



How To Succeed As A Chief Information Security Officer (CISO)

Dale Peterson, CISSP

Director, Network Security Practice

Digital Bond, Inc.

peterson@digitalbond.com



Digital Bond

- ◆ A network security consulting practice
 - Highly experienced, highly credentialed team
 - Security assessments, architecture, policy
- ◆ Very active in critical infrastructure security
 - Clients in water, electric, oil & gas
 - Clients that are SCADA system vendors
 - Wrote initial draft for Control Center standard
 - Selected by DHS for research grant

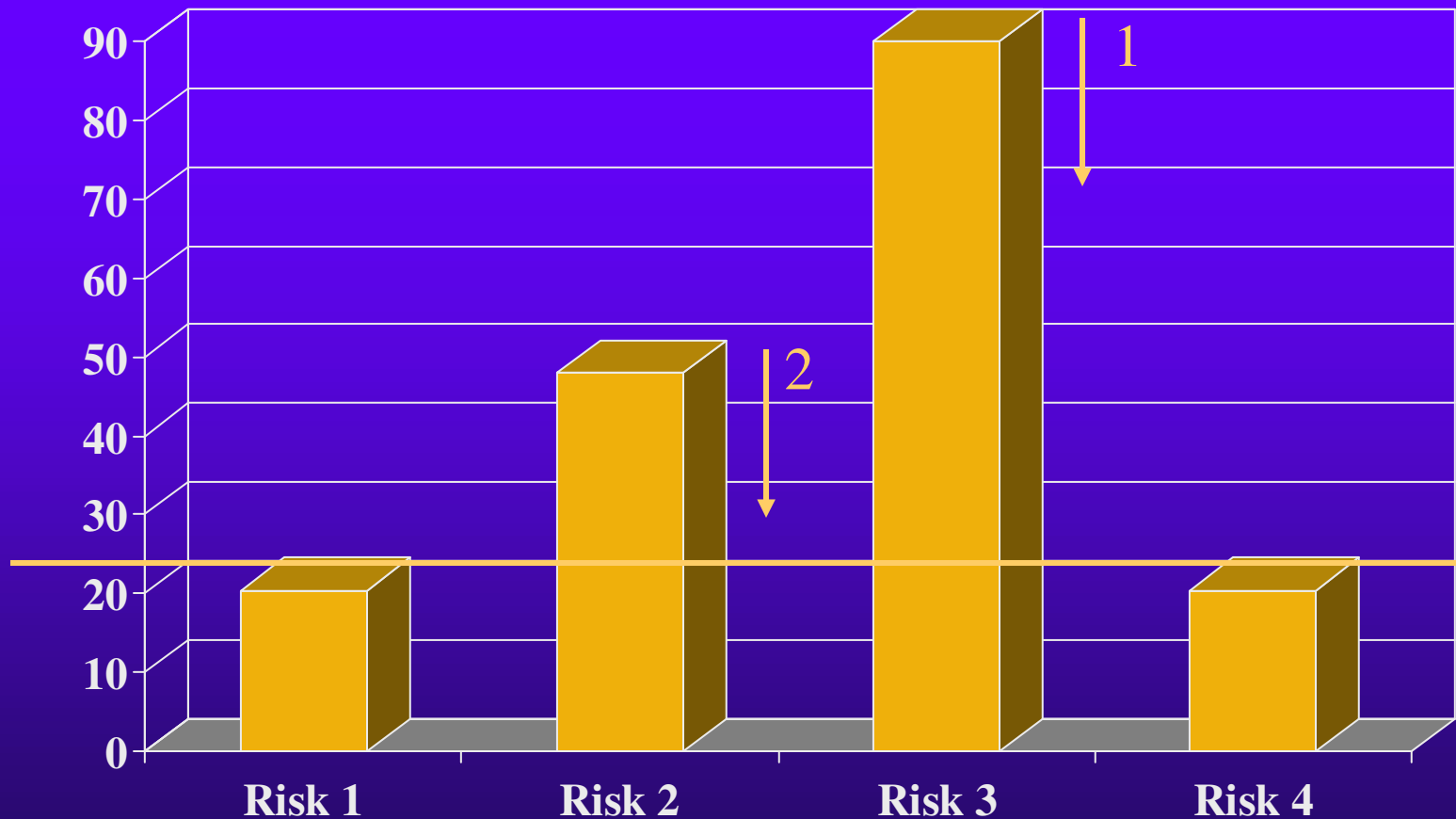


Risk Assessment Results

- ◆ Threat Agents
 - Hackers, disgruntled employees, ...
- ◆ Vulnerabilities
- ◆ Protection
 - Administrative and technical controls
- ◆ Consequences
- ◆ Risks
 - Quantitative or Qualitative Results



Where Do You Spend Money?





The Product Myth

- ◆ If I get a:
 - Firewall
 - Anti-virus gateway
 - Intrusion Detection System (IDS)

I will be secure

- ◆ Products should be purchased only to:
 - Reduce an unacceptable risk
 - Meet a security policy requirement



Administrative Controls

- ◆ Information security documents
 - Security policies, procedures, standards, and guidelines
- ◆ Security training
- ◆ Security awareness program
- ◆ Security audit



Information Security Policy

In a perfect world you do this first!

Security classifications/required protection

- Identify classification levels
 - Usually two or three
- Define and give examples
- What is required?
 - Strong authentication? Encryption? Audit?



Infrastructure Classification Example

- ◆ Confidential Classification
 - Drawings of physical infrastructure
 - Network documentation and configuration
 - Personal privacy information
 - Attorney/client and pre-release financials
- ◆ Confidential Protection
 - Strong, two-factor authentication
 - Encryption in transit or private network
 - All security audit options turned on



Information Security Policy

- ◆ Who the policy covers
- ◆ Information security team
- ◆ Authorized use
 - Connections to the network
- ◆ Legal requirements
 - USA - notice of monitoring

Each Policy Is Unique



Other Security Documents

- ◆ Department Security Policies
 - Based on the audience
 - IT, SCADA, Finance
- ◆ Security Procedures
 - More detailed, more frequently changed
 - Typically written for a limited audience
- ◆ Security Standards
 - Firewall is Vendor X, Version x.x
 - Anti-virus is Vendor Y
- ◆ Security Guidelines



Common Mistakes

- ◆ Policies you don't follow or enforce
 - No personal use of the e-mail system is allowed
 - How does a user know what policies they have to comply with?
- ◆ Policies that are guidelines
 - What does 'should' mean?
 - Always use 'must' or 'shall'
- ◆ Security Policy Cookbooks
 - Selecting from a list of procedures



Common Mistakes

- ◆ Policies that can't be tested
 - “Users must select a strong password”
 - “Administrators must apply the latest security patches to all systems”
- ◆ We recommend creating an audit document in conjunction with the security policy
 - Every must or shall has an audit statement
 - Installs rigor in the policy statements



Security Architecture

- ◆ Provide the required protections
 - No more, no less
 - Policy drives architecture, not vice versa
 - Security requirements for new apps are easy
- ◆ Make it transparent for the user
 - Automatic encryption with SSL or IPSec
 - Firewalls enforcing authorized uses
 - Single sign-on (SSO)



Trend – Internal Security Zones

- ◆ Firewalls are not just for the Internet
- ◆ Create internal zones
 - Mission critical servers
 - SCADA networks
 - Semi-trusted networks for customers and partners
 - Wireless zones



Trend – Microsoft Security

- ◆ Security standards in Active Directory
- ◆ Support for two-factor authentication
 - Smart cards, biometrics, tokens
- ◆ Group Policy
 - Encryption for file servers
 - IP filters / server firewalls
 - Idle timeouts
 - Software settings and more



Trend – Security Monitoring

- ◆ Logs and Intrusion Detection Systems (IDS) generate large amounts of useful info
 - Timely review is important
 - Identify and stop attacks early on
 - If you don't review, you have wasted money
- ◆ Managed Security System Providers(MSSP)
 - Monitor your systems 24x7
 - Co-source / portal approach



Security Awareness & Training

- ◆ Initial training focuses on the policy
- ◆ Vary the media
 - Videos, e-mails, posters, quizzes, demos
 - Small, frequent reminders are more effective
- ◆ Must apply to all users
 - Executives must lead by example



Security Audit

- ◆ Audit tests were created with the policy
 - Objective, practical tests
- ◆ First audit results are typically poor
 - 50% compliance
 - Great training and awareness event
- ◆ Follow on audits should be much better
 - Corrective actions required
 - Must be willing to enforce the policy



Keys for success

- ◆ Spend your time and money wisely
 - Use your risk assessment
 - Determine your security policy and required protection before spending money
 - Automation & transparency whenever possible
 - Awareness program and audit