Jonathan Taormina, CPP, CFE, PCI

<u>POA – INFORMATION SECURITY</u>

CHAPTER 1 INFORMATION ASSET PROTECTION

<u>Information Assets</u> – exist in many forms.

- sensitive and proprietary information, privacy-protected data, intellectual property, intangible assets, and laws defining trade secrets, patents, and copyrights.
- <u>Information asset protection (IAP)</u>
    - "assessing and addressing risk enables business".
- Sun Tzu – sovereign's most precious faculty.
- Silk trade in China – 552 AD.
- Francis Cabot Lowell – textile mills in Scotland.
- Pinkerton – intelligence and counter-intelligence.
- Frederick Taylor, the father of scientific management, engaged in industrial espionage. (ie. Reverse engineering, planting agents, recruiting employees).
- Cold War – "dual-use" – military and commercial applications.
- FBI – Counterintelligence Strategic Partnerships Program.
- Economic Espionage Act (EEA) of 1996 – trade secrets.

<u>Risk Management Approach to IAP</u>

- identify, valuate, assess, likelihood, vulnerabilities, impact, security controls.
- Assess and prioritize risks.
- Goal of the security program is to **optimize risk**, NEVER minimize it.
- Global competition fuels commercial technology theft.

<u>Intentional Threats</u>

1. target and recruit insiders (often from same national background).
2. Economic intelligence.
3. Establishing seemingly innocent business relationships.

<u>Natural Threats</u>

- Many companies dissolved due to loss of information, not facility.
- Off-site critical data backup.
- Warm or Hot sites.

<u>Inadvertent Threats</u>

- MOST frequently overlooked.
- Human error and accidents.

<u>Data Mining</u>

- software-driven collection of open-source data and public information.

<u>Insiders</u>

- exploitation of trusted relationships:
    - vendors, customers, partners, subcontractors, outsourced providers.

- Internationalization of science and commerce.
- Global internet expansion.
- Gambling disorders, diminishing organizational loyalty,
- Ethnic ties to other countries.

Studies:

- 59% - former employees or contractors.
- 41% - current employees or contractors.
- 3 out of 10 – had previous arrest record.
- 80% - exhibited inappropriate behavior prior to incident.
- 31% - others had information about perpetrator's plan.
- 20% - direct threat was made.

Counterfeiting and Piracy – IP rights. Billions of dollars of losses each year.

Risk Assessment and Due Diligence

- identify risks, quantify them, and prioritize them.
- Criteria for risk acceptance and actions for **managing risks**.

Attaining Buy-in

- Executive buy-in is essential.
- Difficult because of the intangible nature of the assets.
- Reputation, competitive advantage, profitability.
- Align information assets with business operations.
- The responsibility for protecting information rests with the leadership.
- Mid-level management can influence security the most by following security practices.

Approaches to Risk Mitigation

- FBI – recognize, identify, implement, secure, "need-to-know" basis, training for employees.
- IAP training delivered repeatedly.
- Document training and IAP awareness efforts.
- Policy statement – to set the tone.
- Random audits.

Physical Security

- Harmonize with physical security.
- Layered Protection (Defense in Depth):
    - Concentric rings or layers of protection.
    - Increasing levels of trust, overlapping and diverse security technologies, successive layers delay, detect, and deter.
- Require authentication – access credentials.
- Document transfers of sensitive records.
- Prototypes and models.

- Manufacturing process and equipment – access control, restrict photography, non-disclosure agreements (NDAs) for contractors.
- Compartmentalization and physical or visual barriers.

Personnel Security

- due diligence investigations of potential partners, vendors, contractors.
- Pre-employment screening.

Privacy Protection

- PII – Personally Identifiable Information.
    - Privacy policies.
    - Review guidelines – US Federal Trade Commission.

Business Practices

- security is a business function.
- Harmonize IAP and general business practices.
- Incorporate IAP into Business Continuity Plan
- Due diligence of outsourced parties before partnering.

Operations Security or Information Risk Management

- OPSEC is a system of information risk management.
- Identify the gaps that remain despite current security measures.
- Particularly valuable for smaller businesses.
- Peripheral information – ie. Supply orders or Hiring Plans.
- Other entity (vendor, etc.) may not have sufficient IAP measures in place.

Domestic and International Travel

- carry information on person, not in checked baggage.
- Be aware of technical surveillance (electronic eavesdropping).
- Avoid hotel fax machines, copy and business centers for sensitive info.

Trade Shows

- rich collection and targeting opportunities.

On- and Off-site Meetings

- IAP strategy for each meeting.
- Site's telecommunications and audiovisual infrastructure.
- Minimize distribution of hard copy information.
- Presentations removed from non company owned equipment.
- 24 hour security of meeting rooms.

Counterfeiting and Illegal Copying

- monitor the internet.
- Audits, inside and outside the organization.
- Record copyrights and trademarks with US Customs and Border Protection.
    - Allows CBP to stop suspected products.

Jonathan Taormina, CPP, CFE, PCI

Legal Protections

- HIPAA – Health Insurance Portability and Accountability Act.
- Gramm-Leach-Bliley Act – Financial Services Modernization Act.
- Monitor pending legislation and confer with counsel.
- Patent – property right granted to inventor for a limited time.
- Trademark – words, names, symbols, devices, or images.
- Copyright – expression of ideas in literary, artistic, and musical works.
- Best way is to register these and membership in anti-counterfeiting orgs.
- US State Department – "IPR tool kit".

Copyrights

- do not have to be registered to be protected.
- Do not allow control of copyrights to agents or distributors.
- Upon discovery of violation – take action immediately.

Trademarks, Trade Dress, and Service Marks

- registration prior to doing business in any country is the primary means of ensuring the mark is eligible for protection.
- Best weapon is prevention.
- Conduct research to identify products that infringe the trademark.

Patents/Trade Secrets

- Patent – requires the inventor publicly disclose the invention's elements.
    - Lasts 20 years.
    - No criminal laws for patent infringement.
- Trade Secret – not disclosed and may last indefinitely.
    - Need not be registered.
    - Must prove added benefit, specifically identified, and reasonable level of protection.
- US International Trade Commission – resolving patent disputes.

International Concerns

- lawyers with experience in anticipated market.
- Nondisclosure agreements (NDA).
- Intellectual property due diligence of market of the country.
- US State Department's Overseas Security Advisory Council (OSAC).

Nondisclosure Agreements and Contracts

- information on any medium considered official record.
- As a condition of employment.
- Continuing obligations even when employment ends.

Technical Surveillance Countermeasures (TCM)

- identify, and neutralize technical surveillance activities (eavesdropping).
- Offices and meeting rooms should be “swept”.
- Networks (wired and wireless).
- Stand alone computers.
- Integrate physical, procedural, and logical protection.
- Antivirus and firewall software.
- Implement formal patch management and configuration management protocols.
- External organizations must maintain an equivalent security posture.
- Intrusion Detection System (IDS):
    - Monitors for malicious programs and unauthorized changes to files and settings.
    - Monitors network traffic and provides alarms.
    - Extrusion system prevents the unauthorized exit of information.

Logical network access control – users are identified and given priveleges.

Application Security – vulnerability due to improper integration of third party software.

Sanitizing information systems and media – overwriting and **degaussing** (magnetic erasure), and physical destruction.

Encryption – only decoded by those for whom intended.

Digital Signature – authenticates the identity of the sender.

Wireless Environment – (WLANs) Wireless are less secured than wired (LANs).

Cell phones, laptops and personal digital assistants (PDAs)

- employees acknowledge policy.
- Discourage use of mobile devices with embedded cameras.
- Software to remotely lock device.
- Be careful of wireless hot spots.

E-conferencing – not necessarily secure.

Outsourcing

- increases the risks to information assets.
- Nondisclosure agreements (NDAs).
- On-site security reviews.
- Physical security and information technology measures.

Response and recovery After an Information Loss

- Investigate root cause, damage assessment and prevention of future loss.
- Damage Assessment of information compromised and implications.
- Recovery and Follow-Up
    - 1. Return to normal business operations ASAP.
    - 2. Implement measures to prevent a recurrence
    - 3. Root cause analysis and implement corrective actions.
    - 4. Database of incidents (suspected and allegations).

Summary of IAP program

- Strive for prevention, respond, recover, protect.
- Protect the information commensurate with its value, based on periodic risk assessments.
- Integrates traditional security, IT security, and legal and administrative functions.
- Cost-effective, risk-based measures.
- Applies to all employees and the extended enterprise.
- IAP manager is responsible for overall policy.
- Other managers and directors – employee understanding and compliance.

Is the information…..public?, internal?, or restricted?

Information Classification and Sharing

- Highly restricted – could seriously damage competitive position.
- Restricted – legal or employee privacy risks.
- Internal use – not intended for public distribution.
- Unrestricted – can be shared inside and outside organization.

Employee Privacy

- privacy of personnel records must be assured.
- Each employee has the right to know what type of personal information the organization maintains.

Securing the Property

- tangible and intangible assets.
- Wear and display appropriate identification.
- Branch managers ensure facilities meet requires access control.

Security Awareness and Training – each employee is responsible. Periodic training.

Public Release of Information – media inquiries to external affairs director.

Publications and Presentations – must follow IAP policy.

IT Resources

- subject to monitoring and review.
- NO expectation of privacy.

Web Presence - any information posted on-line must follow IAP policy.

Extended Enterprise (Trusted Relationships)

- individuals and entities with access to organization's information, assets, people and facilities.
- IAP policy must be documented.
- NDA, contract clauses, memoranda of understanding.
- Obligation to protect may extend beyond period of relationship.

Reporting Suspicious Activity or Suspected Losses or Compromises

- to IAP program manager or security department.
- Very important: does the information provide a competitive advantage?

- avoid faxing across international borders.
- Fax only if other more secure methods are not available.
- Password enabled screensaver with timeout less than 15 minutes.

Managing Technical Reports

- the greatest possibility of compromise is in the **intermediate stages** with the least prospect of detection.
    - Much of the info. with the least focus on protection.
    - Information protection may not catch up.
    - Longest period – provides for complacency.
    - Effective IAP program is Cradle-to-Grave.

Laboratory Notebooks

- responsibility of the scientists and engineers.
- A completed invention is comprised of two events:
    - Conception of the idea.
    - Reduction to practice (carrying out of the invention).
    - Signed document by inventor and 2 witnesses.
        - Witness may NOT be a co-inventor.
- Notebooks:
    - Bound, not loose leaf.
    - Consecutively without blank spaces.
    - Coded terminology only used if fully defined.
    - Not backdated.
    - Errors not erased – draw a line through the error.
    - Acquired from research librarian, numbered consecutively.
    - Upon termination – return notebook to research librarian.
- Disclosure of Invention.

- Provisions for electronic laboratory notebooks:
    - Commensurate with policies on IAP and IT security.

Information Disposal and Destruction

National Association for Information Destruction.

- Every business has information that requires destruction.
- Stored records should be destroyed on a regular schedule:
    - Avoids appearing suspicious.
    - Limits amount to be provided in a legal proceeding.
- Incidental business records discarded daily should be protected:
    - Phone messages, memos, drafts of bids and correspondence.
- Recycling is not an adequate alternative for information destruction.
    - Arrange for recycling after destruction.
- Due diligence is essential.
    - Certificate of Destruction is an important legal record.
- MOST records storage companies DO NOT provide secure shredding services.

CHAPTER 2 THE INCREASING IMPORTANCE OF INFORMATION SYSTEMS SECURITY.

Cybercrime – the use of information systems to commit crime.

Paradigm – a theoretical tool for understanding all the things one thinks about when one considers a scientific school of thought or other rigorous discipline.

Attacks such as:
SQL-injection, **cross-site scripting,** content spoofing, and information leakage.

- **Cross-site scripting** = **80%** of documented security vulnerabilities in 2007.

Multi-factor authentication – ie. Fobs, tokens.

Malware:

- type of data-stealing Trojan horse programs known as "Zeus" allows the attackers to change the display of a bank's login page as a victim is entering credentials.
- Told site is down for maintenance – wait 15 minutes.
- Customer waits, and the thieves use those intercepted credentials to log in as the victim and initiate unauthorized transfers from that account.

Microcomputer Revolution
- started in 1975.

- rise of local-area networks, wide-area networks, and the Internet.

- thefts from on-line banking – do not legally need to be disclosed.

- Hackers used to hack for pleasure or reputation, now it's MONEY.

Bots – software applications that run automated tasks.

- criminals are changing malware code so it is not detected by traditional antivirus systems.
- 27% of attacks in 2008 were targeted attacks written directly to attack a specific company.
- Insiders are no longer the cause of most losses.
- Hygiene Problem – a known problem that can be fixed with due diligence.
- malware and other attacks can circumvent signature-based controls.
- Personal Identification Numbers (PINs) are the hot item – not credit cards.
- "anti-forensics" have been developed to hide one's tracks.

- **Rogueware** – pretends to be security software but really compromises a computer.
- mobile malware is an up and coming profit center.
- IBM – "every Web site should be viewed as suspicious and every user is at risk".

Economics of Information Systems Security

- loss of productivity is more costly than the cost of cleaning up from the virus attack.
- Behavior-based host intrusion prevention systems.
- A party is negligent if the cost (B) of taking adequate measures to prevent harm is less than the monetary loss (L) multiplied by the probability (P) of its occurring ($B<PL$).
- Using corporate resources to protect sensitive information and systems is one of the key objectives of an ISS program.

Factors that an Information Security Standard of Care Must Meet:

- Executive management responsibility.
- Information security policies.
- User awareness training and education.
- Computer and network security.
- Third-party information security assurance – share information only when it is assured that those parties protect the information.
- Physical and Personnel Security.
- Periodic Risk Assessment.

- distinguish information as: public, for internal use, or restricted.

Security convergence is the integration, in a formal, collaborative, and strategic manner, of the cumulative security resources of the organization in order to deliver enterprise-wide benefits through enhanced risk mitigation, increased operational effectiveness, and cost savings.

Supervisory Control and Data Acquisition (SCADA)

- systems that use the internet as the control backbone.
    - Increases the possibility of disruptions.
    - Inherent vulnerabilities of interconnected computer networks.
    - Data exfiltration by outsiders who gain insider privileges (phishing).

Physical Security can use several modes of communication:

1. proprietary connection between one device and another.
2. Industry standard connection between two devices, such as the Weigand protocol between a card reader and controller.
3. Network devices generally speak over TCP/IP (transmission control protocol/internet protocol) – the worldwide standard for communication.

Jonathan Taormina, CPP, CFE, PCI

Devices divided into two types:

1. Embedded Systems (special systems) – typically programmed at the manufacturer and run proprietary or nonstandard operating systems. (video cameras, card readers, access controllers, etc.)
2. Host-based systems – run on more standard operating systems, typically a Windows or Linux operating system.

- Embedded systems are far more difficult to change than Windows operating systems, but all these systems can be compromised.

- IP video surveillance provides many advantages over earlier systems, but it too is vulnerable.

Electronic Access Control usually contain three major components:

1. Card reader or "prox" (proximity) card.
2. Communicates over some medium (wired or wireless) to the controller.
3. Controller – typically talks to a server or application from which it gets its instructions on what to do.

- a legacy HID (Hughes Identification Device) – do not require mutual authentication.
- Card has two components:
  - Secret facility number.
  - Identification number printed on the card.
- "Gecko" – a tool that can give an intruder complete control over a door.
  - Can be built for $10.
- Almost every access control system in use today runs a database on a computer.
- Security professionals should use intelligence and imagination.

Cybercrime: A National Challenge

- weapons of mass DISRUPTION.

CHAPTER 3 THE INFORMATION SYSTEMS SECURITY BODY OF KNOWLEDGE

Information Systems Security (ISS) Program

- cost-effectively manage the risk that critical organizational information could:
  - be compromised, changed without authorization, become unavailable.
- Strive for CIA:
  - Confidentiality, Integrity, and Availability.

ISS Terms

- Information Systems Threat – any circumstance…potential to adversely impact.
- Information Systems Vulnerability – a flaw or weakness….
- Information Systems Risk – product of level of threat and level of vulnerability. Possibility of a threat by exploiting a vulnerability.
- Information Systems Countermeasure – anything that reduces, eliminates, prevents, minimizes, discovers or reports a threat, vulnerability or an attack.
- Potential Threat Risk – potential risk after all ISS countermeasures are applied, for EACH threat.
- Residual Risk – total remaining potential risk after all ISS countermeasures are applied across all threats.

$$\text{Residual Risk} = \frac{\text{Threats} * \text{Vulnerabilities}}{\text{Countermeasures}}$$

- Residual risk falls as countermeasures are applied.

Information System Threats

- Nature – earthquakes, hurricanes, other.
- People – employees and others with legitimate access, Cybercriminals.
- Virtual Threat – a computer program or script illegitimately installed:
  - Sending info. from the device to owner of program (its control).
  - Receiving command and control instructions from its control.
  - Executing commands on the device.
    - Virtual threat agent (ghost in the network) steals, changes or destroys.
    - Ability to go virtual is what differentiates the logical security paradigm from the physical security paradigm.
    - Takes advantage of logic of modern computers and the inherent flaws.
- Cybercriminal must get onto a target computer to use a virtual threat:
  - marketing spyware – collecting info. on sites visited.
  - Keyloggers – recording keystrokes.
  - Koobface – computer worm – targets social networking sites.
  - Zeus – on-line banking Trojan.

Information System Vulnerabilities

- infrastructure.
- Users.
- Custodians – maintaining the infrastructure.
- Executive and senior management – lack of accountability, procedures.
- Processes – ie. Inadequate patch management, change control, planning.

Information System Control Objectives – Detection, Recovery, Compliance.

Information System Countermeasures:

1. Administrative controls – policies, standards, procedures.
2. Technical controls – log-ins, passwords, firewalls.
3. Physical controls – door locks, cameras, guards.

Infrastructure Countermeasures

- Perimeter Security – devices such as: switches, firewalls, etc.
- Device Protection Security – antivirus, desktop firewalls, encrypted hard drives.
- Access Control and Authentication – user IDs, passwords, second-factor key fobs, etc.

Information Systems Infrastructure Management Countermeasures

- Vulnerability and patch management.
- System monitoring and Log review.
- Information systems security Metrics – to measure successes.
- Physical security of the information systems infrastructure.
- IT staff training in information security.

Executive and Senior Management

- Buy-IN.

Community-Based Countermeasures

- everyone in business is responsible. A single machine left unpatched can be the launching pad for a series of attacks on everyone else.

Down the Rabbit Hole: Computer Logic, System Complexity, and Inherent Vulnerability

1936 British mathematician Alan Turing. The Turing Machine.
- beginning of the modern computer age.
- mathematically explored what it means for a number to be computable. i.e., for its successive decimal places to be calculable by finite means.
- decrypted German signals – can be considered a hacker tool used to decrypt sensitive confidential German information.
- Algorithm – a precise method for solving a problem using a finite sequence of precise instructions. Good algorithms contain relatively few bugs.

How Computer Systems Work

- Gordon Moore (Intel) – Moore's law – the processing power in any line of computers will double every 18 months.
- More complexity, enabled by more processing power, leads to greater possibility of error.
- As computers become more interconnected, they become more vulnerable.
- Basic instructions for how a computer gets going are stored in its **hardware**.
    - What to do when it first turns on (Booting up).
- Computer begins to read instructions. Instruction software area – **firmware.**
- Computer then moves on to the **operating system.**
    - Millions of lines of instruction.
    - Input and output.
    - Typically responsible for user authentication.
- Next level of system architecture is **peripherals.**
    - Hard drive, CD-ROM.
- Computer operates in two primary modes:
    - Stand alone – stores and manipulates information in its memory.
        - Volatile memory – only available when the computer is ON.
        - Static memory – information available with no power – OFF.
- **Computations** – data changes and manipulations, which occur in the computer's **processor.**
    - Stand alone mode is the basic Turing model of an algorithm.
- Communications
    - Computers on the Internet communicate via a protocol called **Internet Protocol (IP)** which is also called **TCP/IP (Transport Control Protocol/Internet Protocol).**
    - almost all communications via computer follow a model called:
        - **Open Systems Interconnect (OSI) Seven Layer Network Model.**

Open Systems Interconnect (OSI) Seven Layer Model

- Layer 1 (Physical) - communicating by either sending an electrical impulse or not.

- Layer 2 (Data Link) - communicating logically.
- connected by a wire or in a network to a centralized location typically referred to as an **intermediate distribution facility (IDF).**
- connected to a **switch**. Each computer connected to a switch can speak to any other computer directly connected to the same switch.
- Switches provide little privacy.
- Not only a back-end device that connects computers, but it is also a **host** that can be configured. It runs programs, meaning it can be compromised.

- Layer 3 (Network) - also known as Layer 3 communication.
- computers are unable to see each other directly.
- necessary to have an intermediary – a **router.**

- <u>Remaining layers</u>
- Layer 4 (Transport) – determines the mechanism for how computers are actually going to transport the information between the two computers.
- Layers 5,6,7 (Session, Presentation, Application) address how computers organize data into flows, standardize the data, and perform functions not pertaining directly to network operation.

<u>Data Input Challenges</u> – a computer has three logical points of entry:

1. Input – type into keyboard or other input device.
2. Programs – ask the computer to do something.
3. Communications Stack – this is the dangerous part.
    a. A computer can send input or ask a program to do something from anywhere in the world.

- one mode of attack via input is to enter unusual text into log-in field on a Web page, such as “or 1=1-“ If the computer is not prepared to deal appropriately, the computer may return information the user should not see.
- **<u>Buffer overflow</u>** – another category of attack in which a malicious user or program can give more information to the computer than it is expecting. Can produce a buffer overflow state, giving the computer instructions to do something unintended.
- **<u>Logic errors</u>** – if the programmer does not write the code correctly, a malicious user can actually get it to do something.

<u>**Host**’s: It’s a Party</u>

- a host computer stores information and allows one to manipulate it or communicate with another computer.
- A host needs a mechanism for taking a command – the **platform.**
- Any system that is a computer host is potentially compromisable:
    - **Servers** – serve more than one individual.
    - **Workstations** – not portable.
    - **Laptops** – identical in function to workstations.
- **Personal Digital Assistants (PDAs)** contain as much information as a computer from the 1990s.
- Anything connected or that can connect to a network is at risk.
- Since any device that can communicate with another computer and has memory is referred to as a **host**, a host could also be a **printer**.
- **Rights, permissions, privileges –** things a user is allowed to do.
- **AAA triad** – Authentication – Authorization - Auditing/Accountability.
- **Services** – programs that simply keep the computer going.

Jonathan Taormina, CPP, CFE, PCI

CIA Triad – Confidentiality Integrity Accountability

Confidentiality

- Passwords can be guessed.
- Other options: biometric authentication, fingerprint scanners, hand geometry scanners, or iris scanners.
- **OTP (One Time Password) Tokens** – second-factor authentication.
- **Encryption** – broken over time. Must repeatedly increase the strength.

Integrity

- Encryption can help.
- **Cyclical Redundancy Check (CRC)** – shows if data has been tampered with.
- Most important files – contain user IDs, passwords, and allowed roles (rights, permissions, and privileges.

Availability

- back up data off-site.
- Reliability.
- Redundancy – battery backup and generator.
    - Battery – to shut down.
    - Generator – to keep running.

Managing the IT Infrastructure

- security professionals are responsible for the assets of their company, including assets intertwined with the IT network.
- **IT Infrastructure Library (ITIL) -** International standard.
    - concept of **Service Level Agreements (SLA)** – how one negotiates with IT professionals for the services needed.
- Facilities requirements – ie. Air-conditioning, intrusion detection, access control, video surveillance, etc.
    - Includes any place where someone can connect to the network or gain access to servers.

Real World Computer Systems

- **Internet** – most common type of network connection.
    - Impossible to know who, if anyone, is protecting the data.
- **Firewall** – device in between the Internet and the system to be protected.
    - only one tool in the **defense-in-depth arsenal.**
- **Virtual Private Network (VPN)**- encrypts data from one point to another.

Vulnerabilities

- a specially crafted e-mail can get the mail system to do something undesirable to the recipient.
    - **Escalation of privilege** attacks succeed because the email program is tricked into executing the email as if it were a program rather than simply processing it as text.

  - Web applications generally make such attacks much easier.
- **Brute force password hack** – go through permutations of passwords.
- One can assume that cybercriminals can penetrate user names and passwords.
- **File Transfer Protocols (FTP)** – used to share files. Another mechanism by which others can access a computer.

Related Peripherals

- many portable devices that can both load malicious software and take away data that should not be taken away.
- Printer can be intercepted. Memory should be wiped if confidential information is being printed.

Telecommunications

- **Private Branch Exchange (PBX) –**central core of many corporate telephone systems.
- Proprietary operating systems running on an embedded system burned into hardware or on top of a computer server, like any other application.
- Phone systems should be treated identically to any other computer system.
- Modern **voice over IP (VOIP)** systems may sit on the network but are less prevalent.
  - Often have a **Remote Maintenance and Administration Terminal (RMAT)** that can be used to dial into the system and make configuration changes.
- **Plain old telephone service (POTS)** – old fashioned, two pair phone line that is connected via copper from the phone to the central office (CO).
  - Also referred to as **Analog lines –** and are usually required for fire systems and a good idea for intrusion detection alarm connections.
- **VOIP** – converged onto network. Less expensive because the wiring is the same for a computer.
  - Completely accessible on the network.
  - Has the potential to be compromised.
  - Each phone is a host and goes through the Internet before the phone company.
  - Some companies connect to their central office via the Internet, allowing for additional exposure.
- Critical paths for phone data should have backup power for 12 hours or more.
- Redundancy – a professional VOIP installation typically has two of these machines for redundancy.
  - Redundancy extends to routers, lines, and switches
- Faxing – modern fax machines have memory that stores images.
  - Confidential faxes should be encrypted.
- Cell phones and PDAs are a major concern as well.

Additional Information Security Concepts

- Quality of Service (QoS)
  - Data given priority on the network.

Third-Party Review

- each organization is responsible for managing its vendors.
- Payment Card Industry Data Security Standard (PCI DSS)
  - Cardholder data.
  - PCI DSS assessment.
- Appropriate actions when allowing third-party access:
  - Security review of the third-party.
  - Business case for having the data access.
  - An agreement of the requirements for the access.
  - Reexamination when changes occur.

Information Security Technologies

Intrusion Detection System (IDS)

- monitors network to decipher behavior or patterns/signatures of someone trying to hack the system.

Intrusion Prevention System (IPS)

- variation of the IDS - designed to automatically stop an attack in progress.

Host Intrusion Protection System (HIPS)

- operates on a host system, such as a computer or server.
- Behavior based protection as programmers cannot write signatures fast enough to identify and keep out the onslaught of viruses, worms, Trojans.

Certificate

- mechanism to allow individuals to ensure a secure transaction.
- Asymmetric tools that work like a lock and key.
- Used frequently to enable encryption.

Security Information and Event Manager (SIEM)

- device that looks at all the log activity to point out what is most important to facilitate response to incursions and other problems.

E-mail Gateway

- looks at inbound and outbound emails to determine if security risks exist.
- Reduce the amount of **spam** which can have **malware.**

Web Gateway/Proxy Server

- filter which Web pages can be downloaded.

Data Loss Protection (DLP) – keeps people from sending certain data.

Web Application Firewall

- filters traffic before it hits an organization’s Web site.
- Used to block malicious attacks on **vulnerable code.**

Network Access Control (NAC)

- computers are not admitted to a network unless they are allowed, do not have malicious software, and meet the standards of the network.

802.1x

- Institute of Electrical and Electronics Engineers (IEEE) Standard.
- allows for specific authentication before a computer can come onto the network.
- used with Network Access Control (NAC).

Common Vulnerabilities and Exposures (CVE)

- on-line dictionary of publicly known information security vulnerabilities and exposures.
- Backbone of the National Vulnerability Database.
- Essential in the twin disciplines of vulnerability management and patch management.

ISS Practitioner Frameworks

- protection of information system assets:

ISO/IEC 27001:2005 and ISO/IEC 27002:2005

- international standard for managing information security.
- 11 specific vital information security management practices.
- Framework called Information Security Management System (ISMS).
- Overall management system, based on a business risk approach.

CISSP Common Body of Knowledge

Definitive certification requirements appropriate to the individual ISS professional. (de facto standard for ISS certification)

- Access Control.
- Application development security – (write secure code).
- Business continuity and disaster recovery planning.
- Cryptography – (encoded or encrypted to prevent disclosure).
- Information security governance and risk management – (identifying risks and dealing with them through policies, procedures, and guidelines).
- Legal regulations, investigations, and compliance.
- Operations security.
    - Resources to be protected, best practices, restricting access, abuses of access, appropriate controls, and response to attacks.
- Physical (environmental) security.
- Security architecture and design – (hardware, software, security controls, documentation).
- Telecommunications and network security.

Information Security Governance: Guidance for Boards of Directors and Executive Management

- ISACA’s management maturity model:
  - Snapshot-in-time assessment tool.
  - Identifying an appropriate security management maturity level.
  - Identifying gaps between current maturity level and desired level.
  - Planning organization-wide information security management improvement program.
  - Planning specific information security improvement projects.
- ISACA framework allows for maturity levels, making it possible to measure how well an organization is doing compared to how well it could do.

Generally Accepted Information System Security Practices (GAISP)

- ISSA.
- Ongoing project to collect and document information security principles that have been proven and accepted by practitioners.
- Objective guidance for information security professionals.

The Emerging Legal, Regulatory, and Contractual Landscape Regarding ISS

- designed to obligate organizations to protect sensitive information.

Payment Card Industry Data Security Standard (PCI DSS)

- a uniform set of ISS standards for protecting Credit Card information.

- Build and maintain a secure network:
  - Firewall.
  - Do not use vendor supplied defaults for passwords.
- Protect Cardholder Data
  - Protect.
  - Encrypt.
- Maintain a Vulnerability Management Program.
  - Antivirus software.
  - Secure systems and applications.
- Implement Strong Access Control Measures.
  - Restrict access to “need to know”.
  - Assign a unique ID to each person.
  - Restrict physical access.
- Regularly Monitor and Test Networks.
  - Track and monitor all access to network resources.
  - Regularly test.
- Maintain an Information Security Policy.

Jonathan Taormina, CPP, CFE, PCI

Health Care and Insurance Portability and Accountability Act (HIPAA)

- standard of care for electronic transactions in the **health care field**.
- Business associates of covered entities must also adopt specific security measures.
- US Department of Health regulations regarding the privacy of "individually identifiable health information".
- Risk-driven information security management program.
- Ensure **C**onfidentiality, **I**ntegrity, **A**vailability. (CIA)
- Ensure compliance by work force and by third-parties.
- Requires the proactive management of security information.

Gramm-Leach-Bliley Act (GLBA)

- nonpublic personal information of individuals who obtain financial products or services from **financial institutions.**
- Protect against threats or hazards, unauthorized access.
- Prohibited from disclosing to third-party unless disclosure.
- Increased enforcement activity by the Federal Trade Commission.
- Two-factor authentication to identify users of on-line services.

Children's Online Privacy Protection Act (COPPA)

- children under 13.
- Enforced by Federal trade Commission.

Sarbanes-Oxley Act (SOX)

- Substantial additional responsibilities on officers and directors of public companies.
- Significant criminal penalties on CEOs and CFOs.
- Public companies or hope to become public, or sold to public company.
- Internal controls and procedures.
- Information security.
- Internal control over financial reporting.
- CEO and CFO must personally certify the company's annual and quarterly reports.
- Monitoring and testing procedures.
- Often extended to private companies by state law or regulation, or through market forces.

Red Flag Rules

- sections 114 and 315 of the Fair and Accurate Credit Transaction Act (FACT).
- Identity theft prevention programs.
- Identify "red flags" signaling possible identity theft.
- Identify, detect, respond to red flags to prevent and mitigate identity theft.
- Ensure program is updated periodically.
- Purpose is the early detection and prevention of identity theft.
- "Covered accounts" require protection.

<u>FTC Enforcement Actions</u>

Federal Trade Commission

- adopted a “safeguards rule” which requires each financial institution:
  - comprehensive information security program.
  - No specific rules – it requires that businesses regulate themselves.
- Prohibits unfair and deceptive practices.
- FTC actions began in 1988.
- Actions for:
  - Using clear text.
  - Not limiting wireless access.
  - Not using strong passwords.
  - No firewalls.
  - Failed to detect and prevent unauthorized access.
- Required:
  - Administrative, technical, and physical safeguards.
  - Designated employee to coordinate the information security program.
  - Identify internal and external risks, and implement safeguards.
- CVS violated HIPAA – sensitive financial and medical information.
- Companies that ignore their responsibilities will be held accountable.

<u>State Breach Disclosure and Related ISS and Privacy Laws</u>

- California became the first state.
- Required organizations to notify consumers in the event of a suspected computer breach
- Nevada and Washington – banks to recover costs from retailers and credit card processors for failing to comply with Payment Card Industry (PCI) standards.

<u>US –EU Safe Harbor</u>

- prohibits the transfer of personal data outside the EU except when the recipient demonstrates it will provide an adequate level of protection.

<u>US Department of Commerce – 7 key principles:</u>

1. Notice – inform individuals about the purposes.
2. Choice – opt out.
3. Onward Transfer – to disclose information to a third party, organizations must apply Notice & Choice.
4. Security – reasonable precautions.
5. Data Integrity – personal information must be relevant.
6. Access – individuals must have access to their personal information.
7. Enforcement – assuring compliance.

Responsibility for On-Line Bank Theft

- Cybercriminal launch “man-in-the-middle” attacks to take advantage of technical weaknesses.
- Plant malicious software on a victim’s PC to steal the company’s on line banking credentials to siphon money from the targeted accounts.
- Automated clearinghouse (ACH) withdrawals.
- The convergence of “cyberspace” and “brick and mortar”.

ISMS – Information Systems Security Management.

ISS Risk and Vulnerability Assessment

- risk-based approach.
- Vulnerability assessment to measure compliance against a specific standard.
- ISS assessment addresses the traditional ISS objectives:
    - Protecting, detecting (successful and blocked), recovering, complying with laws, regulations, and contractual obligations, and availability.
- Management and Technical components:
    - Management – formal to informal.
    - Technical – formal snapshot-in-time of security of IT infrastructure.
- Organization’s needs, obligations, and opportunities.
- How effective?
- Gaps between needs and realities - and the capacity to close gaps.

ISS Policy Implementation

- biggest challenge to management is not in the writing of specific policies but in the orderly development and implementation of policies.

Incident Response

- not all incidents can be prevented.
- Policy is not complete until procedures are put in place that allow for handling and recovery of the most devastating of incident.
- Consider a Computer Incident Response Team (CIRT).
- Critical element is the policy document.
- Physical security can be a critical element of the team because of the similarities in incident response between physical and information security paradigms.

Total ISS Management

- Risks, threats, vulnerabilities, and countermeasures.
- “Red Queen Effect” – program must be continually improved to keep up and do a better job tomorrow.
- Cannot be just to provide an appropriate level today. That is the purpose of Information Security Management Systems (ISMS).
- ISMS is based on a process-model perspective of information security management – Understanding requirements; Implementing operating controls; Monitoring and reviewing performance; Continual improvement.

Jonathan Taormina, CPP, CFE, PCI

Plan-Do-Check-Act (PDCA) model:

Establish the ISMS, Implement and Operate, Monitor and Review, Improve.

An ISS Aware Culture

- ultimately depends upon people's behavior.
- Culture of an organization = external adaptation and internal integration.
- Formally – according to the organization chart.
- Informally – the way the work actually gets done.

ISS Cultural Challenge

- ISS is the new kid on the block.
- ISS is nowhere near the core of the organization – only exist because legally required.
- ISS concerns seem disconnected from the business.
- Information systems security contains the word "security".
    - Security will handle without other employees getting involved.
- ISS Security culture touches the rest of the organization when there is a problem.
    - Few natural opportunities for cultural blending.
- Must embed its culture into the culture of the larger organization.
- Leadership must manage cultural evolution.
- The organization must see the world as the Information Security does.
- ISS is forever intertwined with the physical security practitioner.

Community Emergency response Team (CERT) – Carnegie Mellon.

CISSP is the gold standard in Information Security.

Jonathan Taormina, CPP, CFE, PCI

CHAPTER 4 SECURITY CHALLENGES OF CONVERGENCE

Convergence - the integration, in a formal, collaborative, and strategic manner, of the cumulative security resources of the organization in order to deliver enterprise-wide benefits through enhanced risk mitigation, increased operational effectiveness and efficiency, and cost savings.
- security convergence can enhance risk mitigation but can also increase total organizational risk.

Network Risk

- when physical security practitioners put physical security technology onto the network.
- Denial of service (DOS).
- Insertion of inaccurate data.
- Data theft.
- Data modification.
- Data destruction.

CIA Triad – Confidentiality, Integrity, Availability.

Network Case Study : Camera System

- a modern video surveillance system relies heavily on networks.
- Segregated from network by a **firewall** and a **virtual private network (VPN).**
- Network **switch** – connects the network assets together.
- **Server** records the video, and another provides command and control.
- All of the data resides on the **Storage Area Network**.

- Denial of Service – someone can turn off video viewing capability.
- Insertion of Inaccurate Data – adding an invalid video showing no one.
- Data theft – analyze to plan a crime.
- Data modification – showing previously recorded video.
- Data destruction – deleting, hiding evidence of a theft.
- May be able to be controlled from anywhere in the world.

Access Control

- Door reader --- embedded controller --- switch --- server.
- The card reader talks to the embedded controller which talks to the network.

Layer 2 Communication

- computers communicate directly when they can see each other.
- Conversation is forwarded only between the two computers.

Layer 3 Communication

- requires an intermediary.
- The mechanism by which computers can interact across the internet, around the world.
- Every device connected to the network is accessible to everything else connected to the network ---- Vulnerability.

Communications Attacks

- Social engineering – convinces a user to share his credentials.
- Direct hacking – directly accessing by exploiting a vulnerability.
- Malware – attacks a system by installing software on it.
- Web attack – some portion of the Web interface with the user allows for accessing the system.

Social Engineering

- manipulation of people to get them to do something that weakens the security of the network (ie. Giving up their user IDs and passwords).
- Example: a hacker calls and pretends to be from IT and needs your password to fix the system.

Direct Hacking

- a hacker works with the tools under his control to gain access to the network.
- **Brute force password cracker** – try many passwords very quickly.
- Hackers look for vulnerabilities – ie. Leveraging an unknown or unrepaired flaw.

Malware

- viruses, worms, spyware, rootkits, Trojan horses, etc.
- designed to give control of the computer on which it is installed.
- Hacker needs access:
  - General attack – focuses on obtaining access to any system.
  - Focused attack – targets a specific individual.
- Can be received by: e-mails, loading a piece of software, or through Web-based attacks.
- Once loaded on a computer, it can grant remote control to a hacker or perform whatever it is programmed to do.

Web Attacks

- can focus on clients (user workstations) or on servers.
- Dangerous because it can defeat almost every control.
- Can pick up malware by going to a compromised Web site.
- Can be loaded even if the user doesn't click on anything on the site.
- Sites obtain information on the individuals who visit the site.

Injection

- injection flaws, particularly Structured Query Language (SQL) injection are common in Web applications.
- Injection allows an attacker to execute a command directly on a database contrary to allowed access rights.
- Sends input to a server via a form field or URL and returns information it should not return.

Cross-Site Scripting (XSS)

- allows an attacker to run malicious code from a second Web site (controlled by the cybercriminal) on the browser of the person viewing the first Web site.
- Can do whatever it's programmed to, including installing a Trojan horse.

Broken Authentication and Session Management

- compromises passwords, keys, or authentication tokens to assume identity.

Insecure Direct Object References

- failure to prohibit direct access to internal "objects":
    - files, directories, programs, etc.

Cross-Site Request Forgery (CSRF)

- victim's browser is tricked into issuing a command to vulnerable Web application.
- CSRF exploits the trust that a site has in the user's browser.

Security Misconfiguration – not configured properly.

Insecure Cryptographic Storage

Failure to Restrict URL Access

- cybercriminal can type the suspected URL directly into the browser's URL bar, thereby gaining illegitimate access to the pages.

Insufficient Transport Layer Protection

- Web sites that do not protect data in transit with Secure Sockets Layer (SSL) or Transport Layer Security (TLS) are vulnerable to traffic interception and modification.

Unvalidated Redirects and Forwards

- a redirect should be validated by the server before it is executed.

Information Security Management System

- mitigate risk.
- ISMS appropriate for the size of the organization.
- Ongoing risk assessment – fluid process.
- Appropriate management responsibility for the ISMS.
- Senior management must support the process.

Security Policy

Multidisciplinary, multidepartment function.

- affects day-to-day physical security functions.
- Defines what type of devices are allowed on the network.

Organization of ISS

- ISMS policies must apply to vendors as well.
- Cloud providers must adhere to the organization's policies.
- Ensure that its ISMS is appropriate and client will be able to audit vendor.

Asset Management

- special requirements for information as it is transmitted on the network and stored on devices that reside on the network.
- Video could contain highly sensitive content.
- Access control system contains the keys to the organization.

Human Resources Management

- background checks, terms of employment screening, disciplinary process, termination practices, security awareness and training.

Physical and Environmental Security

- secure areas in which ISS assets reside.
- Collaboration between physical and logical security.

Communications and Operations Management

Computer System Turn-On, Shutdown, and Emergency Shutdown Procedure

- generator to charge batteries on **uninterruptible power supply (UPS)**.

Change Management

- physical security units cannot upgrade access control without having a conversation with IT. A change can effect the entire network.

Segregation of Duties

Third-Party Service Delivery

- all service level agreements (SLA) in place for internal providers should also be in place for third parties.

Capacity Management

- in an emergency, significant numbers of people may need to see the video.
- Necessary bandwidth.

System Management

- physical security practitioner must decide if, and when, a camera can be down.

System Acceptance

- process of making sure systems are up to specification.

Malicious Code Protection

- Viruses, Trojan horses, etc. can bring down an entire network.

System Backup

- if not backed up, it could be lost

Network Security Controls

- security systems need to comply with particular types of technologies and controls.

Media Handling

- Data can exist on various media, such as hard drives, USB sticks, or tape backups.
- Protect it from being lost or being compromised.

Security of System Documentation

Exchange of Information

- people who are given access must be trained in security policies.

Jonathan Taormina, CPP, CFE, PCI

On-Line Transactions

- appropriate industry standards.
- Relevant laws and regulations.

Monitoring – various aspects of the network and their systems.

Clock Synchronization

- **Network Time Protocol (NTP)** – all systems should have same time.

Access Control

- Security systems require logical access control.
- User name/password may not be sufficient.
- Identity verification is vital
- **Second-factor authentication** – uses one-time passwords, fingerprint scanners, etc.

Information Systems Acquisition, Development, and Maintenance

- actions should not expose the organization to undue risk.
- Encrypt the video stream.

Business Continuity Management

- In the event that power is not available, it is important that network-based systems, such as access control, maintain functionality.
- Off-site venue may be needed for BC plan.

Compliance

- Security may be nonnegotiable from a legal perspective.

Conclusion

- Convergence of security systems into the network infrastucture.
- Need for a protected data stream, whether the stream is a point-to-point cable or goes across the network.
- Convergence of the physical security paradigm and the logical security paradigm.