



## Organizational Security: When People Are Involved

Mike Ellsworth  
StratVantage Consulting, LLC  
MnIPS Business Security Seminar  
April 16, 2003

Copyright © 2003, StratVantage Consulting, LLC



## The Security Problem

“Computer security is a 40-year-old discipline; every year there’s new research, new technologies, new products, even new laws. And every year things get worse.”

Bruce Schneier, CIO, Counterpane  
Internet Security Inc.

Copyright © 2003, StratVantage Consulting, LLC



## Top Ten User Errors

- Passwords on Post-it Notes
- Leaving your computer on, unattended
- Opening e-mail attachments from strangers
- Poor password etiquette
- Laptops on the loose
- Blabber mouths
- Plug and Play without protection
- Not reporting security violations
- Always behind the times / no virus protection
- Focusing outside the organization

Source: [www.HumanFirewall.com](http://www.HumanFirewall.com)

Copyright © 2003, StratVantage Consulting, LLC



## Where’s the Problem?

- 5<sup>th</sup> Annual Global Information Security Survey by PwC
  - Security breaches at **66 percent** of worldwide sites in the past year
  - External hacking which rose from **46 percent** in 2001 to **55 percent** in 2002
  - Internal sources, such as employee misuse or disgruntled staff, declined year-on-year to **50 percent**

Copyright © 2003, StratVantage Consulting, LLC



## Where’s the Problem?

- But:
  - **53 percent** of European organizations didn’t report security incidents

Copyright © 2003, StratVantage Consulting, LLC



## Where’s the Problem?

- Human Firewall Council Security Management Index (9/02):
  - The vast majority of organizations taking the survey failed to meet what may be considered minimally acceptable standards for managing security across the enterprise.
  - All but one category (physical security) scored an “F” or failing grade across 10 key areas of security management.

Copyright © 2003, StratVantage Consulting, LLC



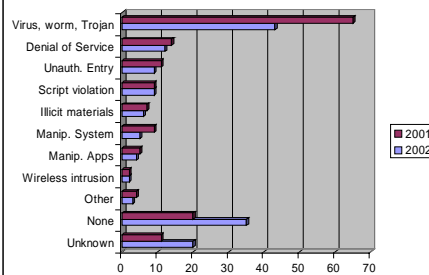
## Where's the Problem?

- Human Firewall Council Security Management Index (9/02):
  - Results suggest a reactive, “Techno-Centric Solution” perspective for security still prevails

Copyright © 2003, StratVantage Consulting, LLC



## Where's the Problem?



Copyright © 2003, StratVantage Consulting, LLC



## Social Engineering

- Use of psychological tricks on legitimate users of a computer system, in order to gain the information (usernames and passwords) needed to gain access to the system

Copyright © 2003, StratVantage Consulting, LLC



## Social Engineering



Copyright © 2003, StratVantage Consulting, LLC



## Social Engineering

- "Hi Bev, this is Sam from the IS Department. We just got in a new corporate screensaver and since you're the VP's secretary you will get it first. It's really cool; wait 'till you see it. All I need is your password so I can log on to your PC from the computer center and install it.
- Oh Great!!!!!! My password is rover. I can't wait to see that new screen saver!!!!!"

Copyright © 2003, StratVantage Consulting, LLC



## Social Engineering

- Other types:
  - **E-mail** – the I Love You virus
  - **“Dumpster Diving”** – hired guns for Oracle dug into Microsoft's trash
  - **In person** – walking into a building and checking password post-it-notes stuck to monitors
  - **Regular mail** – sending a bogus survey offering a cash award for completion and asking sensitive questions

Copyright © 2003, StratVantage Consulting, LLC



## Eight Steps to Better Organizational Security

- **Get top management buy-in and commitment**
  - You'll fail without it
  - More than **40 percent** of CEOs, CFOs, company presidents and managing directors involved setting security policy
  - **52 percent** of those have direct input into information security spending
  - Majority of companies spend less than **\$500,000** a year on security

Source: PwC GISS survey of 4,500 security professionals in 42 countries 9/ 2001  
Copyright © 2003, StratVantage Consulting, LLC



## Eight Steps to Better Organizational Security

- **That includes your board**
  - Three major questions for executives and boards:
    - Is our security policy enforced fairly, consistently and legally across the organization?
    - Would our employees, contractors and partners know if a security violation was being committed?
    - Would they know what to do about it if they did recognize a security violation?

Copyright © 2003, StratVantage Consulting, LLC



## Eight Steps to Better Organizational Security

- **Assign and clarify roles and responsibilities**
  - Set up an information security task force
    - Chief Information Officer
    - Chief Security Officer (Don't have one? – Name one!)
    - Internal Audit Manager
    - Physical Security Manager
    - Representatives from Legal and Human Resources departments

Copyright © 2003, StratVantage Consulting, LLC



## Eight Steps to Better Organizational Security

- **Including rank and file**
  - Spell out information security functions and responsibilities in all job descriptions and organizational structures and reporting relationships

Copyright © 2003, StratVantage Consulting, LLC



## Eight Steps to Better Organizational Security

- **Create an Action Plan with a budget**
  - Asset assessment
    - 40 percent of companies don't classify the sensitivity of their data
  - Risk assessment
    - Include "white hat" hacking
  - Risk mitigation plan

Copyright © 2003, StratVantage Consulting, LLC



## Eight Steps to Better Organizational Security

- **Develop and/or update information security policies (Don't have 'em? – Write 'em!)**
  - **50 percent** of companies don't have written security policies
  - **7 percent** have no information security policies at all
  - **25 percent** have neither reviewed nor measured the effectiveness of their corporate security policy in the past year

Copyright © 2003, StratVantage Consulting, LLC



## Eight Steps to Better Organizational Security

- Policies include:
  - Network acceptable usage
  - Email usage
  - Internet usage
- Don't forget employee termination processes and policies
  - Who lets IT know and when?

Copyright © 2003, StratVantage Consulting, LLC



## Eight Steps to Better Organizational Security

- Develop an organization-wide Information Security Awareness Program (ISAP)
  - Heighten awareness, change attitudes and influence behavior
  - Use "Test Your Security Awareness" at [www.HumanFirewall.com](http://www.HumanFirewall.com)

Copyright © 2003, StratVantage Consulting, LLC



## Eight Steps to Better Organizational Security

- Measure the progress of your Security Awareness/ Education efforts
  - Need to measure it to manage it

Copyright © 2003, StratVantage Consulting, LLC



## Eight Steps to Better Organizational Security

- Adapt and improve according to progress/feedback
  - It's not just one and done
  - Revise, revise, revise
  - Stay current on latest threats

Security is a process, not a destination

Copyright © 2003, StratVantage Consulting, LLC



## Eight Steps to Better Organizational Security

- Develop a Security Incident Response Team (SIRT) and plan
  - It's too late when the crisis hits
  - A multi-disciplinary, multi-departmental response team provides a structured, formal capability to respond to actual or attempted intrusions
  - Be sure to involve Public Relations/ Communications
  - Fewer than **25 percent** of organizations have established a formal SIRT capability

Source: Meta Group white paper, 2002

Copyright © 2003, StratVantage Consulting, LLC



## Remember, Security is a Process, Not a Destination



Copyright © 2003, StratVantage Consulting, LLC



## Further Study

- *Secrets and Lies: Digital Security in a Networked World*, by Bruce Schneier
- *Security Transformation: Digital Defense Strategies to Protect Your Company's Reputation and Market Share* by Mary Pat McCarthy & Stuart Campbell
- [www.misti.com/](http://www.misti.com/)
- [www.sans.org/newlook/resources/policies/bssi3/](http://www.sans.org/newlook/resources/policies/bssi3/)
- [www.baselinesoft.com/ispme.html](http://www.baselinesoft.com/ispme.html)

Copyright © 2003, StratVantage Consulting, LLC



## Further Study

- [www.sans.org/infosecFAQ/aware/lack.htm](http://www.sans.org/infosecFAQ/aware/lack.htm)
- [www.sans.org/infosecFAQ/policy/sec\\_aware.htm](http://www.sans.org/infosecFAQ/policy/sec_aware.htm)
- [www.techrepublic.com/article.jhtml?id=r00520010717aue01.htm&src=search&\\_requestid=65429](http://www.techrepublic.com/article.jhtml?id=r00520010717aue01.htm&src=search&_requestid=65429)

Copyright © 2003, StratVantage Consulting, LLC



## Further Study

- To report information security incidents:  
[www.nipc.gov/incident/incident.htm](http://www.nipc.gov/incident/incident.htm)  
or  
[www.infragard.net/ireporting.htm](http://www.infragard.net/ireporting.htm)

Copyright © 2003, StratVantage Consulting, LLC



## Further Study

- [www.msci.memphis.edu/%7Eryburnp/cl/glossary.html#social\\_engineering](http://www.msci.memphis.edu/%7Eryburnp/cl/glossary.html#social_engineering)
- "Oracle's Boardroom Spy Tricks"  
[www.zdnet.com/zdnn/stories/news/0,4586,2596401,00.html](http://www.zdnet.com/zdnn/stories/news/0,4586,2596401,00.html)
- "Summit: Ban the Internet bad guys!"  
[www.zdnet.com/zdnn/stories/news/0,4586,2566543,00.html](http://www.zdnet.com/zdnn/stories/news/0,4586,2566543,00.html)
- "Kevin Mitnick: Timeline"  
[www.takedown.com/coverage/mitnick-timeline.html](http://www.takedown.com/coverage/mitnick-timeline.html)
- "Mitnick teaches 'social engineering'"  
[www.zdnet.com/zdnn/stories/news/0,4586,2604480,00.html](http://www.zdnet.com/zdnn/stories/news/0,4586,2604480,00.html)

Copyright © 2003, StratVantage Consulting, LLC



## Further Study

- [www.cert.org/advisories/CA-1991-04.html](http://www.cert.org/advisories/CA-1991-04.html)
- "Create Order with a Strong Security Policy"  
[www.networkmagazine.com/article/NMG2000710S0015](http://www.networkmagazine.com/article/NMG2000710S0015)

Copyright © 2003, StratVantage Consulting, LLC



## Thank You!

Mike Ellsworth  
StratVantage Consulting, LLC  
Emerging technology strategy and permission marketing  
[mellsworth@stratvantage.com](mailto:mellsworth@stratvantage.com)  
[www.stratvantage.com](http://www.stratvantage.com)

Receive free emerging technology news and commentary with the Stratvantage News Summary



Copyright © 2003, StratVantage Consulting, LLC