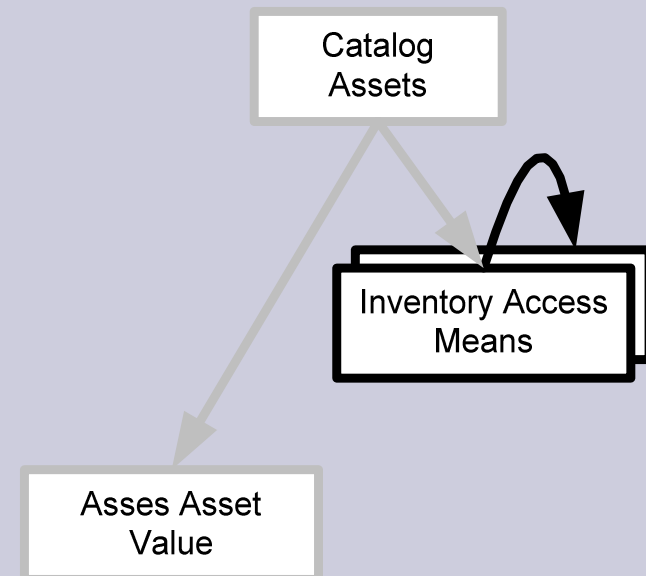


Data access means are a function of the technology

- Data assets in a database have access means provided by the DBMS
- if an application manipulates the data base it adds further technology access means

The Technology 'stack' gets deep

- Account Payable provides a user interface
- Accounts Payable is implemented using SQL Server, which also provides a user interface
- SQL Server is implemented using Winsock, which provides a programmatic interface.
- Accounts Payable is implemented in .Net, which depends on Windows, which provides a file system level interface
- All the interfaces are access means.



Coverage

- How do you know that's all the access means?
 - Open sockets
 - ODBC
 - telnet
 - Physical

Control

Each new program put into production is another exposure

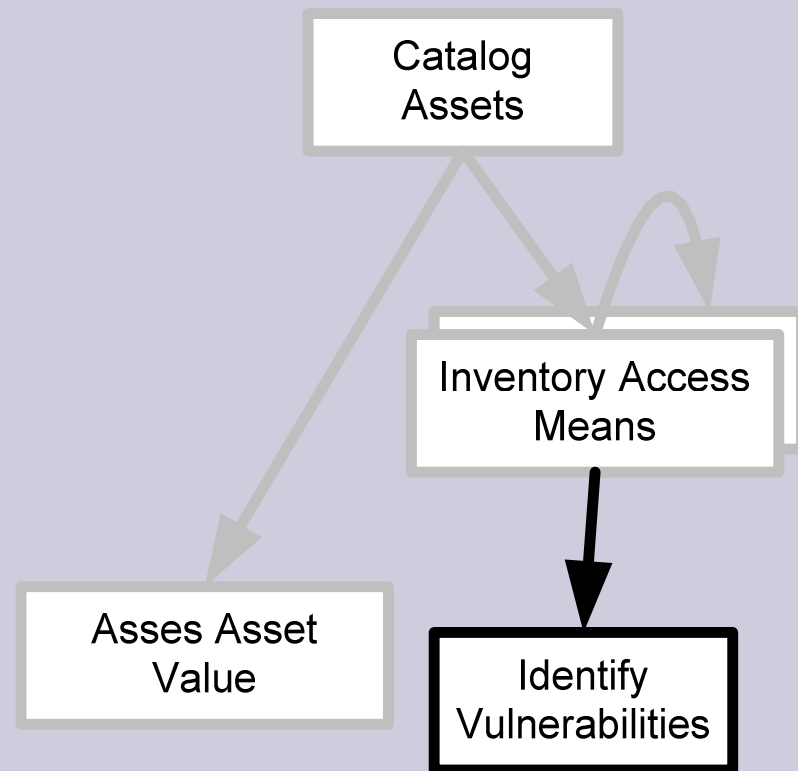
- Developers may create access means for testing and debugging
- Or for later exploitation
- Turn over is a point of control to identify 'rogue' access means

Security Entropy: the evolving 'stack'

- We introduce new technologies to add new capabilities
 - Internet access
 - Cell phone
 - PDA
 - Relational databases
- New technologies add new access means
- Unfortunately, access means have vulnerabilities

Identify vulnerabilities

- For all access means for each asset
- Each technology has (usually) vulnerabilities



Vulnerabilities

- Flaws in commercial products
- Flaws in custom applications
- Procedural flaws

Vulnerabilities

(from Windows and .Net magazine)

- April 24, 2003 | [Ken Pfeil](#) | Security Administrator
[MHTML Arbitrary Code Execution in Microsoft Outlook Express](#)
A vulnerability in Microsoft Outlook Express 6.0 and 5.5 can result in the execution of arbitrary code on the vulnerable system.
- April 24, 2003 | [Ken Pfeil](#) | Security Administrator
[Multiple Vulnerabilities in Microsoft Internet Explorer](#)
Internet Explorer (IE) 6.0, 5.5, and 5.01 contain four newly discovered vulnerabilities, the most serious of which can result in the execution of arbitrary code on the vulnerable system.
- April 23, 2003 | [Mark Joseph Edwards](#) | Security Administrator
[Buffer Overflow in Cisco ACS for Windows](#)
Cisco Secure ACS for Windows contains a buffer overflow condition that can permit a Denial of Service (DoS) attack and a root compromise.
- April 17, 2003 | [Ken Pfeil](#) | Security Administrator
[Buffer Overflow in Windows Kernel Message Handling](#)
A new vulnerability exists in A new vulnerability exists in Windows XP, 2000 and NT 4.0 that could result in the execution of arbitrary code on the vulnerable system.
- April 16, 2003 | [Mark Joseph Edwards](#) | Security Administrator
[Buffer Overflow in Snort Intrusion Detection System](#)
The "stream4 preprocessor" module contains a buffer-overflow condition that can permit a remote attacker to execute arbitrary commands on a system
- April 16, 2003 | [Mark Joseph Edwards](#) | Security Administrator
[Macromedia Flash Player Might Expose Cookies](#)
A problem with Macromedia Flash Player's advertisement-tracking feature can expose user cookies.
- April 15, 2003 | [Ken Pfeil](#) | Security Administrator
[Authentication Bypass Vulnerability in Oracle E-Business Suite](#)
A vulnerability in the communications protocol that Oracle Applications FND File Server (FNDFS) uses can permit an attacker to bypass any OS, database, and application authentication.
- April 14, 2003 | [Ken Pfeil](#) | Security Administrator
[System Compromise Vulnerability in Microsoft Virtual Machine](#)
A vulnerability in Microsoft Virtual Machine can result in the execution of code on the vulnerable system under the user's security context.
- April 14, 2003 | [Ken Pfeil](#) | Security Administrator
[Denial of Service in Microsoft ISA Server 2000 and Microsoft Proxy Server 2.0](#)
A vulnerability in Microsoft's ISA Server 2000 and Proxy Server 2.0 can result in a Denial of Service (DoS) condition on the vulnerable server.
- April 3, 2003 | [Ken Pfeil](#) | Security Administrator
[Man-in-the-Middle Attack on Microsoft Terminal Services](#)
A vulnerability exists in Microsoft's RDP implementation in Terminal Services.

- <-- Page [1] [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [11](#) [12](#) [13](#) [14](#) [15](#) [16](#) [17](#) [18](#) [19](#) [20](#) [21](#) [22](#) [23](#) [24](#) [25](#) [26](#) [27](#) [28](#) [29](#) [30](#) [31](#) [32](#) [33](#) [34](#) [35](#) [36](#) [37](#) -->

Stack & Vulnerabilities

- So.. Vulnerabilities come from access means which come from technologies..
- The deeper your stack, the longer this vulnerability list
- No matter how complete the list, it won't be complete

We've discovered the root causes of security problems:

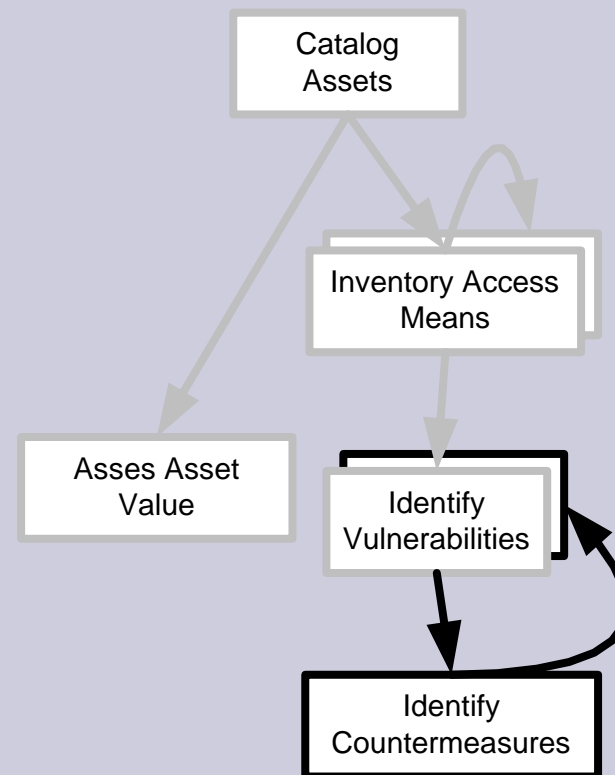
- Application development
- Infrastructure upgrades
- Users

Countermeasures

- A countermeasure is a way to overcome the vulnerability
 - Doors have locks
 - Separation of incompatible duties (check signing v. check preparing)
 - Encryption (snooping on public network)
- Each vulnerability may have one or more countermeasures
- Countermeasures can be technical

Identify countermeasures

- Technical countermeasures may introduce their own vulnerabilities.
- SQL Server is vulnerable to unauthorized use
 - Countermeasure is a username/password
 - Which is vulnerable to password cracking
 - Has countermeasure required password lengths etc.
 - » Vulnerable to written down passwords etc

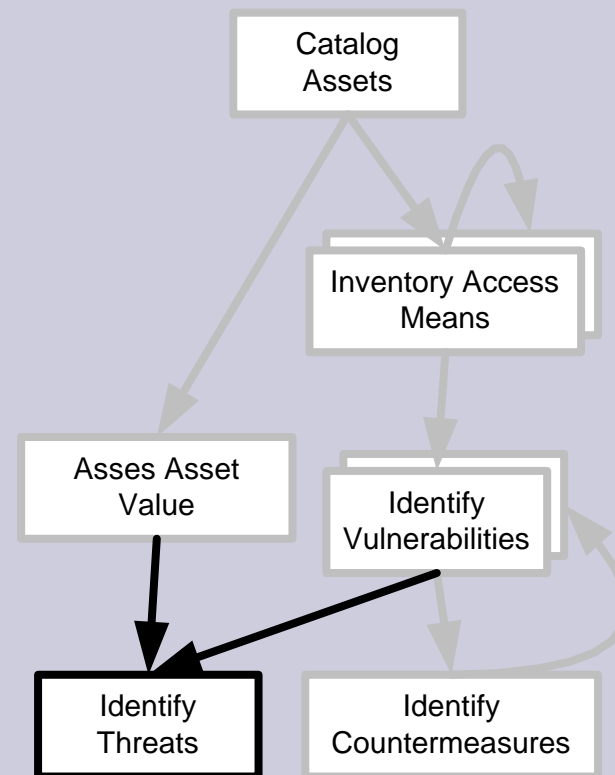


Patch list

- Windows 2000 Security Rollup Package, January, 2002*
- Download size: **481 KB, < 1 minute**
This update is a cumulative update for Windows 2000 that includes every security fix offered for Windows 2000 since the release of Windows 2000 Service Pack 2 (SP2). Download now to get the latest security updates in one cumulative package. Read more...
- * Must be installed separately from other updates
- 811493: Security Update (Windows 2000)
- Download size: **222 KB, < 1 minute**
A security issue has been identified that could allow an attacker to compromise a computer running Microsoft® Windows® 2000 and gain complete control over it. An attacker would need the ability to log onto the computer locally to carry out an attack. You can help protect your computer by installing this update from Microsoft. After you install this item, you may have to restart your computer. Read more...
- Q329115: Security Update (Windows 2000)
- Download size: **7.2 MB, 1 minute**
This update resolves the "Certificate Validation Flaw Could Enable Identity Spoofing" vulnerability in Windows 2000. Download now to help prevent an attacker from attempting identity spoofing using certificates. Read more...
- Q328310: Security Update (Windows 2000)
- Download size: **3.7 MB, < 1 minute**
A security vulnerability has been identified that could allow an attacker to compromise a Windows-based computer and gain complete control over it. The attacker would need the ability to log onto the computer to carry out an attack. You can help protect your computer from this specific vulnerability by installing this update from Microsoft. After you install this update, you may have to restart your computer. Read more...
- Security Update, February 22, 2002
- Download size: **1.8 MB, < 1 minute**
This update resolves the "Malicious SMTP Client Can Send Malformed Command to Windows SMTP Service" security vulnerability in Windows 2000, and is discussed in Microsoft Security Bulletin MS02-012. Download now to help prevent a malicious user from launching a denial of service (DoS) attack via the SMTP (Simple Mail Transport Protocol) service. Read more...
- Security Update, June 7, 2001
- Download size: **336 KB, < 1 minute**
This update addresses the "Predictable Name Pipes Could Enable Privilege Elevation via Telnet" security vulnerability in the Windows 2000 Telnet service that is discussed in Microsoft Security Bulletin MS01-031. Download now to help prevent a malicious user from launching programs on your computer, gaining access to your network or initiating a denial of service attack against your computer. Read more...
- Security Update, May 10, 2001
- Download size: **159 KB, < 1 minute**
This update addresses the "Malformed Hit-Highlighting" security vulnerability in Windows 2000 computers running Indexing Service, and is discussed in Microsoft Security Bulletin MS01-025. Download now to help prevent a malicious user from reading files on your Web server. Read more...

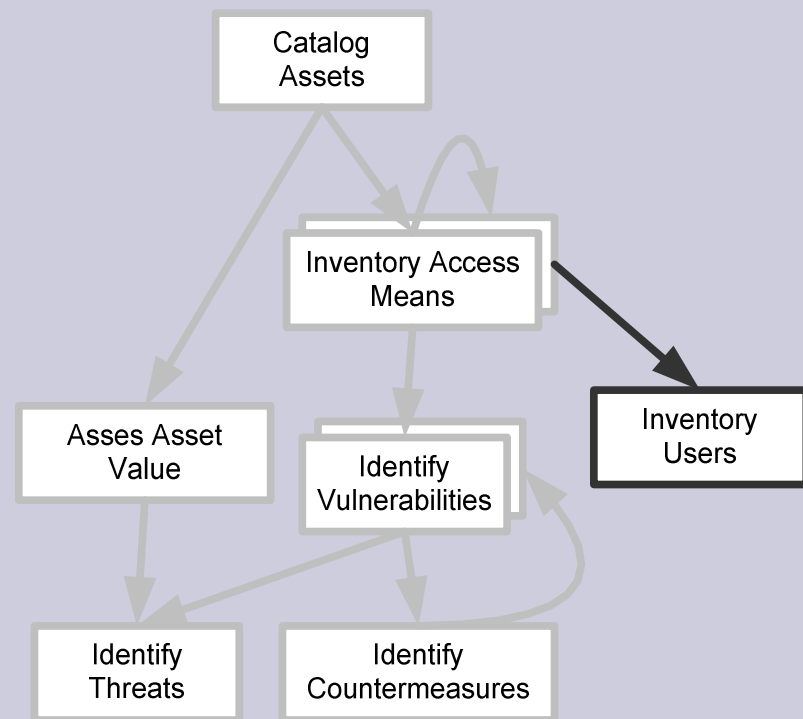
Identify possible threats

- Threats are means of exploiting vulnerabilities
- More probable with high value assets
- Changing the vendor file is a threat exploiting an unauthorized use vulnerability in the SQL Server access means for the Vendor File Data asset.



Inventory all the known users

- Risk is a function of users
- For all access means
- For all data assets
- Systems and people
- People vs. roles



‘Dynamic’ Trust level

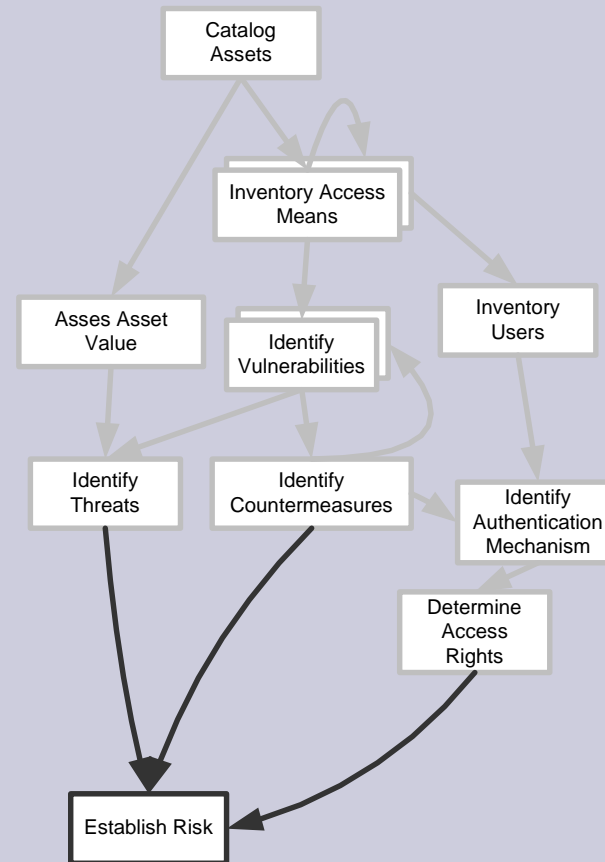
- The way you were authenticated determines your trust level
- What you can see is partially dependent on who you are
- And partially dependent on how we know this (your trust level)

Identify ‘Administrators’

- Associate countermeasures with people
- Reconcile Administrator rights and their User rights
- Delegation – should I be able to permit you to do what I cannot do?

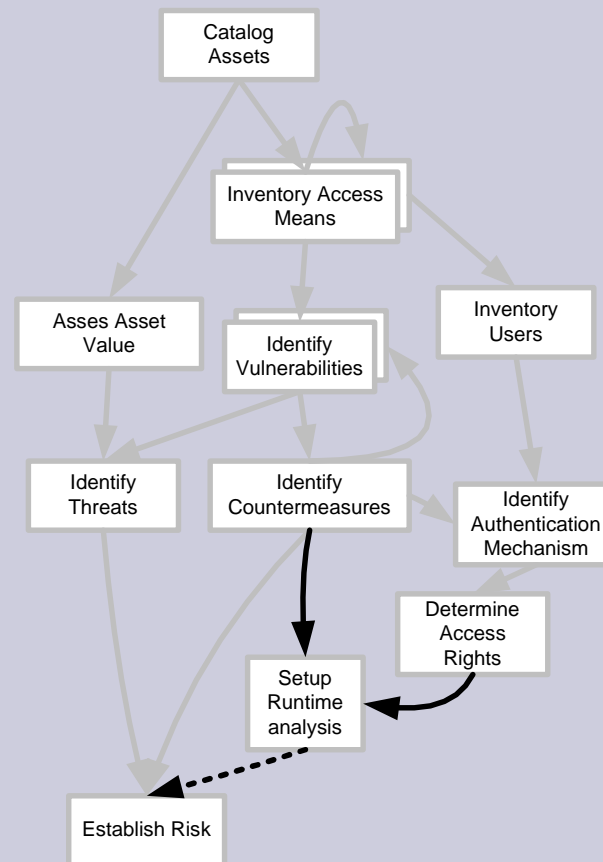
Establish Risks

- For a given asset risk is:
 - Increased by vulnerabilities
 - Decreased by countermeasures
 - Increased with the probability of threat, which is a function of value to others
 - Increased with value to us
 - Increased by the number of users, access rights and trust level



Real time adjustment

- Logs are a countermeasure based on detection not prevention
- Logs contain user activities – both allowed and denied
- Log analysis can reveal a threat and target vulnerability
- Intrusion detection



That was the methodology

What to do with it?

Concrete steps

- Collect the meta data proscribed by the methodology
- Build a database repository to structure it
- Evaluate security issues against the repository

What you could get out if it

- Prioritize effort by establishing risk by asset
- Relate new technology flaws to assets
- Identify what assets are threatened by new technology flaws
- Justify proposed spending in terms of risk
- Establish the security impact of technology changes.
- Have a quantified rather than intuitive understanding of risk

Rationalize countermeasures

- Identify countermeasure which redundantly protect vulnerabilities
- We want more countermeasures
 - They reduce risk
- We want fewer countermeasures
 - They reduce data asset accessibility
 - They introduce vulnerabilities
 - They have a cost
- This is a trade-off between value of the asset and the cost of the protection

Why is this hard?

- A lot of data
 - Even simple applications have lots of technical dependencies
 - Even simple technologies can have lots of vulnerabilities
- A lot of complexity
 - A recursive problem
 - Tough to keep in your head or manila folder
- Hard to see the context through the technology
- Fortunately, many applications share the same technologies so this is not infeasible

Concluding thoughts

- This is about simplifying a complex problem
- About aggregating technical detail to a comprehensible level
- Creating the management level view
- Creating a framework for thinking about the problem.

Concluding thoughts

- Security is a systemic problem
- Should be addressed architecturally
- Should minimize technologies

- Without a 'big picture' you're a prisoner of technical complexity

Get out of Jail



Drinking from a fire hose?

- If this went by too fast, and you'd like a copy of this presentation
- Contact us or email
 - simon@semanticarts.com
 - Mention IPMA security presentation