
It Security Scenarios: Strategies & Technology for the next 5 years

CSO Interchange

Jay Heiser

4 Seasons Hotel
London, England
8 December 2005

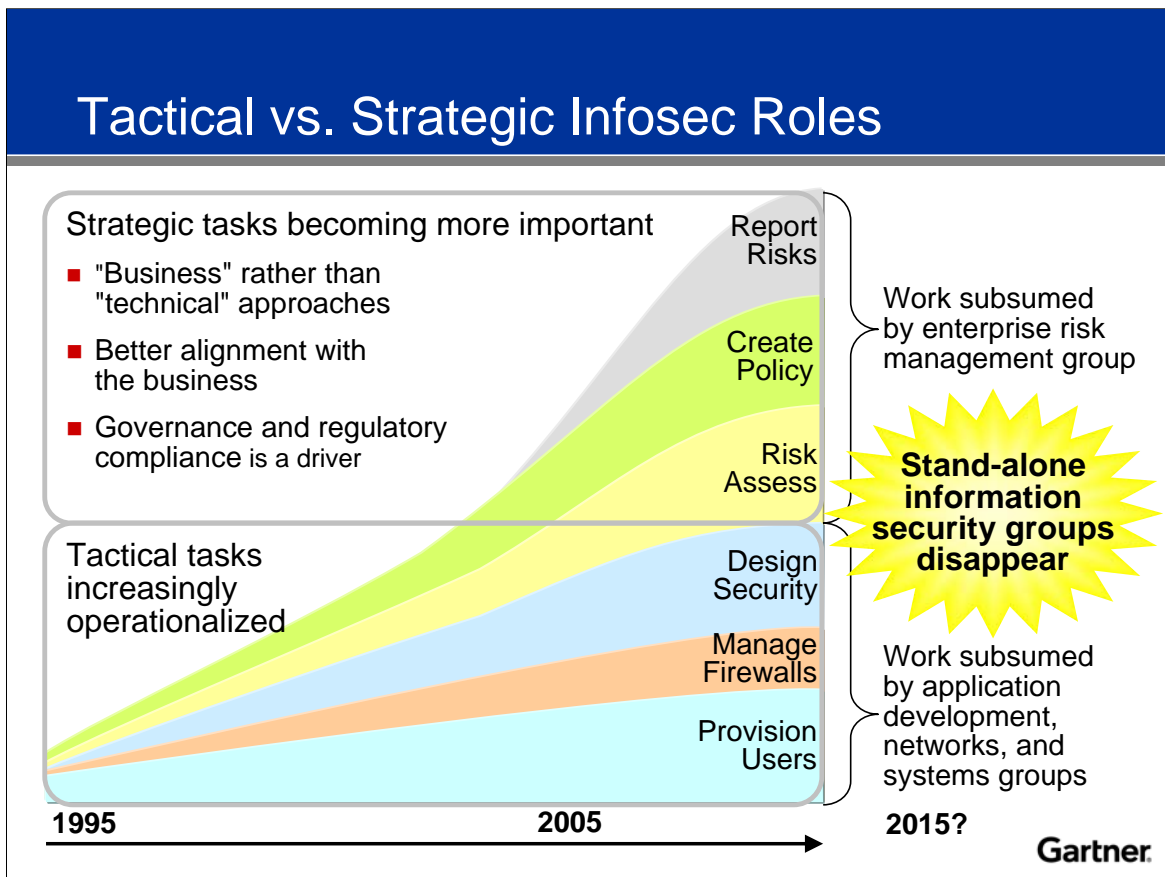


Arguably, the information security profession has spent most of the past 10 to 15 years addressing nuisance threats from outside the company (that is, "hackers"). During the same time period, a growing number of sophisticated cybercrimes have made the news. Home banking customers have lost money through "phishing" attacks, credit card information has been stolen in wholesale quantities and sophisticated industrial espionage attacks have been carried out through the use of "spyware."

Organized crime has been involved in "cyberspace" for at least a decade, and criminals continue to become more sophisticated in their abilities. Software providers have learned a great deal about the techniques and processes involved in creating better code, but any additional robustness tends to be overcome by the introduction of new features, which always bring new vulnerabilities.

Security professionals are making progress, but so are the attackers. The rate of failure may be decreasing, but the number of high-loss incidents seems to be increasing.

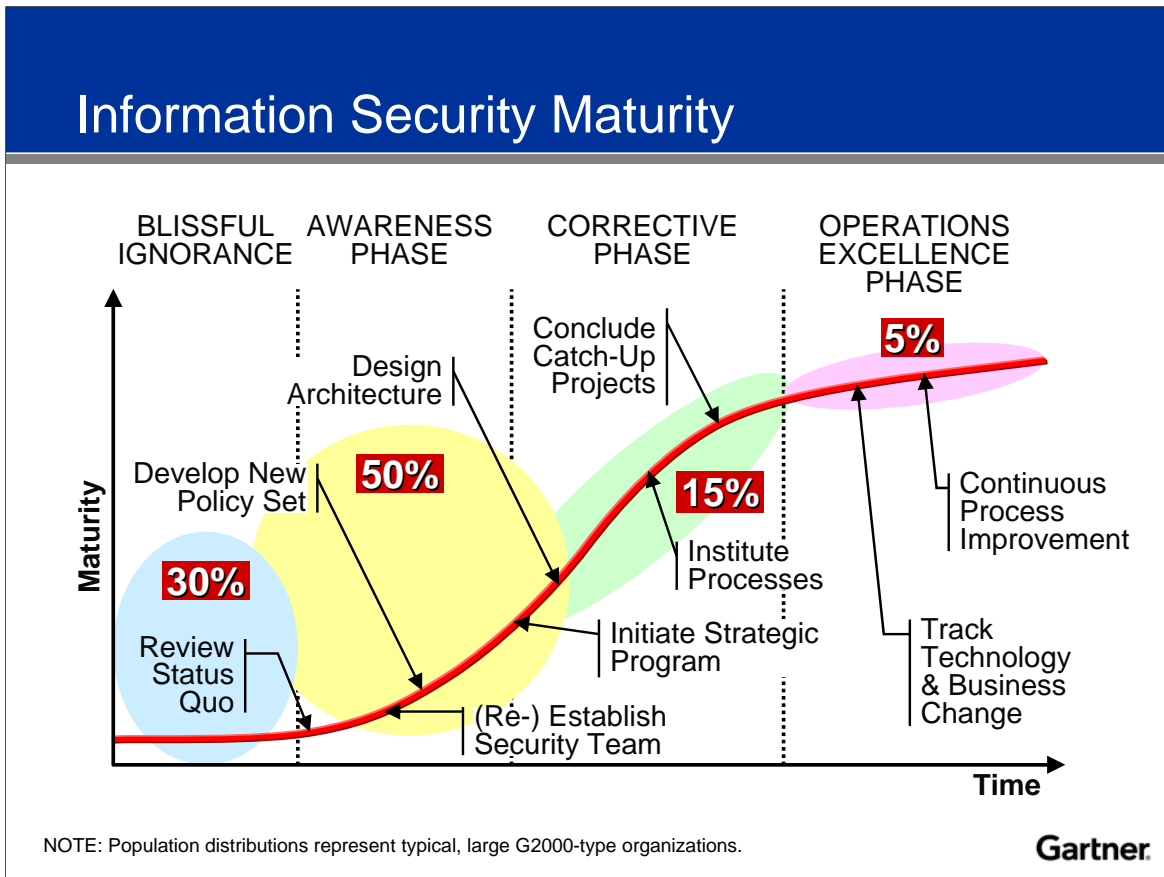
Strategic Planning Assumption: Organizational experimenting will continue, as 70 percent of enterprise-class organizations will make changes in their information security reporting structure during the next 3 years (0.8 probability).



Ten years ago, information security tasks were predominately operational. User provisioning, security configuration and perimeter management have changed in detail during the past decade, but they have not changed in significance. Organizations have transferred knowledge of these tasks to persons with relatively less experience, and the available products have become more sophisticated and automated, which allows the same functions to be performed at a lower personnel cost. These functions can be categorized as tactical.

During the same 10 years (and, arguably, at an increasing rate during the past two to five years), the emphasis in the information security space has become more strategic — particularly at the very largest corporate and government organizations. The ability to determine what constitutes risk, and particularly the privilege of reporting that risk to executive decision makers, is a highly political activity. In most cases, it is a privilege that has been denied to technically oriented information security specialists, who have been forced to report their concerns up through the filter of the CIO's organization.

Information security is being given greater independence. The CISO is being given a reporting mechanism that lies outside the IT department through either a "dotted-line" report to a CFO, CRO or CCO, or even a direct report. This is viewed as an important governance mechanism — particularly in highly regulated organizations. In theory, the CISO is able to provide a more realistic picture of IT risk when not subjected to the pressures of accommodating IT's agenda.

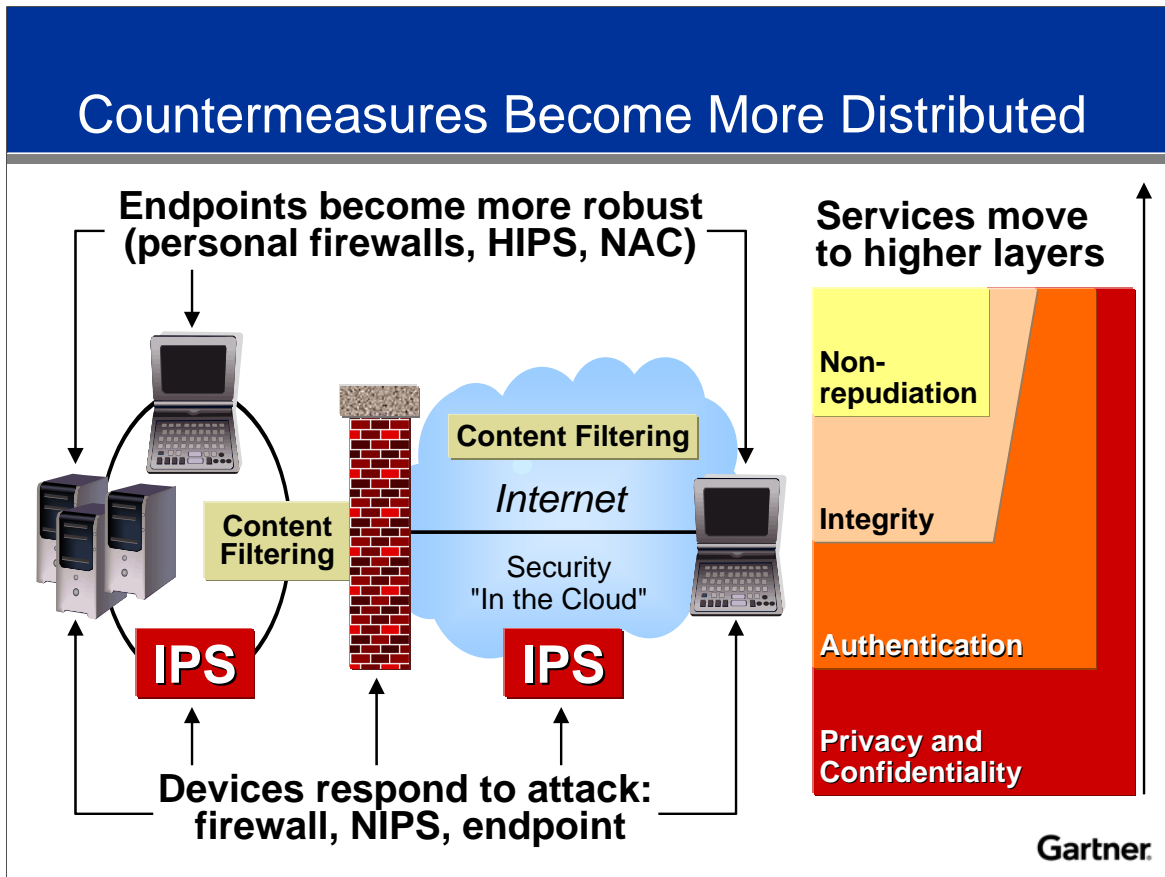


Client Issue: What does an IT security director need to know about organizational risk management?

This graph shows the relative maturity of organizations with regard to security programs. Along the curve are the milestones that mark a maturing organization, starting with an assessment of current state and then the establishment of a security team. Moving up the curve we see the initiation of a strategic program as the beginning of the first real improvement. It is part of this program where we see the creation of domains and the associated trust levels (or security baselines) that will characterize a mature and useful program.

Real progress hits with an architecture that supports domains and trust. Instituting processes move an organization out of the ad hoc reactive mode and into the proactive mode. Processes are repeatable, survivable and measurable, and they can be improved on an ongoing basis.

At the top of the curve, organizations have reached a maturity level where they have organized all the processes and now focus on improving good practice. Notice that we show 80 percent of organizations in the initiation phase or the lowest levels of this maturity. Fifteen percent are working hard on maturing their processes and few, less than 5 percent, are in the highest levels of maturity.

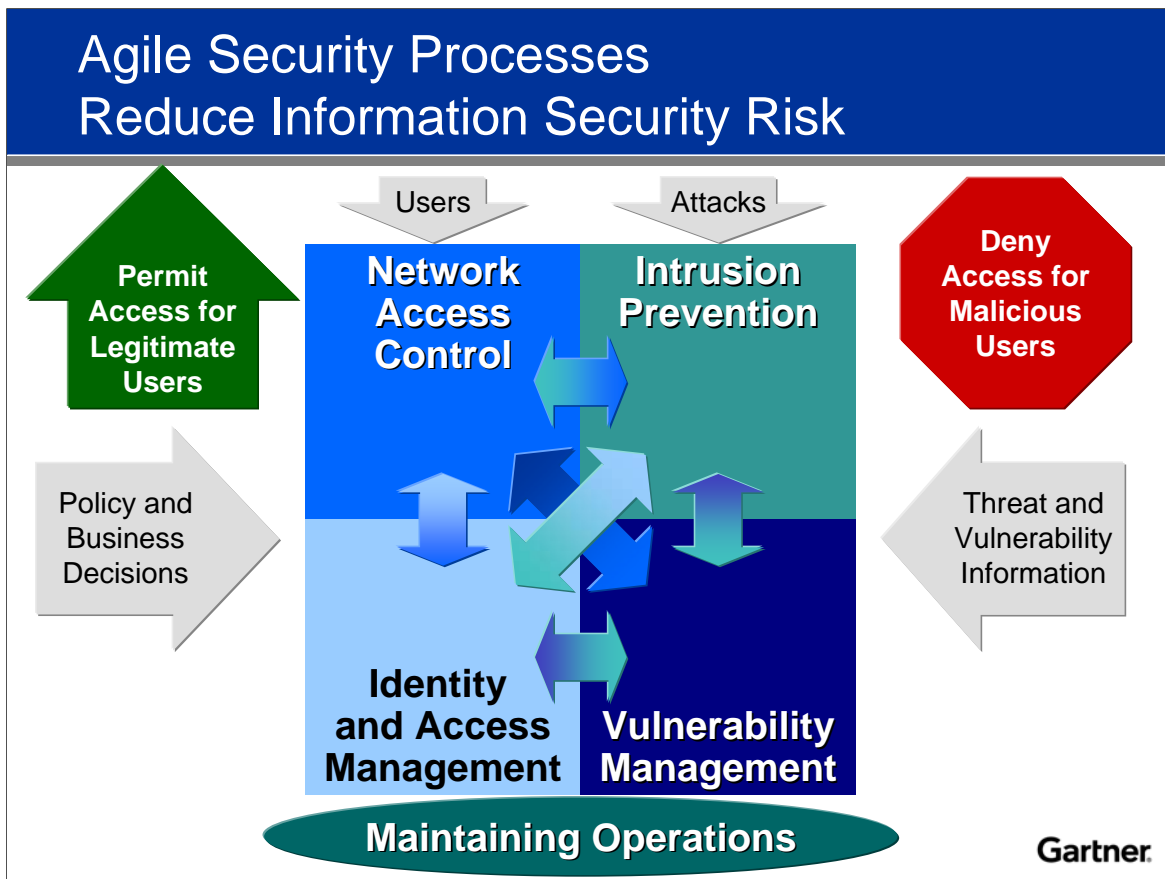


In the past, security tended to focus on the firewall. This was a useful expedient, and firewalls continue to represent one of the most significant forms of security control. However, security functionality is being spread out across the entire Internet, largely because PCs (particularly laptops) are suffering increasingly from attacks that firewalls cannot address. Most of these attacks are external in origin, but some originate from inside the organization, and these can be quite costly.

Greater levels of security technology will be applied to all endpoints, but particularly to Windows-based systems, and systems that travel. Centrally administered technology is becoming a common means of ensuring that the security functionality is performing consistently. In addition, security is subject to outsourcing, which will continue to become more popular in areas where outsourcing is relatively straightforward, such as filtering content for hostile code or spam.

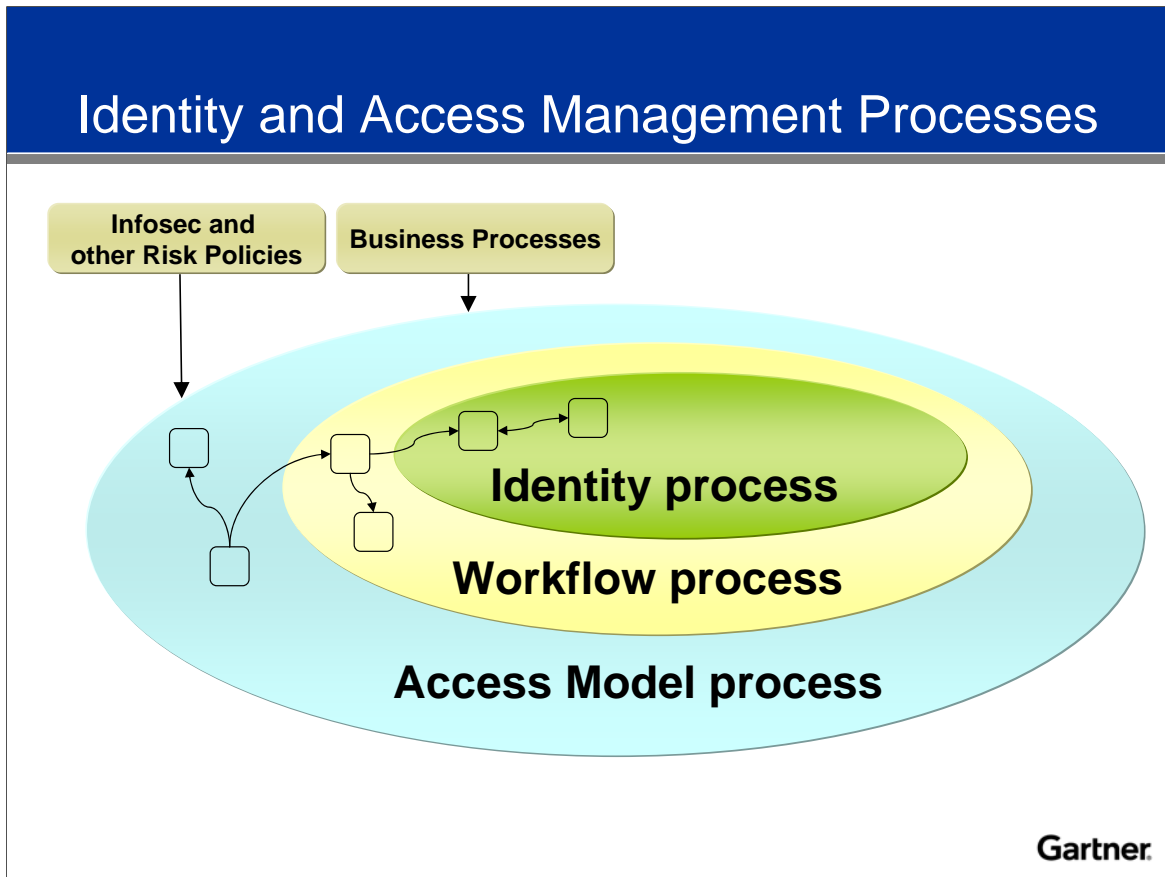
Increased distribution involves a change in the network or hardware abstraction layer where services are applied as well. It is no longer feasible to rely on the platform infrastructure to protect access to data or to provide assurance as to its origin. Technologies such as digital rights management and Web services security protocols are encapsulating security controls along with the data. This provides greater flexibility and greater granularity, and it allows the security mechanisms to persist through time and space.

Strategic Planning Assumption: Through 2007, 80 percent of damage-causing events will be preventable by careful implementation of NAC, intrusion prevention, IAM and vulnerability management processes (0.7 probability).



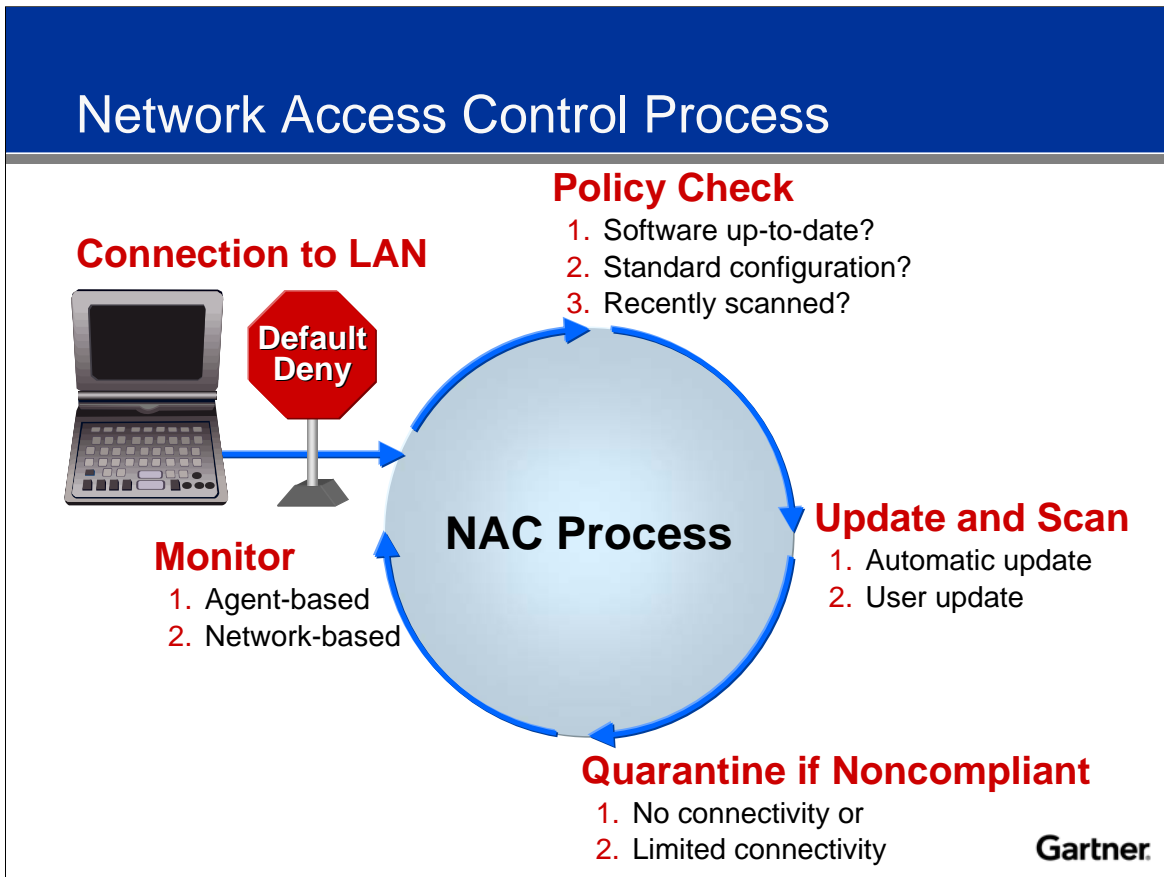
In its search for the "grand unified theory of security," Gartner has defined four high-level security processes that are key to the effectiveness and efficiency of enterprise security programs. These processes are network access control (NAC), intrusion prevention, identity and access management (IAM), and vulnerability management.

These processes address most of the active security efforts that organizations need to avoid compromising their systems, network and data. Many other important security activities (such as business continuity planning or disaster recovery, and incident response) make up a complete security program, but these four key processes represent the primary areas where external threats and new technologies demand agile security processes to meet constantly changing demands.



Identity management and the provisioning of access to company resources involves the careful execution of three processes: the access model process, the workflow process and the identity process. The access model process maps established business policies to roles and rules to be used when creating and managing an identity. Relevant factors include information security policies, separation of duties (SOD) rules, customer requirements and external influences, such as government and industry regulations. The workflow process takes established business policies, such as business processing and approval requirements, and establishes the step-by-step flow of how an identity is created.

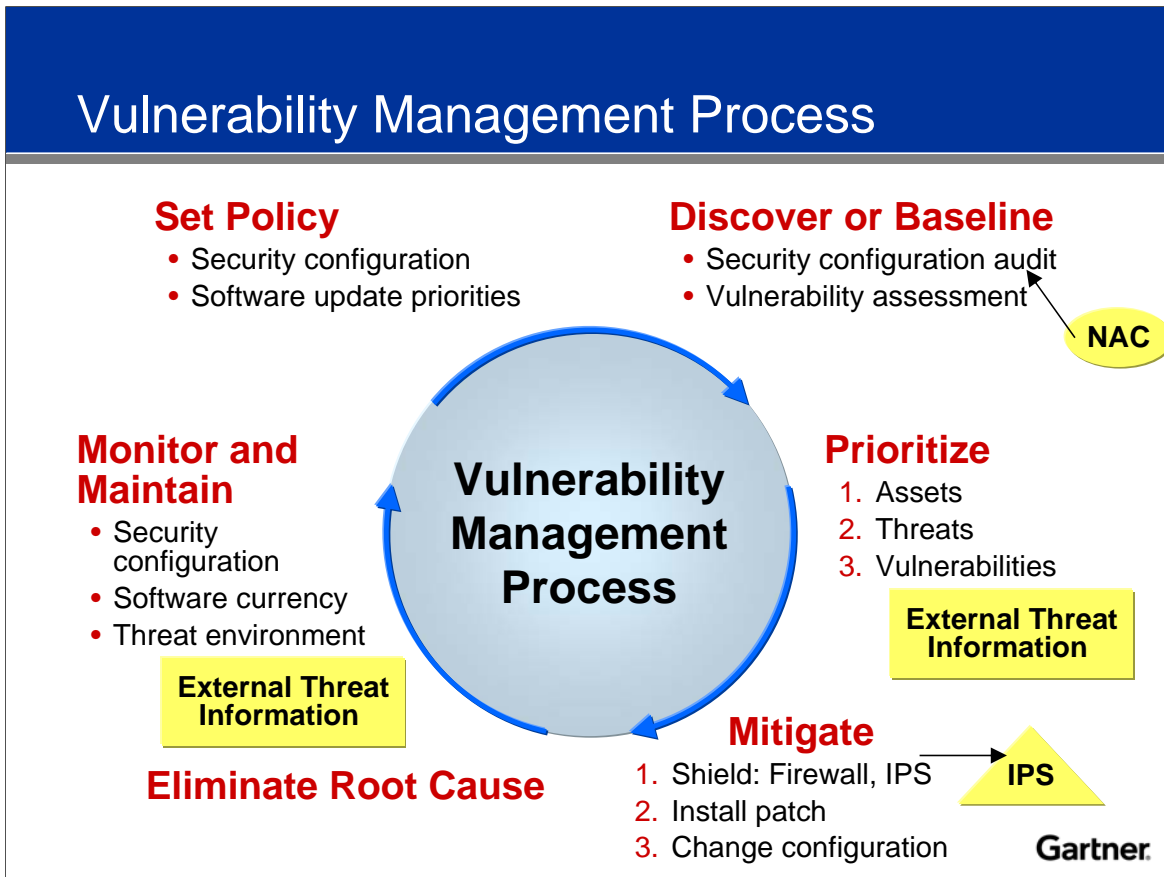
The identity process is where the mapping of the roles, rules and workflow for a specific user comes together to create an account (or set of accounts) on a target or, more likely, a set of target platforms. This ensures that the user will have all the account attributes and privilege assignments needed to access company resources. Each process includes six common actions: create, use, change, report, log and retire.



Perimeter firewalls and antivirus gateways are circumvented when PCs connect remotely via a VPN, or when a laptop or other mobile platform is brought into the office and directly connected to the corporate network. Four damage scenarios are possible:

- A corporate laptop that is only occasionally connected to the internal network is not accessible for patch installation. It spends time outside the corporate firewall, is corrupted with a worm and connects to the internal network via an IP Security (IPsec) VPN or remote-access server (RAS) connection.
- A home PC that is used by an employee for work purposes is corrupted with a worm and establishes an IPsec VPN or other RAS connection to the internal network.
- A laptop or other mobile platform that is owned by a contractor or other external entity is infected with a worm and connects to the internal network via an IPsec VPN, RAS or an Ethernet port at a corporate site.
- An employee's personal mobile device is infected with a worm and is connected to the network via an Ethernet port at a corporate site.

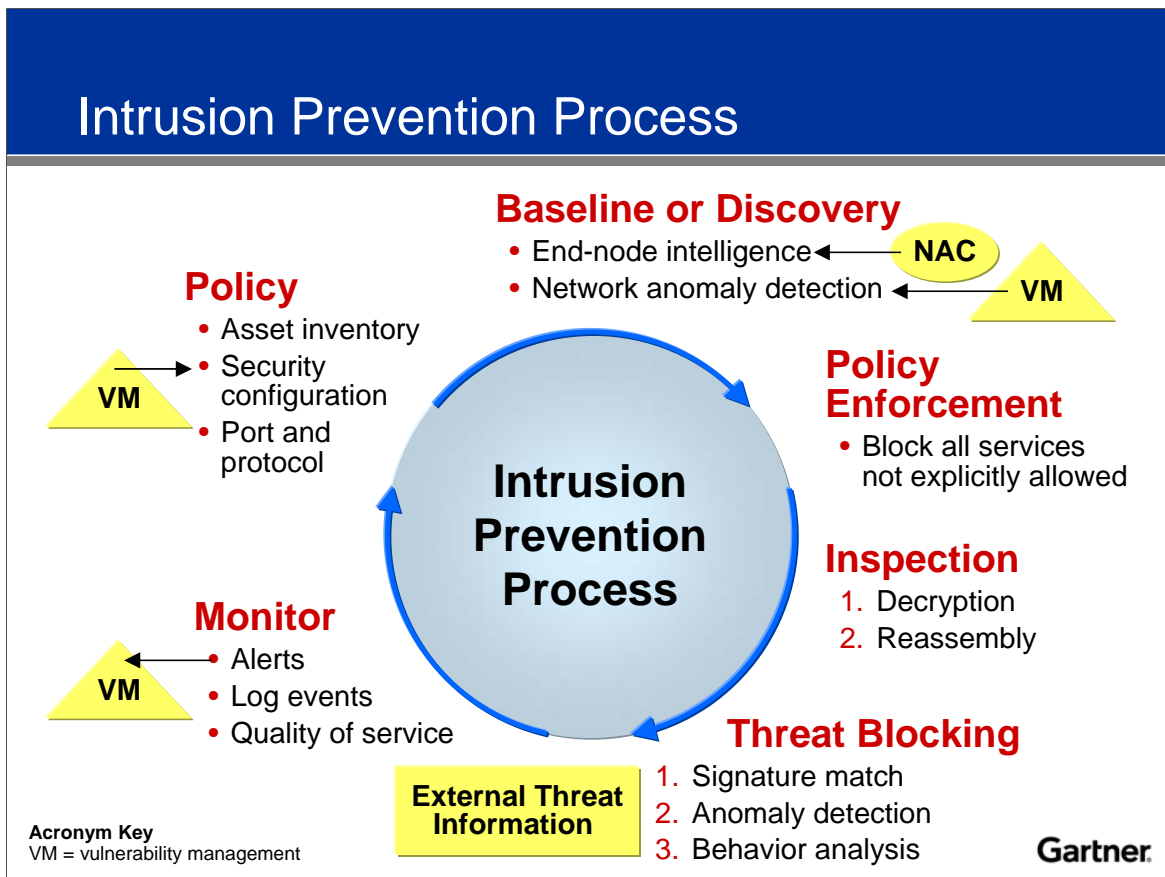
An NAC solution compares the security state of a device that is attempting to connect to a network with a set of policy attributes that define which security conditions must be met to allow network access. The scope of an NAC solution needs to encompass external and internal network connections by managed and unmanaged devices. The NAC solution should cover these network connection scenarios: IPsec and SSL VPNs, wired and wireless LANs, and dial-in via RASs.



A vulnerability management effort should start with the definition of policies for security configuration management, along with those for identity and access. The next step is to discover all systems that can access the corporate network and then baseline the systems with respect to known vulnerabilities and policy compliance. Mitigation efforts need to be based on a prioritized list. Prioritization should be based on knowledge of the current threat environment and the business use or criticality of vulnerable assets. Effective network and host-level shielding can protect vulnerable assets until mitigation work can be completed. The next step is to mobilize a wide variety of operations and support groups to mitigate high-risk vulnerabilities.

Eliminating a vulnerability is important, but eliminating the root cause will prevent the reintroduction of vulnerabilities that have been resolved. In many cases, the root cause lies in weak system configuration or user administration processes or inadequate or nonexistent change management. In addition, a comprehensive vulnerability management program should include active vulnerability and compliance monitoring, and well-defined incident response and control processes.

Strategic Planning Assumption: By 2006, organizations that rely only on proxy or stateful packet inspection will experience successful application-layer attacks at twice the rate of organizations that use leading deep-packet inspection approaches (0.6 probability).



Firewalls have always carried out their role of defending the network perimeter well. However, because attacks do slip past their simple rule sets, which are often misconfigured, there has long been a desire for additional layers of network defense. For several years, it was hoped that intrusion detection systems (IDSs) would fulfill this role, but they pose a problem for most IT departments: IDS agents need to be monitored continuously to be effective. In most cases, IT was surprised by the level of constant support that IDSs needed. This gave rise to the managed security service market.

Products have been developed that approach the problem of internal defense more logically. A security administrator would rather install agents that act to protect the hosts and networks on which they reside than agents that report when malicious activity is occurring. Intrusion prevention is not an easy task because it requires efficient detection of malicious attacks. Network IDS vendors are struggling constantly to decrease false positives, while increasing throughput. Well-designed network agents should use a combination of signature, protocol anomaly detection and traffic analysis to minimize false positives. The concept of state awareness will allow network agents to scale to the multigigabit speeds needed. They should be in line to allow them to drop sessions. Host intrusion detection agents should lock down the operating systems and applications that reside there. Violations of policy at the system call or network layers should be blocked.

IT Risk Management & Compliance

*Andreas Wuchner
Head Global IT Security*

December 2005

© 2005 Novartis Pharma AG

Author: Andreas Wuchner

Date: 28.11.2005



IT Risk Management



Who & What

Health Status

Risk Assessment
Business Impact
Analysis

$$\text{RISK} = \frac{(\text{Threat} \times \text{Vulnerability})}{\text{Countermeasures}} \times \text{Business Value}$$

Preventive Controls

The Technology View



U1 BIND Domain Name System (0)

No vulnerabilities found in this category.

U2 Web Server (12)

- ▶ 5 Apache Chunked-Encoding Memory Corruption Vulnerability (23)
- ▶ 5 OpenSSL SSLv2 Malformed Client Key Remote Buffer Overflow Vulnerability (4)
- ▶ 5 OpenSSL ASN.1 Parsing Vulnerabilities (3)
- ▶ 4 OpenSSL ASCII Representation Of Integers Buffer Overflow Vulnerability (4)
- ▶ 4 htmlscript CGI Directory Traversal Vulnerability (1)
- ▶ 3 Apache Tomcat Servlet Mapping Cross Site Scripting Vulnerability (4)
- ▶ 3 "test-cgi" CGI Vulnerability (5)
- ▶ 5 Apache Win32 Batch File Remote Command Execution Vulnerability (13)
- ▶ 5 PHP Strip_Tags() Function Bypass and Heap Overflow Vulnerability (5)
- ▶ 5 Apache Basic Authentication Module Valid User Login Denial of Service Vulnerability (1)
- ▶ 5 PHP Post File Upload Buffer Overflow Vulnerability (2)
- ▶ 4 Apache Mod_SSL Buffer Overflow Vulnerability (4)

U3 Authentication (0)

No vulnerabilities found in this category.

U4 Version Control Systems (1)

- ▶ 5 CVS Malformed Entry Modified and Unchanged Flag Insertion Heap Overflow Vulnerability (1)

U5 Mail Transport Service (4)

- ▶ 3 Sendmail ETRN Command Denial of Service Vulnerability (11)
- ▶ 5 Sendmail Header Processing Buffer Overflow Vulnerability (22)
- ▶ 5 Sendmail Address Prescan Possible Memory Corruption Vulnerability (2)
- ▶ 5 Sendmail Prescan() Variant Remote Buffer Overrun Vulnerability (4)

U6 Simple Network Management Protocol (SNMP) (5)

- ▶ 4 Writeable SNMP Information (439)
- ▶ 4 Wired-side SNMP WEP key exposure in 802.11b Access Points (3)
- ▶ 3 Readable SNMP Information (803)
- ▶ 5 Multiple Vendor SNMP Request and Trap Handling Vulnerabilities (880)
- ▶ 5 Sun Solaris snmpXdmdid Buffer Overflow Vulnerability (2)

U7 Open Secure Sockets Layer (SSL) (5)

- ▶ 5 OpenSSL SSLv2 Malformed Client Key Remote Buffer Overflow Vulnerability (4)
- ▶ 5 OpenSSL ASN.1 Parsing Vulnerabilities (3)
- ▶ 4 OpenSSL ASN.1 Parsing Error Denial of Service Vulnerability (4)
- ▶ 4 OpenSSL ASCII Representation Of Integers Buffer Overflow Vulnerability (4)
- ▶ 5 OpenSSL Timing Attack RSA Private Key Information Disclosure Vulnerability (8)

U8 Misconfiguration of Enterprise Services NIS/NFS (3)

- ▶ 3 NFS Exported Filesystems List Vulnerability (31)
- ▶ 5 Statd Format Bug Vulnerability (1)
- ▶ 5 NFS Exported Directories Mountable by Unauthorized Users (14)

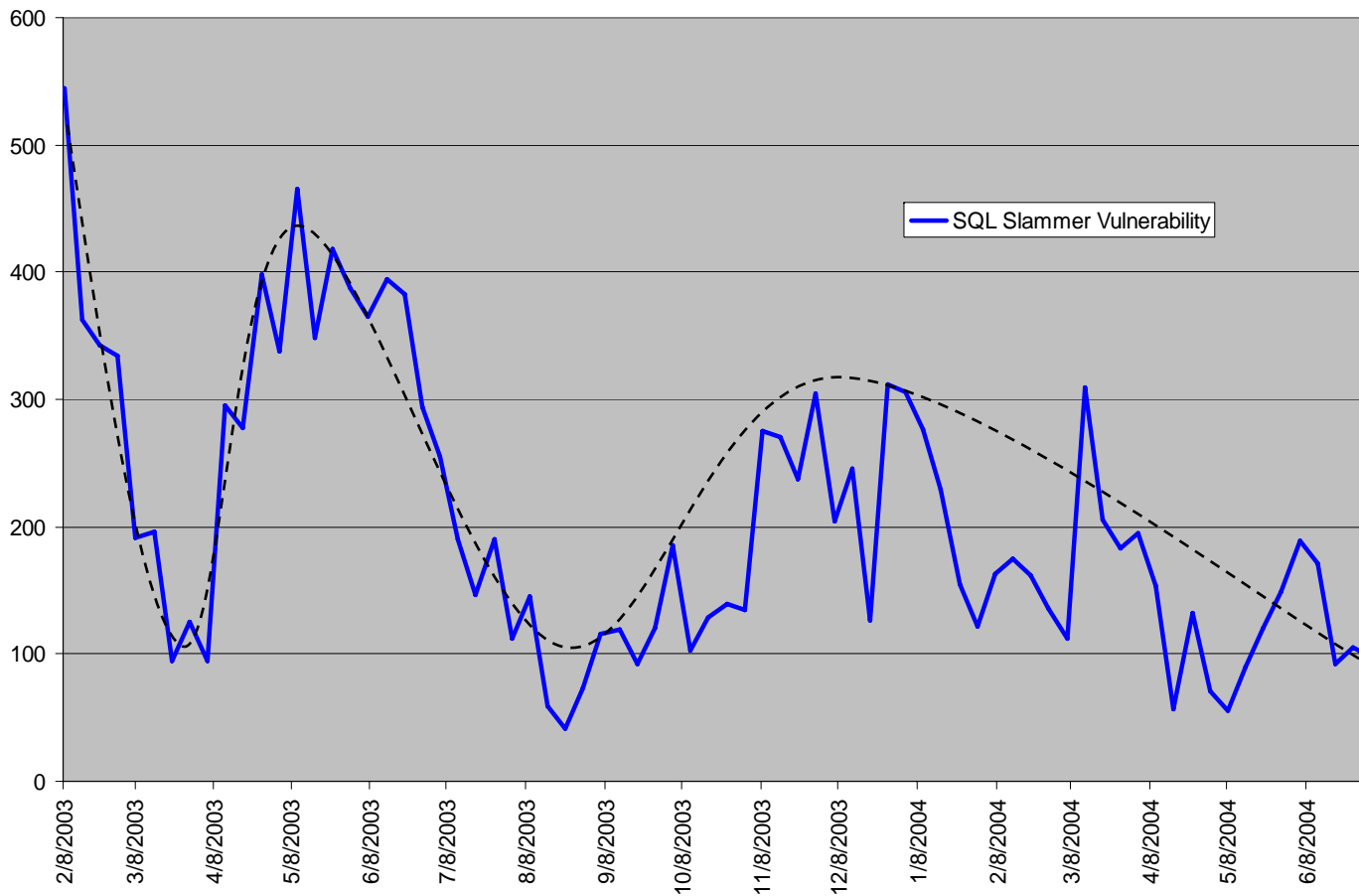
U9 Databases (12)

- ▶ 5 MySQL COM_CHANGE_USER Password Length Account Compromise Vulnerability (1)
- ▶ 5 MySQL COM_TABLE_DUMP Memory Corruption Vulnerability (1)
- ▶ 5 MySQL COM_CHANGE_USER Password Memory Corruption Vulnerability (1)
- ▶ 3 MySQL Authentication Algorithm Vulnerability (3)
- ▶ 5 MySQL mysqld Privilege Escalation Vulnerability (1)
- ▶ 5 MySQL libmysqlclient Library Read_Rows Buffer Overflow Vulnerability (1)
- ▶ 4 Oracle Database Server ORACLE.EXE Buffer Overflow Vulnerability (17)
- ▶ 4 Oracle Database Link Buffer Overflow Vulnerability (72)
- ▶ 4 Oracle Database Server EXTPROC Buffer Overflow Vulnerability (56)
- ▶ 4 Multiple Oracle Buffer Overflow Vulnerabilities (26)
- ▶ 4 MySQL Double Free Heap Corruption Vulnerability (1)
- ▶ 4 MySQL Password Handler Buffer Overflow Vulnerability (3)

U10 Kernel (1)

- ▶ 2 Linux ICMP Kernel Information Leakage Vulnerability (13)

The Technology View

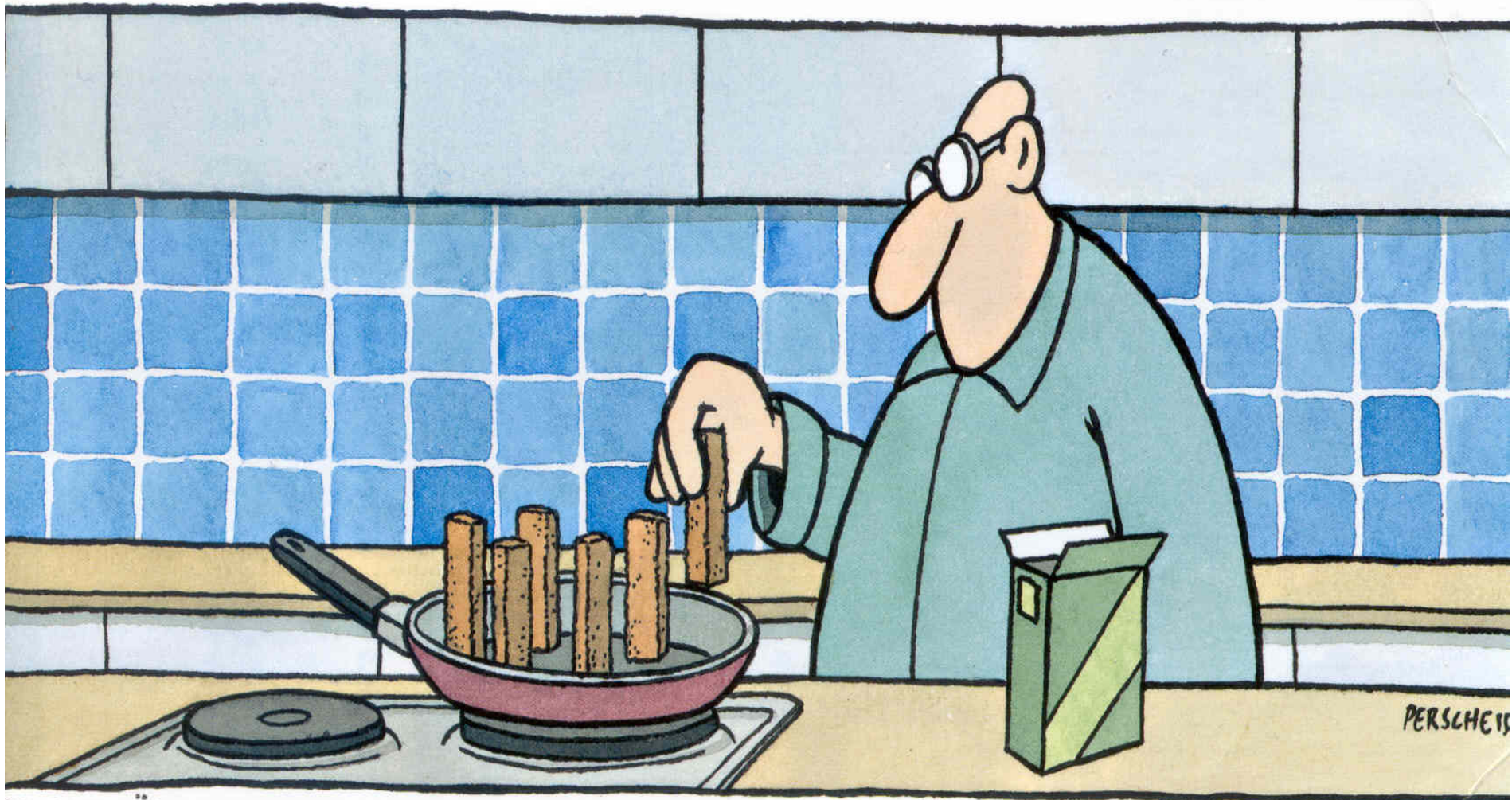


**MS-SQL 8.0 UDP
Slammer Worm Buffer
Overflow Vulnerability**

**CAN-2002-0649
Qualys ID 19070**

Released: July 2002

Compliance ?

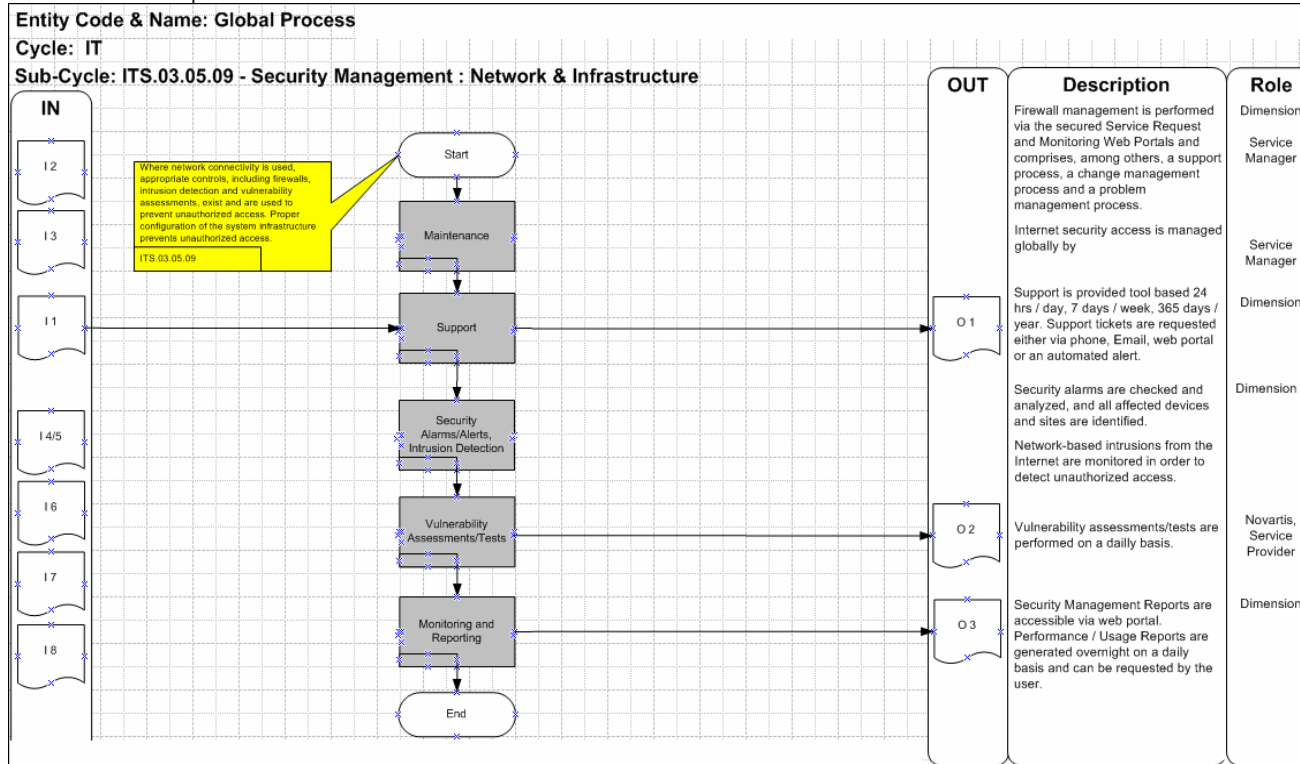


DIE FISCHSTÄBCHEN UNAUFGETAUT DER PACKUNG ENTNEHMEN UND 5-7 MIN. VON ALLEN SEITEN BRATEN.

The Control's View



| | |
|------------------------------------|---|
| Sub Cycle Description | Security Management - Network and infrastructure |
| Key Control Objective Description | Managing systems security includes both physical and logical controls that prevent unauthorized access. These controls typically support authorization, authentication, nonrepudiation, data classification and security monitoring. Actions performed in this area align with the control activities, information and communication, and monitoring components of COSO. Deficiencies in this area could significantly impact financial reporting. For instance, insufficient controls over transaction authorization may result in unreliable financial reporting and disclosure controls. |
| Key Control Activities Description | 1) Where network connectivity is used, appropriate controls, including firewalls, intrusion detection and vulnerability assessments, exist and are used to prevent unauthorized access. Proper configuration of the system infrastructure prevents unauthorized access. |



Operational Integrity of IT



| | GxP Compliance | Information Security | Business Continuity Mgmt. | Finance Compliance |
|-----------------------------------|---|---|--|--|
| External Regulation | U.S. 21 CFR, EU Guides, OECD, ICH Guidelines, ... | | | U.S.: Sarbanes-Oxley Act |
| Industry Best Practice | | | | |
| | | ISF (Info. Security Forum) | | |
| | | | | |
| | COBIT (Control Objectives for Information and related Technology) | | | |
| Internal Regulation | ITIL (IT Infrastructure Library) | | | |
| | | ISO 17799 / BS 7799 | | |
| | Quality System: - Functional Quality Manuals incl. Computerized Systems General Requirements Development and Validation Operation and Retirement Infrastructure | Policy & Key Directives: - Security Policy - Group Policy on Information Security - Key Directives Information Security | Corp. HSE and BC Guideline: Business Continuity Management | COSO - Control Objects for Sarbanes-Oxley <i>(under development)</i> |
| IT Quality Handbooks | | | | |

The Needs



- Translation is needed
- Complex technology into control oriented language
- Automation as much as possible
- Continues collection of data
- Color based reporting system
- Easy interface for the control testers (internals without technology background)
- Easy interface for the auditors (control & process experts)

The Approach



Discovery

Accurate identification of systems
Accurate identification of vulnerabilities of these systems

Assessment

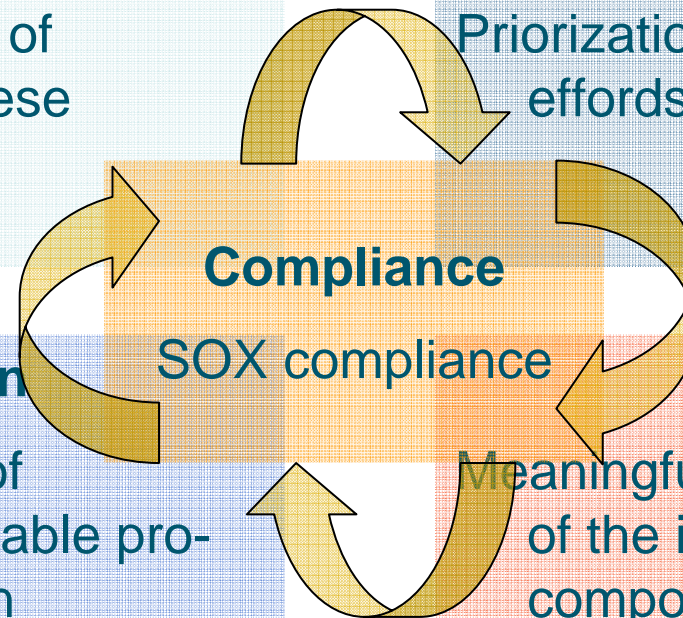
Calculation of thread severities
Priorization of remediation efforts

Remediation

Continious discovery of vulnerabilities to enable pro-actively remediation
Pro-active reduction of vulnerabilities to reduce the impact of possible threads

Analysis

Meaningful reports on the status of the infrastructure components on global, regional an local level



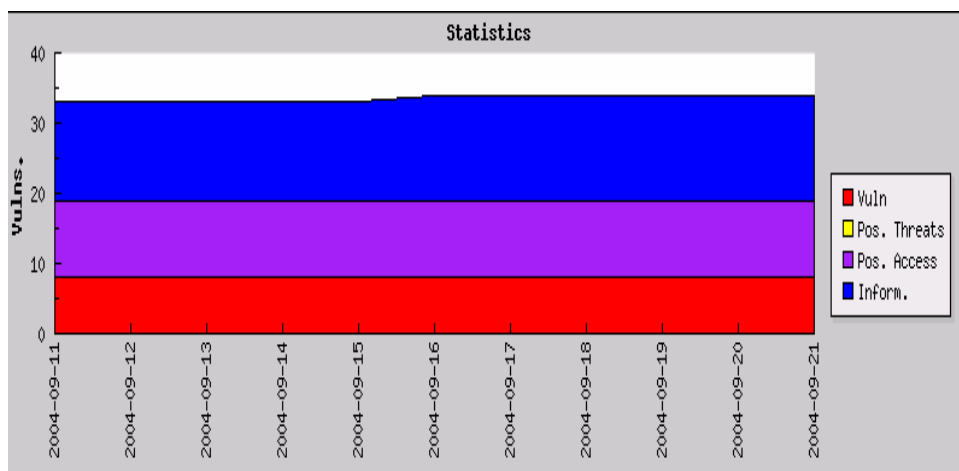
The SeTraSys Tool (www.setrasys.net)



[Taipei NP]

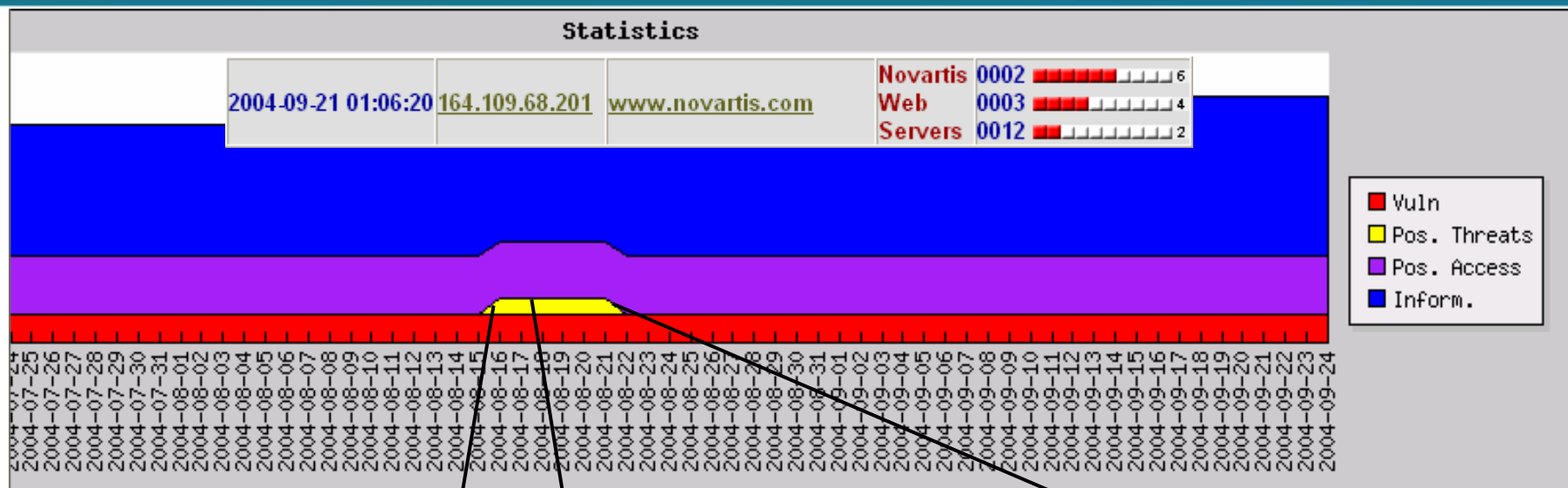
| Last succ. scan: | | Last succ. scan within 72h | | Targets (within 72h): | | | | |
|------------------|-------|----------------------------|-------|-----------------------|---------------------------|------------|-----------|---------------------|
| Amount | Level | Amount | Level | Scandate | IP | Sym. Name | Location | Amount / Sev. Level |
| 3 | | 3 | | 2005-03-04 18:00:10 | 10.10.0.1 | FW 1 | Taipei NP | 0001 |
| 5 | | 5 | | | | | | 0001 |
| 4 | | 4 | | | | | | 0014 |
| 27 | | 27 | | 2005-03-04 18:00:10 | 10.10.0.2 | Router ISP | Taipei NP | 0002 |
| | | | | | | | | 0005 |
| | | | | | | | | 0003 |
| | | | | | | | | 0013 |

Statistic:



- Detailed overview by country / side
- Granular detail view for every single device
- Trend / statistic available per country / side

The SeTraSys Tool (www.setrasys.net)



- Additional threat appears
- Automated mail to owner will be sent
- Change management process initiation

- Threat evaluation
- Testing
- Qualifications
- Documentation

- Threat disappeared
- Automated mail to owner will be sent
- Change ticket closing
- Normal operation

Detected vulnerabilities (2)

6 Web Server HTTP Trace/Track Method Support Cross Site Tracing Vulnerability (Port: 80)

4 Web Server Predictable Session ID Vulnerability (Port: 80)

Possible Threats (0) (-1)

Solved:

4 Apache mod_usertrack Predictable ID Generation Vulnerability

Scan Results www.novartis.com

Questions?

Contact

Andreas Wuchner

Email: andreas@wuchner.info

Thank you for your interest



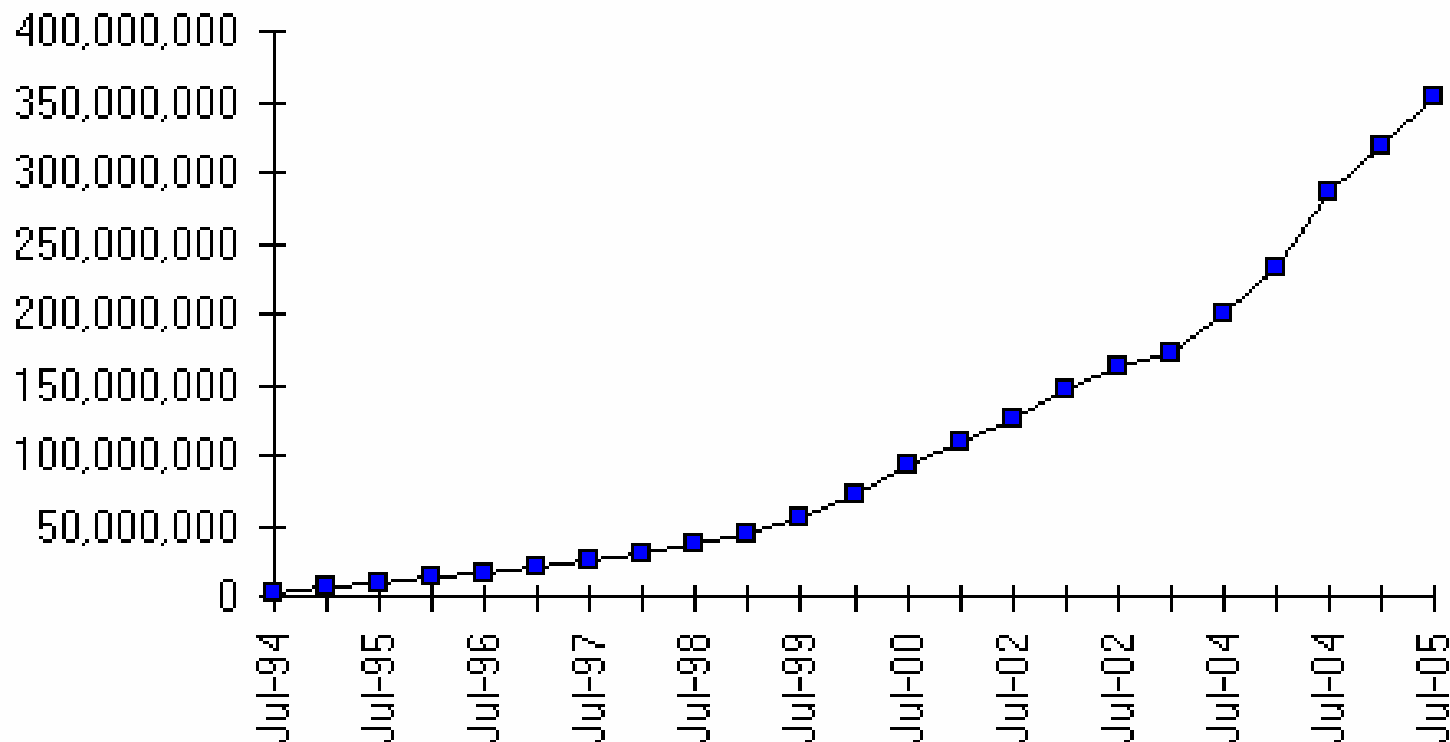
QUALYS CSO INTERCHANGE DECEMBER 2005

MAKING THE INTERNET THE
CHANNEL OF CHOICE

Richard Hackworth, HSBC Holdings plc

Well, the Internet infrastructure continues to grow

Internet Domain Survey Host Count



Source: Internet Software Consortium (www.isc.org)

On-line vendors seem to be making their choices

- Internet advertising spend increased 21% in 2004, and increasing faster than TV
- On average 2004 web advertising was about 3.6% of ad spend, 5.4% in US and 7.7% in Sweden. Expect web advertising spend to be 4.4% in 2007 *(Zenith Optimedia, April05)*
- 79% US on-line retailers are profitable, average margin 21%, average marketing growth rate in region of 10% - 20% pa *(Interactive Advertising Bureau, Nov04)*

There appear to be several reasons for this growth

(Interactive Advertising Bureau, Nov04)

- The consumer is in control
- The internet makes marketers more accountable
- Growing economy
- Broadband is transforming consumer access
- ‘Search services’ are growing and attract more advertising \$’s
- The Internet is attacking TV advertising (quoted as \$60Bn pa in US)

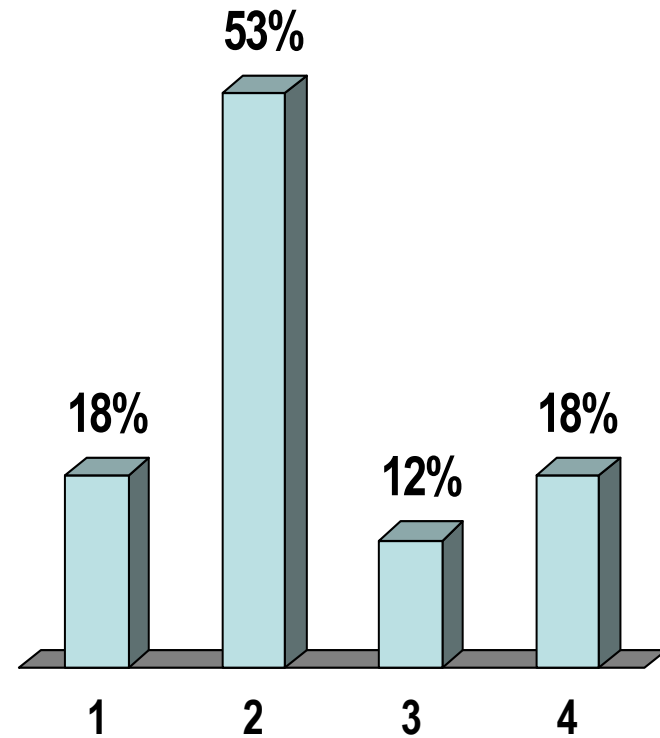
On the other hand maybe not all are convinced

- Consumer confidence in e-business security is weak. Less than 70% of on-line customers feel secure (less than 60% in the US)
- 80% - 90% of on-line consumers are familiar with identity theft and at best only 80% of online banking customers think Banks do enough to protect customers (and between 70% and 40% for other sectors) (*RSA Security Index, November 2005*)
- 80% of US consumers interested in receiving personalised content, 60% willing to spend more than 2 minutes providing personal information to drive personalisation, but 63% concerned that this data is not secure (*Choice Stream Personalisation Survey, May 2005*)
- US consumers receive an average of 5 phishes pa, 15% of recipients clicked it (*Gartner Phishing Study, July 2005*)
- Perhaps size matters – 54% of phishes reported directed at CitiBank (*CipherTrust 2005*)
- The US Secret Service receives about 100 calls and 300 – 500 items of correspondence from actual or potential victims of '419' frauds per day (*FraudWatch International*)

What do you think?

If you compare e-commerce to other more traditional retail channels such as in-store shopping, do you think e-commerce is

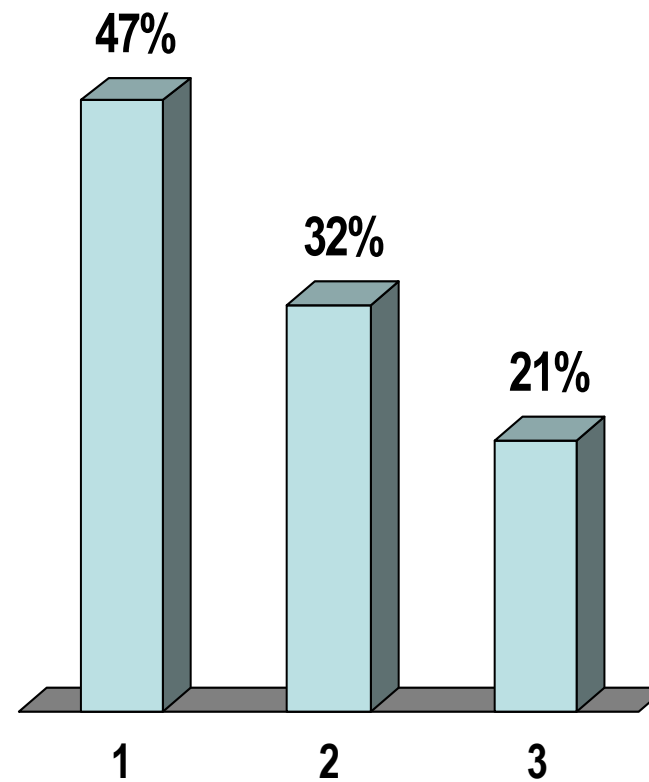
1. prohibitively risky
2. significantly more risky
3. the same
4. less risky



What do you think?

How adequate do you think current commercial law is in dealing with e-commerce risks?

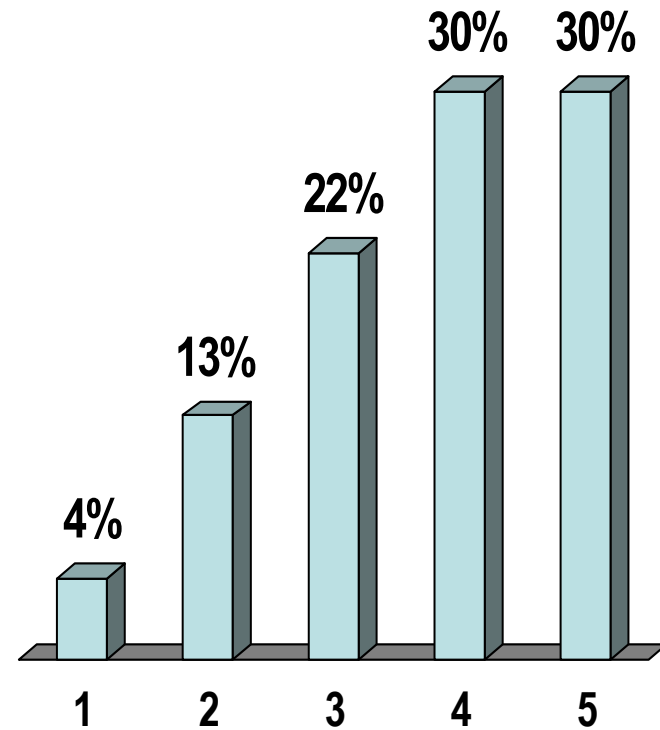
1. completely inadequate
2. somewhat inadequate
3. OK



What do you think?

How would you feel if you had to carry and use a personal security token?

1. Very put out
2. Mildly inconvenienced
3. Don't mind
4. See it as a plus
5. Don't understand why they haven't been introduced sooner



At the end of the day, who has to resolve the issues?

- Who owns the issues – the consumer, the service provider or the technology suppliers?
- Who has the wherewithal to protect e-space?
- Who makes the choices and who benefits?
- Who do you want to take the lead?