Locking Up Your Storage Network

Making SANs Secure

Session ID #: 1445

Kamy Kavianian, CISSP
Director, Product Marketing
Network Security and Architecture
Brocade Communications Systems

BROCADE
The intelligent platform for networking storage

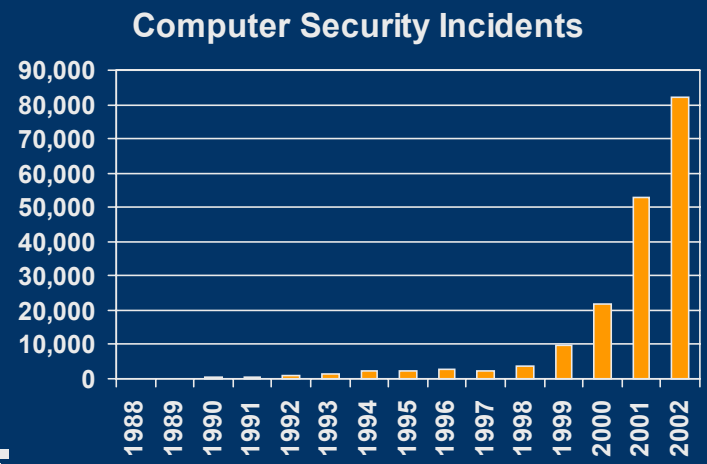
August 14, 2003

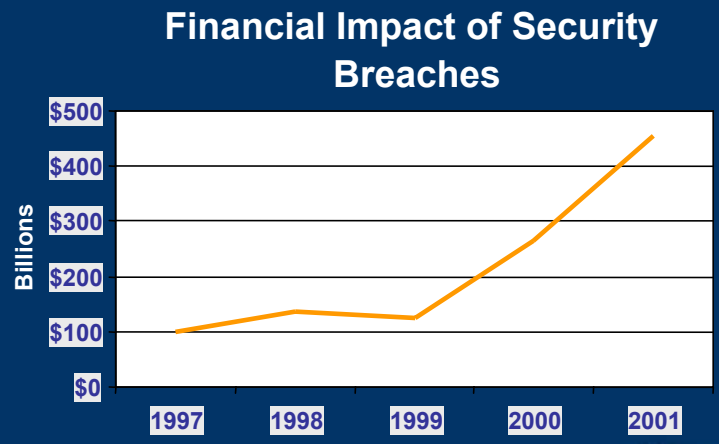
Agenda

- Security market and challenges
- SAN security vulnerabilities and threats
- SAN security scenarios
- Fabric based security
- Security appliances
- More information

SAN and General Security Landscape

- **Storage Security became an essential aspect of customers' deployment strategies** *(Yankee Group, 2002)*
- **Security Threats are Growing in Numbers and Sophistication**
  (Source: www.cert.org/stats/cert_stats.html)
  - 2000 incidents = 21,756
  - 2001 incidents = 52,658
  - 2002 incidents = 82,094
- **Eighty percent of all network security managers claim their biggest security threat comes from their own employees.** *(Source Gartner, May 2002)*
- **The financial impact of security breaches has escalated dramatically**
  (Source: PWC\ASIS\U.S. Chamber of Commerce, 2002)
  - Estimated losses totaled $59 billion in 2001
  - Average cost per incident was $404,000
  - Greatest impacts were increased legal fees, company embarrassment, loss of revenue and competitive advantage.





Source: 1Q 2002 CSI/FBI Computer Crime and Security Survey

2003 Storage Market Survey

Theme: Flexibility, Data protection, and Cost control

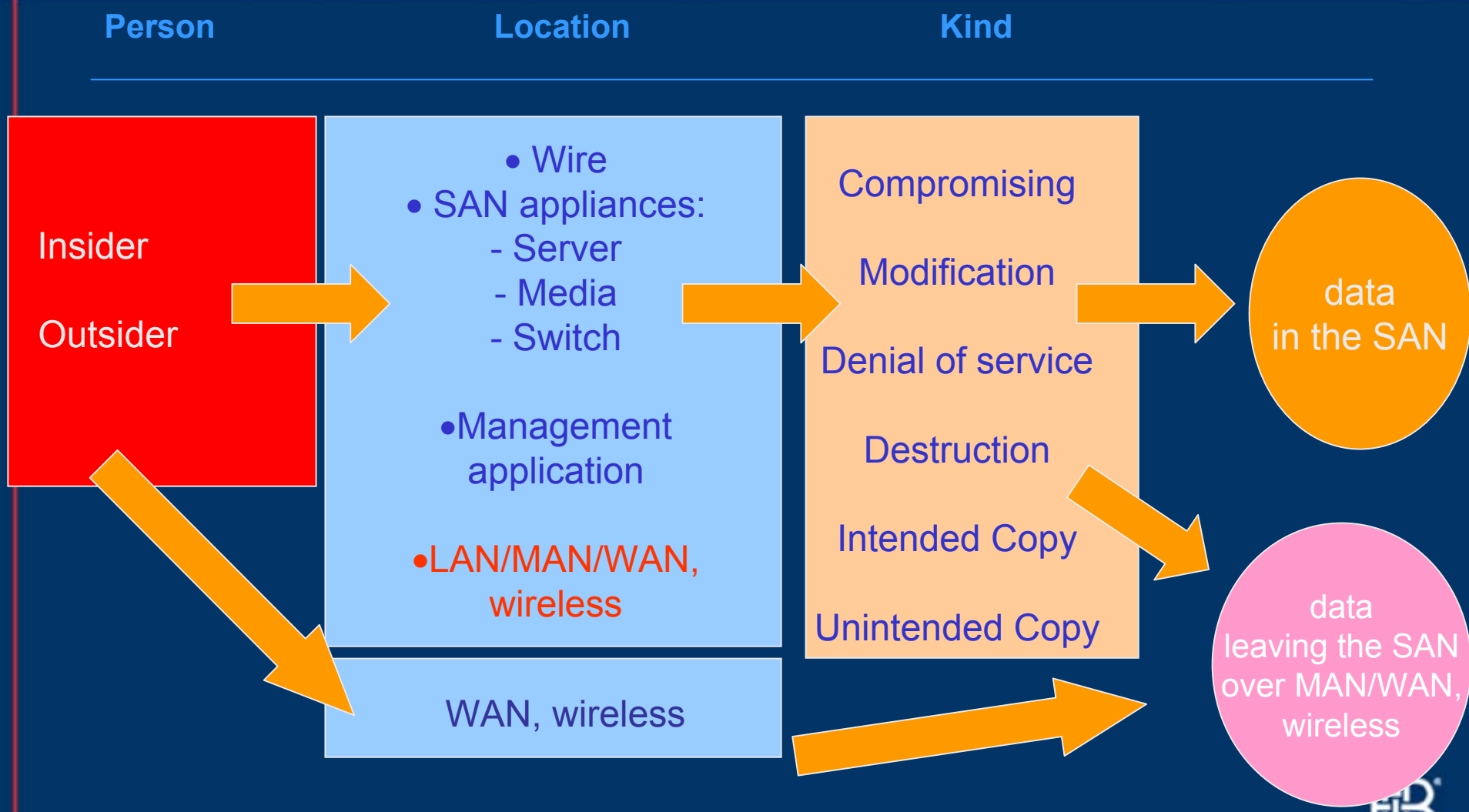
Cost	71%
Reliability	61%
Compatibility with existing systems	54%
Security	**54%**
Maintenance	51%
Scalability	41%
Interoperability	41%
Other projects have higher priority	20%
Recruiting talented employees to manage technology	19%
Integration of products from multiple vendors	17%

Source: *InfoWorld 2003 Storage Survey*

Why Secure SANs?

- Security is a fundamental requirement for enterprise SANs, just like any other network
  - Many entry points into the SAN (users, devices, apps)
  - SANs interconnected over WANs / MANs (DWDM, SONET, IP etc.,)
  - SAN management applications
- SANs require change management controls (configuration integrity) to prevent, disruption, network downtime, and improve availability
- New regulations
  - HIPAA (healthcare)
    - Health Insurance Portability & Accountability Act of 1996 (August 21), Public Law 104-191Act.
  - Financial Modernization Act (Graham-Leach-Bliley Act)
  - California SB 1386 (privacy)
- Multi-tenant environments have new security requirements
  - Security enables sharing of SAN resources among multiple customers securely
  - Reduces multi-tenant network infrastructure costs and enables economies of scale

Types of Threats
(ANSI T11.3 FC-SP & IETF IPstorage)



Level of Threats against SANs (ANSI T11.3 FC-SP)

- T11.3 Security Working Group has identified 17 threats
- Classification of possibility of appearance: High (1) , medium (15) , low (1)

	Persons
*** High: Use of management applications (Local, MAN/WAN, & wireless)	Insider & Outsider (intentional or unintentional)
** Medium: Use of server, switch and direct access to media	Insider and Outsider
* Low: Direct access to the wire	Insider (intentional or unintentional)