JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Regulatory Requirements

VULNERABILITY MANAGEMENT

Vulnerability Management Requirements

- As you begin to develop your vulnerability management program, you must understand the requirements you might have…

- Regulatory Requirements
  - (HIPAA, GLBA, PCI DSS, FISMA, etc.)

- Corporate Policy-based Requirements
  - (Targets, frequency, etc.)

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Regulatory Requirements

- Laws and regulations that govern information storage and processing
  - HIPAA
  - GLBA
  - FERPA
- Laws and regulations that require vulnerability management programs
  - PCI DSS
  - FISMA

Payment Card Industry Data Security Standard (PCI DSS)

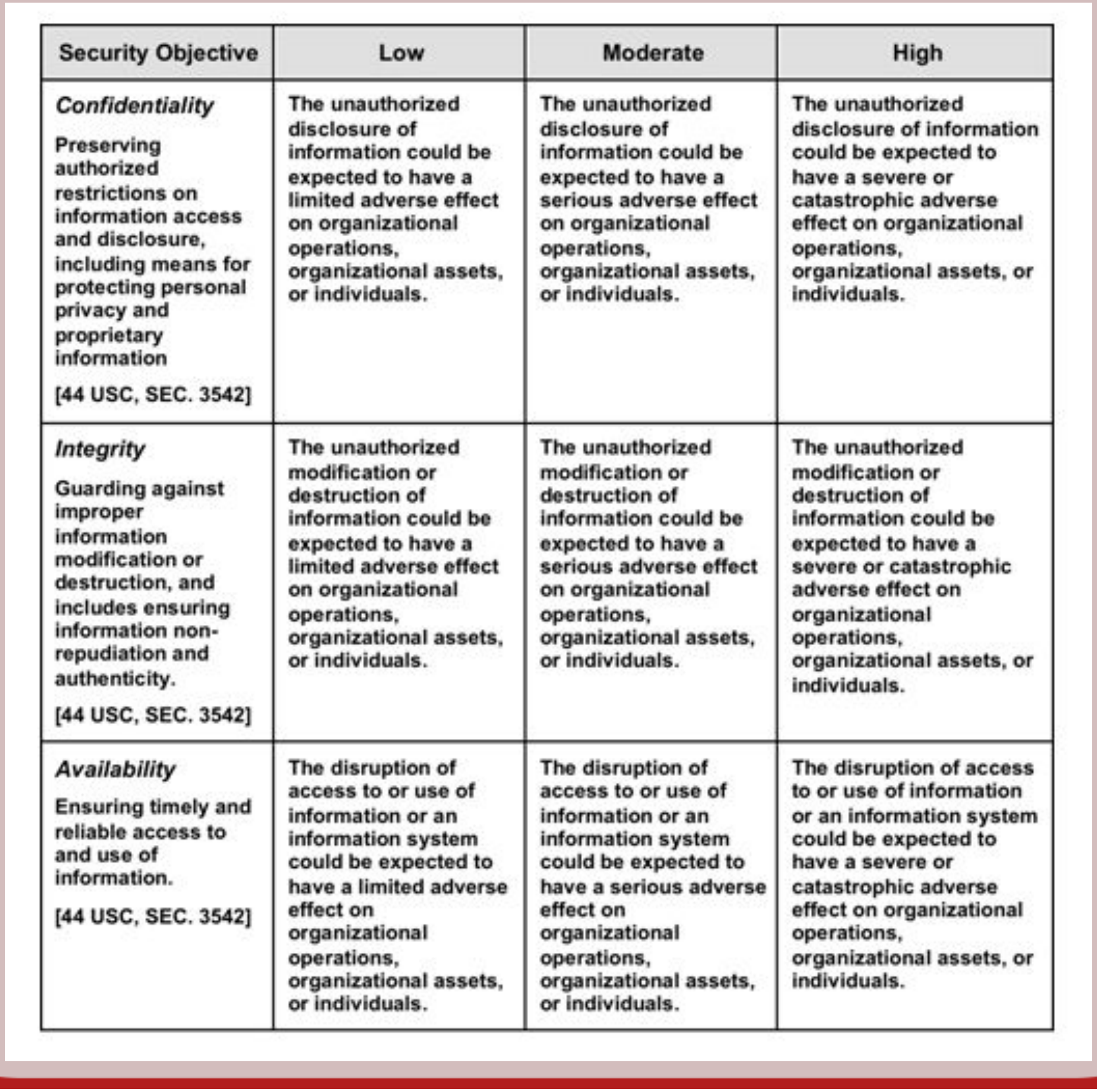
- Specifies security controls for credit card processors and merchants
- Most specific of any requirement for vulnerability management
- Examples:
  - Internal and external scans must be conducted
  - Scanned at least quarterly and all major changes
  - Internal scans by qualified personnel
  - External scans by Approved Scanning Vendor
  - Remediate any high-risk vulnerabilities and rescan until a “clean” report is achieved

Federal Information Security Management Act (FISMA)

- Specifies security controls for government
  - Both agencies and organizations that run systems

- Systems are classified as low, moderate, or high impact which dictate the requirements

Federal Information Security Management Act (FISMA)



Security Objective	Low	Moderate	High
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information [44 USC, SEC. 3542]	The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 USC, SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 USC, SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

FISMA Requirements

- Scan systems when new threats emerge
- Use tools/techniques that are interoperable
- Analyze scan reports from assessments
- Remediate vulnerabilities based on risk
- Share findings with other agencies to eliminate similar vulnerabilities in other systems