Limiting Digital Crime

An executive guide to security best practices

John Wurzler
Safeonline LLC

www.safeonline.com

HP WORLD 2002
Conference & Expo

Limiting digital crime

An executive guide to security best practices

- Where do the new risks reside?
- Why does every business need a comprehensive risk management program?
- What is the assess, mitigate, insure approach?
- What is a digital insurer looking for?

Where do the risks reside?

- **Liability risks**
  - Libel and slander
  - Copyright and trademark infringement
  - Virus transmission
  - Unauthorized access or use
  - Loss of services
  - Data privacy and protection
  - Professional errors & omissions
- **Losses**
  - Expensive downtime
  - Sales & productivity losses
  - Corrupted data
  - Damage to reputation, consumer confidence & loyalty
  - Lawsuits for breach of contract
  - Liability payouts
  - Legal penalties

Why are the risks growing?

- Failure to acknowledge or accept the risks
- Lack of understanding of the legal requirements to manage the risks
- Failure to realise business dependency on critical infrastructure
- Legal framework can’t keep pace with innovation – no commonly accepted standards
- Failure to understand that technology solutions are only a part of the mix
- No obvious internal owner – cross company problem needs a cross company solution

Why do you need a risk management program?

- To be compliant
- To protect shareholder value against catastrophic financial loss
- To find out where your exposures lie
- To examine what the impact of these exposures might be
- To put controls in place to limit your risks
- To transfer the residual risk to an insurer
- To regularly review your measures to ensure the program remains effective

What is the assess, mitigate, insure approach?

A comprehensive risk management programme

= Assessment + Mitigation + Insurance

What is the purpose of risk assessment?

- Impartial, proactive assessment of organizational vulnerabilities
- Tells you:
  - What must be managed to comply with the law, industry standards & company policy
  - What should be managed to protect business assets, time and resources
  - Which threats to eliminate, which to minimize and which to insure

What is the risk mitigation mix?

The absence of any one element creates
a major gap in your risk mitigation

- **Policy**
  - Information security
  - Acceptable use
  - Disaster recovery
  - Data access & storage
- **Technology**
  - Access control
  - Detection and monitoring
  - Audit tools
- **Process**
  - Risk review
  - Detection and response
  - 3rd party engagement
  - Legal / compliance sign-off
- **Training**
  - IT security training
  - Induction training
  - Regular reinforcement

What can digital risk insurance offer a business?

- Risk mitigation can never be 100% - you cannot mitigate unforeseen events
- Standard Commercial General Liability (CGL) policies now specifically exclude digital risks
- Provide evidence of best practice to shareholders, investors and auditors as digital risk insurance is only offered to those willing to mitigate their risks
- Empowers a company to use technology to its full potential

What level of digital risk insurance is needed?

- What is compulsory?
  - Required by law to protect employees, shareholders and ability to practice
- Where do we need to protect assets?
  - Needed to ensure longevity of the business
  - Total cost of the risk of downtime
  - Required to meet contractual and legal/compliance obligations

Assess · Mitigate · Insure

Best practices for a secure future

- By achieving digital insurability, organizations can leverage their technology infrastructure to deliver the real business benefits it was designed for without having to carry the additional risk on their balance sheet