

Security on a Shoestring

IT Security Implementation
At
Philips Consumer Electronics

Let's make things better.

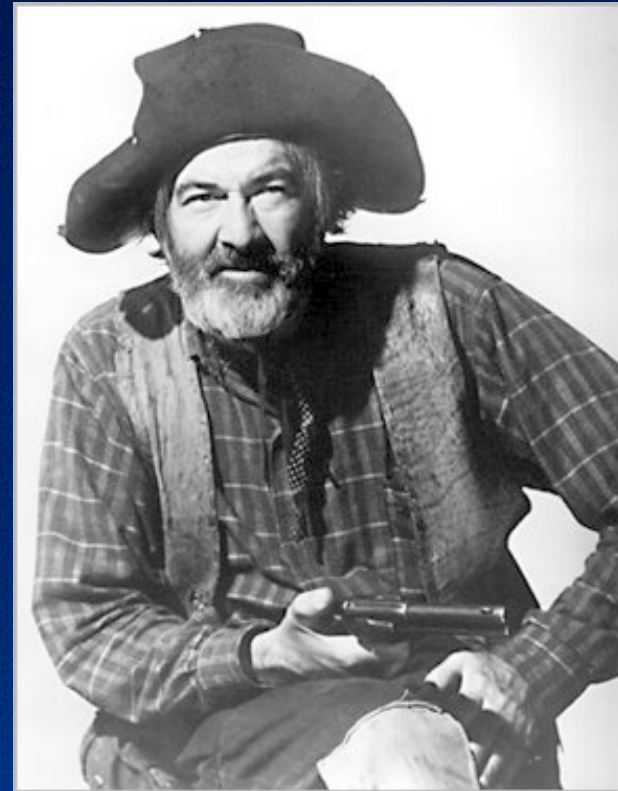


PHILIPS

Security on a Shoestring

Why me?

- A good fit
- Inquisitive
- No guts, no glory
- Peter Principle



Security on a Shoestring



- No budget
- No weapons
- No staff
- Policies posted but who knows where
- Everybody knows your name!

Security on a Shoestring

Methodology

Keep it simple

Hint

Security is basically
common sense

Security on a Shoestring

- What's needed?
 - *Support*
 - *Policies*
 - *Tools*
 - *Enforcement*

Security on a Shoestring

Support

Who's responsible?

- *Security Manager – develop policies*
- *CIO – implement program*
- *IT Department managers – execute and enforce*
- *Business Manager – employee adherence*
- *Employees – comply*
- *HR – post policies and notify employees*

Security on a Shoestring

Support

- **HELP!!!**

- *Network Administrators*
- *Database Administrators*
- *Communications Specialists*
- *Business Applications Analysts*
- *Outside Security Network*
- *Anyone else you can think of*

Security on a Shoestring

■ Policies

- *Protects both people and information*
- *Manage Risk*
- *Basis for procedures*
- *Evaluate*
 - Clear
 - Concise
 - Realistic

Security on a Shoestring

Policies

- What kind of policies
 - *Physical Security*
 - *Data Classification*
 - *Software Management and Distribution*
 - *Virus Protection*
 - *Email Services*
 - *Internet Use*
 - *Business to Business*
 - *Self Audit*
 - *Incident Response Capability*

Security on a Shoestring

- Inform the User Community
 - *Publish for all to see*
 - *Training*
 - Ethics training when hired
 - Workshops
 - Intranet web site

Security on a Shoestring

■ Logon Banner

- This is a Philips Consumer Electronics North America computer system, which may be accessed only for official PCE-NA business by authorized personnel. Unauthorized access or use of this computer system may subject violators to criminal, civil, and/or administrative action.
- The software used on this business computer is the valued intellectual property of the respected software vendors and, as such, is protected by national and international copyright laws. Software shall only be used according to the respective license agreements. Unauthorized copying of software is prohibited, except for usage according to the license agreements.
- Use of this system is subject to monitoring and recording by systems personnel. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible unauthorized activity it may be used as evidence for disciplinary action, including criminal prosecution.

Security on a Shoestring

■ Physical Security

- *Limited access to computer centers*
- *UPS systems required*
- *Network security features implemented*
- *Network security monitored and audited*
- *Sensitive data stored on servers*
- *Backups scheduled*
- *Business continuity plans developed and tested*

Security on a Shoestring

■ Userids

- *Assigned to people, not departments*
- *Thou shalt not share your userid*
- *Access approved by managers*
- *Passwords*
 - Rules invoked
 - Instruct users on creating good passwords
 - Philips → ph1L1ps → @ph!L!p\$.c0m
 - Irregular attempts to crack

Security on a Shoestring

- Laptop security musts
 - *Keep your laptop in sight*
 - *Always in carry-on luggage*
 - *Tape a business card to laptop*
 - *Avoid leaving in hotel baggage room*
 - *Lock laptop or remove hard drive*

Security on a Shoestring

- Data Classification
 - *Classified by data owner*
 - *Least access philosophy*
 - *To encrypt or not to encrypt*

Security on a Shoestring

- Software Management
 - *Computers are owned by the company not the person using it.*
 - *Standard application tool box to simplify support*
 - *Installation done by desk top support*
 - *Monitor to insure legality*

Security on a Shoestring

■ Virus Protection

- *Update scan definitions frequently*
- *Scan email*
- *Report all incidents*
- *Hoaxes*
- *Research possible infections*
 - NAI Virus Information Library
<http://vil.nai.com/vil/default.asp>
 - F-Secure Virus Info Center
<http://www.f-secure.com/virus-info/>

Security on a Shoestring

■ Email Use

- *Company owned asset*
 - No expectation of privacy
 - Subject to legal disclosure
- *Encouraged for business purposes*
- *Use governed by Company Code of Conduct*
- *SPAM*
 - Broadcast messages can be junk mail
 - Set rules to eliminate

Security on a Shoestring

■ Internet Use

- *Provided for company use*
 - No expectation of privacy
 - Monitoring can lead to discipline
- *Sites blocked via Cybercop*
- *Downloaded files must be scanned for malicious code (viruses, worms, trojans)*
- *Encrypt data sent over the Internet*

Security on a Shoestring

- Audit Policies and Procedures
 - *Maintain stable and secure enterprise*
 - *Facilitate swift resolution of performance or security events*
 - *Includes physical and network processes*

Security on a Shoestring

■ Tools

- *Nmap – network mapper*
- *Nessus – vulnerability scanner*
- *L0phtCrack – NT password auditor*
- *Snort – lightweight network intrusion detector*
 - Not on network in right location
 - Working with Engineering group
- *ISS BlackIce PC Protection*
- *TOP 75 Security Tools*
 - <http://www.insecure.org/tools.html>

Security on a Shoestring

- Enforcement
 - *Work closely with HR*
 - *Wear the Black Hat when necessary*
 - *Wave the red flag when necessary*
 - *Walk tall and pretend to carry a big stick.*

Security on a Shoestring

■ Resources

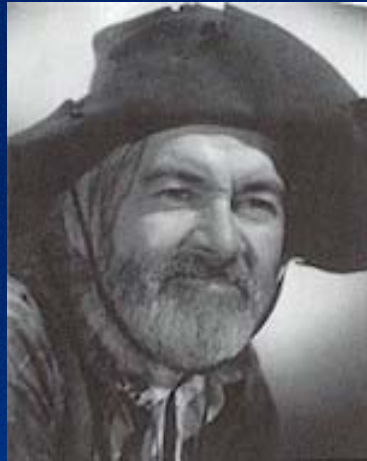
- *SANS* <http://www.sans.org>
- *Cert* <http://www.cert.org>
- *Microsoft*
- *Infragard*

Security on a Shoestring



Security on a Shoestring

Happy Trails, Buckaroos!



Let's make things better.



PHILIPS