

IT Security for Non-IT Departments

**National Association of County Collectors,
Treasurers and Finance Officers**

**2008 Annual Conference
July 11, 2008**





Agenda

Overview

Background

Objectives

Information Security – Level Set

Definition

Key Concepts

Information Security – Today's Environment

Importance of Information Security

Managing the Risks

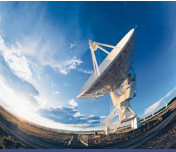
Responding to Incidents

Information Security – Wrap Up



Overview - Objectives

- Increase awareness of industry views of IT Security
- Discuss key concepts associated with IT Security
- Examine how IT Security affects our office/workplace
- Increase awareness of importance of appropriate levels of control



Agenda

Overview

Background

Objectives

Information Security – Level Set

Definition

Key Concepts

Information Security – Today's Environment

Importance of Information Security

Managing the Risks

Responding to Incidents

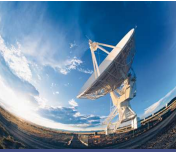
Information Security – Wrap Up



Information Security - Definition

There are a multitude of 'definitions' associated with IT Security.

- **What does the terminology IT Security mean to you?**



Information Security - Definition

A widely accepted industry view suggests that IT Security is the preservation of the Confidentiality, Integrity, and Availability of Information.

- **Confidentiality** – ensuring that information is only available to those who have been authorized to access it
- **Integrity** – safeguarding the accuracy and completeness of information and associated processing methods
- **Availability** – ensuring that authorized users have access to the information when needed

Getting the 'right' information, to the 'right' people, at the 'right' time

- Over time the 'security industry' has moved away from the term IT Security and gravitated towards Information Security
 - The terminology IT Security somewhat ignores the intrinsic value of the information being 'handled' through a wide variety of technologies
- Information security is considered to be part of a broader view identified as information protection
 - This includes Disaster Recovery and Records Management

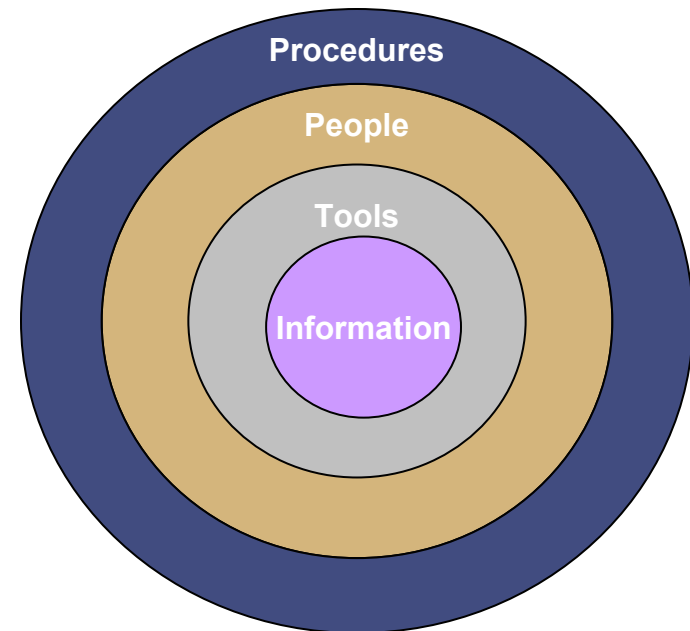


Information Security – Key Concepts

At a high level all organizations tend to ‘look’ alike, in that every organization has some degree/level of policies and procedures in place which govern people and the tools that they use to manage information.

From an Information Security perspective, appropriate consideration needs to be given to each of these layers

- **Procedures** – policies and guidelines that govern across the organization (i.e. security standards, etc)
- **People** – administrators, users and operators who actually run the organization/office
- **Tools** – the various technologies (i.e. software, hardware, communication devices, etc) that are used by the people to operate/manage the business
- **Information** – a key asset of the organization

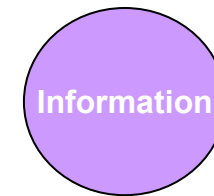


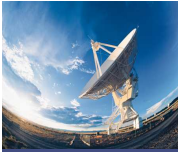


Information Security – Key Concepts

Information is a key asset of any organization. An important aspect of Information Security is recognizing the value of information, and understanding that not all information is equal.

- Not all information requires the same degree of security/protection
 - Within any given record it is possible to have different security requirements (i.e. a public record containing personal identification such as SSN)
 - Classifying information is important in order to determine the types and levels of security required
-
- **What types of information do you have to protect/secure?**
 - **What types of regulations are you subject to related to information protection security?**

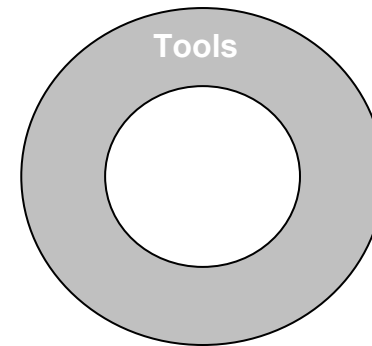




Information Security – Key Concepts

There are multiple layers of technologies (tools) that are deployed and utilized within an organization in order to manage/run operations. An important aspect of Information Security is understanding the various layers and applying the appropriate controls.

- Networks (firewalls, routers, switches)
- Operating Systems (servers, workstations, terminals, mainframes)
- Databases
- Web Services
- Applications (email, financial applications, spreadsheets, etc)
- Devices (handheld devices, cell phones, storage devices)



- **What types of technologies do you have in your environments?**

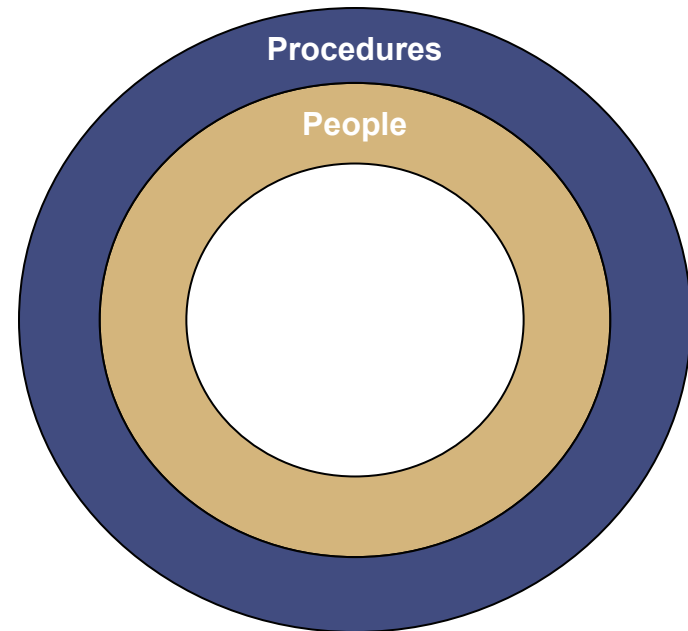


Information Security – Key Concepts

Procedures and people tend to go 'hand in hand', in that people both develop/maintain policies and procedures, as well as follow/abide by them. An important aspect of Information Security is identifying the appropriate level of controls required to effectively protect your organization's information.

Key elements include:

- Senior Management commitment and support
 - Knowledge of regulatory, contractual and other policy compliance requirements
 - Policies and procedures
 - Security awareness and education
 - Monitoring and compliance
 - Incident handling and response
 - Combination of preventative and detective controls
 - Detailed plans, processes and procedures
 - Good inventories of information elements and technical elements
-
- **Who manages security in your organization?**
 - **How do you interface with these groups?**
 - **Does your senior management understand information protection risks and issues?**
 - **Does senior management support programs that address these issues?**

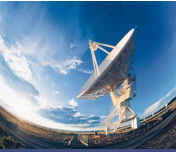




Information Security – Key Concepts

The following are some general qualifying questions that assist with assessing an organization's current state as it relates to Information Security practices:

- Have you identified your critical information assets and put appropriate security measures in place based on their relative value to the business?
- Do you enforce the segmentation of assets, users and transactions based on physical (network flows) and logical (access) infrastructure?
- Are there specific regulatory requirements, especially with regards to internal controls over disclosing sensitive data that you are most concerned about?
- Do you have a holistic security strategy and the ability to consistently apply security policies across different organizations?
- Are you able to address the new breed of organized, orchestrated attacks with your current staff and resources?
- Do you have the capability to adequately deploy intrusion prevention technology to protect your environment with your current staff skills and resources?
- Are you able to determine if/where individuals in your department or agency are deploying rogue wireless access points and whether the proper security mechanisms have been enabled to protect those access points?
- Have you linked your IT Security systems with Fraud detection systems to enable you to correlate IT threats with potential vulnerabilities in the business processes? Will you have adequate IT and business records to support a thorough forensic and audit investigation?
- Have you considered outsourcing some of your security operations to ensure that the latest technology and intelligence is focused on addressing problems in a timely and cost effective manner?



Agenda

Overview

Background

Objectives

Information Security – Level Set

Definition

Key Concepts

Information Security – Today's Environment

Importance of Information Security

Managing the Risks

Responding to Incidents

Information Security – Wrap Up



Information Security – Importance of Information Security

In today's environment, there are a number of factors that contribute to the overall importance of Information Security

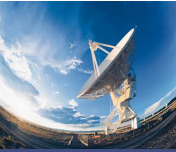
- Prolific use of technology to collect, process, store, transmit and report various types of information
- Dependency on technology is increasing
- There are very few “dedicated systems” – almost everything is interconnected
- Technology is getting easier and cheaper, increasing the number of threats and vulnerabilities in these technology environments
- Regulatory environment is getting more stringent and requirements are growing
- Policies and standards are reflecting this changing environment
- Crimes using technology are getting more numerous and easier to perpetrate (identity theft is a relevant example)



Information Security – Importance of Information Security

In today's environment, there are a number of threats to the various technologies that assist us in managing information:

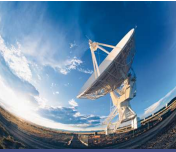
- Unauthorized access to and use of information
 - Accidental disclosure of information
 - Loss of critical information
 - Denial of Service – availability of systems
 - Trojans / Viruses
 - Poor Application Security
 - Lack of Embedded Security – Governance & Controls
 - Poor configuration management
 - Social Engineering e.g. Phishing
 - Insider attacks using Backdoors
 - Lack of Policy Compliance by Employees, Contractors
 - State Sponsored Terrorism
 - Cyber Criminals
 - Insiders Colluding with States – Corporate Espionage
-
- **What types of threats do you face in your organization?**



Information Security – Managing the Risks

As discussed, there are a number of risks associated with managing/maintaining/utilizing information across technologies. The challenge is to manage these risks as cost-effectively as possible. Consideration needs to be given to the following:

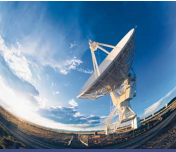
- Physical access control
- Logical access control
- Access approval process
- Information classification and handling procedures
- Using encryption when handling sensitive data
- User IDs and good passwords
- Acceptable use policies
- Email usage and handling policies
- Device security (workstations, laptops, PDAs, etc.)
- File sharing
- Remote access – working from home or on the road
- Business partner access
- Change management
- Business continuity and disaster recovery plans
 - Inventories
 - Business impact analysis
 - Detailed plans that will keep the business going
 - Incident response procedures



Information Security – Managing the Risks

In order to mitigate defined risks, there are three (3) types of controls that can be used:

- **Administrative** – policies and guidelines that govern across the organization (i.e. security standards, etc); from an Information Security perspective these controls drive the requirements for the other types of controls
- **Preventative** – controls that are in place to prevent threats from impacting environments/facilities
 - **Physical** – controls that monitor the workplace and computing facilities; from an Information Security perspective this includes restricting access to data centers and ensuring appropriate separation of duties
 - **Logical** – various technologies (i.e. software and data) that enable users to control access to information and computing environments
- **Detective** – controls that detect threats or incidents



Information Security – Managing the Risks

Administrative –

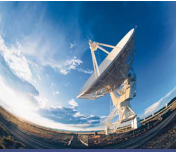
- Policies, Standards and Guidelines
- Operational Processes
 - Change management
 - Incident response
 - Disaster recovery
- Awareness Training
- Detailed Plans
 - Business Continuity Plans



Information Security – Managing the Risks

Preventative –

- User IDs and passwords
- Strong authentication
- Access control models
- Network access controls (firewalls)
 - File system protection
 - Database protection
 - Application security
- Encryption
- Secure configuration management
- Vulnerability management and patching
- Anti-virus software
- Spam filtering



Information Security – Managing the Risks

Detective –

- Logging of critical activities
 - Security activities
 - Critical business activities
- Intrusion detection software
- Assessment and audit processes
- Incident response processes

- **What types of controls are implemented in your environments?**
- **What types of security controls do you operate?**



Information Security – Responding to Incidents

Elements of Incident Response and Disaster Recovery

- Define a core incident response team made up of necessary groups (security, privacy, IT, business groups, business continuity, Legal, Public Relations)
- Define and document roles and responsibilities
- Define and document processes
- Develop communications plan for both internal and external parties
- Determine types of incidents that will require forensic activity and protection of evidence



Information Security – Responding to Incidents

When an incident occurs, enact the plan

- Notify the computer incident response team contact
- Initial assessment
- Communication
- Control damage and minimize risk (triage)
- Identify type and severity of compromise
- Protect evidence
- Notify external agencies if appropriate and/or necessary
- Recover systems
- Compile and organize incident documentation
- Assess incident damage and cost
- Post mortem
 - Fix root cause throughout environment
 - Review success of response plan and make changes if necessary
 - Update policies, if necessary

- **What types of incidents have you seen in your environments?**
- **What was done about it?**



Agenda

Overview

Background

Objectives

Information Security – Level Set

Definition

Key Concepts

Information Security – Today's Environment

Importance of Information Security

Managing the Risks

Responding to Incidents

Information Security – Wrap Up



Information Security – Wrap Up

So the question is, how does this affect you

- Governed by security policies and standards handed down by:
 - Federal, state, county and local governments
 - Your entity's IT organization
 - Your entity's security organizations
- In most business environments, the users are a critical part of the overall security program
- In decentralized environments, compliance is the end user/technology owner's responsibility
- Although IT and security will provide many methods, processes and technology for protecting information, it will be 'your' responsibility to ensure these are implemented and operating effectively
- It will be 'your' responsibility to ensure compliance

“The human factor is the weakest link in the security chain”



Resources

There are numerous resources available related to the topic of Information Security

- SANS Institute- www.sans.org
- Information Security Systems Association (ISSA) – www.issa.org
- Information Systems Audit and Control Association (ISACA) – www.isaca.org
- ISO 27001 www.iso.org
- Information Security Forum (ISF) – www.securityforum.org
- CSO Magazine – www.csoonline.com
- Carnegie Mellon Computer Emergency Response Team (CERT) – www.cert.org
- National Institute of Standards and Technology (NIST) – csrc.nist.gov