How to Tell if Management is Serious About Information Security

Eugene H. Spafford
Purdue University CERIAS

Company Benefits of an Internet Presence

- eMail
- Marketing
- Customer Service
- eCommerce
- Collaboration with Partners
- Distributors, Suppliers, Stockholders, and on and on and on ...
- Information
- Entertainment
The Weight of Events

- Over $10 billion in on-line commerce this year will attract miscreants
- Network population and access continuing to surge
- On-line
  - Over 200 million users
  - In over 150 countries
  - Increasing at a rate of 150% per year
    All with access to your networks?

Management Should Be Concerned

- 1997 Global Information Security Survey
  - Industrial Espionage via compromised networks
    - 6% of respondents in 1996
    - 38% of respondents in 1997, up 600%!
  - Malicious acts by outsiders
    - 17% of respondents in 1996
    - 42% of respondents in 1997, up 250%!
...But...

- Costly IT Personnel to develop and maintain
  - Hardware/Software/Network infrastructure
  - Organizational delivery of timely content
  - Continual updates

- IT Security is an expensive add-on with no bottom line contribution

- Security has the reputation of “you can’t”

- Security personnel still think in terms of 100%

Evidence

If management is serious about security, then there are some clear indicators.

Let’s look at some of them.
**Policy**

- Company-wide policy
- Kept up-to-date
- Everyone is aware of the policy
- Developed with care and is comprehensive in nature

**User Education**

- Users are trained when hired
- Retraining opportunities are made available
- Some forms of evaluation are also in place
Security Staffing

- Dedicated IT security staff
- Staff is well-qualified for positions
- Staff has authority as well as responsibility
- Users know about the staff

IT Security Reporting

- There is a mandatory security reporting policy
- Security incidents are reported to the highest level
- Reporting feeds back into the policy and training
**Tools & Training**

- Security tools are kept up-to-date and deployed
- Staff members are trained in the use of the tools
- Tools are appropriate for the task

**Awareness**

- Awareness materials are regularly posted and updated
- Security awareness is promoted rather than threats
- Visitors and contractors are made aware of security concerns
**Incident Response**

- The company has an identified IRT
- The IRT is reachable 24 hours at a time
- The IRT is staffed appropriately
- The IRT is allowed to train and drill

**Downloads & Imports**

- User downloads are regulated or prohibited
- Some form of scanning is made for viruses, locally or at the perimeter
- Copyright is checked
- Incidents are traced for effect
**Upgrades**

- Software is kept up to date
- Hardware is kept up to date
- Upgrades are made consistently
- Security patches are kept up to date

**Disaster Recovery**

- There is an identified disaster recovery plan
- Regular backups are made of critical data
- There is a designated disaster recovery manager
- Walk-throughs have been performed recently
Conclusion

If management is serious about information security, then it is funded and staffed as an intrinsic part of doing business. Exactly like coding security, it is built-in rather than added-on afterwards.

How does your company compare?

Thanks!

Presentation is at
<http://www.cs.purdue.edu/homes/spaf/>