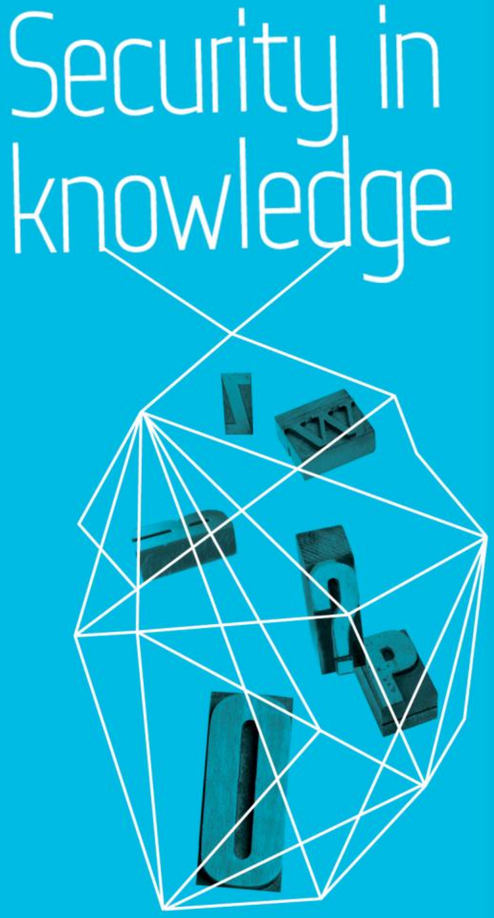
RSACONFERENCE2013

The Five Habits of Highly Secure Organizations



Ben Rothke, CISSP, CISA

Information Security

Wyndham Worldwide Corp.

Session ID: STU-R35B

Session Classification: Intermediate

WYNDHAM WORLDWIDE

Agenda

- Discussion of effective information security habits, characteristics and practices
  - great practices of security-conscious companies
  - not directly related to ITIL, ISO 17799, etc.
  - based on my past experience at a large spectrum of Fortune 500 and Global 2000 companies
  - primarily financial services, pharmaceutical, aviation and healthcare

Why it’s important you are here

- Computer security is simply attention to detail and good design
- focusing on the five habits of this presentation will enable you to ensure your organizations data assets are secured
  - rather than blindly wasting your budget on security appliances that do nothing more that look cool in a rack

Key Take Away Thoughts

- Effective infosec is built on risk management, good business practices and project management
  - while the mathematics of cryptography is rocket science, most aspects of information security are not
- successful information security programs have all occurred by focusing on security from a framework of risk mitigation
- cost of security hardware and software purchased has absolutely no corresponding effect to the level of security

The five habits

1. CISO
2. Risk Management
3. Invests in people, not products
4. Policies and Procedures
5. Awareness and Training

Habit #1 – CISO

- Accountants achieve efficiency and effectiveness under the guidance and coordination of a CFO
  - security teams will reach their optimal levels under a CISO
- infosec is more than a single technology. It involves:
  - physical, psychological and legal aspects, such as training, encouraging, enforcing and prosecuting
  - strategic planning, skilled negotiating and practical problem solving
- only an individual with strong business savvy and security knowledge can oversee security planning, implement policies and select measures appropriate to business requirements - that person is the CISO

CISO

- Characteristics of a great CISO
  - deep understanding of technology, combined with understanding of the organizations function, politics and business drivers
  - gold medal CISO: Electrical engineer with an MBA
  - silver medal CISO: NSA veteran with corporate experience
- never a yes-man to the CxO or Board of Directors
- invests in people, not technology
  - corollary: vendors intimidated by CISO due to technical prowess
- not intimidated by a screaming SVP trying to force firewall admin to violate policy
  - but also willing to evaluate the policy to determine whether it is reasonable

CISO

- CISO works at the executive level
  - serves on the executive council or equivalent
  - be on CIO's architectural strategy council or equivalent
  - direct or dotted-line manager of all information security staff
- without executive level control, will face difficulty when bridging the gap between business process demands and security technology requirements
- CISO at the non-executive level – expect Spaf's Law:
  - *"if you have responsibility for security but have no authority to set rules or punish violators, your own role in the organization is to take the blame when something big goes wrong"*
    - Prof. Gene Spafford - CS Dept. - Purdue University

Habit #2 – Risk Management

- How management often perceives risk
  - risk = evil hacker

This is risk management…

Blogs
App dev
Social engineering
Hardware
China
Internal practices
Fraud
Token management
Telco
Unhappy customers
Hackers
External
Forensics
Database
Third-party
Physical security
Clients
External
Crypto keys
Google
Documentation
Wireless
Worms
Data destruction
Audit
Risk matrix
Political
Consultants
Data center
Terrorists
Poor risk assessment
Vulnerabilities
Organized crime
Spyware
Web-scripting
Malicious end-users
Operations test
Software Patches
Vendor bankruptcy
Legal liability
Illegal downloads
Customers
Background checks
Lack of budget
Regulatory
Hactivists
DR/BCP
Environmental compliance
Operational
Viruses
Power grid
phishing
VoIP
Contractors
Unions
India
Revocation processes
Disgruntled employees
Backup tapes
Malicious software
Malware
Lack of staff
Rogue employee
Insecure software
Windows
Procedural violations

Risk Management

- comprehensive risk management program must be created around these four areas:

1. Identification
2. Analysis
3. Mitigation
4. Monitoring

Habit #3 – People, not products

- People, not products
  - huge mistake companies make is expecting security products to solve their security problems
- they buy myriad products without being able to answer:
  - **what is your security problem and how do you expect this security product to solve it?**
- why you are buying a product?
  - create detailed requirements for its use
  - processes and procedures
  - metrics to measure its effectiveness and value

PEOPLE
NOT PRODUCTS

The big lie of security products

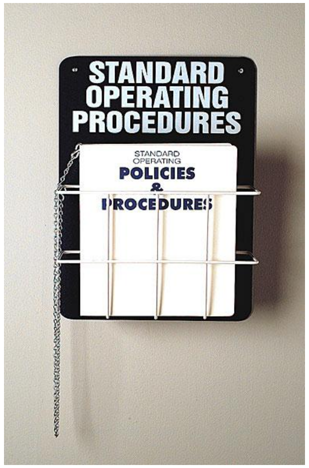
- Vendors want you to think their product is the best; but all products are for the most part indistinguishable
  - by the time a product hits version 3, competition has matched it feature for feature
- observation: most established COTS security products are essentially indistinguishable from each other and can achieve what most organizations require:
  - Check Point vs. Cisco
  - eEye vs. McAfee
- don’t obsess on the products. Focus on your staff, internal procedures and specific requirements

Habit #4 - Policies & Procedures

- Comprehensive security policies are required to map abstract security concepts to *your* real world implementation of your security products
- policy defines the aims and goals of the business
- no policies = no information security…. and
- no policies enforcement = no information security

Information security procedures

- SOP's ensure Chicago firewall admin builds & configures corporate firewalls in the same manner as Tokyo admin
- immense benefits of Standard Operating Procedures
  - standardize operations among divisions and departments
  - reduce confusion
  - designate responsibility
  - improve accountability of personnel
  - record the performance of all tasks and their results
  - reduce costs
  - reduce liability



Information Security SOP

- Organizations that take the time and effort to create infosec SOP’s demonstrate their commitment to security
  - by creating SOP’s, costs are drastically lowered (greater ROI), and their level of security is drastically increased
- another example: Aviation industry lives and dies (literally) via their SOP’s
  - SOP’s are built into job requirements and regulations
  - today’s airplanes are far too complex to maintain and operate without SOP’s
  - information security might not be as complex as a Boeing 777, but it still requires appropriate SOP’s

Habit #5 – Awareness & Training

- Users who read and trust the Weekly World News will invariably choose an insecure Java applet over security
- information security and associated risks aren't intuitive
  - invest in training users to properly use the tools given to them
- effective information security training and awareness effort can't be initiated without first writing information security policies

HACKERS CAN TURN YOUR HOME COMPUTER INTO A BOMB

...& blow your family to smithereens!

By RANDY JEFFRIES / Weekly World News

WASHINGTON — Right now, computer hackers have the ability to turn your home computer into a bomb and blow you to Kingdom Come — and they can do it anonymously from thousands of miles away!

Experts say the recent "break-ins" that paralyzed the Amazon.com, Buy.com and eBAY websites are tame compared to what will happen in the near future.

Computer expert Arnold Yabenson, president of the Washington-based consumer group National CyberCrime Prevention Foundation (NCPF), says that as far as computer crime is concerned, we've only seen the tip of the iceberg.

"The criminals who knocked out those three major online businesses are the least of our worries," Yabenson told Weekly World News.

"There are brilliant but unscrupulous hackers and there who have developed technologies that the average person can't even dream of. Even people who are familiar with how computers work have trouble getting their minds around the terrible things that can be done.

"It is already possible for an assassin to send someone an e-mail with an innocent-looking attachment connected to it. When the receiver downloads the attachment, the electrical current and molecular structure of the central processing unit is altered, causing it to blast apart like a large hand grenade.

"As shocking as this is, it shouldn't surprise anyone. It's just the next step in an ever-escalating progression of horrors conceived and instituted by hackers."

Yabenson points out that these dangerous sociopaths have already:

- Vandalized FBI and U.S. Army websites.
- Broken into Chinese military networks.
- Come within two digits of cracking an 17-digit Russian security code that would have sent deadly missiles hurtling toward five of America's major cities.

"As dangerous as this technology is right now, it's going to get much scarier," Yabenson said.

"Soon it will be sold to terrorists cells and fanatical religious-fringe groups.

"Instead of blowing up a single plane, these groups will be able to patch into the central computer of a large airline and blow up hundreds of planes at once.

"And worse, this e-mail bomb program will eventually find its way into the hands of anyone who wants it.

"That means anyone who has a quarrel with you, holds a grudge against you or just plain doesn't like your looks, can kill you and never be found out."

KABOOM! It might not look like it, but an innocent home computer like this one can be turned into a deadly weapon.

Sickos can wreak death and destruction from thousands of miles away!

Arnold Yabenson.

WEEKLY WORLD NEWS

COMPUTER VIRUS SPREADS TO HUMANS!

[illegible] suffers hacking cough, fever & runny nose

Awareness and Training

- Awareness defines the rules for computer use
- users must be clearly educated as to what *acceptable use* means
- define exactly what a *confidential document* is
- what is a good password?
- what emails should be forwarded?
- can I set up my own wireless network?

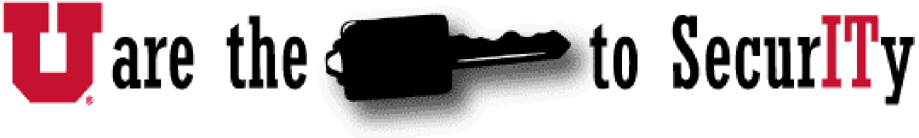


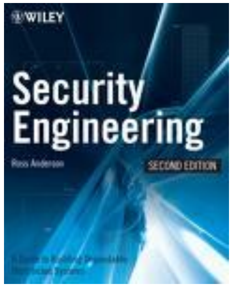
Image source: www.secureit.utah.edu/images/ISA/isa_banner2009.gif

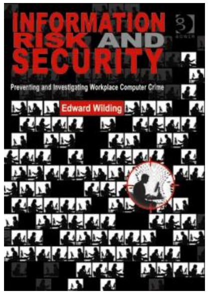
Awareness and Training

- Dark moment in computer security awareness #358
  - 1998 – US President Bill Clinton and Irish Prime Minister Bertie Ahern used digital signature technology to append their personal signatures to a statement endorsing broad e-commerce policy concerns
  - Clinton and Ahern are videotaped entering the passphrase for their private keys
  - at the conclusion of the ceremony, they swap the smart cards that contain their private keys

Required reading

- *Security Engineering: A Guide to Building Dependable Distributed Systems*
  - Ross Anderson
  - Free digital copy http://www.cl.cam.ac.uk/~rja14/book.html
- *Information Risk and Security*
  - Edward Wilding
- *NIST Information Security Handbook: A Guide for Managers*
  - http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf
- *Security Strategy: From Requirements to Reality*
  - Bill Stackpole and Eric Oksendahl




INFORMATION RISK AND SECURITY
Preventing and Investigating Workplace Computer Crime
Edward Wilding

NIST Special Publication 800-100

Information Security Handbook: A Guide for Managers

NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Recommendations of the National Institute of Standards and Technology

Pauline Bowen
Joan Hash
Mark Wilson

INFORMATION SECURITY

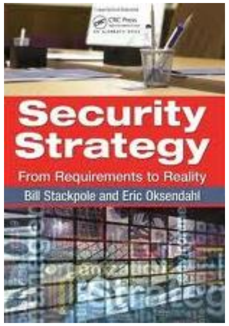
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

October 2006

U.S. Department of Commerce

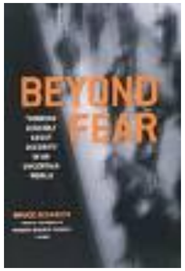
Technology Administration

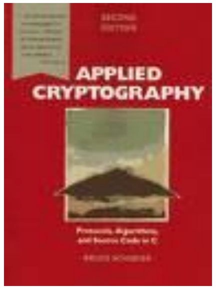
National Institute of Standards and Technology

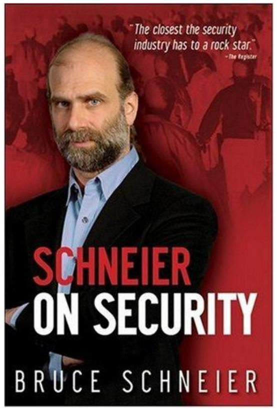

CRC Press
Security Strategy
From Requirements to Reality
Bill Stackpole and Eric Oksendahl

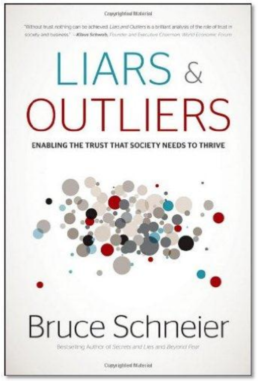
Required listening

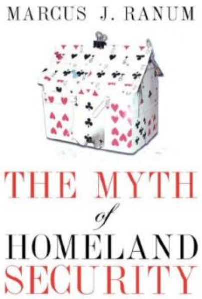
- Bruce Schneier / Marcus Ranum
  - Two really smart guys who understand security and risk, and don’t believe in the common wisdom of security pixie dust
  - visit their web sites – www.schneier.com / www.ranum.com
  - *Crypto-Gram* – Schneier’s monthly e-mail newsletter
    - http://www.schneier.com/crypto-gram.html






"The closest the security industry has to a rock star." – The Register
SCHNEIER ON SECURITY
BRUCE SCHNEIER





Summary

- Effective information security takes:
  - hard work
  - leadership
  - commitment
  - knowledge
  - responsibility
  - dedication
- when implemented in the 5 habits, those are the characteristics of highly secure organizations

Ben Rothke, CISSP CISA

Manager – Information Security

Wyndham Worldwide Corporation

www.linkedin.com/in/benrothke

www.twitter.com/benrothke

www.slideshare.net/benrothke