

Defense in Depth: Enterprise Information Security in Challenging Times



William A. Estrem, Ph.D.
College of Business
University of St. Thomas

Agenda

- What are the key trends, opportunities, and threats that will impact organizations in the future?
- How can organizations manage their Information Technology assets to protect against a variety of threats?
- What guidelines, standards, and best practices can be observed to build a coordinated multilevel security architecture?



April 16, 2003

Copyright 2003 - Wm A. Estrem Associates

2

Emerging Trends

- Global tensions
 - Increased threats of cybercrime
 - Increased governmental scrutiny of information
- Continued economic pressures
 - Focus on corporate responsibility and accountability
 - Virtualization of enterprise functions
 - Downsizing and outsourcing
- Expansion of telecommunications capabilities
 - Pervasive accessibility
 - Surplus capacity
- Commoditization of Information Technology
 - Increased viability and acceptance of Open Source
 - Progress on key Information Technology standards



April 16, 2003

Copyright 2003 - Wm A. Estrem Associates

3

A False Sense of Security

- Enterprise Security is a mess
 - Multiple competing and incompatible solutions
 - Developers don't build in effective security
 - Users circumvent security in self-defense
- e-Business raises the bar
 - Current standards are woefully inadequate
 - Point solutions won't scale
 - Interoperable solutions are needed



April 16, 2003

Copyright 2003 - Wm A. Estrem Associates

4

Fear, Uncertainty, and Doubt

- Management is fearful of the risks
- Management is uncertain that investments in security infrastructures will yield assurance
- Management is doubtful that they can safely manage the policies involved in deploying significant business solutions in the extended enterprise
- As with other infrastructure investments, it is difficult to justify using traditional ROI models

Net Result: A barrier to deployment

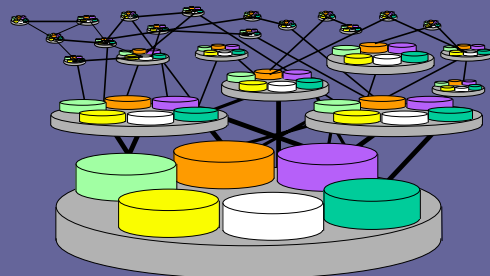


April 16, 2003

Copyright 2003 - Wm A. Estrem Associates

5

Oh, What a Tangled Web We Weave...



April 16, 2003

Copyright 2003 - Wm A. Estrem Associates

6

Toward the Virtual Enterprise

April 16, 2003 Copyright 2003 - Wm A. Estrem Associates 7

Being Virtual

- Federation across the Value Chain requires the ability to dynamically establish secure, trusted connections using standards-based methods
- Utility computing methods such as Web Services and Grid Computing could enhance inter-organizational communications and collaboration
- Web-based protocols such as HTTP can pass through firewalls more readily than conventional protocols

April 16, 2003 Copyright 2003 - Wm A. Estrem Associates 8

Virtual Enterprise: Critical Success Factors

- **Fluidity**
 - "Soft-wired" organizational structure
 - Roles vs. rigid job descriptions
 - Dynamic/continuous teaming to get work done
- **Flatness**
 - Flattened information channels for sharing, reassuring, lobbying, coaching, etc.
 - Constant informal involvement vs. formal/meeting intervention
- **Trust**
 - Collaboration among members is expected
 - Individual performance and "reputation risk" matters
- **Culture**
 - Chemistry varies within each organization – no one model works for everyone

All of these factors must exist in some degree to be successful.
Source: Philip Evans (2000), *Blown to Bits*

April 16, 2003 Copyright 2003 - Wm A. Estrem Associates 9

Learning to Share

- **Information Exchange**
 - Integration of disparate business processes and technologies
 - Accommodating different information management practices
 - Managing the lifecycle of information across the virtual organization
- **Cultural Differences**
 - Strategy, policy and procedural conflicts
 - Transorganizational project management
 - Change Management
- **Legal Constraints**
 - Transnational legal and regulatory compliance
 - Intellectual property management
 - Risk Management

April 16, 2003 Copyright 2003 - Wm A. Estrem Associates 10

Evolution of Information Systems

April 16, 2003 Copyright 2003 - Wm A. Estrem Associates 11

Web Services

April 16, 2003 Copyright 2003 - Wm A. Estrem Associates 12

Web Services Standards

- Worldwide Web standards such as XML, HTTP are fairly mature and robust
- Web Services standards such as UDDI, WSDL, and SOAP are still immature
- Next Generation Web Services standards such as security, workflow and transactions are very early in their development

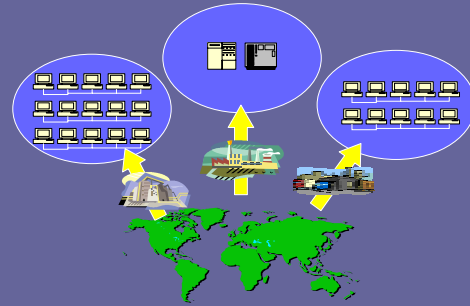


April 16, 2003

Copyright 2003 - Wm A. Estrem Associates

13

Grid Computing



April 16, 2003

Copyright 2003 - Wm A. Estrem Associates

14

Grid Computing

- Fusion of several recent trends:
 - Internet and Worldwide Web
 - Web Services
 - Open Sourcecode
 - Cluster computing
 - Autonomic computing



April 16, 2003

Copyright 2003 - Wm A. Estrem Associates

15

Grid Computing

- What can a Grid do?
 - Exploiting underutilized resources
 - On-demand access to resources
 - Parallel CPU operations
 - Applications
 - Enabling Virtual Organizations
 - Reliability
 - Manageability
- Types of Grids
 - Computational
 - Data
 - Storage
 - Access
- Topologies
 - IntraGrid
 - ExtraGrid
 - InterGrid



April 16, 2003

Copyright 2003 - Wm A. Estrem Associates

16

Utility Computing

- Technological Capabilities
 - Higher degree of interoperability between systems
 - Flexible, loosely coupled integration
 - Enhanced collaborative capabilities
- Organizational Impacts
 - Users will be able to dynamically locate and compose applications to meet their individual requirements
 - Organizations could experience increased flexibility and effectiveness
- Economic Forces
 - Software by the sip
 - New pricing and distribution models
 - What will be the "cost of ownership"?



April 16, 2003

Copyright 2003 - Wm A. Estrem Associates

17

Trends in Information Security

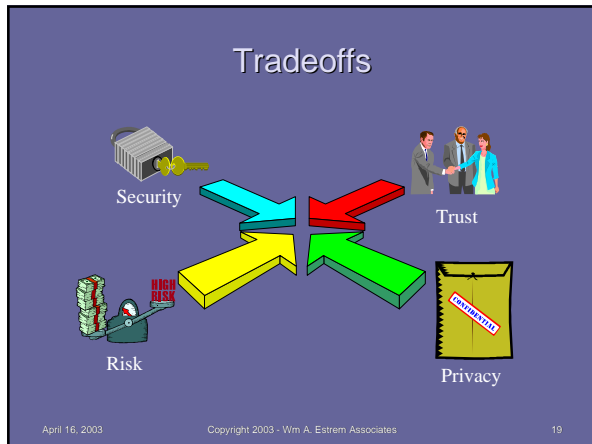
- Shifting the focus from Technical Measures to Trust Management and Loss Prevention
- Evidence-based Security Systems
- Digital Rights Management Systems
- Defense in Depth
 - Positive Identification - Strong Authentication
 - Extensible Policy-based Authorization
 - Standardized security functions embedded in components
 - Pluggable, Modular, Interoperable across vendor architectures
 - Must be extended across enterprise boundaries



April 16, 2003

Copyright 2003 - Wm A. Estrem Associates

18



- ## Critical Issues for Enterprise Security
- Enforcing business policy across the enterprise
 - Business Rules & Policies
 - Authorities and Permissions
 - Preventing losses from:
 - Fraud
 - Theft
 - Disclosure
 - Protection from malicious attack
 - Spoofing
 - Lurking/Eavesdropping
 - Intrusion
 - Denial of Service
-
- April 16, 2003 Copyright 2003 - Wm A. Estrem Associates 20

- ## Balancing Security and Privacy Issues
- Individuals are increasingly aware of and concerned about privacy issues
 - Organizations must balance security and policy enforcement against the needs to safeguard the privacy of customer information
 - What are we entitled to do with customer information?
 - What are our obligations?
 - Notification
 - Choice
 - Access
 - Protection
-
- April 16, 2003 Copyright 2003 - Wm A. Estrem Associates 21

- ## Saving Private Data
- Protection of organizational information assets
 - Business continuity
 - Ability to respond appropriately to request for information
 - Patriot Act
 - Sarbanes-Oxley Act
-
- April 16, 2003 Copyright 2003 - Wm A. Estrem Associates 22

- ## Defining an Enterprise Security Architecture
- Understand your organization's culture and context
 - Define Roles and Responsibilities
 - Company Employees
 - Trading Partners, Suppliers, Contractors, Customers
 - Document Business Practices, Standards and Procedures
 - Principles
 - Policies
 - Standards
 - Procedures and Workflows
 - Regulatory Compliance
 - Access and Accountability
 - Audit, Control and Reporting
 - Business Continuity Plan
-
- April 16, 2003 Copyright 2003 - Wm A. Estrem Associates 23

- ## Enterprise Security: Key Functional Requirements
- Identification and Authentication
 - Authorization and Access Control
 - Data Privacy and Integrity
 - Firewalls, Proxies, and Virtual Private Networks
 - Secure Mobility
 - Virus Protection, Intrusion Detection, and Content Control
 - Auditing, Detection, and Monitoring
 - Business Continuity
-
- April 16, 2003 Copyright 2003 - Wm A. Estrem Associates 24

Business Continuity

- Disaster Preparedness
 - Redundant Systems and Networks
 - Parallel Systems with Automatic Failover
 - Outsourced Services – Adequate Service Level Agreements?
 - Hot Sites
 - Effective Backup and Offsite Storage
 - Emergency Power Supplies
- Business Continuity Planning
 - Scenarios: Expect the unexpected
 - Establish Operational Plans
 - Rehearse & Evaluate



April 16, 2003

Copyright 2003 - Wm A. Estrem Associates

25

ISO 17799

Best Practices for Information Security

- Business Continuity Planning
- System Access Control
- System Development and Maintenance
- Physical and Environmental Security
- Compliance
- Personnel Security
- Security Organization
- Computer & Network Management
- Asset Classification and Control
- Security Policy

April 16, 2003

Copyright 2003 - Wm A. Estrem Associates

26

Looking Forward

- Global political, social, and economic tensions increase the need for effective enterprise security
- Enterprise security is challenging and costly because of the lack of standards and inconsistent vendor implementations of the standards that do exist
- The increasing virtualization of enterprise functions demands the implementation of standards that enable interoperability of security systems
- Deploying an enterprise security architecture requires a comprehensive, global, architectural perspective
- The emphasis on technical countermeasures must shift toward more business-focused solutions that balance security, trust, risk, and privacy issues
- Security and Privacy are not fads...

April 16, 2003

Copyright 2003 - Wm A. Estrem Associates

27

References on Information Security

- Computer Security Resource Center
 - <http://csrc.nist.gov/>
- Computer Emergency Response Team (CERT)
 - <http://www.cert.org/>
- Critical Infrastructure Assurance Office
 - <http://www.ciaa.gov/>
- U.S. Department of Justice: Cybercrime.gov
 - <http://www.usdoj.gov/criminal/cybercrime>
- National Strategy to Secure Cyberspace
 - <http://www.whitehouse.gov/ncsc/p/>
- ISO 17799 Information
 - <http://www.iso-17799-security-world.co.uk/what.html>

April 16, 2003

Copyright 2003 - Wm A. Estrem Associates

28

References on Information Privacy

- Electronic Freedom Frontier
 - <http://www.EFF.org>
- Electronic Privacy Information Center
 - <http://www.epic.org>
- European Commission – Information Society
 - http://europa.eu.int/information_society/index_en.htm
- TRUSTe
 - <http://www.truste.com>
- U.S. Department of Justice: Cybercrime.gov
 - <http://www.usdoj.gov/criminal/cybercrime/privacy.html>
- U.S. Healthcare financing Administration – HIPAA Information
 - <http://www.hcfa.gov/medicaid/hipaal/>
- U.S. Federal Trade Commission - Gramm-Leach-Bliley Act
 - <http://www.ftc.gov/privacy/glbact/index.html>

April 16, 2003

Copyright 2003 - Wm A. Estrem Associates

29