
Implementing info security governance
Robert Malmgren
rom@rom.ab.com
+46-708-330378

1


Implementing info security governance

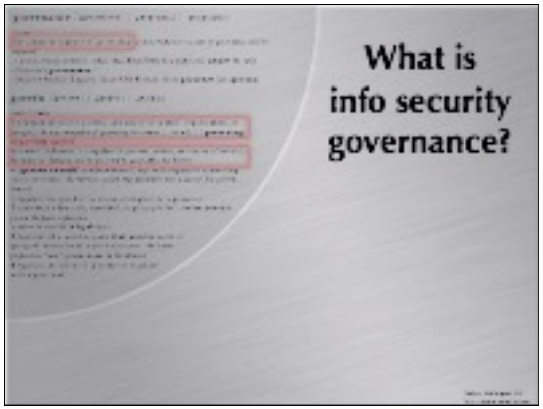
1


What is info security governance?

2


What is
info security
governance?

2


What is
info security
governance?

2


What is
info security
governance?

2

What is info security governance?

Information security governance

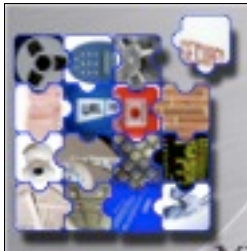
- [Blurred]

2

What is info security governance?

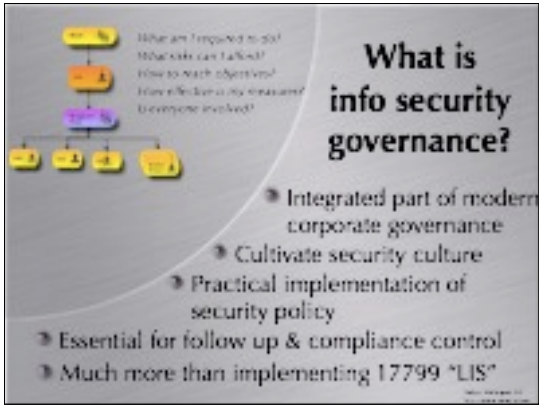
2

What is info security governance?

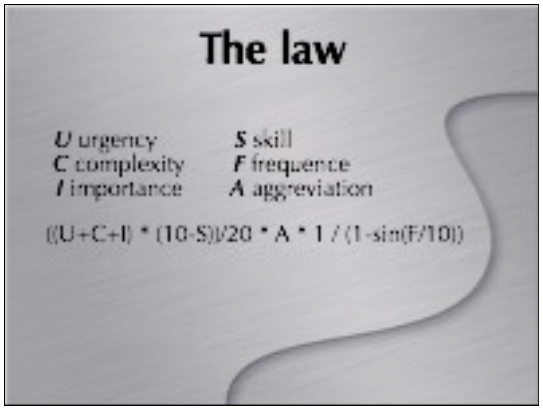


- Integrated part of modern corporate governance
- Cultivate security culture
- Practical implementation of security policy
- Essential for follow up & compliance control
- Much more than implementing 17799 "LIS"

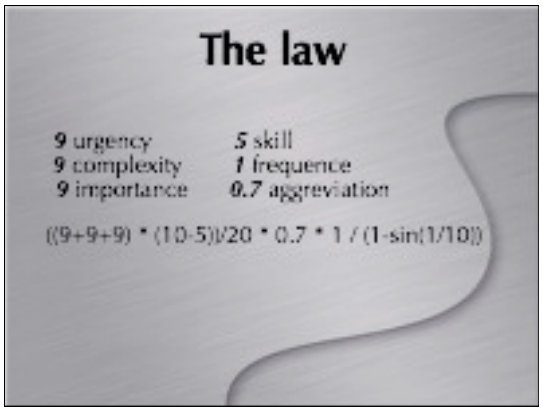
2


What is info security governance?
Integrated part of modern corporate governance
Cultivate security culture
Practical implementation of security policy
Essential for follow up & compliance control
Much more than implementing 17799 "LIS"

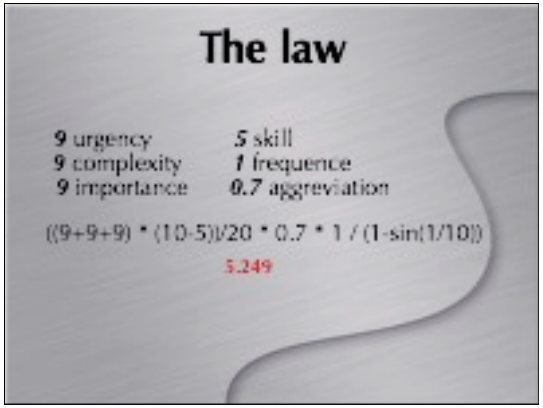
2


The law
U urgency
C complexity
I importance
S skill
F frequence
A aggreviation
((U+C+I) * (10-S))/20 * A * 1 / (1-sin(F/10))

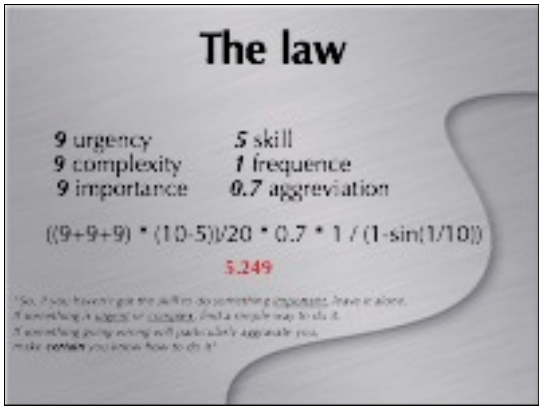
3


The law
9 urgency
9 complexity
9 importance
5 skill
1 frequence
0.7 aggreviation
((9+9+9) * (10-5))/20 * 0.7 * 1 / (1-sin(1/10))

4


The law
9 urgency
9 complexity
9 importance
5 skill
1 frequence
0.7 aggreviation
((9+9+9) * (10-5))/20 * 0.7 * 1 / (1-sin(1/10))
5.249

4


The law
9 urgency
9 complexity
9 importance
5 skill
1 frequence
0.7 aggreviation
((9+9+9) * (10-5))/20 * 0.7 * 1 / (1-sin(1/10))
5.249

4


The context
Business
Business requirements
Application / system
Basic infosec
Data storage
Network

5

The context

5

Standard setup...

- Standard type of IT infrastructure
- Standard type of staffing, both technical staff and management
- Matrix organisation
- Company has not realized the value of their information assets

6

"Default solution"

- Product driven
- Projects are ...
  - started without good initial setup
  - finished without cooperation with receivers
- In the end the costs for the solution is to high but it still doesn't meet the original objectives

7


Strategies
Funding
Business knowledge
IT knowledge
Security knowledge
The gap between executive management, CIO, operations and the users
Enterprise wide architecture - local commitment

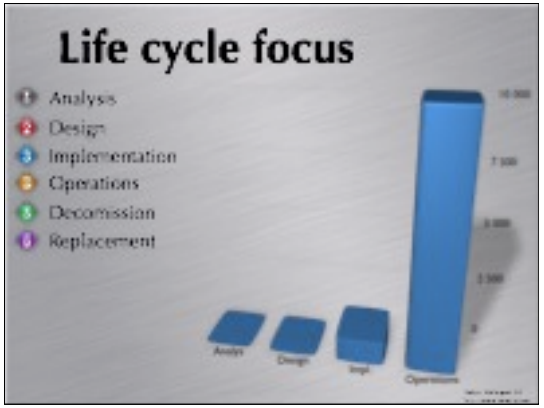
8


When all you have is a hammer, everything looks like a nail
"...when Vista arrives that won't be a problem"
"We'll just need to install some more firewalls"
We need to move away now from beeing focused on products and simple services. Start to think in terms of processes and better methodologies
Product or process?

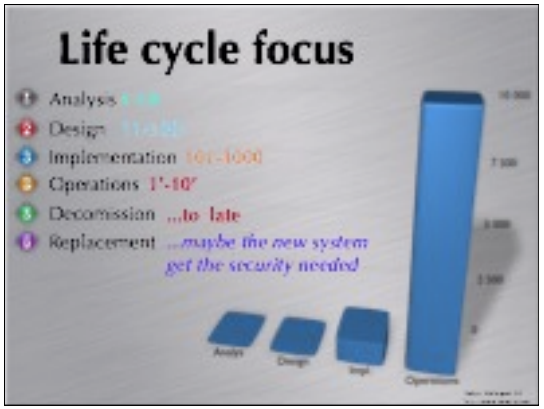
9


Life cycle focus
1 Analysis
2 Design
3 Implementation
4 Operations
5 Decomission
6 Replacement

10


Life cycle focus
Analysis
Design
Implementation
Operations
Decomission
Replacement

11

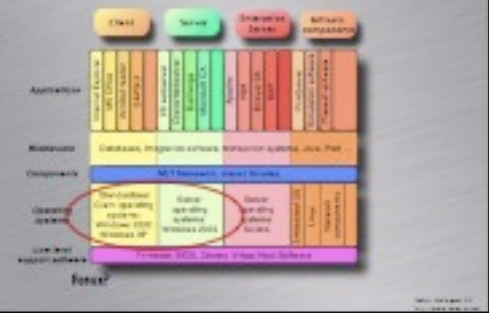

Life cycle focus
Analysis
Design
Implementation
Operations 1'-10'
Decomission ...to late
Replacement ...maybe the new system
get the security needed

11


Patching: playing catching-up

12

Patching: playing catching-up



12

- How to transform "I think" to "I know"?
  - Tools and methods for measurement of real level of security / compliance
  - Processes to continously monitor and react to events

Knowledge is king

13

- How to transform "I think" to "I know"?
  - Tools and methods for measurement of real level of security / compliance
  - Processes to continously monitor and react to events

Knowledge is king

13

- How to transform "I think" to "I know"?
  - Tools and methods for measurement of real level of security / compliance
  - Processes to continously monitor and react to events

Knowledge is king

13

- How to transform "I think" to "I know"?
  - Tools and methods for measurement of real level of security / compliance
  - Processes to continously monitor and react to events

Knowledge is king

13

- How to transform "I think" to "I know"?
  - Tools and methods for measurement of real level of security / compliance
  - Processes to continously monitor and react to events

Knowledge is king

13

- How to transform "I think" to "I know"?
  - Tools and methods for measurement of real level of security / compliance
  - Processes to continously monitor and react to events

Knowledge is king

13

- How to transform "I think" to "I know"?
  - Tools and methods for measurement of real level of security / compliance
  - Processes to continously monitor and react to events

Knowledge is king

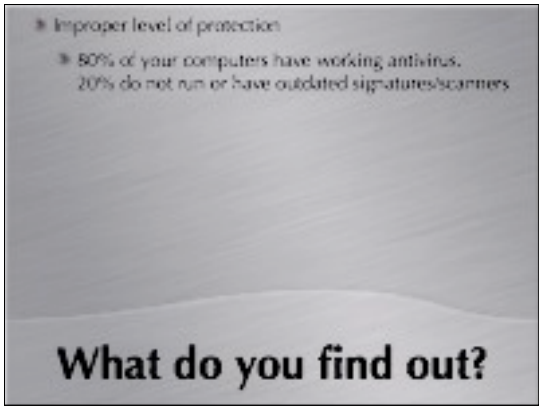
13

What do you find out?

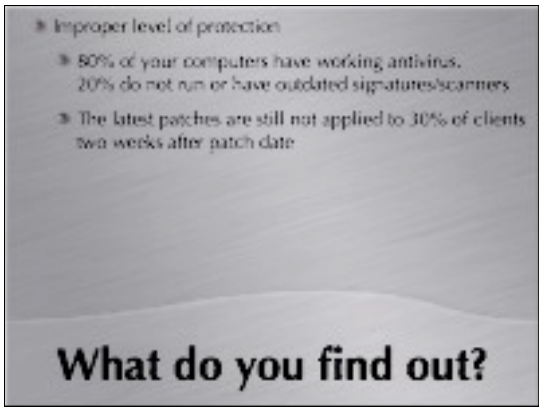
14


Improper level of protection
What do you find out?

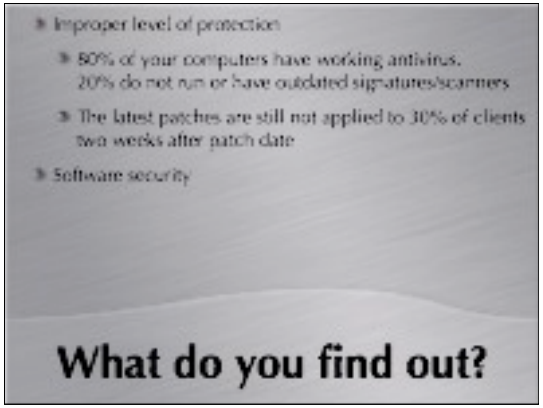
14


Improper level of protection
80% of your computers have working antivirus. 20% do not run or have outdated signatures/scanners
What do you find out?

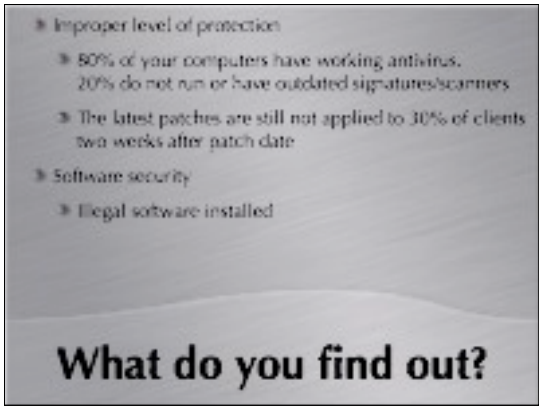
14


Improper level of protection
80% of your computers have working antivirus. 20% do not run or have outdated signatures/scanners
The latest patches are still not applied to 30% of clients two weeks after patch date
What do you find out?

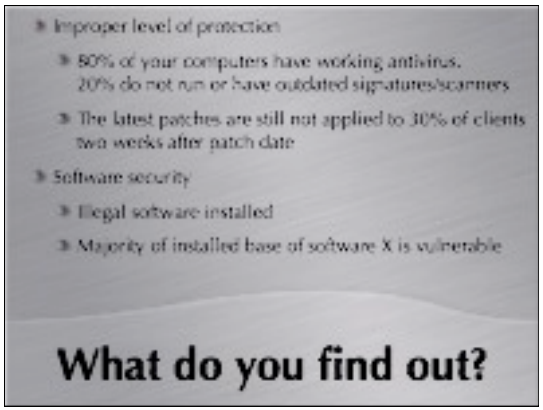
14


Improper level of protection
80% of your computers have working antivirus. 20% do not run or have outdated signatures/scanners
The latest patches are still not applied to 30% of clients two weeks after patch date
Software security
What do you find out?

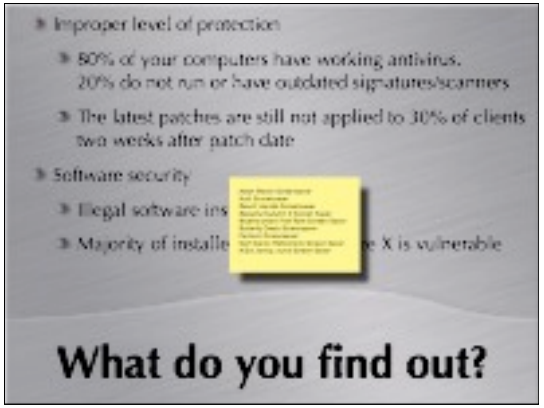
14


Improper level of protection
80% of your computers have working antivirus. 20% do not run or have outdated signatures/scanners
The latest patches are still not applied to 30% of clients two weeks after patch date
Software security
Illegal software installed
What do you find out?

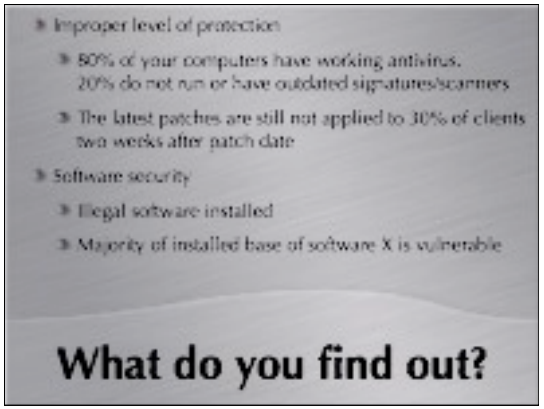
14


Improper level of protection
80% of your computers have working antivirus. 20% do not run or have outdated signatures/scanners
The latest patches are still not applied to 30% of clients two weeks after patch date
Software security
Illegal software installed
Majority of installed base of software X is vulnerable
What do you find out?

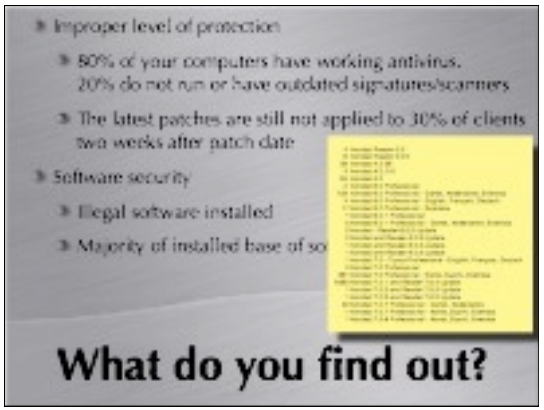
14


Improper level of protection
80% of your computers have working antivirus. 20% do not run or have outdated signatures/scanners
The latest patches are still not applied to 30% of clients two weeks after patch date
Software security
Illegal software ins
Majority of installe
e X is vulnerable
What do you find out?

14


Improper level of protection
80% of your computers have working antivirus. 20% do not run or have outdated signatures/scanners
The latest patches are still not applied to 30% of clients two weeks after patch date
Software security
Illegal software installed
Majority of installed base of software X is vulnerable
What do you find out?

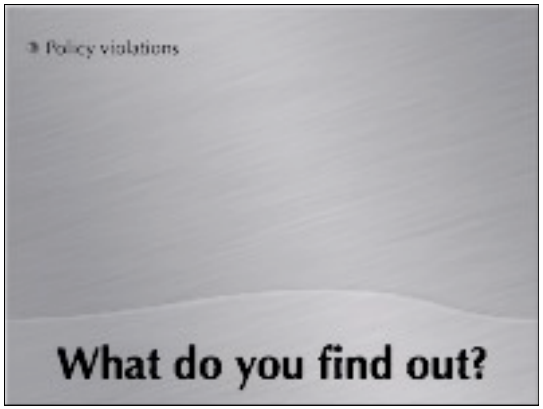
14


Improper level of protection
80% of your computers have working antivirus. 20% do not run or have outdated signatures/scanners
The latest patches are still not applied to 30% of clients two weeks after patch date
Software security
Illegal software installed
Majority of installed base of so
What do you find out?

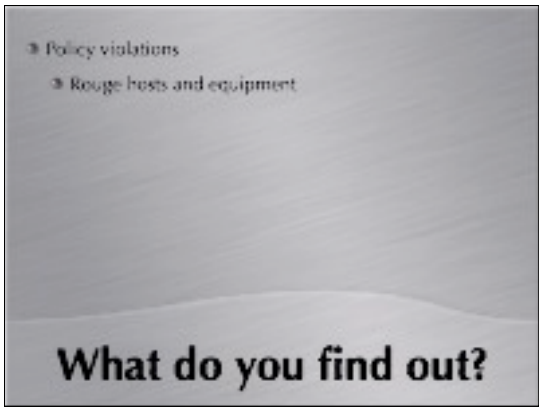
14


What do you find out?

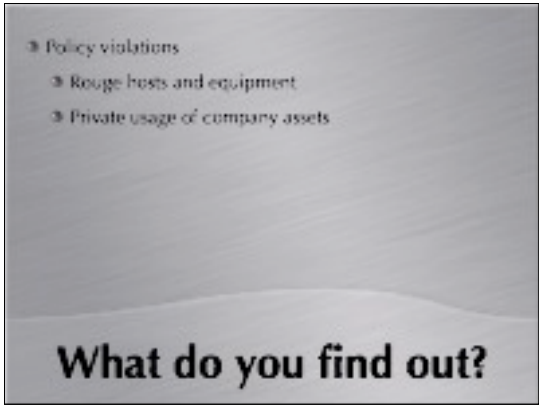
15


Policy violations
What do you find out?

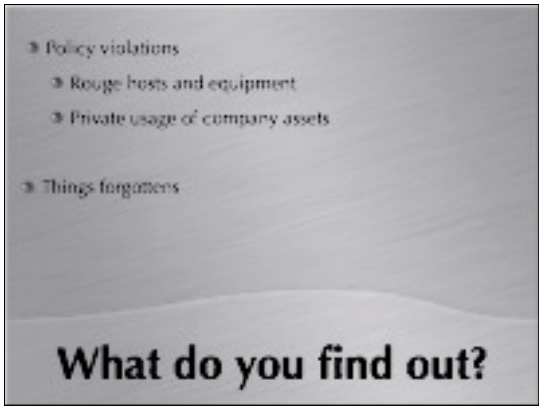
15


Policy violations
Rouge hosts and equipment
What do you find out?

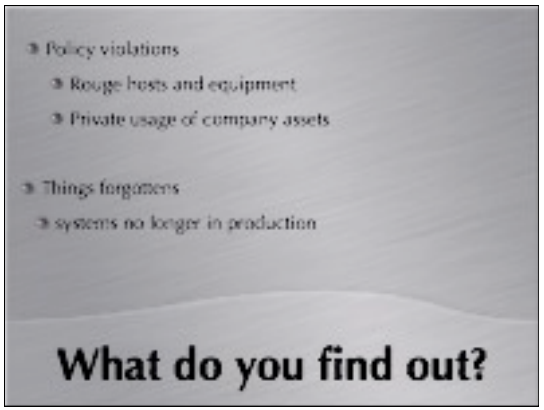
15


Policy violations
Rouge hosts and equipment
Private usage of company assets
What do you find out?

15


Policy violations
Rouge hosts and equipment
Private usage of company assets
Things forgotten
What do you find out?

15


Policy violations
Rouge hosts and equipment
Private usage of company assets
Things forgotten
systems no longer in production
What do you find out?

15

- Policy violations
  - Rouge hosts and equipment
  - Private usage of company assets
- Things forgotten
  - systems no longer in production
  - connections that nobody in charge have knowledge about

What do you find out?

15

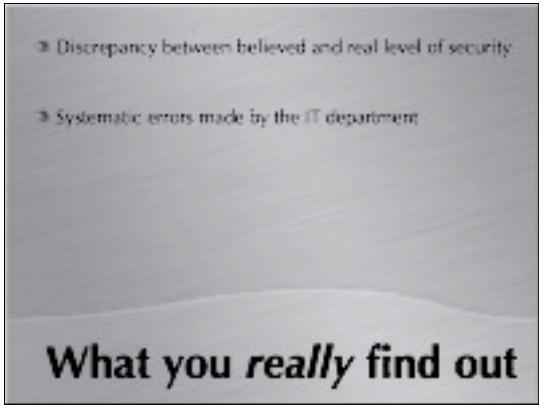
What you *really* find out

16

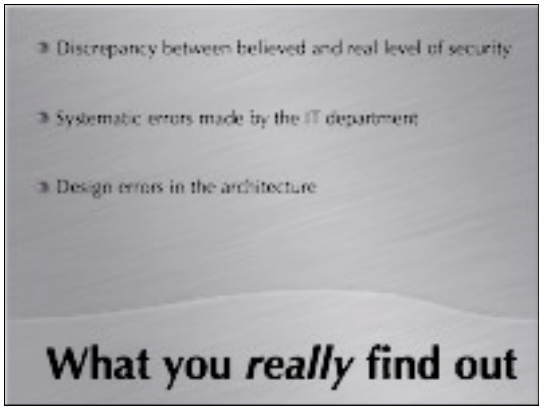
- Discrepancy between believed and real level of security

What you *really* find out

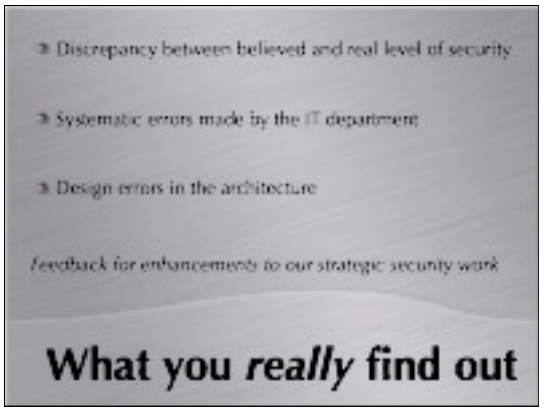
16


Discrepancy between believed and real level of security
Systematic errors made by the IT department
What you *really* find out

16


Discrepancy between believed and real level of security
Systematic errors made by the IT department
Design errors in the architecture
What you *really* find out

16


Discrepancy between believed and real level of security
Systematic errors made by the IT department
Design errors in the architecture
Feedback for enhancements to our strategic security work
What you *really* find out

16

What is the status?

- **Hot infosec business focus**
  - IBM snaps up ISS, McAfee buys Preventsys, Symantec aquire BindView, Sygate and Foundstone
- Roll your own
  - 1 FTE for development and operations
  - Lots of effort for cleaning-up and fixing

17

Finishing up

- To govern, your strategies and practices must be adequate, achieve objectives and continously adapt to changing parameters such as threat landscapes
- Know what you are doing and find simpe way of doing it
- Quality improvements is to find and eliminate the weak links in the governance!

18

Summary

We must to regain control

We do not need *more* security, we need **better** security and **smarter** usage of information we already have

Implement methods and tools to aid the strategical security work

19