open.michigan

Author(s): Don M. Blumenthal, 2010

Citation Key

for more information see: http://open.umich.edu/wiki/CitationPolicy

Use + Share + Adapt

{ Content the copyright holder, author, or law permits you to use, share and adapt. }

Public Domain – Government: Works that are produced by the U.S. Government. (USC 17 § 105)

Public Domain – Expired: Works that are no longer protected due to an expired copyright term.

Public Domain – Self Dedicated: Works that a copyright holder has dedicated to the public domain.

Creative Commons – Zero Waiver

Creative Commons – Attribution License

Creative Commons – Attribution Share Alike License

Creative Commons – Attribution Noncommercial License

Creative Commons – Attribution Noncommercial Share Alike License

GNU – Free Documentation License

Make Your Own Assessment

{ Content Open.Michigan believes can be used, shared, and adapted because it is ineligible for copyright. }

Public Domain – Ineligible: Works that are ineligible for copyright protection in the U.S. (USC 17 § 102(b)) *laws in your jurisdiction may differ

{ Content Open.Michigan has used under a Fair Use determination. }

Fair Use: Use of works that is determined to be Fair consistent with the U.S. Copyright Act. (USC 17 § 107) *laws in your jurisdiction may differ

Our determination **DOES NOT** mean that all uses of this 3rd-party content are Fair Uses and we **DO NOT** guarantee that your use of the content is Fair.

To use this content you should **do your own independent analysis** to determine whether or not your use will be Fair.

Enterprise Security Program Technology and Planning

510 - Data Security and Privacy: Legal, Policy, and Enterprise Issues
University of Michigan School of Information
Week 12

Technology

- Strategy
- Components
- Administration

Strategy

- Intersection of business and information
- Planned growth
- Separation of systems
  - Zones
  - Layers
  - Defense in depth

Strategy Considerations

- Becoming more complex over time
  - One gateway before; now many
- Priorities
  - Legal more likely to be clear than business and tech
- Zones
  - Systems such as extranet, intranet
  - Mission ranking such as critical, high priority….
- Layers
- Best products vs integrated approaches

Components

- Architecture
- AAA
  - By system and application
  - Authentication – who
  - Authorization – permission
  - Accounting – auditing and resource use
- Discrete systems
  - IDS
  - Firewall
  - Authentication

Authentication Factors

- Single – something you know
- Two – something you have
- Three - something you are
- Four – where you are

Overload

- Risk of too much information
- Set priorities and decide on resources
- Organize
  - Events
  - Alerts
  - Incidents

Administration

- Testing
  - Scan and remedy
  - Internal and external review
  - Metrics
  - Updates
- Change management
  - To handle future requirements

InfoSec Roadmap

- Information security methodology
- Business requirements framework
  - Current state
  - Requirements analysis; current and future
- InfoSec program components
  - People, processes, technology
- Roadmap to future
  - How to get there

High-level Analytical Components

- **CIA**
- **Least privilege**
- **Speed vs control**
  - Access and speed vs confidence and control

Security Assessment

- Take components and apply
- Examine
- Perform gap analysis
  - Separate strategic from tactical
- Roadmap presents alternatives for addressing gaps

Assessing Alternatives

- Tech vs business
  - With legal lurking over all
- Benefits vs probability
- Benefits vs cost
- Downtime from problem
- Initial and ongoing costs
- Non-proprietary
- Led to security problems and other nuisances

The Future

- Simplification
  - Multipurpose appliances combine safeguards
- Proactive tools
  - Heuristic malware analyses
- Improved management
  - For systems and applications
  - Technical solutions to identify and address issues; combinations, pattern analyses
  - Refined review/audit techniques