



Introduction to Information Systems Security

April 18, 2000

Presented by your ISSA-TOC

Your ISSA Chapter Board

- **Chris Anderson, CISA**
Ernst & Young
chris.anderson@ca.eyi.com
- **Anton Aylward, CISSP**
ArQana
anton_aylward@arqana.com
- **Graham Dougall, CISSP**
Manulife
dougallg@manulife.com
- **Kim Johnston, B.Sc**
Kyberpass
kjohnston@kyberpass.com
- **Keith Parsons, CISSP**
Scotiabank
keith.parsons@scotiabank.com
- **Patsy Tousignant, B.Comm**
CP Rail
patsy_tousignant@cpr.ca
- **Anna Wilson, CISSP**
W.S.I.B.
wilsona@istar.ca

Session Agenda

- **WHAT** is information systems security?
- **WHY** is it necessary?
- **WHO** needs to be involved?
- **WHERE** is it required in my organization?
- **HOW** do I proceed to succeed?



What is Information Systems Security?

- Information Security InfoSec
- Systems Security SysSec
- Computer Security CompSec
- Network Security NetSec
- Communications Security CommSec

Security IS a Management Issue !



Remember
this!

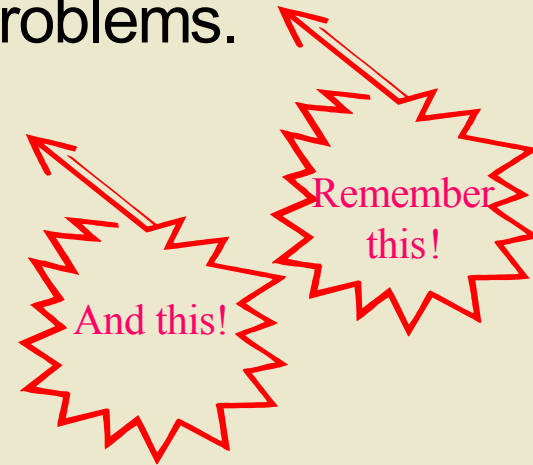
April 18, 2000

(c) 2000 Keith Parsons & Anton Aylv

What is Information Systems Security?

This is What it is all about

- **Security mission:** Preserve and Protect the Corporate Resource!
- Technology cannot solve Management problems.
- Management commitment is mandatory.
- A good security program includes:
 - Policies
 - Standards
 - Procedures and Processes
 - Guidelines, Awareness and Education



Why is Security Necessary?

- **Threats to the Corporate infrastructure**
 - External attacks from the Internet (DDoS)
 - Viruses entering undetected
 - Disgruntled staff attacks from inside
 - Errors, omissions at any time
 - Possible natural situations (fire, flood, winds)

Why is Security Necessary?

- **Risks to Corporate assets and resources**
 - Loss of information confidentiality
 - Loss of information integrity
 - Loss of information availability
 - Loss of information authenticity

Why is Security Necessary?

- **Impacts to the Company from incidents**
 - Loss of business credibility
 - Loss of business resources
 - Loss of business revenues
 - Loss of the business

Why is Information Systems Security necessary?

- Greater dependency on information systems to conduct business functions.
- Greater global distribution of system resources, control and management responsibilities.
- Greater inconsistencies of applied standards
- Security perceived as an inhibitor rather than an enabler
- Stuff happens from inside an organization.... Some accidents are some deliberate



Who needs to be involved in Information Systems Security?

- Security is a team effort in all organizations
 - Senior Management (Policies)
 - Technical Management (Standards)
 - Business Management (Processes)
 - HR, Legal and Audit (Compliance)
 - Security Group (Expertise)
 - User Groups (Awareness)

Where is security required in my organization?

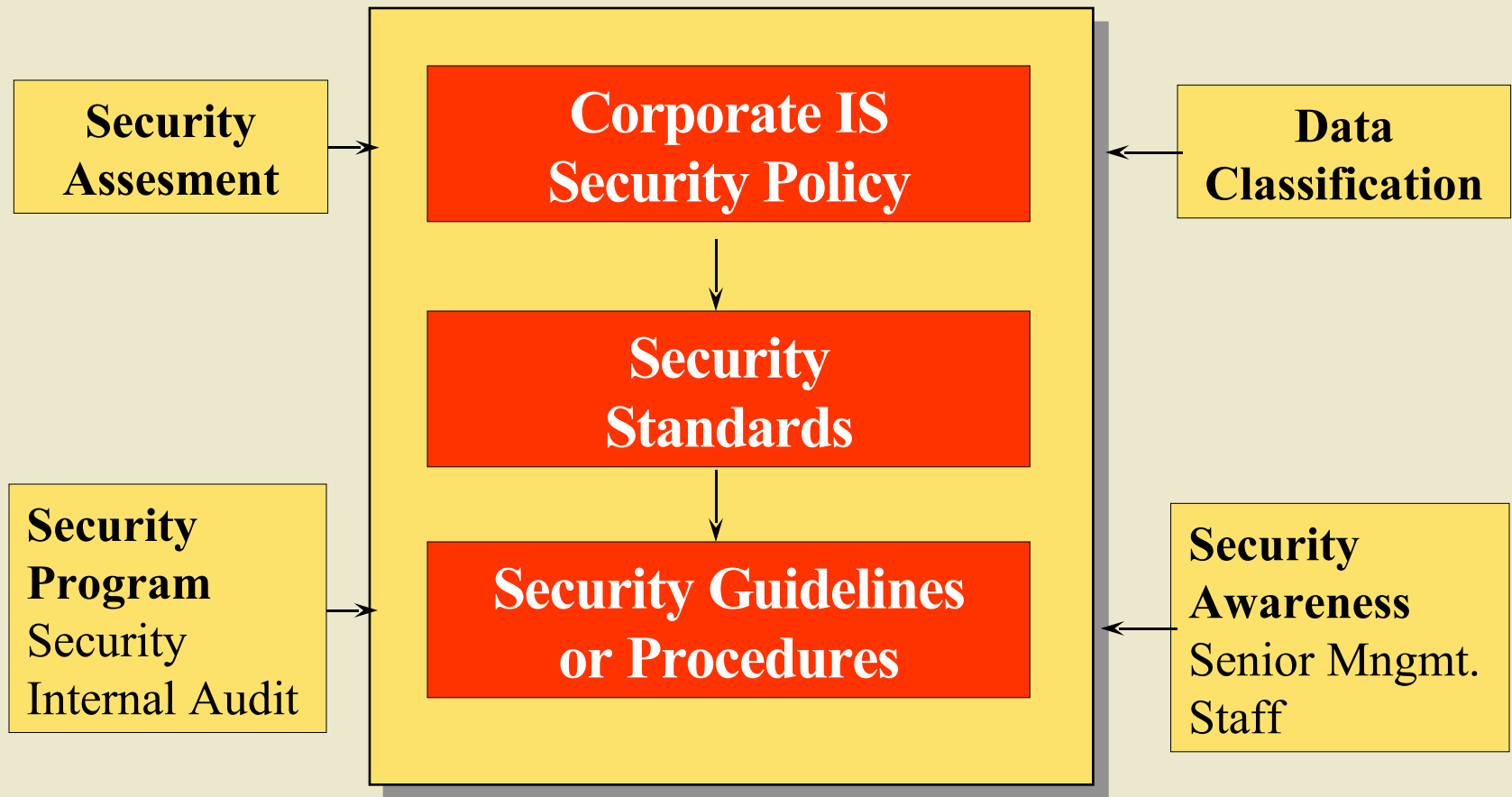
- Everywhere
- Security IS Everybody's Business !



How do I proceed to succeed in securing my organization?

- **We hope that's what you are here to find out**

Security Topology: IT Security Framework



Corporate IS Security Policy

What?

Why?



Policies

Where?

Who?

CC This and the next two slides is all important stuff. Remember it!

- **Policy** needs to be business driven
- **Policy** needs the cooperation and support of many areas of the organization
- **Policy** needs endorsement from Senior Management
- **Policy** needs to be direct and understandable
- **Policy** needs to be tied to standards and vice-versa
- **Policy** needs to be easily complied to by staff
- **Policy** needs to exist in all organizations

Corporate IS Security Policy

- The goal of the IS security **policy** is to define specific requirements pertaining to the use of information systems within the organization.
- A definitive **policy** spells out its purpose and scope and assigns responsibilities at various levels of the organization on keeping assets and resources secure.
- Compliance and enforcement objectives are also defined within the **policy**.
- The **policy** is a document of Corporate governance.

Corporate IS Security Standards



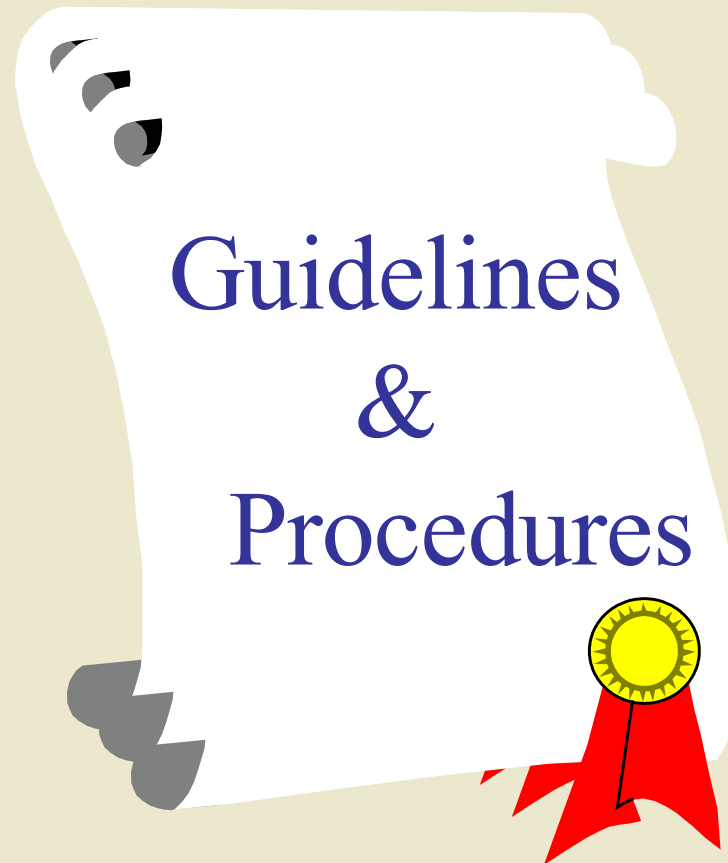
Corporate IS Security Standards

- **Standards** need to be business driven
- **Standards** need the support and buy-in from different areas of the organization (systems, network, etc.)
- **Standards** need to be realistic and achievable
- **Standards** need to be tied to policy and vice-versa
- **Standards** need to be dynamic and changeable
- **Standards** need to exist in all organizations

Corporate IS Security Standards

- Security **standards** are achieved through discussion and agreement with other areas on how certain IS components need to be deployed.
- Compromises between the groups is often achieved.
- Workable **standards** allow for a definitive policy to be complied with at all levels of the organization.
- Security **standards** provide a benchmark for review and auditability of IT resources.

Corporate IS Security Guidelines, and Procedures



Corporate IS Security Guidelines, and Procedures

- G&P need to be tied to standards and policy
- G&P need to be realistic and achievable
- G&P need to be dynamic and changeable
- G&P need to exist in all organizations

Corporate IS Security Guidelines, and Procedures

- **G&P** allow for users of IT resources to more fully understand the reasons for securing IS resources and assets and assist in complying to the policy.
- **G&P** educate system users and enhance their awareness of security.
- When joined with security policies and standards, the **G&P** become pivotal in a secure environment.

Assessing the Threats, Risks and Impacts



Assessing the Threats, Risks and Impacts

- **Threat:** The possibility of something bad happening to my organization from internal or external sources..
- **Risk:** The probability of a threat happening to my organization due to internal conditions.
- **Impact:** The result of the threat meeting the risk within my organization.

Realizing Threats, Risks and Impacts

- **Threats:**
 - External hackers scanning and probing
 - DDoS attacks launched from the Internet
 - Unauthorized access to resources
 - Virus infection
 - Internal attacks from disgruntled staff
 - Errors and omissions during routine processes
 - HW/SW failures
 - Fire, flood, power loss, emergency evacuation

Realizing Threats, Risks and Impacts

- **Risks:**
 - No governing policies or standards
 - No management commitment
 - Lax controls on system components
 - Security mechanisms not optimum
 - No processes for handling incidents
 - No knowledge of what to do
 - Mindset of maybe if I ignore it, it'll just go away

Realizing Threats, Risks and Impacts

- **Impacts:**

- Confidentiality breached
- Integrity lost
- Availability gone
- Bad press attacks credibility
- Loss of faith from clients
- Loss of the business

Recap from 40,000 feet

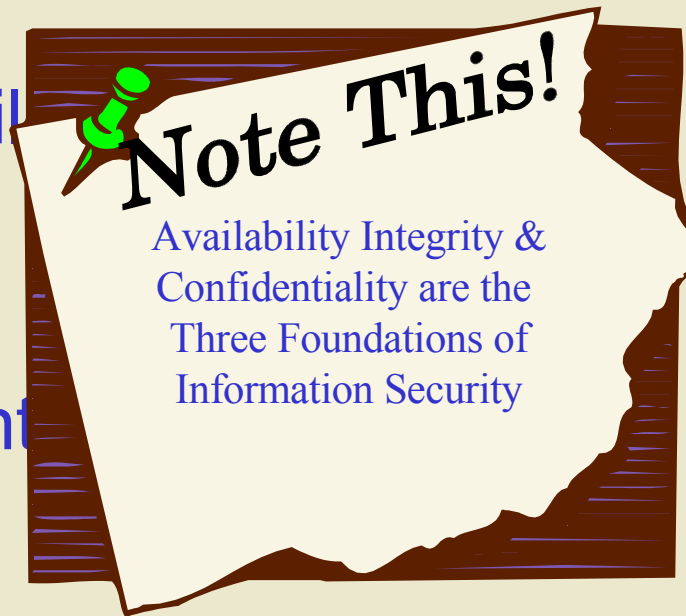
- From a high level we have viewed some of the basics of Information Systems Security.
- We have an understanding of the need for Policies, Standards, Guidelines and Procedures and,
- We have an understanding of the Threats, Risks and Impacts to our organizations that justifies the need for security.
- We know what can happen so let's descend to treetop levels and start to do something about it..

Your Security Program

- **Security Cornerstones**
- **Security Keypoints**
- **Security Components**
- **Security Elements**

Cornerstones of a comprehensive Security Program

- Systems and information **availability**
- Information and data **integrity**
- Information and data **confidentiality**
- Accountability at all levels
- Incident auditability, response and recovery



Cornerstone: Availability

- Information systems up time
- Accessibility to data repositories, libraries and warehouses
- Appropriate labeling
- Hardening of systems through defined access control mechanisms
- Incorporating legacy and client server requirements
- Allowing for routine maintenance windows
- Redundancy, fault tolerance and clustering

Cornerstone: Integrity

- $A = A$ yesterday, today and tomorrow
- Controlling system changes and data updates
- Proper backup, restoration and archiving processes
- Detecting unauthorized changes
- Data protection methods (authentication)

Cornerstone: Confidentiality

- Privacy laws demand this
- Access restrictions based on least privilege (need to know - need to use)
- Information and data need to be classified (Public, Internal, Restricted, Confidential)
- Data protection methods (encryption)
- Restrictions on hard copy material
- Appropriate transmission, transportation, storage, disposal and destruction of information assets

Cornerstone: Accountability

- Obligations of staff to comply with corporate policies and code of conduct
- Defined responsibilities of Managers for their staff
- Requirements on and off hours, on and off premises
- Moral, ethical and legal ramifications
- Knowing who did what, when and proving it

Cornerstone: Incidents

- Obligations of the Company when something occurs
- Ability to react and recover using audit logs, Intrusion Detection Systems (IDS), other security tools and support (3rd party) resources
- Ability to protect authorized staff required to do specific security duties

Keypoints of a Comprehensive Security Program

Remember
this from
earlier!

- Security is **Management** Issue - not a technical one
- **Unknown** Assets and Resources cannot be secured
- Assess the risks and weigh the benefits
- Security is a **Team Effort**
- **100% security is unachievable**

Keypoint: Security is a Management Issue

- Without Management commitment security will fail
- Security for the sake of security will also fail
- Security needs to be managed and controlled based on the **real needs** of the organization
- Some exposures and risks will remain
- Security should **not** report to IT but work with IT.



Keypoint: Unknown Assets cannot be secured

- Assets and resources need to be inventoried, assigned ownership and classified to adequately secure.
- Interdependencies of assets and resources need to be defined
- Whatever is not required should be removed

Who Me?



Keypoint: Assess the Risk

- Security cannot control many of the threats but can be prepared to mitigate the organization's risk and impact to them.
- Get the facts ... don't rely solely on media reports
- Always assume it will happen here even if others don't and know your defenses
- **Amber** flags are good, **Red** flags are dangerous.

Keypoint: Security is Team Effort

- Truth is, you often need them more than they need you, explore their vested interests then assist them
- Be pragmatic and honest about security issues
- Understand and address their objections and concerns
- Make allies early in the process (Audit, QA, Change Management, Systems & Network Management)

Keypoint: Absolute Security does not exist.

- Weigh all of the relevant factors
- Security cannot solve certain problems
- We have seen the enemy - they are we!
- Some risks will be accepted by the organization
- Keep abreast of changing trends in protection and threats

Components of a Comprehensive Security program

All of the security components that make up your organization's ability to do business need to be considered

- Information Security InfoSec
- Systems Security SysSec
- Computer Security CompSec
- Network Security NetSec
- Communications Security CommSec
- People Security HumSec

Component: Information Security

- Not all information is digitally stored so include it.
- Ascertain current practices with a view to enhance
- Consider authentication and encryption as well as clean desks, erasing white boards and being cautious of what is spoken of outside the office
- Keep up to date on your industry's rules and regulations regarding information storage and handling

Component: Systems Security

- **What** is your system comprised of?
- **What** are the interdependencies within the system?
- **Who** owns these systems?
- **How** critical are they?

Implement security at the architecture level

Component: Computer Security

- **What** falls under this heading in your organization (desktops, laptops, mainframes)?
- **Who** owns these systems?
- **How** critical are they?

Implement security at the architecture level

Component: Network Security

- **What** constitutes your network that differs from Systems or Computer security?
- **Does** your network include communication facilities (e.g. Internet access)
- **Should** controls be centralized or localized?

Implement security at the architecture level

Component: Communications Security

- Should include PBX and voicemail systems that could be exploited by criminals
- Toll fraud a big concern
- Work with voice services groups or external service provider (I.e. Centrex Service)

Implement security at the architecture level

Component: People Security

- Work with HR to verify credentials before hiring
- Exercise caution with consultants, contractors and vendors with wide systems access
- Non-disclosure confidentiality agreements
- Advise all personnel of your processes
- Terminations, resignations, leaves of absence

Elements of a Comprehensive Security Program

- User Identification and Authentication
- Monitoring
- Incident Handling

Element: User identification and Authentication

- Users need to be uniquely identified and authenticated to all processes
 - Something they **know** (ID and password)
 - Something they **have** (Card, photo ID)
 - Something they **are** (Biometrics)

Element: Monitoring

- All resources should have audit logs on
- Logs should be routinely reviewed
- Suspicious activities need to be investigated
- Procedures required with respect to personnel activities on systems (e.g. Internet sites)
- Personnel need to know systems are monitored.

Element: Incident Handling

- Treat all incidents as potentially serious
- Involve others where necessary
- Gather all relevant facts
- Avoid conclusions and finger pointing
- Ensure accuracy during hand-off and completion
- Cooperate with law enforcement as required

NOW... What About YOU!

Action Plan for the Professional Achievement

- Focus on efficiency and effectiveness
- Demonstrate and communicate your value
- Adapt to changes
- Develop new skills
- Act as an internal consultant
- Plan and manage your career thoughtfully
- Never stop learning
- Never stop questioning
- Benefit from the experience of others

Security Information and Support Organizations

- **ISSA** Information Systems Security Association
- **CIPS** Canadian Information Processing Society
- **ISACA** Information Systems Audit & Control Association
- **DRIE** Disaster Recovery Information Exchange
- **CISA** Canadian Industrial Security Association

Security and Related Professional Designations

- **CISSP** Certified Information Systems Security Professional
- **CISA** Certified Information Systems Auditor
- **CPP** Certified Protection Professional
- **ISP** Information Systems Professional of Canada