INFO 6027: F2022

Week 11

Physical Security, Human Resources and SETA

FANSHAWE

Housekeeping

- Test #2 is marked. What did you think of the test?
- Assignment 3. **Any questions?**

In the News…

- **Palo Alto Networks error exposed customer support cases, attachments - https://www.bleepingcomputer.com/news/security/palo-alto-networks-error-exposed-customer-support-cases-attachments/?&web_view=true**

- **Phishing uses Azure Static Web Pages to impersonate Microsoft https://www.bleepingcomputer.com/news/microsoft/phishing-uses-azure-static-web-pages-to-impersonate-microsoft/?&web_view=true**

- **What the Newly Signed US Cyber-Incident Law Means for Security**
- https://www.darkreading.com/attacks-breaches/new-cyber-incident-law-not-a-national-breach-law-but-a-major-first-step?&web_view=true

- Why more employees need data literacy skills - Data literacy is the ability to read, write and communicate data in context. This includes an understanding of data sources and constructs, analytical methods and techniques applied, and the ability to describe the use case, the application and the resulting value

  - https://haveibeenpwned.com/

Our Agenda for This week…

- Describe the components of a security education, training, and awareness (SETA) program
  - Explain how organizations create and manage SETA programs

- Describe the employment practices in information security.
  - Hiring, firing, etc.

Security Education, Training, and Awareness (SETA)

FANSHAWE

Let’s Discuss

- **What are the Security Awareness Training Topics?**

Social Engineering

Phishing

OS Hardening

Let’s Discuss

- **12 Essential Security Awareness Training Topics for 2022 as per usecure:**

1. **Phishing attacks**
2. **Removable media**
3. **Passwords and Authentication**
4. **Physical security**
5. **Mobile Device Security**
6. **Working Remotely**
7. **Public Wi-Fi**
8. **Cloud Security**
9. **Social Media Use**
10. **Internet and Email Use**
11. **Social Engineering**
12. **Security at Home**

Security Awareness, Training, and Education (SETA)

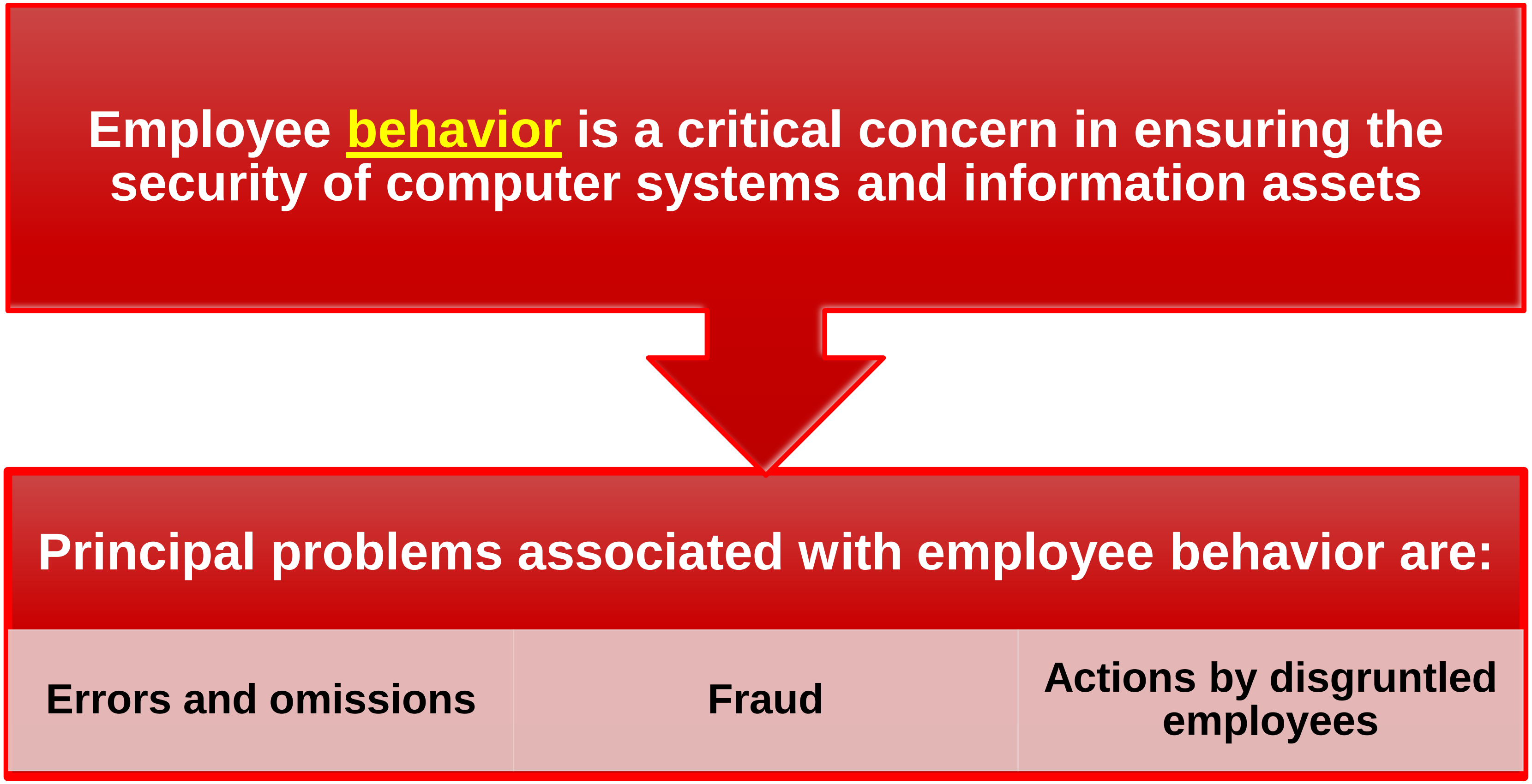
- **SETA is mentioned prominently in multiple standards**
  - **ISO 27002 (***Code of Practice for Information Security Management***)**
  - **NIST Special Publication 800-100 (***Information Security Handbook: A Guide for Managers***).**

SETA – Benefits to Organizations

SETA programs provide four major benefits to organizations:

1. Improving employee **behavior**
2. Increasing employee **accountability**
3. **Mitigating liability** for employee behavior
4. **Complying** with regulations and contractual obligations (reporting violations)

Human Factors



Employee behavior is a critical concern in ensuring the security of computer systems and information assets

Principal problems associated with employee behavior are:

Errors and omissions

Fraud

Actions by disgruntled employees

SETA programs can
reduce the problem of __________ and __________.

How SETA helps

- SETA programs serve as a **deterrent to fraud** and actions by disgruntled employees

- Ongoing SETA programs are also important in **limiting** an organization’s **liability**
  - Show that **Due care** has been taken

- Finally, SETA programs may be needed to comply with regulations and contractual obligations .
  - Ex. OHSA

NIST SP 800-16 (*Information Technology Security Training Requirements: A Role- and Performance-Based Model*) *summarizes the four layers as follows:*

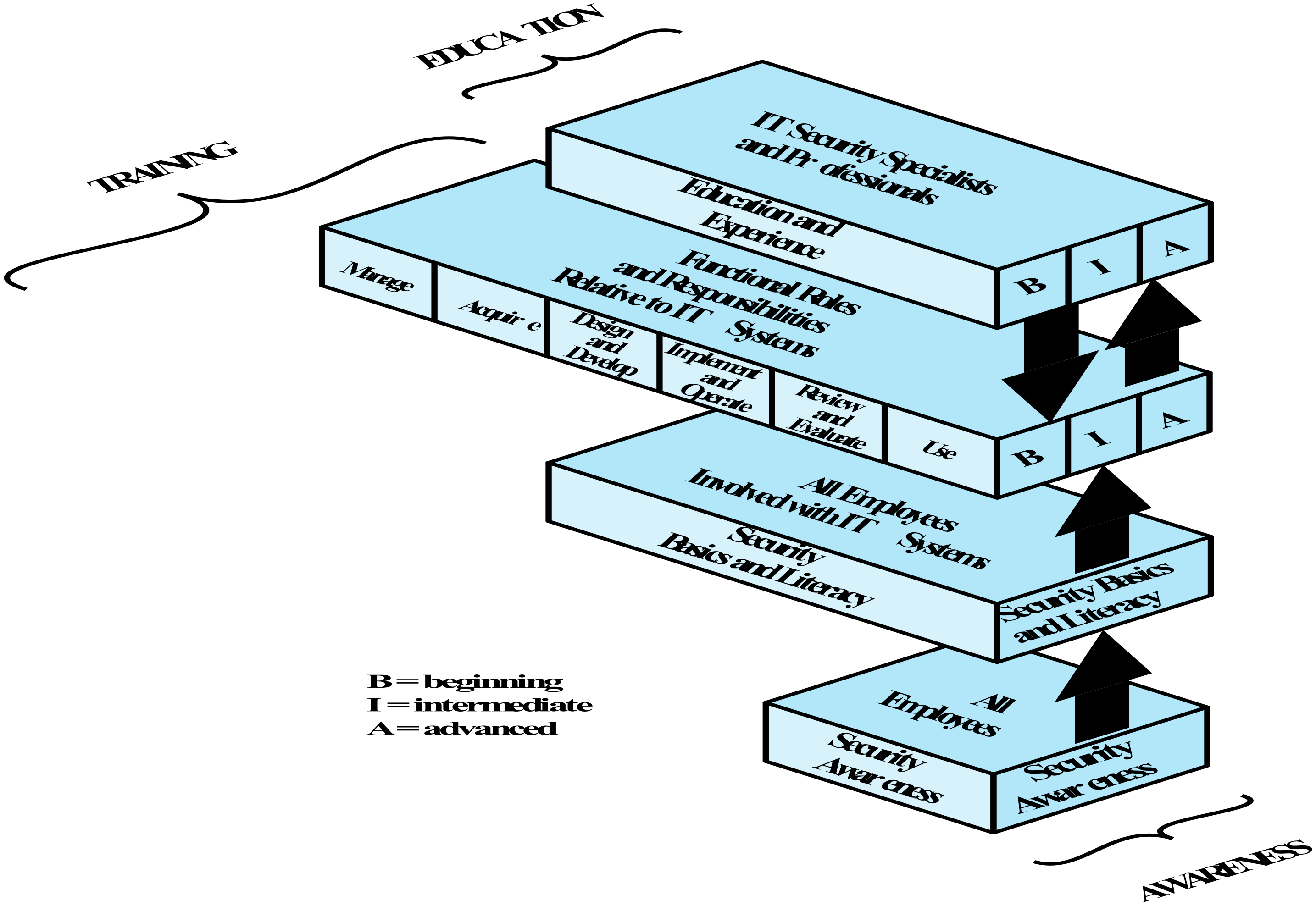


Figure 17.1 Information Technology (IT) Learning Continuum

Table 17.1 Comparative Framework

	Awareness	**Training**	**Education**
Attribute	"What"	"How"	"Why"
Level	Information	Knowledge	Insight
Objective	Recognition	Skill	Understanding
Teaching method	**Media** —Videos —Newsletters —Posters, etc.	**Practical instruction** —Lecture —Case study workshop —Hands-on practice	**Theoretical instruction** —Discussion seminar —Background reading
Test measure	True/false Multiple choice (identify learning)	Problem solving (apply learning)	Essay (interpret learning)
Impact timeframe	Short term	Intermediate	Long term

Implementing SETA Programs

- SETA program
  - –Designed to reduce accidental security breaches
  - –Consists of three elements: security **education**, security **training**, and security **awareness**

Awareness, training, and education programs offer **two major benefits**:

1. Improving employee **behavior**
2. Enabling the organization to hold employees **accountable** for their actions. (now they can’t say they didn’t know)

Implementing SETA Programs

- Purpose of SETA is to **enhance security**:
  - By building in-depth knowledge, to design, implement, or operate security programs for organizations and systems
  - By developing skills and knowledge so that computer users can perform their jobs while using IT systems more securely
  - By improving awareness of the need to protect system resources
    - Increased awareness can lead to reporting
    - Increased awareness may lead to recognition of attempts, and through that recognition, a prevention of an attack

Awareness

NIST SP 800-100 (*Information Security Handbook: A Guide for Managers*) describes the content of awareness programs, in general terms, as follows:

"Awareness tools are used to promote information security and inform users of threats and vulnerabilities that impact their division or department and personal work environment by explaining the what but not the how of security, and communicating what is and what is not allowed.

Awareness not only communicates information security policies and procedures that need to be followed, but also provides the foundation for any sanctions and disciplinary actions imposed for noncompliance. Awareness is used to explain the rules of behavior for using an agency's information systems and information and establishes a level of expectation on the acceptable use of the information and information systems."

List of goals for a security awareness program

1. Raise staff awareness of information technology security issues in general.
2. Ensure that staff are aware of local, state, and federal laws and regulations governing confidentiality and security.
3. Explain organizational security policies and procedures.
4. Ensure that staff understand that security is a team effort and that each person has an important role to play in meeting security goals and objectives.
5. Train staff to meet the specific security responsibilities of their positions.
6. Inform staff that security activities will be monitored.
7. Remind staff that breaches in security carry consequences.
8. Assure staff that reporting of potential and realized security breakdowns and vulnerabilities is responsible and necessary behavior (and not trouble-making behavior).
9. Communicate to staff that the goal of creating a trusted system is achievable.

Implementing Security Awareness

- Seeks to inform and focus an employee's attention on security issues within the organization
  - Aware of their responsibilities for maintaining security and the restrictions on their actions
  - Users understand the importance of security for the well-being of the organization
  - Promote enthusiasm and management buy-in
- Program must be tailored to the needs of the organization and target audience
- Must continually promote the security message to employees in a variety of ways
- Should provide a security awareness policy document to all employees

Implementing Security Awareness

- One of the least frequently implemented, but most effective security methods is the security awareness program
- Security awareness programs:
  - Set the stage for training by changing organizational attitudes to realize the importance of security and the adverse consequences of its failure
  - Remind users of the procedures to be followed

Security Awareness Programs

- Awareness can take on different forms for particular audiences
- A security awareness program can use many methods to deliver its message
- Recognize that people tend to practice a tuning out process (acclimation)
  - Awareness techniques should be **creative** and **frequently** changed

Promoting Security Awareness

- Many security awareness components are available at little or no cost
  - –Others can be very expensive
- Examples of security awareness components
  - –Videos
  - –Posters and banners
  - –Lectures and conferences
  - –Computer-based training
  - –Newsletters
  - –Brochures and flyers
  - –Trinkets (coffee cups, pens, pencils, T-shirts)
  - –Bulletin boards

Basically anything small, simple (and sometime subtle) that reminds people to thing about information security

Promoting Security Awareness

Security newsletter

–A cost-effective way to disseminate security information

–Newsletters can be in the form of hard copy, e-mail, or intranet

–Topics can include threats to the organization’s information assets, schedules for upcoming security classes, and the addition of new security personnel

***The goal is to keep the idea of information security uppermost in users’ minds and to stimulate them to care about security*

Newsletters might include:

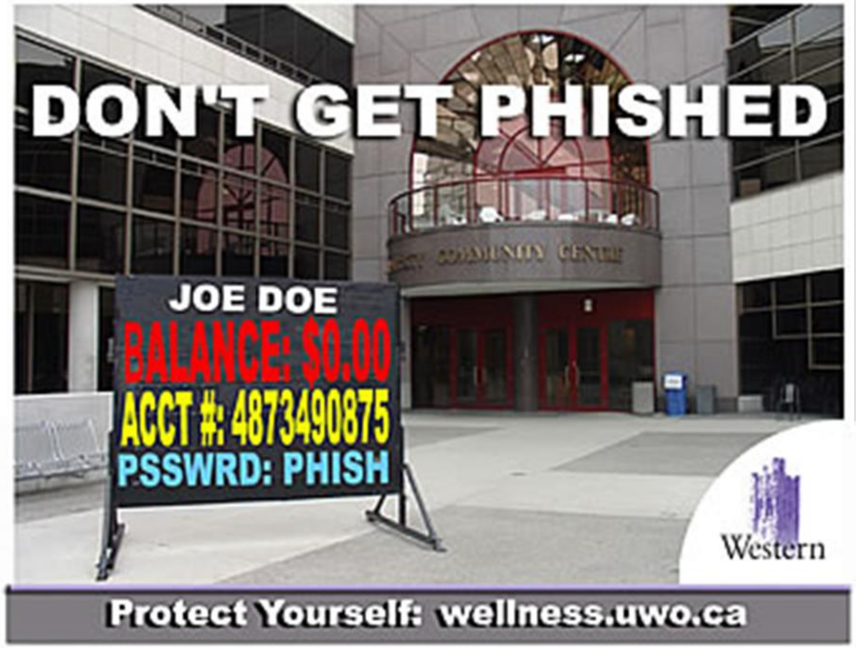
- Summaries of key policies and key news articles
- A calendar of security events, including training sessions, presentations, and other activities
- Announcements relevant to information security
- How-to’s

Promoting Security Awareness

- Security poster series
  - –A simple and inexpensive way to keep security on people's minds
  - –Professional posters can be quite expensive, so in-house development may be the best solution
  - –Keys to a good poster series:
    - Varying the content and keeping posters updated
    - Keeping them simple, but visually interesting
    - Making the message clear
    - Providing information on reporting violations

Security Awareness Posters: Western University

Passwords are like...
Underwear
The Longer, The Better!
Be Smart: wellness.uwo.ca
Western



Passwords are like...
Underwear
Don't Share Them.
Be Smart: wellness.uwo.ca
Western

Promoting Security Awareness

- Organizations can establish Web pages or sites dedicated to promoting information security awareness
  - The challenge lies in updating the messages frequently enough to keep them fresh
- Tips on creating and maintaining an educational Web site
  - See what's already out there
  - Plan ahead
  - Keep page loading time to a minimum
  - Seek feedback
  - Assume nothing and check everything
  - Spend time promoting your site

SETA - Security Awareness

- Security awareness conference
  - Have a guest speaker or even a mini-conference dedicated to the topic
    - Perhaps in association with the semi-annual National Computer Security Days: October 31 and April 4

TRAINING IN
PROGRESS

Security Training Program – “HOW”

Designed to teach people the skills to perform their IS-related tasks more securely	• *What* people should do and *how* they should do it
General users	• Focus is on good computer security practices (phys env’t, pw, reporting)
Programmers, developers, system maintainers	• Develop a security mindset in the developer, build IS into lifecycle, resist attacks,
Managers	• How to make tradeoffs involving security risks, costs, benefits
Executives	• Swsec and Netsec, Risk management goals, measurement, **leadership by example**

Implementing Security Training

- Involves providing detailed information and hands-on instruction
  - To develop user skills to perform their duties securely
- Management can either develop customized training or outsource
- Customizing training for users
  - By functional background
    - General user
    - Managerial user
    - Technical user
  - By skill level
    - Novice
    - Intermediate
    - Advanced

Training Techniques

- Using the wrong method
  - Can hinder the transfer of knowledge
    - Leading to unnecessary expense and frustrated, poorly trained employees
- Good training programs take advantage of the latest learning technologies and best practices
- Recent developments
  - Less use of centralized public courses and more on-site training
- Training is often for **one or a few individuals**
- Other best practices – training moving to **modular** method
  - Increased use of short, task-oriented modules
    - Available during the normal work week

Training Techniques (cont’d)

- Selection of the training delivery method
  - Not always based on the best outcome for the trainee
- Types of delivery methods
  - One-on-one
  - Formal class
  - Computer-based training (CBT)
  - Distance learning/web seminars
  - User support group
  - On-the-job training
  - Self-study (non-computerized)

Training Techniques (cont’d)

- Training delivery methods
  - –Use a local training program
  - –Use a continuing education department
  - –Use another external training agency
  - –Hire a professional trainer, a consultant, or someone from an accredited institution to conduct on-site training
  - –Organize and conduct training in-house using organization’s own employees

Implementing Training

- Seven-step methodology to implementing a training program:
  - –Step 1: Identify program scope, goals, and objectives
  - –Step 2: Identify training staff
  - –Step 3: Identify target audiences
  - –Step 4: Motivate management and employees
  - –Step 5: Administer the program
  - –Step 6: Maintain the program
  - –Step 7: Evaluate the program

Education

Security Education

- Education is the most “in depth” program
- Targeted at security professionals and those whose jobs require **expertise** in security
- Fits into “employee career development programs” category
- Often provided by outside sources
  - Ex. University/College courses
  - Specialized short-term training programs from knowledge providers like Boot camps and Online seminars/webinars

Implementing Security Education

- Employees within information security may be encouraged to seek a **formal education**
  - –If not prepared by their background or experience
  - –A number of institutions of higher learning, including colleges and universities, provide formal coursework in information security
  - –**Certifications** are also available – need to consider industry value
  - –**Is *informal* training sufficient? Why do some employers demand formal education?**

Implementing Security Education

- A knowledge map
  - –Can help potential students assess information security programs
  - –Identifies the **skills and knowledge** obtained by the program’s graduates
    - –Links courses with outcomes
  - –Creating the map can be difficult because many academics are unaware of the numerous sub-disciplines within the field of information security
    - Each of which may have different knowledge requirements
    - Ex. A student on a path to become a manager vs one to become a technician…

Implementing Security Education

- Depth of knowledge
  - Indicated by a level of mastery using an established **taxonomy** of learning objectives or a simple scale such as: “understanding → accomplishment → proficiency → mastery.”
- Because many institutions have no frame of reference for which skills and knowledge are required for a particular job area
  - They may refer to the **certifications offered in that field**

Implementing Security Education

- Once the knowledge areas are identified, common knowledge areas are aggregated into **teaching domains**
  - From which **individual courses can be created**
- Course design
  - Should enable a student to obtain the required knowledge and skills upon completion of the program
  - Identify the prerequisite knowledge for each class

Bringing it all together..

Implementing SETA programs

SETA Best practices

- –Focus on people
- –Refrain from using technical jargon
- –Use every available venue
- –Define learning objectives, state them clearly, and provide sufficient detail and coverage
- –Keep things light
- –Don’t overload the users
- –Help users understand their roles in InfoSec
- –Take advantage of in-house communications media
- –Make the awareness program formal
  - Plan and document all actions
- –Provide good information early, rather than perfect information late

10 mandates of infoSETA

1. Information security is a people, rather than a technical, issue
2. If you want them to understand, speak their language
3. If they cannot see it, they will not learn it
4. Make your point so that you can identify it and so can they.
5. Never lose your sense of humor
6. Make your point, support it, and conclude it
7. Always let the recipients know how the behavior that you request will affect them
8. Ride the tame horses (avoid political or controversial subjects)
9. Formalize your training methodology
10. Always be timely, even if it means slipping schedules to include urgent information

Security Awareness/Training

- Security **awareness and security training** are **designed to modify** any employee **behavior** that endangers the security of the organization’s information
- Make employees **accountable** for their actions
- Helps with **dissemination** and **enforcement** of policy
- Demonstrating **due care** and **due diligence** can help **indemnify** the institution against lawsuits

HR Security

HR Security

- **“Experts Say Employee Error Accounts for Most Security Breaches”** (link)
- “*human error actually accounted for nearly two-thirds of security compromises, far exceeding causes like insecure websites and hacking.”*
- 789% increase in e-mail phishing attacks containing malicious code, including ransomware (2016)
- “**security awareness and training** is the key to improved security. Yet, it is **one of the most neglected areas in many businesses' information security programs.”**

Employment Practices and Policies

- **Personnel security**: hiring, training, monitoring behavior, and handling departure.
- a large majority of perpetrators of significant computer crime are individuals who **have legitimate access now**, or who have recently had access.
- Managing personnel with **potential access** is an essential part of information security

Employee Involvement in Security Breaches

Is Either Intentional or Accidental

- *Accidental*
  - Unwittingly aid in the commission of a violation by failing to follow proper procedures
  - Forgetting security considerations
  - Not realizing that they are creating a vulnerability
- *Intentional*
  - Knowingly violate controls, ignore procedures, or intentionally circumvent security measures put in place.

Threats from Internal Users

Threats from internal users include the following:

- Unauthorized access (self or others)
- Altering data
- Deleting production and backup data
- Crashing systems
- Destroying systems
- Misusing systems for personal gain
- Holding data
- Stealing data

Security in the Hiring Process

What is the objective of the hiring process: (ISO 27002)

- “To ensure that employees, contractors and third-party users understand their responsibilities”
- Implying that employees are not the only threat who need to be educated. ☺

An Employment Agreement

- To be signed prior to the job offer which includes confidentiality and non-disclosure agreement.
- Employee and organizational responsibility for information security.
- Reference to organizations Security Policy.
- Acknowledgement that the employee has reviewed and agrees to abide by the policy.

Background Checks

- Need appropriate background checks and screening
  - Investigate accuracy of resume
  - An employer may be held liable for negligent hiring
  - Former employers aren’t honest in their references

General guidelines for checking applicants include the following:

- Ask for as much detail as possible
- Investigate the accuracy of the details
- Arrange for experienced staff members to interview candidates and discuss discrepancies.

For highly sensitive positions

- Have an investigation agency do a background check
- Criminal record and credit check
- Check the applicant’s credit record for evidence of large personal debt and the inability to pay it. Discuss problems, with the applicant.
- Consider conducting a polygraph examination of the applicant (if legal). Although polygraph exams are not always accurate, they can be helpful if you have a particularly sensitive position to fill.
- Ask the applicant to obtain bonding for his or her position.

During Employment – ISO 27002

Objectives with respect to current employees:

- Ensure that employees, contractors, and third-party users are aware of information security threats and concerns and their responsibilities and liabilities with regard to information security
- Are equipped to support the organizational security policy in their work
- Reduce the risk of human error

Two essential elements of personnel security during employment are:

- A comprehensive security policy document
- An ongoing awareness and training program for all employees

Security principles:

- Least privilege – both logical and physical (this is a risk reduction strategy)
- Separation of duties
- Limited reliance on key employees – unexpected illness/departure. Avoid "unique knowledge and skills"

Termination of Employment – ISO 27002

- Termination security objectives:
  - Ensure employees, contractors, and third party users exit organization or change employment in an orderly manner
  - The return of all equipment and the removal of all access rights are completed

Critical actions:

- Remove name from all authorized access lists
- Inform guards that ex-employee general access is not allowed
- Remove personal access codes, change physical locks and lock combinations, reprogram access card systems
- Recover all assets, including employee ID, documents, data storage devices
- Notify by memo or email appropriate departments

Email and Internet Use Policies

- **Why do Many orgs give their employees an email account**
  - Facilitates inter-office communication
- Organizations are incorporating specific e-mail and Internet use policies into their security policy document
- Concerns for employers:
  - Work time consumed in non-work-related activities
  - Computer and communications resources may be consumed, compromising the mission that the IS resources are designed to support
  - **Risk of importing malware**
  - Possibility of harm, harassment, inappropriate online conduct (could also damage reputation of org, liability situation,

Suggested Policies Relating to Email and Internet

- Business use only
- Policy scope
- Content ownership
- Privacy
- Standard of conduct
- Reasonable personal use
- Unlawful activity prohibited
- Security policy
- Company policy
- Company rights
- Disciplinary action

Summary

- Security awareness, training, and education
  - Implementing security education, training, and awareness programs
    - Motivation
    - A learning continuum
    - Awareness
    - Training
    - Education

- **Employment practices and policies**
  - Security in the hiring process
  - During employment
  - Termination of employment

FANSHAWE

References and Reminders

References

- Computer Security – Principles & Practices
  - By: William Stallings, Pearson - Prentice Hall
- Management of Information Security – M Whitman
- ISO27000 series of Standards.

Reminders:

- Three weeks to go. You should be thinking about how you will prepare for the final exam **(worth 40%)**
- Assignment 3 has been posted – don't procrastinate!
- **Next week we will discuss InfoSec Physical Security, Laws and Ethics**
  - So please read the chapter prior to watching/listening to the lesson