

CS378: Information Assurance and Security

IA in Business

Dr. Bill Young
Department of Computer Sciences
University of Texas at Austin

Last updated: February 10, 2012 at 08:18

IA developed in a military context, but has obvious benefits for commercial enterprises. [Like what?](#)

Relating IA to Business Needs

IA developed in a military context, but has obvious benefits for commercial enterprises. [Like what?](#)

- Enabling safe operation of business services
- Safeguarding assets
- Providing for recovery in case of disaster
- Assisting the organization in meeting regulatory requirements
- Obviating embarrassing disclosures of security lapses

Imagine that you are a consultant or IA officer in a business context. Some of you may well have that role in the future.

[What are your goals/responsibilities? How does IA in business contexts differ from IA in Military contexts?](#)

Importance of IA

Financial losses attributable to malicious hacking, online corporate espionage and other computer crimes have a huge impact on commercial activity in this country.

The Computer Security Institute estimates total losses due to computer crime of more than \$10 billion annually, mostly from financial fraud and proprietary information theft.

In one survey, 59% of companies reported attacks initiated from the Internet, and 38% reported attacks initiated from internal company computers.

The traditional emphasis of IA in corporations is in information security, particularly for networks and multi-user systems. However, there are often misconceptions about what is possible.

“Perfect security” is impossible to achieve in practice. [Why?](#)

The traditional emphasis of IA in corporations is in information security, particularly for networks and multi-user systems. However, there are often misconceptions about what is possible.

“Perfect security” is impossible to achieve in practice. [Why?](#)

- Real world systems are remarkably complex.
- Security cannot be just a feature of a product; it is part of a process to manage risk.
- The existence of countermeasures that could provide perfect security would imply that there is no risk—i.e., it has all been mitigated. However, it is likely that some threats and vulnerabilities have not yet been identified.

Business IA Expectations

“One of the most difficult achievements in technology is getting the resolve to spend on the possibilities of what if.” –Ron Barrett, *Making High Availability Pay for Itself* (2009)

Business planning always involves a tradeoff between cost and benefits. [Why?](#)

Business IA Expectations

“One of the most difficult achievements in technology is getting the resolve to spend on the possibilities of what if.” –Ron Barrett, *Making High Availability Pay for Itself* (2009)

Business planning always involves a tradeoff between cost and benefits. [Why?](#)

Business is inherently profit-driven. Deployment of security infrastructure in a business requires not only that costs must be justified, but that it meets the needs of the organization and users.

Costs come in various forms. If the security burden is so high for the users that it interferes with productivity, security functions will be bypassed reducing effectiveness of the system. [Give some examples.](#)

Examples: A cumbersome login process may have users logged in for weeks at a time. An IDS that gives repeated false alarms will be disconnected.

“The number one reason for abandoning (on-line) transactions, as stated by survey respondents, was that the process was taking too long (48%). The research revealed people will opt for speed over the risks of maintaining their security online.” (Online Security: A Human Perspective, Oracle Systems, 2010)

If security is a cost, what motivates businesses to implement it?

If security is a cost, what motivates businesses to implement it?

- Potential for loss
- Business reputation
- Competitive advantage
- Legislative and regulatory mandates
- others (?)

“Now that the Privacy Rights Clearing House maintains a comprehensive list of all known data breaches since 2005, major breaches live on in infamy long after the incident.” (Real World Data Loss Prevention Benefits, Sophos report, 2010)

“A recent survey reported that computer security is the critical attribute of corporate networks for 78 percent of executives. Another survey reported that security outweighed other concerns by a factor of three as the driving concern for IT improvements.” (Landoll, The Security Risk Assessment Handbook, 2006)

- *Computer Security Act* (1987): minimum security standards for Federal Agencies
- *Family Educational Rights and Privacy Act* (1974): protects student records in education
- *Health Insurance Portability and Accountability Act* (1996): regulates privacy and security in health care
- *Children's Online Privacy Protection Act* (COPPA) (1998): regulates privacy of children's online information
- *Gramm-Leach-Bliley Act* (1999): regulates security and privacy of financial records
- *Government Information Reform Act* (2000): redefines minimal security standards for government systems
- *Sarbanes-Oxley Act* (2002): regulates financial disclosure and audit for publicly held companies
- *North American Electric Reliability Council Cyber Security Standards* (2004): regulates security within electric systems industry

Regulations often define “best practice” within a *particular industry*. Different industries have different standards. Why should that be?

“The term best practices is commonly used to connote a set of documented strategies, procedures, or methods employed by highly successful organization to effectively achieve results in particular circumstance.” –The Perfect Online Course by Orellano et al., p. ix.

“There is no single definition of the ‘best practices’ for an information security program. ... In fact, the term ‘best practices’ for information security is really a misnomer or even could be considered a myth.” (Landoll)

Discuss this assertion.

Security safeguards are generally identified as:

technical: access control, identification and authentication, encryption, intrusion detection, etc.

non-technical: management and operational controls (e.g., security policies), operational procedures, and personnel, physical, and environmental security.

The *Family Educational Rights and Privacy Act* of 1974, is a federal law that pertains to the release of and access to educational records.

FERPA applies to personally identifiable information in educational records.

- student's name
- names of family members
- addresses
- personal identifiers such as social security numbers
- personal characteristics or other information that make the student's identity easily traceable.

Educational records are all records that contain information directly related to a student and are maintained by an educational agency or institution, or by a party acting on its behalf.

These do not include:

- sole possession records: only accessible to the maker and used as personal memory aid.
- medical or psychological treatment records that include those maintained by physicians, psychiatrists, and psychologists;
- employment records, provided that employment is not contingent upon being a student;
- law enforcement records;
- records collected about an individual after that person is no longer a student.

Any student has a right to

- inspect and review his or her educational records;
- request to amend his or her educational records;
- have some control over the disclosure of information from his or her educational records.

Directory Information

UT designates some information as *Directory information* that may be disclosed without the student's permission, including

- Student's name
- Local, permanent, and email addresses
- UT eid public username
- Telephone listing
- Date and place of birth
- Major fields of study
- Dates of attendance
- Enrollment status
- Degrees, awards, and honors received, including selection criteria
- Most recently attended previous educational institution
- Classification
- Expected graduation date
- Certain other.

Who Can See Your Records

Nondirectory information may not be released without prior written consent from the student. Exceptions include:

- access by appropriate university administrators, faculty members, or staff members who require access to educational records in order to perform their legitimate educational duties;
- officials of other schools in which the student seeks or intends to enroll;
- in connection with a student's application for, or receipt of, financial aid.

Which of the following does FERPA describe: goals, consequences, policies, mechanisms? Keep that question in mind for each of the other legislative mandates.

Health Insurance Portability and Accountability Act (HIPAA)

(1996) establishes safeguards that health care providers must use to protect personal information. The goal is to:

... improve the portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and healthcare delivery, to promote medical savings accounts, to improve access to long-term care services and coverage, and to simplify the administration of health insurance.

HIPAA is concerned with several issues:

- Addresses the ability to transfer insurance when changing jobs, and maintaining insurance after leaving a job.
- Addresses protecting the privacy of medical records as they are transferred among physicians, hospitals, clinics, pharmacies, and insurance providers.
- Many affected organizations use access control to limit the availability of online medical records.

HIPAA involves two separate rules with fairly specific IA components:

- 1 Security Standards Final Rule;
- 2 Standards for the Privacy of Individually Identifiable Health Information Final Rule.

In this context, explain the difference between security and privacy.

HIPAA: Security Standards Rule

Healthcare entities must:

- Ensure the confidentiality, integrity and availability of all “electronic protected health information” they create, receive, maintain, or transmit;
- Protect against anticipated threats or hazards to the security or integrity of such information;
- Protect against anticipated uses or disclosures of info that are not permitted or required;
- Ensure compliance by its workforce with all provisions of the bill.

HIPAA does not mandate specific technical solutions. Is this a good idea or not? Why “anticipated” threats?

HIPAA Admin Security Safeguards

HIPAA either requires (R) or addresses (A) various specific administrative security safeguards:

- *Security Management*: including risk analysis, risk management, sanction, system activity review.
- *Assigned Security Responsibility*.
- *Workforce Security*: authorization and supervision, clearance, termination procedures.
- *Information Access Management*: isolating clearinghouse functions, access authorization, access establishment and modification.

- *Security Awareness and Training*: reminders, malicious software, log-in monitoring, password management.
- *Security Incident Procedures*: response and reporting.
- *Contingency Planning*: data backup, disaster recovery, emergency mode plan, testing and revision, application and data criticality analysis.
- *Evaluation*.
- *Business Associate Contracts and Other Arrangements*.

HIPAA defines certain **physical security** safeguard categories:

- *Facility Access Controls*: contingency operations, facility security plan, access control and validation, maintenance records.
- *Workstation Use*.
- *Workstation Security*.
- *Device and Media Controls*: disposal, media reuse, accountability, data backup and storage.

HIPAA also defines certain **technical security** safeguard categories:

- *Access Control*: unique user ID, emergency access procedures, automatic logoff, encryption and decryption.
- *Audit Controls*.
- *Integrity*: mechanism to authenticate electronic protected health info.
- *Person or Entity Authentication*.
- *Transmission Security*: integrity controls, encryption.

The Privacy Rule is less specific than the Security Rule. It demands protection of “individually identifiable health information” defined as:

Information that is a subset of health information, including demographic information collected from an individual, and (1) is created or received by a health care provider, health plan, employer, or health care clearinghouse, and (2) relates to the past, present, or future physical or mental health, or condition of an individual; the provision of health care to an individual, or the past, present, or future payment for provision of health care to an individual, and (a) that identifies the individual, or (b) with respect to which there is reasonable basis to believe that the individual can be used to identify the individual.

To disclose information, authorization is required including:

- description of the information
- identification of those authorized to disclose or use
- statement of purpose of the use or disclosure
- expiration date for the authorization
- signature of the individual, parent or guardian
- statement of and procedures for revoking the authorization
- consequences of not signing an authorization
- potential re-disclosure of the info by recipient

Items from a “limited data set” may be disclosed, but must not contain any specific identifying info such as names, SSNs, URLs, etc. *What do you think this “limited data set” provision is about?*

The Health Information Technology for Economic and Clinical Health Act (HITECH) is Title XIII of the 2009 American Recovery and Reinvestment Act (ARRA). It expands the reach of HIPAA.

Reserves \$22 billion to “advance the use of health information technology” to move toward Obama’s promised e-health records.

- Expands HIPAA data privacy and security requirements to include “business associates” of entities subject to HIPAA.
- Strengthens HIPAA enforcement measure to include civil and criminal penalties.
- Monetary penalties become mandatory for “willful neglect.”

Penalties are funneled back to HHS Office of Civil Rights enforcement, leading some to fear that this may encourage more punitive enforcement.

Sarbanes-Oxley Act (SOX) (2002) affects all US publicly traded companies.

The rules were designed to:

...protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws ... to protect the interests of investors and further the public interest in the preparation of informative, accurate, and independent audit reports for companies the securities of which are sold to, and held by and for, public investors.

- Congress dramatically increased fines and penalties for fraudulent corporate financial reporting.
- Section 404 requires disclosure of the management’s internal controls over financial reporting.
- Provisions apply to all corporations required to file annual reports by U.S. Securities and Exchange Commission.
- CIOs are responsible for the security of the Enterprise Resource Planning (ERP) systems which generate financial reports.
- Does not mandate particular internal control methodology.

In a survey of 217 companies with annual revenues of \$5 billion, average one-time start-up cost was \$4.26 million, or 0.0825 percent of annual revenue.

The IT community cares for the following two reasons:

- ① Requires certifying the accuracy and attesting to the reliability of financial reports.
- ② Mandates adequate internal controls to ensure the accuracy and reliability of IT systems and operational procedures used to generate financial reports.

A large percentage of these internal controls is expected to relate to the design, development, operation and interaction with information systems. I.e., ensuring data, information, systems, and network integrity.

What does this mean for IT management at a publicly traded company?

Financial Services Modernization Act (1999) (also known as Gramm-Leach-Bliley Act or GLBA) eliminates many of the barriers between banks, brokerage firms, and insurance companies.

Title V of GLBA declares that:

“each financial institution has ... a continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers’ nonpublic personal information.”

Nonpublic personal information is defined as:

“personally identifiable financial information: (i) provided by a consumer to a financial institution; (ii) resulting from any transaction with the consumer or any service performed for the consumer; or (iii) otherwise obtained by the financial institution.”

It also requires banks:

- “to insure the security and confidentiality of customer records and information;
- to protect against any anticipated threats or hazards to the security or integrity of such records;
- to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.”

Financial institutions must provide customers with information relating to their privacy policies and procedures (and changes to it). Customers can *opt out* of any disclosures they don’t like.

Why “anticipated threats”? Discuss the pros and cons of opt out vs. opt in policies.

Despite GLBA, a 2003 study found that:

- ① 66 percent of financial institutions surveyed had one or more Web forms that collected personally identifiable information but did not use SSL encryption;
- ② 91 percent of these institutions used weak SSL encryption, such as 40-bit RC4, rather than the 128-bit encryption then recommended by federal bank regulators.

Upshot: A regulation is only as good as its enforcement.

Do you think the figures would be a lot better today?

What do you think are the major threats to business information?

What do you think are the major threats to business information?

- *Human error or failure*: mistakes of authorized users may compromise confidentiality, integrity, availability.
- *Intellectual property compromise*: software piracy, unauthorized duplication violating software licensing. Business Software Alliance (www.bsa.org) active to reduce this.
- *Espionage/trespass*:
 - Industrial espionage: companies gathering competitive information on other companies. May also involve national intelligence services.
 - Shoulder surfing or dumpster diving: opportunistic acquisition of carelessly guarded or discarded information.
 - Hackers: have techniques and tools to locate and target vulnerabilities in order to trespass.

- *Extortion*:
 - After assets (e.g. credit card numbers) are stolen, blackmailing the target to pay
 - If the target refuses to pay, the assets might be sold to other criminals.
- *Sabotage*:
 - The most common form is web page defacement. 95% of large organizations reported in 2005 “more than 10 incidents” involving the website, though not all were successful attacks.
 - More damaging is damage to infrastructure control systems, for defense, utilities, telecommunications, etc. (In 1996 a juvenile hacker compromised the phone system used by Worcester, MA air traffic control, fire department and '911' system.)

- *Theft*: loss of electronic assets more difficult to detect than loss of physical assets.
- *Software attacks (malware)*: viruses, worms, trojan horses, DoS attacks, etc.
- *Forces of Nature*:
 - Major disasters: (fire, flood, earthquake, lightning, landslide, tornado, hurricane, tsunami); effects can often be mitigated via insurance and physical design
 - Small-scale attacks: (rodents, electrostatic damage, dust, conductive contamination).

- *Other Factors:*

- Quality of service issues:
 - Service providers (power, network connectivity) may experience failure or degradation in quality.
 - Backup services, where available, may not provide same quality of service as normal providers.
- *Hardware and software failures*
- *Technology obsolescence:* many organizations still depend on Windows NT or Window 2000, even though these are not actively maintained.

According to a 2005 CSI/FBI Computer Crime and Security Survey:

- 56% of organizations had known, unauthorized use of computer systems.
- Approximately the same number of incidents resulted from insider threats as from outsiders.
- Top three causes of loss: viruses, unauthorized access, theft of proprietary information
- 97% of organizations use firewalls, 96% use antivirus software, approximately the same percentage as in 2004.
- Actual losses are typically not known, as only 20% of organizations report intrusions.
 - 43% claim reporting to law enforcement would hurt their stock/image
 - 33% claim competitors would use this to their advantage

There are several points in an org chart where IA decisions can originate. Organizations typically drive IA decisions in one of two patterns:

- **Bottom-up:** IA decisions originate from those closest to the information assets such as system administrators and technologists.
- **Top-down:** senior management determines the policies, goals and outcomes for IA projects.

If you were tasked to develop a comprehensive IA program for your company or agency, which approach would you choose (or perhaps some hybrid of the two)?

In a *bottom-up* approach, those closest to information assets (system administrators) originate IA decisions.

- In the 1990s as companies attached to the Internet, system administrators often were responsible for identifying the need for security technology, selecting appropriate products, and deploying the products.
- Administrators have in-depth knowledge of the systems being managed, and are most aware of associated vulnerabilities and threats.
- Such IA projects are often funded as one-time special projects or as part of an overall infrastructure cost to the business of having IT services.

Is the bottom-up approach a viable long-term solution for business-critical information systems?

The bottom-up approach appears most frequently in:

- R&D organizations operating their own unique IT infrastructure
- groups creating or tracking emerging technologies
- small or decentralized organizations.

Is the bottom-up approach a viable long-term solution for business-critical information systems?

No!

- Solutions may not have buy-in from all involved parties, such as systems' end users.
- Approach likely does not have senior management awareness or participation. Costs and benefits not known to management, so cannot budget for IA.
- In large organizations, different IT teams may select incompatible technologies for solving similar problems.
- Turnover of IT staff may create an unrecognized knowledge gap.

In a *top-down* approach, the IA program is initiated by senior business management, which determines policy, goals and outcomes for IA projects.

Program's processes may flow through organization in several ways:

- 1 Each level of management writes increasingly more specific statements on the IA process, and delegates implementation to the level below.
- 2 An IA project team may be set up, responsible for implementation and coordinating with each line-of-business.
- 3 A federated approach, such as in multinationals, in which each part of the company chooses an approach to implementation, but may be required to coordinate on selected areas across the organization.

Top-down projects are often more likely to receive consistent funding, be integrated into organizational culture, and involve all necessary parties for a successful outcome.

The IA program should have a *champion* within senior management.

- Could be Chief Information Officer (CIO), Chief Information Security Officer (CISO), or VP of information technology or network operations.
- Establishes business goals of the program and ensures integration of requirements into budget and planning.
- The champion may also establish an integration roadmap or timeline to ensure that projects move ahead.

IA projects in a top-down approach typically follow a system development lifecycle model. The IA project is thus tracked similarly to other IT projects within the organization.

How should you organize IA management within your company?
How does UT do it?

Chief Information Officer: establishes IA strategy and communicates with other managers.

Chief Information Security Officer: responsible for information security across the organization.

Chief Technology Officer: often responsible for special projects, not part of normal IT operations.

VP for Information Technology: responsible for IT services.

VP of Network Operations: responsible for operating data networks and related servers.

Other VPs and managers: may have their own IT infrastructure for line-of-business services.

Auditors: certify that the organization has correctly reported, and may validate the IA services that protect the data for such reports.

Possible roles with an IA deployment project:

Champion: promotes the project and ensures its visibility to appropriate management.

Team leader: manager who tracks the project status and ensures it meets goals.

Policy specialists: identify security policies appropriate for the organization.

Risk assessment specialists: coordinate risk assessment process used in IA and financial/business risk management.

Security professionals: specialists in information security (technical and non-technical).

System administrators: responsible for administering the systems and networks being protected.

End users: selected users validate that the approach does not disrupt business activities.

Lead developers: IA projects may need custom software engineering to integrate with existing systems.

Three roles of data ownership:

- **Data owners** are responsible for the security and use of a particular category of data, and are typically senior managers.
- **Data custodians** are responsible for implementing the security and storage of data, often CISO or system administrators' responsibilities. Backup and recovery is of primary interest to the data custodian.
- **Data users** are the end users who interact with the data in order to fulfill a business function, and are typically integral in maintaining the security of data.

Explain the relationships among these various roles.

Multiple groups fill each role, as data flow throughout the organization.

- The process of creating new data, such as new accounts for customers in a database, is called *provisioning*.
- The authoritative database known to have correct (or best) information and supplies updates is called the *System of Record* database.

A *community of interest* is a group (may be distributed) with similar interests and a common goal within an organization.

Information Security: protects the organization's information systems and information from attack.

Information Technology:

- Manage IT costs, ease-of-use, timeliness, performance.
- May conflict with information security community as goals are not always aligned.

Organizational:

- General management, and the rest of the organization.
- To IT, these are "end users"; to Information Security, these are "subjects."
- Goals of IT and information security must be aligned with organizational goals.

Describe effects of having multiple communities of interest.

A *security office* may be responsible for developing organizational security policies, and implementing certain policies, such as physical site security.

A *telecommunications office* may be responsible for maintaining the security of voice, video and data communications.

The functions of the *INFOSEC Officer* varies, and may include:

- managing an information security team
- reviewing operations which might impact information security (e.g., adding a modem dial-in line).
- performing risk assessments
- compiling documents of best practices for information security

In government and contractor organizations:

- The *COMSEC Custodian* is responsible for safeguarding of communications security devices used in discussing classified information and training end users.
- The *OPSEC Manager* is responsible for identifying potential adversaries and their information targets, and developing security countermeasures.

A security systems development lifecycle is a methodology:

- A methodology is a formal approach to problem solving based on a structured sequence of procedures.
- The lifecycle will have an end goal, as well as intermediate milestones, and a project team will be held accountable to meeting milestones and the end goal.

The process is started by an event or conditions, e.g. responding to a break-in or meeting shareholder/regulatory requirements.

Often the lifecycle is based on the Waterfall model, and a feasibility analysis at the end of each phase:

- 1 Investigation
- 2 Analysis
- 3 Logical design
- 4 Physical design
- 5 Implementation
- 6 Maintenance and change

In some organizations, one or more of these phases may be outsourced. (According to a 2005 survey: 26% outsource up to 20% of security functions; 63% outsource none)

Phases of Security Systems Development Lifecycle

• *Investigation*

- Specify objectives, constraints and scope of the project, and develop cost-benefit analysis.
- Begin an *enterprise information security policy* document, as well as dictates from management of expected outcomes and budget.
- Organize project teams, determine whether the organization has necessary resources and commitment for success.

• *Analysis*

- Assess the organization, current systems and policies, and functions and interactions of the new system.
- Analyze legal constraints, current threats and countermeasures.
- Begin risk management process.

Phases of Security Systems Development Lifecycle

• *Logical design*

- Create a system solution for the business need. Select applications, data, and ranges for technology alternatives. The logical design is implementation independent.
- Establish IA policies, including
 - incident response: actions to take when an attack occurs
 - disaster recovery: immediate recovery of information and systems after a loss
 - continuity planning: how business will continue in the event of a loss.

• *Physical design*

- Select specific technologies, perform build-vs-buy tradeoffs and establish success criteria
- Develop *information security blueprint* document and physical security measures
- Present entire solution to management for approval and signoff.

- *Implementation*

- Create or acquire software and test components.
- Train users and test whole system.
- Provide sponsors with a performance review and acceptance test results.

- *Maintenance and Change*

- Support and modify the system as needed for the rest of its life cycle.
- Monitor and validate, upgrade countermeasures, repair and recover as needed.
- Longest and possibly most expensive phase.