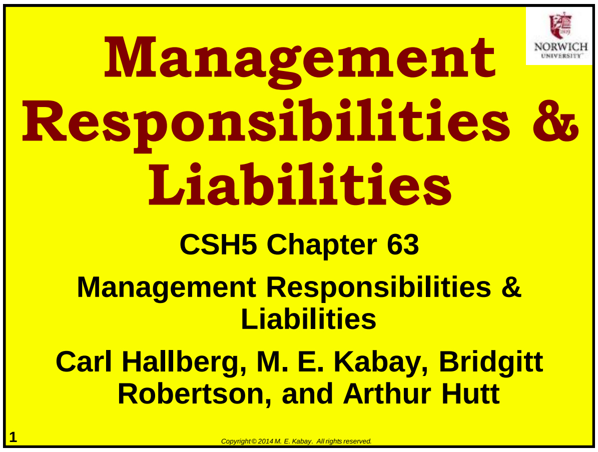


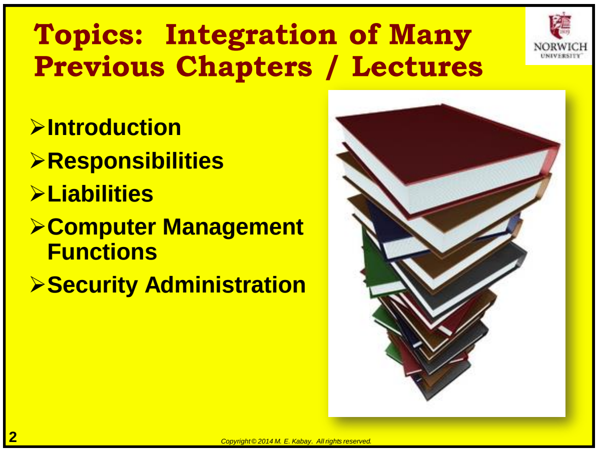
Management Responsibilities & Liabilities

CSH5 Chapter 63

Management Responsibilities & Liabilities

Carl Hallberg, M. E. Kabay, Bridgitt Robertson, and Arthur Hutt

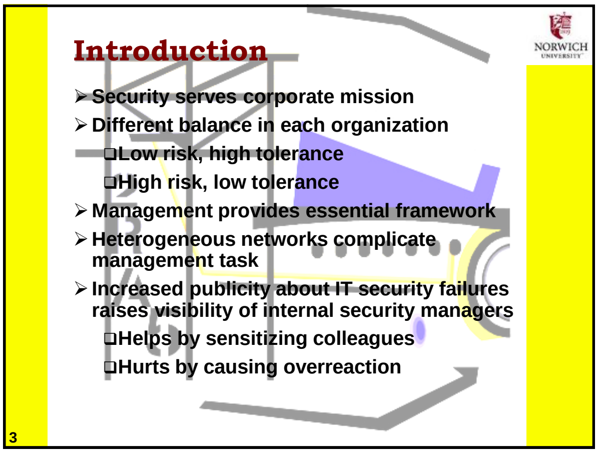
1



Topics: Integration of Many Previous Chapters / Lectures

- Introduction
- Responsibilities
- Liabilities
- Computer Management Functions
- Security Administration

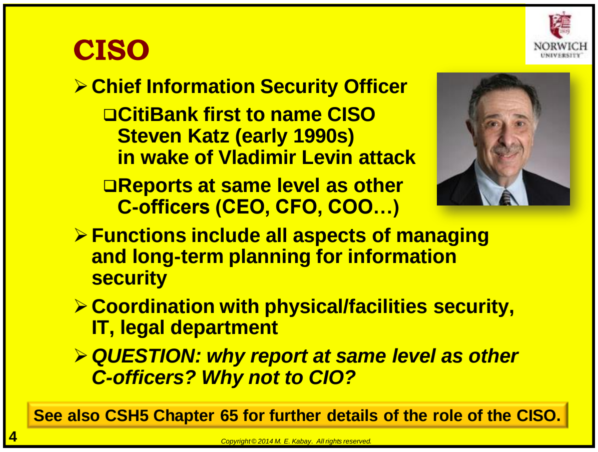
2



Introduction

- Security serves corporate mission
- Different balance in each organization
  - ❑Low risk, high tolerance
  - ❑High risk, low tolerance
- Management provides essential framework
- Heterogeneous networks complicate management task
- Increased publicity about IT security failures raises visibility of internal security managers
  - ❑Helps by sensitizing colleagues
  - ❑Hurts by causing overreaction

3

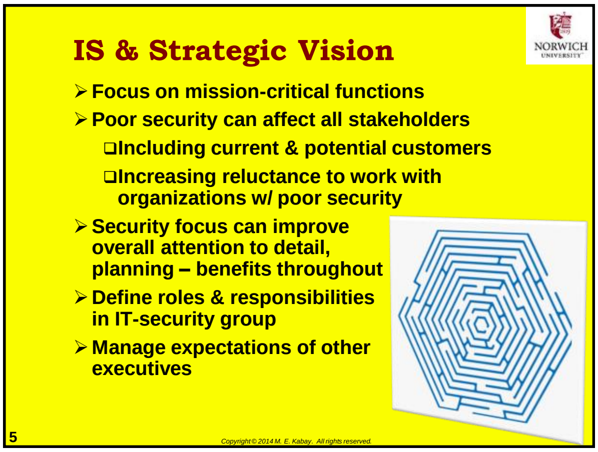


CISO

- Chief Information Security Officer
  - ❑CitiBank first to name CISO Steven Katz (early 1990s) in wake of Vladimir Levin attack
  - ❑Reports at same level as other C-officers (CEO, CFO, COO…)
- Functions include all aspects of managing and long-term planning for information security
- Coordination with physical/facilities security, IT, legal department
- *QUESTION: why report at same level as other C-officers? Why not to CIO?*

See also CSH5 Chapter 65 for further details of the role of the CISO.

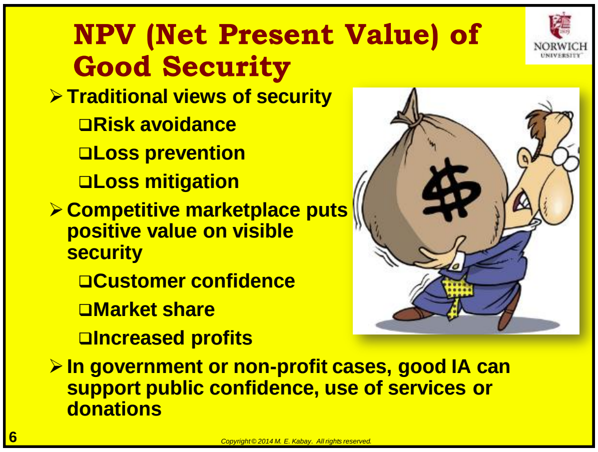
4



IS & Strategic Vision

- Focus on mission-critical functions
- Poor security can affect all stakeholders
  - ❑Including current & potential customers
  - ❑Increasing reluctance to work with organizations w/ poor security
- Security focus can improve overall attention to detail, planning – benefits throughout
- Define roles & responsibilities in IT-security group
- Manage expectations of other executives

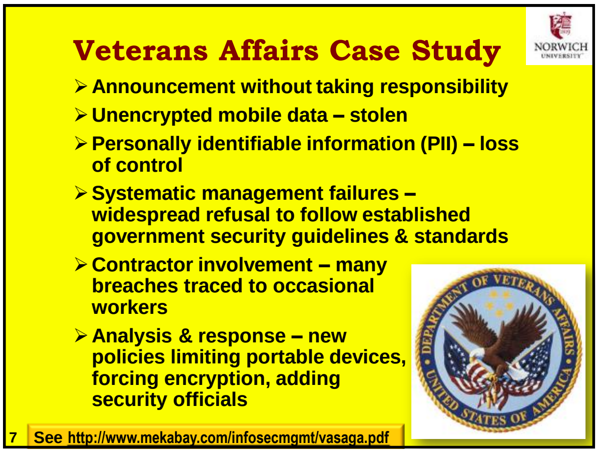
5



NPV (Net Present Value) of Good Security

- Traditional views of security
  - ❑Risk avoidance
  - ❑Loss prevention
  - ❑Loss mitigation
- Competitive marketplace puts positive value on visible security
  - ❑Customer confidence
  - ❑Market share
  - ❑Increased profits
- In government or non-profit cases, good IA can support public confidence, use of services or donations

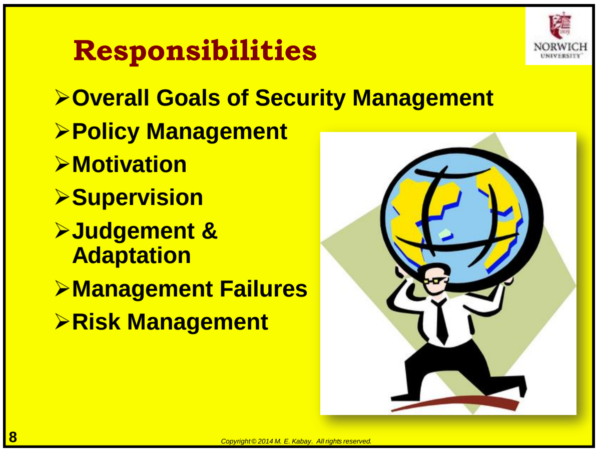
6



Veterans Affairs Case Study

- Announcement without taking responsibility
- Unencrypted mobile data – stolen
- Personally identifiable information (PII) – loss of control
- Systematic management failures – widespread refusal to follow established government security guidelines & standards
- Contractor involvement – many breaches traced to occasional workers
- Analysis & response – new policies limiting portable devices, forcing encryption, adding security officials

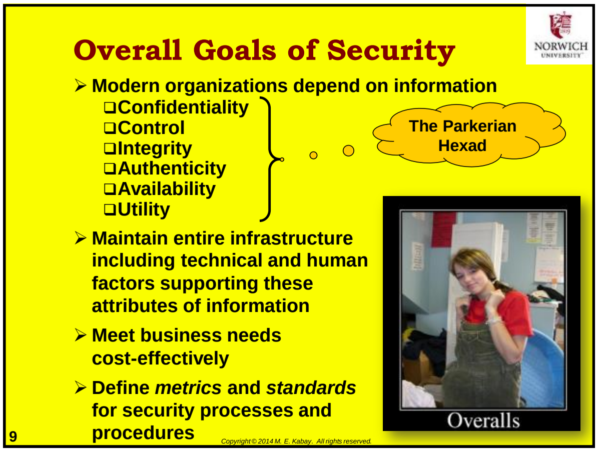
7 See http://www.mekabay.com/infosecmgmt/vasaga.pdf



Responsibilities

- Overall Goals of Security Management
- Policy Management
- Motivation
- Supervision
- Judgement & Adaptation
- Management Failures
- Risk Management

8 Copyright © 2014 M. E. Kabay. All rights reserved.



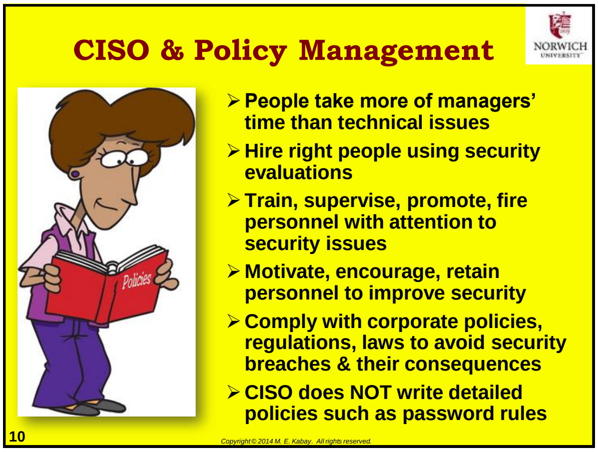
Overall Goals of Security

- Modern organizations depend on information
  - ❑Confidentiality
  - ❑Control
  - ❑Integrity
  - ❑Authenticity
  - ❑Availability
  - ❑Utility

The Parkerian Hexad

- Maintain entire infrastructure including technical and human factors supporting these attributes of information
- Meet business needs cost-effectively
- Define *metrics* and *standards* for security processes and procedures

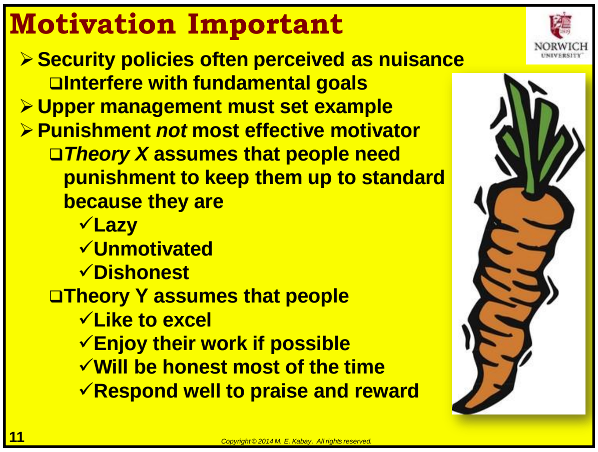
9 Copyright © 2014 M. E. Kabay. All rights reserved.



CISO & Policy Management

- People take more of managers' time than technical issues
- Hire right people using security evaluations
- Train, supervise, promote, fire personnel with attention to security issues
- Motivate, encourage, retain personnel to improve security
- Comply with corporate policies, regulations, laws to avoid security breaches & their consequences
- CISO does NOT write detailed policies such as password rules

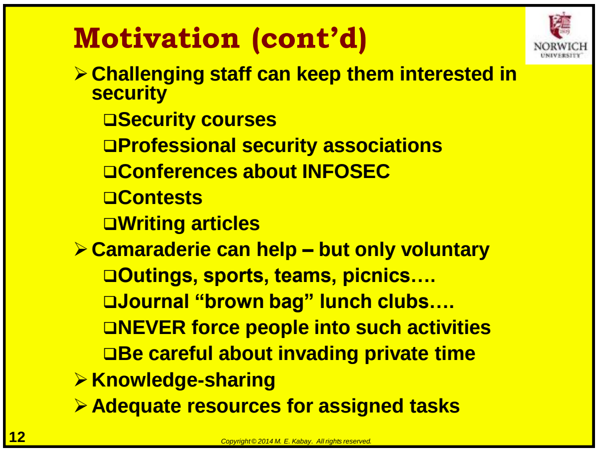
10 Copyright © 2014 M. E. Kabay. All rights reserved.



Motivation Important

- Security policies often perceived as nuisance
  - ❑Interfere with fundamental goals
- Upper management must set example
- Punishment *not* most effective motivator
  - ❑*Theory X* assumes that people need punishment to keep them up to standard because they are
    - ✓Lazy
    - ✓Unmotivated
    - ✓Dishonest
  - ❑Theory Y assumes that people
    - ✓Like to excel
    - ✓Enjoy their work if possible
    - ✓Will be honest most of the time
    - ✓Respond well to praise and reward

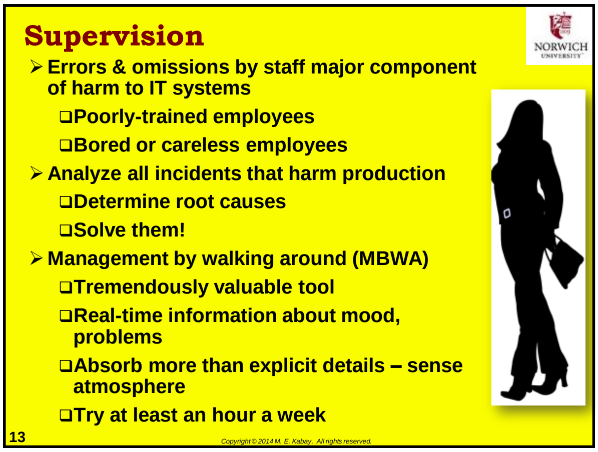
11 Copyright © 2014 M. E. Kabay. All rights reserved.



Motivation (cont'd)

- Challenging staff can keep them interested in security
  - ❑Security courses
  - ❑Professional security associations
  - ❑Conferences about INFOSEC
  - ❑Contests
  - ❑Writing articles
- Camaraderie can help – but only voluntary
  - ❑Outings, sports, teams, picnics….
  - ❑Journal "brown bag" lunch clubs….
  - ❑NEVER force people into such activities
  - ❑Be careful about invading private time
- Knowledge-sharing
- Adequate resources for assigned tasks

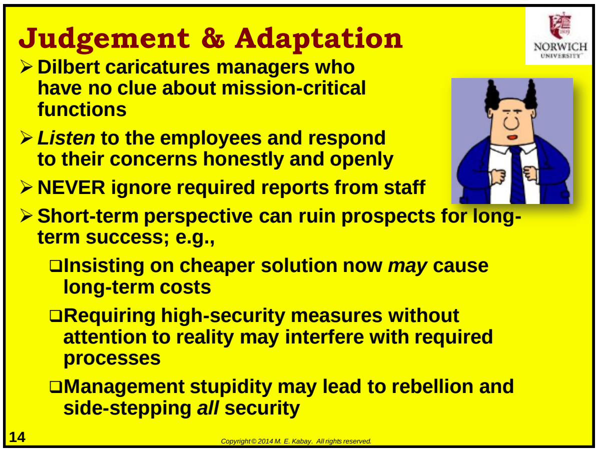
12 Copyright © 2014 M. E. Kabay. All rights reserved.



Supervision

- Errors & omissions by staff major component of harm to IT systems
  - ❑Poorly-trained employees
  - ❑Bored or careless employees
- Analyze all incidents that harm production
  - ❑Determine root causes
  - ❑Solve them!
- Management by walking around (MBWA)
  - ❑Tremendously valuable tool
  - ❑Real-time information about mood, problems
  - ❑Absorb more than explicit details – sense atmosphere
  - ❑Try at least an hour a week

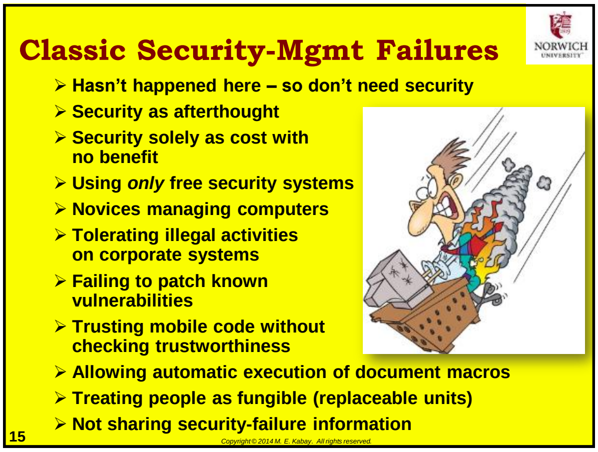
13



Judgement & Adaptation

- Dilbert caricatures managers who have no clue about mission-critical functions
- *Listen* to the employees and respond to their concerns honestly and openly
- NEVER ignore required reports from staff
- Short-term perspective can ruin prospects for long-term success; e.g.,
  - ❑Insisting on cheaper solution now *may* cause long-term costs
  - ❑Requiring high-security measures without attention to reality may interfere with required processes
  - ❑Management stupidity may lead to rebellion and side-stepping *all* security

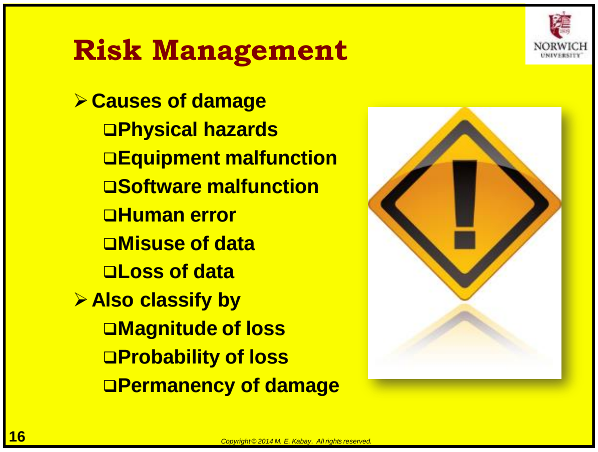
14



Classic Security-Mgmt Failures

- Hasn't happened here – so don't need security
- Security as afterthought
- Security solely as cost with no benefit
- Using *only* free security systems
- Novices managing computers
- Tolerating illegal activities on corporate systems
- Failing to patch known vulnerabilities
- Trusting mobile code without checking trustworthiness
- Allowing automatic execution of document macros
- Treating people as fungible (replaceable units)
- Not sharing security-failure information

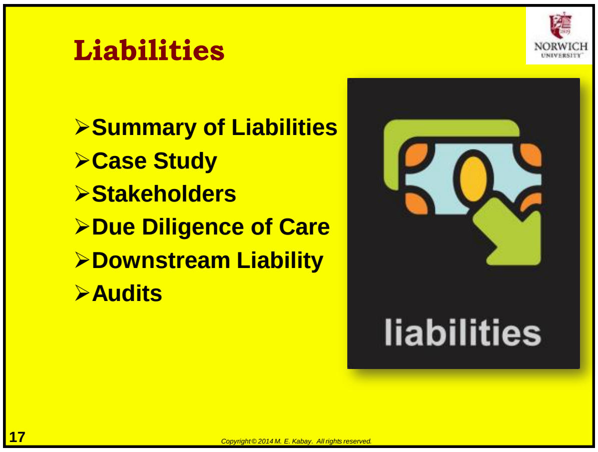
15



Risk Management

- Causes of damage
  - ❑Physical hazards
  - ❑Equipment malfunction
  - ❑Software malfunction
  - ❑Human error
  - ❑Misuse of data
  - ❑Loss of data
- Also classify by
  - ❑Magnitude of loss
  - ❑Probability of loss
  - ❑Permanency of damage

16

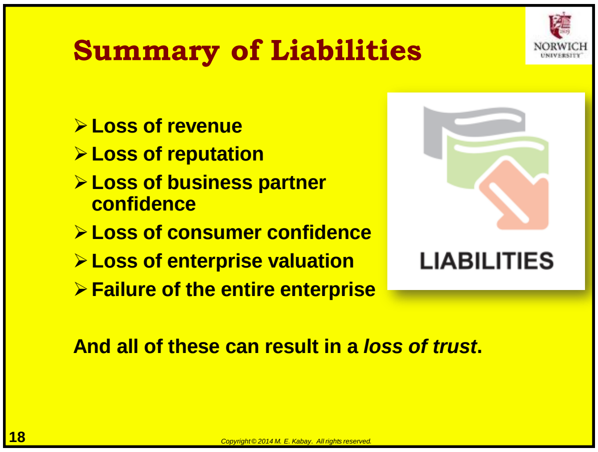


Liabilities

- Summary of Liabilities
- Case Study
- Stakeholders
- Due Diligence of Care
- Downstream Liability
- Audits

liabilities

17



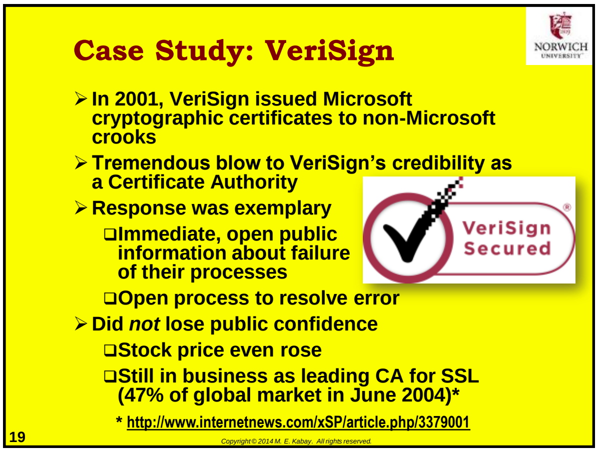
Summary of Liabilities

- Loss of revenue
- Loss of reputation
- Loss of business partner confidence
- Loss of consumer confidence
- Loss of enterprise valuation
- Failure of the entire enterprise

LIABILITIES

And all of these can result in a *loss of trust*.

18

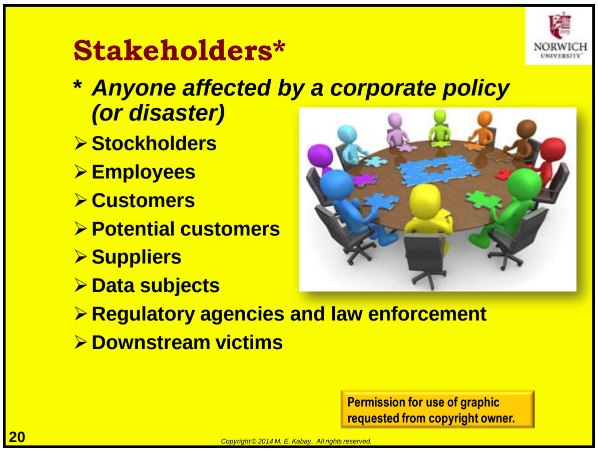


Case Study: VeriSign

- In 2001, VeriSign issued Microsoft cryptographic certificates to non-Microsoft crooks
- Tremendous blow to VeriSign's credibility as a Certificate Authority
- Response was exemplary
  - ❑Immediate, open public information about failure of their processes
  - ❑Open process to resolve error
- Did *not* lose public confidence
  - ❑Stock price even rose
  - ❑Still in business as leading CA for SSL (47% of global market in June 2004)*

* http://www.internetnews.com/xSP/article.php/3379001

19



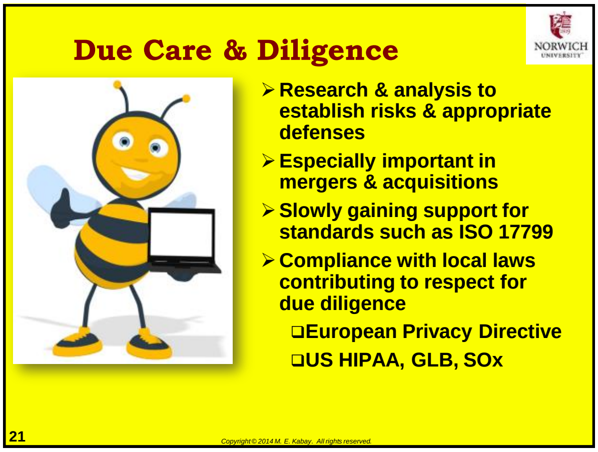
Stakeholders*

* *Anyone affected by a corporate policy (or disaster)*

- Stockholders
- Employees
- Customers
- Potential customers
- Suppliers
- Data subjects
- Regulatory agencies and law enforcement
- Downstream victims

Permission for use of graphic requested from copyright owner.

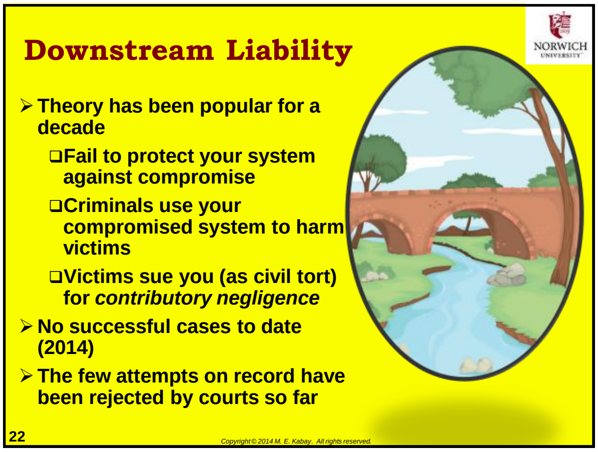
20



Due Care & Diligence

- Research & analysis to establish risks & appropriate defenses
- Especially important in mergers & acquisitions
- Slowly gaining support for standards such as ISO 17799
- Compliance with local laws contributing to respect for due diligence
  - ❑European Privacy Directive
  - ❑US HIPAA, GLB, SOx

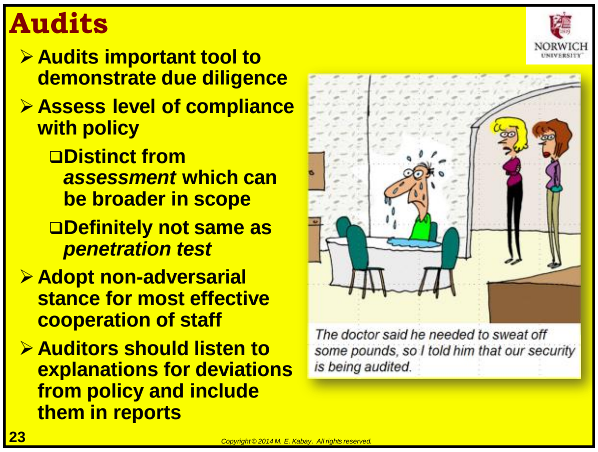
21



Downstream Liability

- Theory has been popular for a decade
  - ❑Fail to protect your system against compromise
  - ❑Criminals use your compromised system to harm victims
  - ❑Victims sue you (as civil tort) for *contributory negligence*
- No successful cases to date (2014)
- The few attempts on record have been rejected by courts so far

22

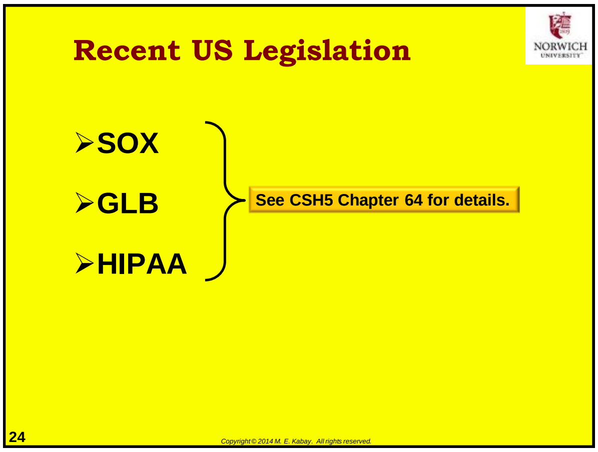


Audits

- Audits important tool to demonstrate due diligence
- Assess level of compliance with policy
  - ❑Distinct from *assessment* which can be broader in scope
  - ❑Definitely not same as *penetration test*
- Adopt non-adversarial stance for most effective cooperation of staff
- Auditors should listen to explanations for deviations from policy and include them in reports

The doctor said he needed to sweat off some pounds, so I told him that our security is being audited.

23



Recent US Legislation

- SOX
- GLB
- HIPAA

See CSH5 Chapter 64 for details.

24

Division of Corporation Finance:
Sarbanes-Oxley Act of 2002 –

- Implemented 2002
  - ❑Enacted after the Enron and WorldCom scandals
  - ❑Developed by Paul Sarbanes (D-MD) & Michael Oxley (R-OH)
- Regulates corporate financial records
  - ❑Penalties for abuse
  - ❑Defines types of records to archive
  - ❑Prohibits data falsification
- For more information, see
  - ❑http://www.sec.gov/divisions/corpfin/faqs/soxact2002.htm

25

Gramm-Leach Bliley Act

- "GLB" or "GLBA"
- Enacted 1999; effective mid-2001
- Every financial institution shall protect the security and confidentiality of its customers' confidential personal information
- Data subjects must
  - ❑Be informed of privacy policies and
  - ❑Have opportunity to inspect and correct their own records
- For more info, see http://www.ftc.gov/privacy/privacyinitiatives/glbact.html

26

HIPAA

- Health Insurance Portability and Accountability Act of 1996
  - ❑AKA "Kennedy-Kassebaum Act"
- Title I protects employees' health insurance coverage when they change or lose their jobs
- Title II
  - ❑Standards for patient health, administrative and financial data interchange
  - ❑Privacy & security of health information records and transactions
- Took effect 2001; compliance targets through 2004
- For more information, see
  - ❑http://www.cms.hhs.gov/HIPAAGenInfo/

CMS Centers for Medicare & Medicaid Services

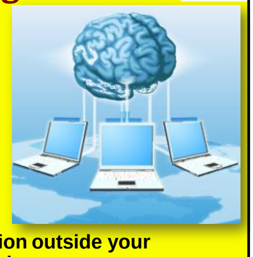
27

Computer Management Functions

- Overview of Management
- Planning for Computer Security
- Organizing
- Integrating
- Controlling

28

Overview of Management

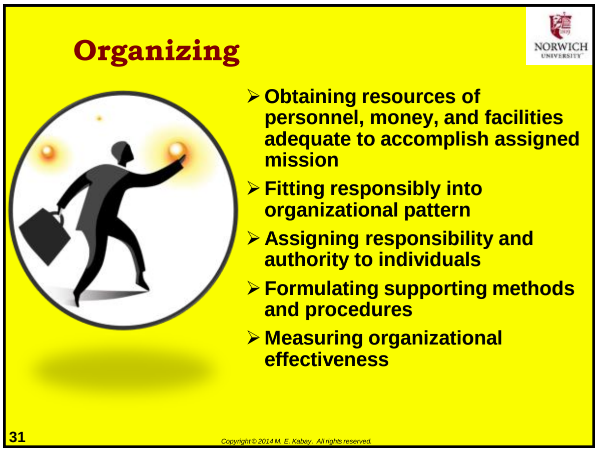


- Understand that security management is a *process*, not a *state*
- The better your security, the less immediate evidence there may be of its effects
  - ❑Therefore keep records of attacks
  - ❑Include intrusion-detection outside your perimeter as well as inside
- Define scope with clear metrics and standards to establish success or failure
  - ❑E.g., define specific *service-level agreements* (SLAs) for availability

29

Planning for Computer Security

- Communicate constantly with upper management
  - ❑No surprises
  - ❑Never blind-side your boss
- Coordinate security of IT with all other sectors (e.g., HR, PR, finance, accounting, production, research…)
- Communicate goals and successes throughout the organization
  - ❑Security-awareness tools (as previously discussed)
  - ❑Newsletters, reports etc.

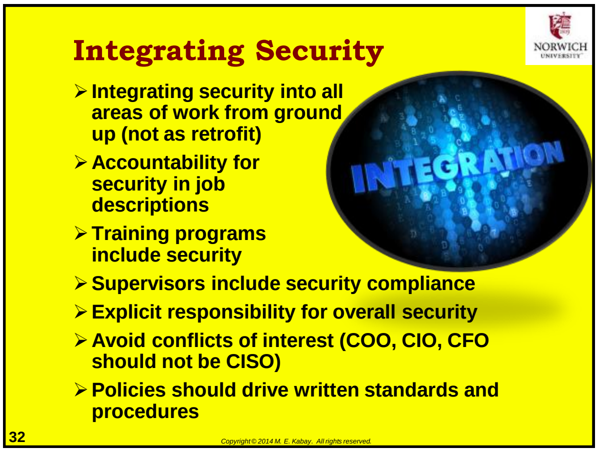


Organizing

- Obtaining resources of personnel, money, and facilities adequate to accomplish assigned mission
- Fitting responsibly into organizational pattern
- Assigning responsibility and authority to individuals
- Formulating supporting methods and procedures
- Measuring organizational effectiveness

31

Copyright © 2014 M. E. Kabay. All rights reserved.

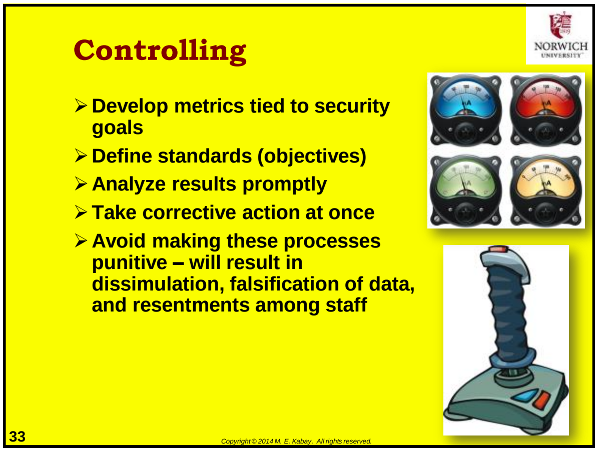


Integrating Security

- Integrating security into all areas of work from ground up (not as retrofit)
- Accountability for security in job descriptions
- Training programs include security
- Supervisors include security compliance
- Explicit responsibility for overall security
- Avoid conflicts of interest (COO, CIO, CFO should not be CISO)
- Policies should drive written standards and procedures

32

Copyright © 2014 M. E. Kabay. All rights reserved.



Controlling

- Develop metrics tied to security goals
- Define standards (objectives)
- Analyze results promptly
- Take corrective action at once
- Avoid making these processes punitive – will result in dissimulation, falsification of data, and resentments among staff

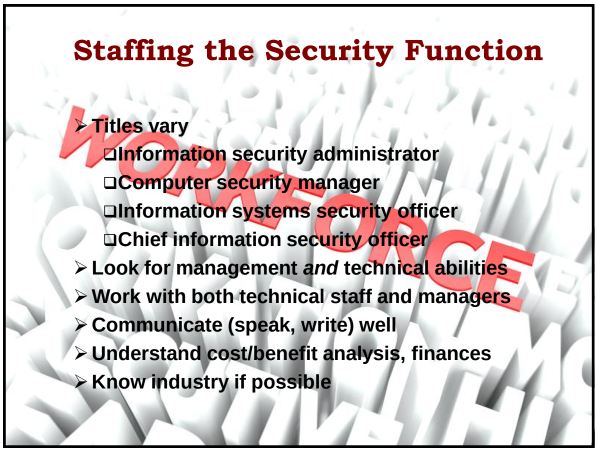
33

Copyright © 2014 M. E. Kabay. All rights reserved.

Security Administration

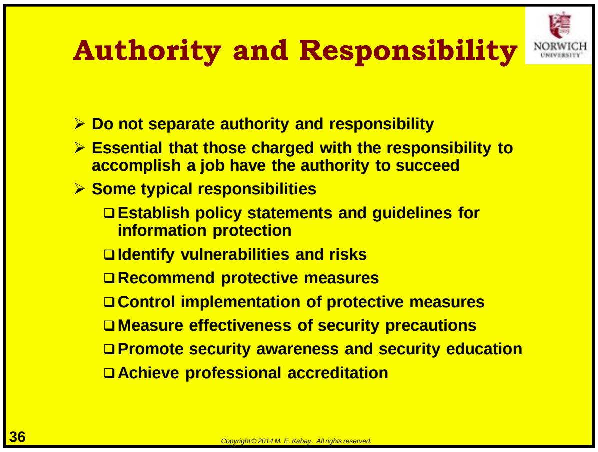
- Staffing the Security Function
- Authority and Responsibility
- Professional Accreditation & Education

IMPROVE
SERVICE
EFFICIENCY
PLANNING
SUCCESS



Staffing the Security Function

- Titles vary
  - ❑Information security administrator
  - ❑Computer security manager
  - ❑Information systems security officer
  - ❑Chief information security officer
- Look for management *and* technical abilities
- Work with both technical staff and managers
- Communicate (speak, write) well
- Understand cost/benefit analysis, finances
- Know industry if possible

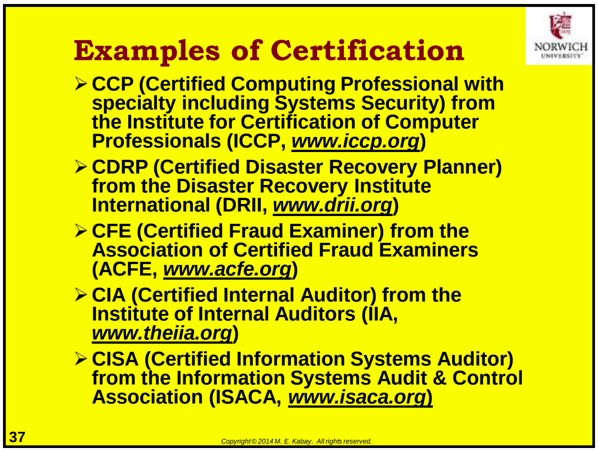


Authority and Responsibility

- Do not separate authority and responsibility
- Essential that those charged with the responsibility to accomplish a job have the authority to succeed
- Some typical responsibilities
  - ❑Establish policy statements and guidelines for information protection
  - ❑Identify vulnerabilities and risks
  - ❑Recommend protective measures
  - ❑Control implementation of protective measures
  - ❑Measure effectiveness of security precautions
  - ❑Promote security awareness and security education
  - ❑Achieve professional accreditation

36

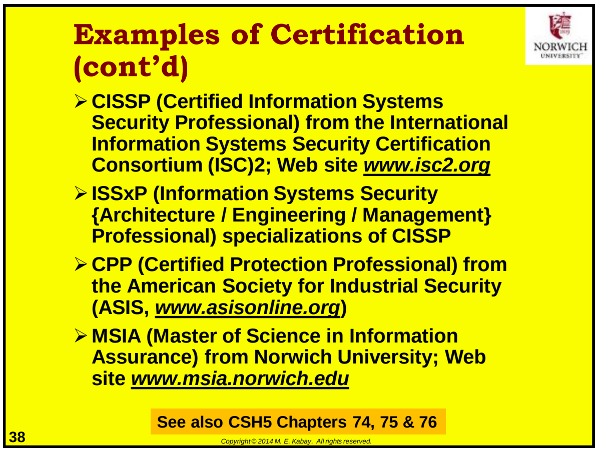
Copyright © 2014 M. E. Kabay. All rights reserved.



Examples of Certification

- ➢ CCP (Certified Computing Professional with specialty including Systems Security) from the Institute for Certification of Computer Professionals (ICCP, *www.iccp.org*)
- ➢ CDRP (Certified Disaster Recovery Planner) from the Disaster Recovery Institute International (DRII, *www.drii.org*)
- ➢ CFE (Certified Fraud Examiner) from the Association of Certified Fraud Examiners (ACFE, *www.acfe.org*)
- ➢ CIA (Certified Internal Auditor) from the Institute of Internal Auditors (IIA, *www.theiia.org*)
- ➢ CISA (Certified Information Systems Auditor) from the Information Systems Audit & Control Association (ISACA, *www.isaca.org*)

37

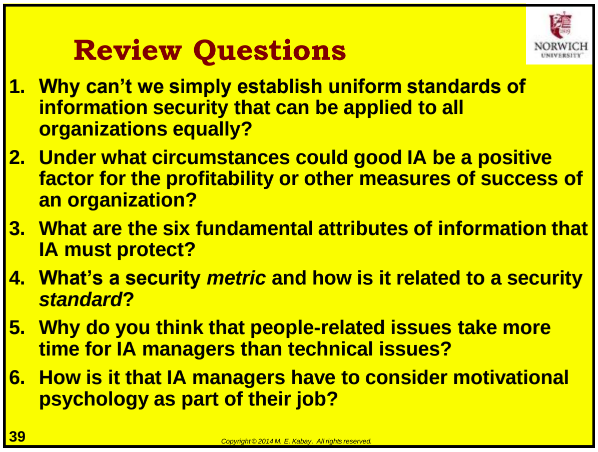


Examples of Certification (cont'd)

- ➢ CISSP (Certified Information Systems Security Professional) from the International Information Systems Security Certification Consortium (ISC)2; Web site *www.isc2.org*
- ➢ ISSxP (Information Systems Security {Architecture / Engineering / Management} Professional) specializations of CISSP
- ➢ CPP (Certified Protection Professional) from the American Society for Industrial Security (ASIS, *www.asisonline.org*)
- ➢ MSIA (Master of Science in Information Assurance) from Norwich University; Web site *www.msia.norwich.edu*

See also CSH5 Chapters 74, 75 & 76

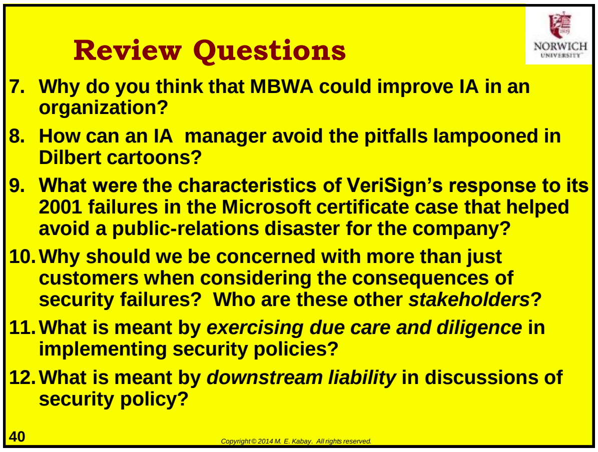
38



Review Questions

1. Why can't we simply establish uniform standards of information security that can be applied to all organizations equally?
2. Under what circumstances could good IA be a positive factor for the profitability or other measures of success of an organization?
3. What are the six fundamental attributes of information that IA must protect?
4. What's a security *metric* and how is it related to a security *standard*?
5. Why do you think that people-related issues take more time for IA managers than technical issues?
6. How is it that IA managers have to consider motivational psychology as part of their job?

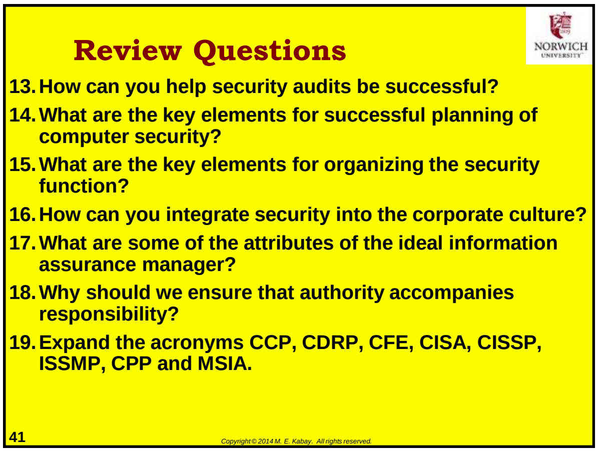
39



Review Questions

7. Why do you think that MBWA could improve IA in an organization?
8. How can an IA manager avoid the pitfalls lampooned in Dilbert cartoons?
9. What were the characteristics of VeriSign's response to its 2001 failures in the Microsoft certificate case that helped avoid a public-relations disaster for the company?
10. Why should we be concerned with more than just customers when considering the consequences of security failures? Who are these other *stakeholders*?
11. What is meant by *exercising due care and diligence* in implementing security policies?
12. What is meant by *downstream liability* in discussions of security policy?

40



Review Questions

13. How can you help security audits be successful?
14. What are the key elements for successful planning of computer security?
15. What are the key elements for organizing the security function?
16. How can you integrate security into the corporate culture?
17. What are some of the attributes of the ideal information assurance manager?
18. Why should we ensure that authority accompanies responsibility?
19. Expand the acronyms CCP, CDRP, CFE, CISA, CISSP, ISSMP, CPP and MSIA.

41

DISCUSSION

42