




Corporate Security Awareness

The Common Sense of Compliance

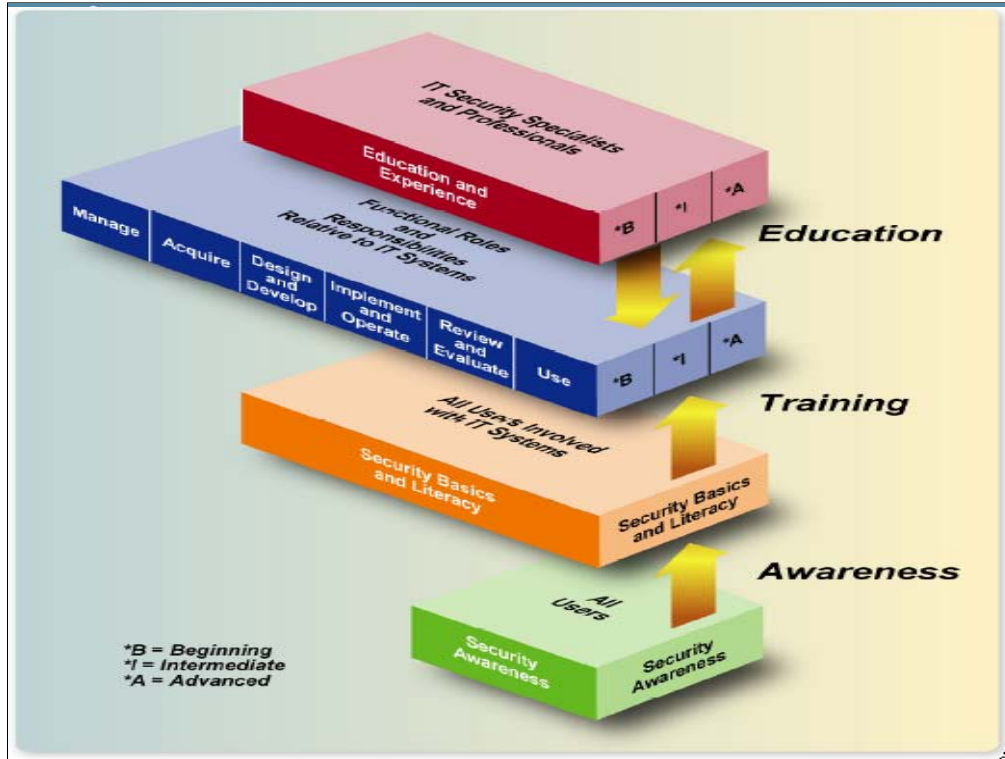


Information Theft

- Physical
 - Vendor/Client Fraudulent Activities
 - Stolen Assets (i.e. backup tapes)
 - Compromised Assets (vengeful employees)
 - Other (Dumpster Diving, et al)
- Social Engineering
 - Chat Rooms, Instant Messaging
 - Web spaces, Blogs, Forums
 - Shadowing, Eavesdropping
- Logical
 - Phishing, Pharming, Spam
 - Network/Domain Hijacking, Man-in-the-middle Attacks
 - Spyware, Keyloggers, Viruses

70% of all information theft is still physical

Talk about newer cyber-threats: especially spear-phishing



Explain purpose of comprehensive security awareness as building block for all other initiatives.



Awareness Training

- Legal requirements for data
 - Ownership of data
 - Intellectual property protection
- Security requirements for users
 - Privacy expectations
 - Auditing requirements for users activities
 - Secure workspace requirements (passwords, etc)
 - Acceptable use policy for Internet, eMail and IM
 - Sensitivity to threats, risks and vulnerabilities
 - Physical, personal and information vulnerabilities
 - Responsibility of users to report issues

People's behavior is based upon their principles and their values.

An effective awareness program helps the workforce adopt the organization's principles and values.

The message is persuasive when the information is relevant to their values



Speak briefly on each, give some examples.

FFIEC

Multi-Factor (1½ factor) authentication for any remote transactions

SOX

“... affects only public companies, but has far broader applications than GLB and includes criminal penalties for individual executives who fail to comply with its provisions.”

“Section 302 deals with Corporate Responsibility For Financial Reports. Computer security comes into play here because your executives need to know that your data has not been tampered with. Somebody in your organization, if your company qualifies under the act, is going to have to sign off that the data is accurate and hasn't been tinkered with.”

“Section 404 deals with Management Assessment Of Internal Controls. Here again, computer security plays a role. Someone up there (maybe even you) is going to have to outline the controls that are in place that are safeguarding your company data and assess how well those controls are working.”

“Section 409 deals with Real Time Disclosure. On the surface, this doesn't sound like a computer security issue, but your organization is going to be the one providing the numbers and they have to be accurate and easily available for quick distribution. That means that the numbers need to be fully automated and that they are protected from accidental or intentional loss. Further, that information cannot be tampered with once issued.”

GLB

“The Gramm-Leach-Bliley Act of 1999 (sometimes called the Financial Modernization Act, and usually known as **GLB**) is intended to ensure protection of consumers' private financial data, which the Act refers to as Nonpublic Personal Information (NPI). **GLB** applies to a wide range of financial institutions and other organizations that maintain NPI related to their customers.”

“The areas of greatest concern to most companies, and to corporate messaging managers, are the Financial Privacy Rule, which covers the collection, use, and disclosure of NPI, and the Safeguards Rule, which describes the processes companies must take to protect NPI.”

“The Financial Privacy Rule is relevant to messaging because it covers the implementation of opt-out policies and privacy notices. For the most part, these are technology independent.”

“The Safeguards Rule is more directly related to messaging infrastructure. It states that companies must maintain security programs that are commensurate with their size and complexity, as well as with the sensitivity of the NPI. More specifically, the Rule covers the use of technologies to prevent interception, automated enforcement of corporate policies related to message content, and general email security provisions.”

ISO 17799

- security policy, objectives and activities that properly reflect business objectives
- a sound understanding of security risk analysis, risk management and security requirements
- an approach to security implementation which is consistent with the organization's own culture
- clear management commitment and support
- effective 'marketing' of security to employees (including managers)
- proper distribution and guidance on security policy to all employees and contractors
- provision of adequate education and training
- a balanced and comprehensive measurement system to evaluate performance in IS management and

feedback suggestions for improvement



Security Objectives

- Corporate Liability Protection
- Client Data Protection
- Personal Identity Protection

Regulations were not made to point fingers...

- Good business practices with a technical twist
- Needed to be verbalized when governing bodies failed
- (opinion) started early '80s when corporations started choosing short-term profit without regard for long-term effects
- Ensures corporate focus as well as accountability

A corporation's only true assets are

- real estate (or other non-depreciable physical asset),
- intellectual property (including its knowledge base),
- customer base.

A presentation slide with a dark blue background. The top section has a lighter blue header with the title 'Corporate Liability Protection' in white. To the left of the title is a graphic of several interlocking puzzle pieces. Below the header, the text 'Ability to safeguard intellectual property' is centered. Underneath this, there are two bullet points, each starting with a white circle. The background of the slide features faint, abstract white and light blue shapes that resemble puzzle pieces or organic forms.

Corporate Liability Protection

Ability to safeguard intellectual property

- Maintains/builds shareholder/owner trust
- Higher company valuation

The ability to protect IP is almost as important as the ability to exploit IP. When **both** are accomplished in an effective and visibly positive manner, the shareholder/owner trust in the upper-level management decision process greatly improves. This effect can lead to more “leash” to expand decision-making capabilities. Although it is intangible, consider the opposite. Failure to protect IP (or exploit IP) will lead to a more conservative stance, stifle innovation and eventually stagnate growth.



Client Data Protection

Ability to protect customer/vendor data

- Maintains/builds client relationships
- Longer customer engagements
- Build market share

Along with IP, a corporation's client base is paramount to its success. Most business models address either increasing market share through customer quantity or customer quality. As many retail banks have found, failure to protect client data can be devastating to market share. However, many are only beginning to realize the potential tangible gains of making consumer protection more explicit and visible. Similarly, wholesale businesses need to be cognoscente of the indirect role they play in client data protection.



Personal Identity Protection

Ability to protect employees and constituents

- Mitigates employee misconduct
- Less turnover
- More manageable workforce

Elaborate on the FUD factor, but try not to diverge too long on this subject.



Security Goals

- Everyone should be **AWARE** of their environment
- Policies that are **EASY** to understand and implement



Policy Goals

- Avoid
 - Prevention / Awareness
 - 99% User Responsibility
- Trap
 - Early-Detection / IDS
 - Facilitated by Technology
 - Still 50% User Responsibility
- Mitigate
 - Reaction / Notification
 - Regulated Responsibility
 - User responsibility to report

“Cockpit Resource Management”

Pre-plans all possible problem scenarios

Developed by the FAA in response to the crash of United Airlines Flight 173 on December 28, 1978.

Avoid: Do everything reasonable to prevent the opportunity for attack.

Trap: Be aware of “triggers” that indicate an impending attack.

Mitigate: Always plan for “when” and not “if” an attack happens.

In the loosest interpretations, compliance is the documentation of processes.

In the strictest terms, compliance is the validation of processes.

Policies should be written using a consistent interpretation.

Overall... make it EASY to understand and act on !!!



Policy Focus

- Data**
 - Accurate, Secured, Archived, Accessible
- Processes**
 - Well-defined, Documented, Repeatable, Audited
- Decisions**
 - Well-defined, Documented

Data:


Data Origination and Identification -- Endpoints, Transports, Users
Data, Meta-Information and Business Intelligence -- Accurate,
Secured, Archived, Accessible
Data Manipulation, Auditing and Archival Processes -- Accurate,
Audited
Data Disposal -- Secure, Audited

Processes:

Well-defined and documented
Repeatable
Audited

Decisions:

Behavioral – provide guidelines
Business – well-defined and documented



Policy Areas

People	Systems
<ul style="list-style-type: none">• Visitor / Guest Policies• Business Focus<ul style="list-style-type: none">• Day-to-Day Activities• Roles and Responsibilities• Separation of Duties• Role Based Access Control<ul style="list-style-type: none">• Least Privilege• Tiered Access• Write-Up and Read-Down• Secure Communications• Security Awareness• Disruptive Technologies	<ul style="list-style-type: none">• Workstations• Communication Devices• Network Infrastructure<ul style="list-style-type: none">• IDS / IPS• DMZ• Logging / Archiving• Auditing Practices• Physical Access Controls• Process Documentation• Business Continuity<ul style="list-style-type: none">• Disaster Recovery• Secure Data Backup

Speak briefly on each with one example.



Policy Walkthrough

Disruptive Technologies

Avoid

- Communicate policies when
 - There exists significant *or unrealizable* security risks
 - Liabilities outweigh the benefits

Trap

- Keep an open communication channel
 - Research new disruptive technologies
 - Document findings and review as technology matures

Mitigate

- Embrace new disruptive technologies
 - When appropriate
 - In a secure way (i.e. sandbox)

We want a positive spin...



Disruptive Technologies

Peer/Collaborative Tools

Usage:

- Remote offices, tele-workers and B2B relationships

Benefits:

- Increased productivity
- Decrease travel

Liabilities:

- Strict time/subject management, possibly a facilitator
- Coordination issues
- Conflict resolution
- Security/Confidentiality of subject matter

Be positive, give examples of acceptable peer technologies. Talk about security issues.



Disruptive Technologies

Un-tethered Devices

Usage:

- Portability and mobility

Benefits:

- Allows for more productive work on the road
- Allows corporate applications to PUSH information

Liabilities:

- Primary source of corporate IP theft (physical theft)
- Lack of security / encryption
- Lack of accountability

Be positive, give examples of acceptable personal devices. Talk about security issues.



Disruptive Technologies

Personal Spaces

Usage:

- Inter-company communications
- Knowledge Bases

Benefits:

- Allows for more effective grassroots communication

Liabilities:

- Source of corporate IP theft (social engineering)
- Lack of corporate protocol
- Lack of information confidentiality

Be positive, give examples of acceptable personal spaces. Talk about security issues.



Questions

John C. Checco, CISSP
John.Checco@CheccoServices.com
1-845-942-4246