The Information Security Process

Emiliano Kargieman
The Information Security Process

**Agenda**

- The briefest introduction to IS
- Cybercrime indicators, threats and trends
- Defense Strategy: How to react?
- The technology
The Information Security Process

Intro

Information Security

• The Context: The information Age

• The Fundamentals
  – Privacy
  – Authenticity and Integrity
  – Disponibility
  – Non-Repudiation

• The Purpose
  – Dissuasion
  – Prevention
  – Auditing
Current Scenario: “if it ain’t broken, don’t fix it”.

- Complexity and flexibility of information systems increases, security decreases.
- Legacy systems are not maintained or audited
- Low level of awareness in decision makers
- Lack of security focus from Software/HW vendors and Integrators.
- Lack of a global framework to analyze and understand security
- Lack of Security “Best Practices”

And Then…

- Unforeseen vulnerabilities
- High risk, high level of exposure
- High administrative efforts
- Risk is managed reactively, it’s all damage control.
Cybercrime: Indicators and Trends
Indicators of cybercrime are historically hard to find.

Incidents are not usually reported

- Most common reasons for not reporting a security incident according to a survey by the FBI/CSI

![Bar chart showing reasons for not reporting security incidents]
To be reported, attacks need to be detected first!

- A 1996 Survey of the Defense Information Systems Agency, showed the following results on a systematic attack against government targets:

- This is still true: Most attacks go undetected!
Sources of information

  [www.gocsi.com](http://www.gocsi.com)
- Information Security Magazine 2001 Industry Survey
  [www.infosecuritymag.com](http://www.infosecuritymag.com)
- GAO/AIMD-96-84 (DISA)
- Honeynet project
  [www.project.honeynet.org](http://www.project.honeynet.org)
- Bugtraq mailing list
  [www.securityfocus.com](http://www.securityfocus.com)
- ARIS
  [www.securityfocus.com](http://www.securityfocus.com)
- CERT
  [www.cert.org](http://www.cert.org)
- SANS Incidents
  [www.incidents.org](http://www.incidents.org)
- Dshield project
  [www.dshield.org](http://www.dshield.org)
Recent Indicators

CSI/FBI Survey 2001


- Performed by
  - Computer Security Institute
  - San Francisco FBI’s Computer Intrusion Squad

- Results for the years 1996 – 2001 are analyzed
Recent Indicators

CSI/FBI Survey 2001 (cont.)

- 538 surveyed
- USA
- Public and Private sectors
- 27% 10000+ employes
- 39% $1 000 000 000+ revenues
### CSI/FBI Survey 2001 (cont.)

**Unauthorized system use in the last 12 months (%)**

<table>
<thead>
<tr>
<th>Year</th>
<th>Yes</th>
<th>No</th>
<th>NA</th>
</tr>
</thead>
<tbody>
<tr>
<td>1996</td>
<td>64</td>
<td>25</td>
<td>11</td>
</tr>
<tr>
<td>1997</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1998</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1999</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2000</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2001</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The Information Security Process

Recent Indicators

CSI/FBI Survey 2001 (cont.)

Quantifiable loss in the last 12 months

- 2001: 78% admitted loss, but only 37% could quantify it!
CSI/FBI Survey 2001 (cont.)

<table>
<thead>
<tr>
<th>Type of attack</th>
<th>Loss</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unauthorized access (from inside)</td>
<td>$6,064,000</td>
</tr>
<tr>
<td>Financial fraud</td>
<td>$92,935,500</td>
</tr>
<tr>
<td>Telecommunication fraud</td>
<td>$904,100</td>
</tr>
<tr>
<td>Theft of proprietary information</td>
<td>$151,230,100</td>
</tr>
<tr>
<td>Virus</td>
<td>$45,288,150</td>
</tr>
<tr>
<td>Laptop theft</td>
<td>$8,849,000</td>
</tr>
<tr>
<td>Network abuse (from inside)</td>
<td>$35,001,650</td>
</tr>
<tr>
<td>Denial of Service</td>
<td>$4,283,600</td>
</tr>
<tr>
<td>Sabotage</td>
<td>$5,183,100</td>
</tr>
<tr>
<td>System intrusion</td>
<td>$19,066,601</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>$368,805,801</strong></td>
</tr>
</tbody>
</table>
The Information Security Process

Recent Indicators

CSI/FBI Survey 2001 (cont.)

What actions where taken after the intrusion?

- The vulnerability was patched: 94
- The intrusion wasn't reported: 40
- The intrusion was reported: 36
- The company took legal advise/actions: 30

Attack technology evolves

- Attack frameworks
  - Easy to use malicious code
  - Reduces knowledge needed to attack
  - Allows for coordinated multiparty attacks

- Attack automation
  - Distributed DOS / Very complex worms / Directed Virus
  - Faster target acquisition
  - Large scale attacks with low resources
  - Brute-force attack paths
# The Honeynet project

<table>
<thead>
<tr>
<th>Recent Indicators</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Honeynet project</td>
</tr>
</tbody>
</table>

- “Know your enemy...”
- Decoy network of 8 computers running:
  - Linux
  - Solaris
  - Windows
- No efforts to attract attackers
- Monitored from April 2000 to February 2001
The Honeynet project

Some Results

- The estimated lifetime for a Linux RedHat default install is less than 72 hours.

- Some systems were compromised less than 15 minutes after being plugged to the network.

- The estimated lifetime for a default install of windows 98 is less than 24 hours.

- During February 2001, 206 complete port-scans were registered.
Defense Strategy: How to react?
<table>
<thead>
<tr>
<th>Defense Strategy</th>
<th>The perception of risk</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• There is no real security.</td>
</tr>
<tr>
<td></td>
<td>• Security is only the perception of risk.</td>
</tr>
<tr>
<td></td>
<td>• Security management <em>is</em> risk management.</td>
</tr>
<tr>
<td></td>
<td>• To increase security, risk needs to be:</td>
</tr>
<tr>
<td></td>
<td>– Modeled</td>
</tr>
<tr>
<td></td>
<td>– Quantified</td>
</tr>
<tr>
<td></td>
<td>– Minimized over time</td>
</tr>
</tbody>
</table>
Starting from a model of the flow of information in an organization, where players communicate, process and store information.
Entry points

- Each of these actions and interactions possesses its own risk.
The Information Security Process

Risk quantification

Countermeasures = Threats x Vulnerabilities x Impact

Practices and technologies

Attackers' profile,
Resources available,
Attacker profile,
Software flaws,
Biased policies,
Bad protocols,
Etc.

Loss,
The Information Security Process

<table>
<thead>
<tr>
<th>Modeling Risk</th>
<th>Threats</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Quantified by attacker profile, knowledge, financial resources, human resources, reach, interests:</td>
</tr>
<tr>
<td></td>
<td>– Amateur</td>
</tr>
<tr>
<td></td>
<td>– Hacker</td>
</tr>
<tr>
<td></td>
<td>– Hacker group</td>
</tr>
<tr>
<td></td>
<td>– Unsatisfied employee</td>
</tr>
<tr>
<td></td>
<td>– Competition</td>
</tr>
<tr>
<td></td>
<td>– Organized Crime</td>
</tr>
<tr>
<td></td>
<td>– Intelligence Agency</td>
</tr>
<tr>
<td></td>
<td>– Terrorist organizations</td>
</tr>
</tbody>
</table>
The Information Security Process

Modeling Risk

Threats evolve

Example of projected evolution of threat share by attacker profile

- Terrorist groups
- Intelligence agencies
- Organized Crime
- Competing companies
- Groups of individuals
- Individuals
<table>
<thead>
<tr>
<th>Modeling Risk</th>
<th>Vulnerabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Design flaws</td>
</tr>
<tr>
<td></td>
<td>– Critical Information systems</td>
</tr>
<tr>
<td></td>
<td>– Networks</td>
</tr>
<tr>
<td></td>
<td>– Security Architecture</td>
</tr>
<tr>
<td></td>
<td>• Implementation flaws</td>
</tr>
<tr>
<td></td>
<td>– Operating system vulnerabilities</td>
</tr>
<tr>
<td></td>
<td>– Application vulnerabilities</td>
</tr>
<tr>
<td></td>
<td>– Hardware vulnerabilities</td>
</tr>
<tr>
<td></td>
<td>• Misuse or misconfiguration</td>
</tr>
<tr>
<td></td>
<td>• Policy weaknesses</td>
</tr>
<tr>
<td></td>
<td>• Unclear responsibilities</td>
</tr>
<tr>
<td>Modeling Risk</td>
<td>Impact</td>
</tr>
<tr>
<td>---------------</td>
<td>--------</td>
</tr>
<tr>
<td></td>
<td>• Attack consequences, quantified by Economic loss, Negative publicity, etc.</td>
</tr>
<tr>
<td></td>
<td>– Loss of proprietary information</td>
</tr>
<tr>
<td></td>
<td>– Corruption of critical information</td>
</tr>
<tr>
<td></td>
<td>– Financial Fraud</td>
</tr>
<tr>
<td></td>
<td>– Interruption of critical processes</td>
</tr>
<tr>
<td></td>
<td>– Sabotage</td>
</tr>
<tr>
<td></td>
<td>– Telecommunication fraud</td>
</tr>
<tr>
<td>Modeling Risk</td>
<td>Countermeasures</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------</td>
</tr>
<tr>
<td></td>
<td>• Security tools, software and mechanisms</td>
</tr>
<tr>
<td></td>
<td>– Network devices</td>
</tr>
<tr>
<td></td>
<td>– Crypto</td>
</tr>
<tr>
<td></td>
<td>– Access control</td>
</tr>
<tr>
<td></td>
<td>– Etc.</td>
</tr>
<tr>
<td></td>
<td>• Procedures</td>
</tr>
<tr>
<td></td>
<td>• Emergency response</td>
</tr>
<tr>
<td></td>
<td>• Auditing capabilities</td>
</tr>
<tr>
<td></td>
<td>• Visibility</td>
</tr>
<tr>
<td></td>
<td>• Training</td>
</tr>
<tr>
<td></td>
<td>• (We’ll go into more detail later)</td>
</tr>
</tbody>
</table>
A risky game

\[ \text{Risk} = \sum R_i \ll mT \]
There are no recipes

• The Information infrastructure and the information flow are unique to each organization.

• Threats, vulnerabilities, impact, they all depend on the process we are trying to protect.

• All these variables and factors evolve over time, so does risk.

• Security emerges from the unique qualities of an information system.

• There are no silver bullets.
The Information Security Process

Strategy | Nor Bottom-up ...

- Start securing platforms, buying and installing appliances and security software.
- It only gets you lost in the day to day operation.
- No sense of direction.
- No real understanding of risks.
- Security policies are what you can manage, not what you want or need.
- It does not contemplate the “holistic” properties of security.
### The Information Security Process

<table>
<thead>
<tr>
<th>Strategy</th>
<th>... nor Top-down</th>
</tr>
</thead>
</table>

#### THINK
- Define policy, requirements, select tools, plan roll-out, implement.
- Hard to show short term results.
- Usually over-promises and under-delivers.
- When the implementation is finished, the context changed.
- It does not contemplate the dynamic properties of security.
The Information Security Process

**Strategy**

It's a process!

<table>
<thead>
<tr>
<th>THINK</th>
<th>DO</th>
</tr>
</thead>
</table>

- Policies, user modeling, security architecture are allowed to evolve.
- The tools we use help shape the vision we have of the security infospace.
- Small iterations let us set milestones easier to control.
- Easier to define and adapt to a fixed budget.
- Can show short term and medium term results.
The Information Security Process

Strategy | One iteration

- Policy Definition
- Risk Modeling
- Security Architecture
- Visibility and Control
Risk Modeling

- Model the information flow on the organization
- Assess risk for the processes involved:
  - Assess threats, vulnerabilities, impact.
  - Assess the efficacy of present countermeasures
- Model attack scenarios
- Quantify risk
- Identify short, medium and long term actions.
Policy Definition

• Organizational analysis
• Definition of roles
• Assignment or tasks and responsibilities
• Formalization of security procedures
• Definition of security parameters and norms for the use of information systems
• Analysis of functional roles
• Profile scopes and definitions
• Contingency plans
• Strategies for development and roll-out of information systems
• Criteria for the evaluation of IT projects.
Security Architecture

- Policy enforcement
  - Building blocks
    - Physical Security
    - Identification, Authentication and Authorization
    - Base software security
    - Application security
    - Network security
    - Integrity / Data protection
  - Operations
    - Operational procedures
    - Training
  - Contingency operations
    - Automatization
Visibility and Control

- The Security Infospace concept
- Real Time or Near Real Time
  - Augment, Cross-reference, Enhance
  - Visualize
  - Normal behavior, attack conditions
  - Alarms
  - Trigger procedures
- Off-Line
  - In-depth auditing
  - DWH, Trends
  - Forensics
The Information Security Process

Strategy | Iterations

THINK

- Segregation
- Profiles
- Critical Processes
- Assessment
- Planning
- Compromise
- Building infrastructure
- Increase granularity
The Technology
A small, functional taxonomy of tools

• Analysis and formalization
  – Tools that help in the processes of risk modeling and policy definition.

• Enforcement
  – Tools that are used to enforce security policies

• Auditing and Control
  – Tools used to gain knowledge of our particular “security infospace” and that help in the process of detecting and responding to security breaches.
Analysis and Formalization

• Tools
  – Network discovery tools
  – Vulnerability scanners
  – Intrusive attack tools
  – Organizational modeling tools
  – Risk Modeling tools

• Services
  – Security Intelligence
  – Penetration Testing
  – Policy definition
  – Contingency planning
  – Etc.
Enforcement

- Tools
  - Identification, Authentication and Authorization
    - PKI, Biometrics, Tokens, SSON, Platform dependant (OS specific)
  - Base software security
    - Network services wrappers, Filesystem restrictions, Consistency checks, Security upgrades and patches, etc.
  - Application security
    - Certification/authorization APIs, Versioning control, Application dependants.
  - Network security
    - Firewalls, VPNs, Content filtering
  - Integrity / Data protection
    - Antivirus, Backups, Consistency checkers.
Auditing and Control

- Tools
  - Network based Intrusion detection systems
  - Host based intrusion detection systems
  - Audit trails and log acquisition tools
  - Log centralization tools
  - Visualization tools
  - Analysis tools
  - Alarm and Reporting systems
  - Forensics tools
  - Security Operation Centers

- Services
  - Managed Security Services
Core Security Technologies
The company

- Dedicated fully to Information Security (IS)
  - Focused on providing business enabling IS technology
- Founded in 1996
- Formed by world-class security experts
- Headquartered in New York
- Head count: 70 (February 2002)
- Over 20 IS software vendors currently using CORE’s technology
- Over 30 technical papers and security advisories published
- 4 patents filed and / or pending
Our solutions
Some of our clients

- Banco Privado de Inversiones
- BankBoston
- Ernst & Young LLP
- FEMSA (Coca Cola)
- Foundstone Inc.
- Greenlight.com
- IEEE
- KPMG
- MBA - Merchants Bank de Argentina

- Metrored
- Microsoft Inc.
- Network Associates Inc.
- Organización Veraz
- PriceWaterhouseCoopers
- Proofspace Inc.
- Real Networks Inc.
- SecurityFocus.com
- Secure Networks Inc.
- Siemens
- UOL International
- Vyou.com
Thank you!

Contact me for a copy of the presentation

ek@corest.com