SECURITY AND PERSONNEL

HUMAN FACTORS

- **Employee behavior** is a critical concern in ensuring the security of computer systems and information assets.
- Research show that employee actions, both malicious and unintentional, cause considerable computer-related loss and security compromises.
- The principal problems associated with employee behavior are errors and omissions, fraud, and actions by disgruntled employees.

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**

HUMAN FACTORS

- Security awareness, training, and education programs can assist in reducing incidences of these problems.
- Such programs can serve as a deterrent to fraud and actions by disgruntled employees by increasing employees' knowledge of their **accountability** and of potential penalties.
- Employees cannot be expected to follow policies and procedures of which they are unaware.
- Further, enforcement is more difficult if employees can claim ignorance when caught in a violation.
- Ongoing security awareness, training, and education programs are also important in limiting an organization's **liability**.
- Such programs can bolster an organization's claim that a standard due care has been taken in protecting information.
- Finally, security awareness, training, and education programs may be needed to comply with **regulations and contractual obligations**.

AWARENESS

- Benefits from security awareness include the following:
  1. Employees are aware of their responsibilities for maintaining security and the restrictions on their actions in the interests of security and are motivated to act accordingly.
  2. Users understand the importance of security for the well-being of the organization.
- To emphasize the importance of security awareness, an organization should have a security awareness policy document that is provided to all employees. The policy should establish three things:
  1. Participation in an awareness program is required for every employee. This will include an orientation program for new employees as well as periodic awareness activities.
  2. Everyone will be given sufficient time to participate in awareness activities.
  3. Responsibility for managing and conducting awareness activities is clearly spelled out.

TRAINING

- A security training program is designed to teach people the skills to perform their IT-related tasks more securely. Training teaches what people should do and how they should do it. Depending on the role of the user, training encompasses a spectrum ranging from basic computer skills to more advanced specialized skills.

Designed to teach people the skills to perform **their IT-related tasks more securely**	• What people should do and how they should do it
General users	• Focus is on good computer security practices
Programmers, developers, system maintainers	• Develop a security mindset in the developer
Management-level	• How to make tradeoffs involving security risks, costs, benefits
Executive-level	• Risk management goals, measurement, leadership

EDUCATION

- The most in-depth program is security education.
- This is targeted at security professionals and those whose jobs require expertise in security.
- Security education is normally outside the scope of most organization's awareness and training programs.
- It more properly fits into the category of employee career development programs.
- Often, this type of education is provided by outside sources such as:
  - College courses
  - Specialized training programs
  - Inhouse/Industry practical training

EMPLOYMENT PRACTICES AND POLICIES

- This deals with personnel security: hiring, training, monitoring behavior, and handling departure.
- Research shows that majority of perpetrators of significant computer crime are individuals who have legitimate access now, or who have recently had access.
- Thus, managing personnel with potential access is an essential part of cyber security.
- Employees can be involved in security violations in one of two ways.

1. Some employees unwittingly aid in the commission of a security violation by failing to follow proper procedures
   - Unwittingly aid in the commission of a violation by failing to follow proper procedures by:
     - Forgetting security considerations
     - Not realizing that they are creating a vulnerability
2. Other employees knowingly violate controls or procedures to cause or aid a security violation.

EMPLOYMENT PRACTICES AND POLICIES

- Threats from internal users include the following:
  - Gaining unauthorized access or enabling others to gain unauthorized access
  - Altering data
  - Deleting production and backup data
  - Crashing systems
  - Destroying systems
  - Misusing systems for personal gain or to damage the organization
  - Holding data hostage
  - Stealing strategic or customer data for corporate espionage or fraud schemes

SECURITY IN THE HIRING PROCESS

- **Objective:**
  - To ensure that employees, contractors and third-party users:
    - Understand their responsibilities
    - Are suitable for the roles they are considered for
    - To reduce the risk of theft, fraud or misuse of facilities
- Need appropriate background checks and screening
  - Ask for as much detail as possible about employment and educational history
  - Investigate accuracy of details
  - Arrange for experienced staff members to interview candidates
- For highly sensitive positions
  - More intensive investigation is warranted
  - Have an investigation agency to do: background, Criminal record and credit check

EMPLOYMENT AGREEMENTS

Employees should agree to and sign the terms and conditions of their employment contract, which should include:

I. Employee and organizational responsibilities for cyber security

II. A confidentiality and non-disclosure agreement

III. Reference to the organization's security policy

IV. Acknowledgement that the employee has reviewed and agrees to abide by the policy

DURING EMPLOYMENT

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

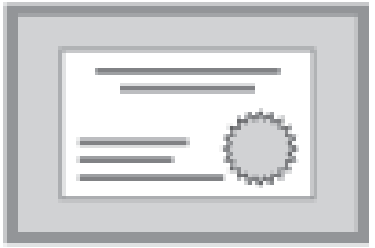
Two essential elements of personnel security during employment are:

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

Security principles:

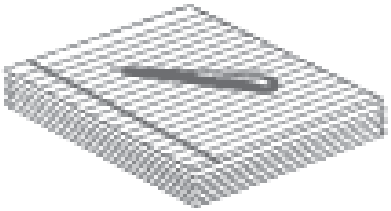
- Least privilege
- Separation of duties
- Limited reliance on key employees

Background checks



Certifications

Policies



Covenants and agreements

Contracts

POSITIONING AND STAFFING THE SECURITY FUNCTION

- The security function can be placed within:
  - IT function
  - Physical security function
  - Administrative services function
  - Insurance and risk management function
  - Legal department
- Organizations balance needs of enforcement with needs for education, training, awareness, and customer service
- Selecting personnel is based on many criteria, including supply and demand
- At present, cyber security industry is in a period of high demand

QUALIFICATIONS AND REQUIREMENTS

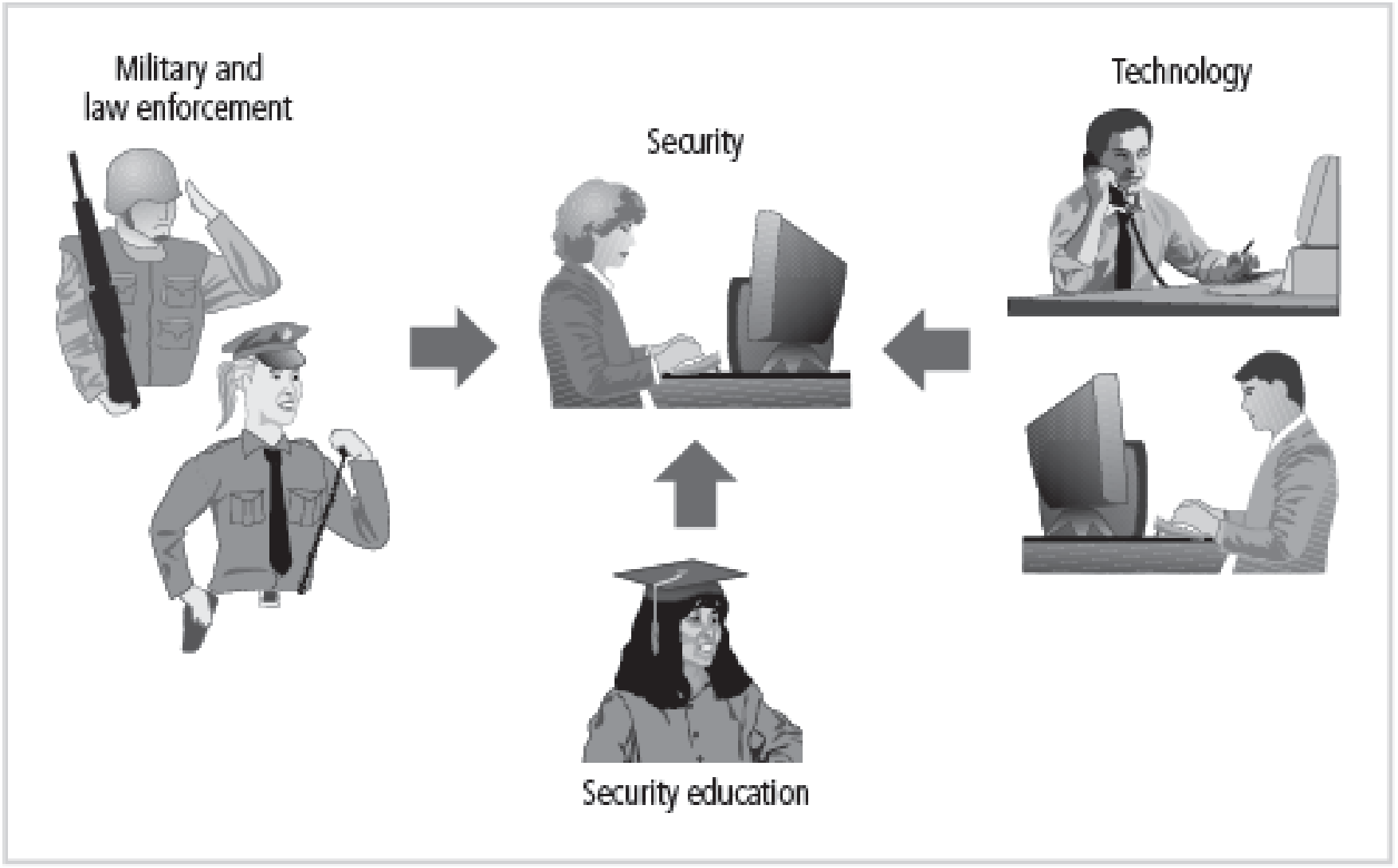
- The following factors must be addressed:
  - General management should learn more about skills and qualifications for positions
  - Upper management should learn about budgetary needs of information security function
  - IT and general management must learn more about level of influence and prestige the information security function should be given to be effective
  - Organizations typically look for technically qualified information security generalist
  - Organizations look for information security professionals who understand:
    - How an organization operates at all levels
    - Information security is usually a management problem, not a technical problem
    - Strong communications and writing skills
    - The role of policy in guiding security efforts

QUALIFICATIONS AND REQUIREMENTS

- Most mainstream IT technologies
- The terminology of IT and information security
- Threats facing an organization and how they can become attacks
- How to protect organization's assets from information security attacks
- How business solutions can be applied to solve specific information security problems

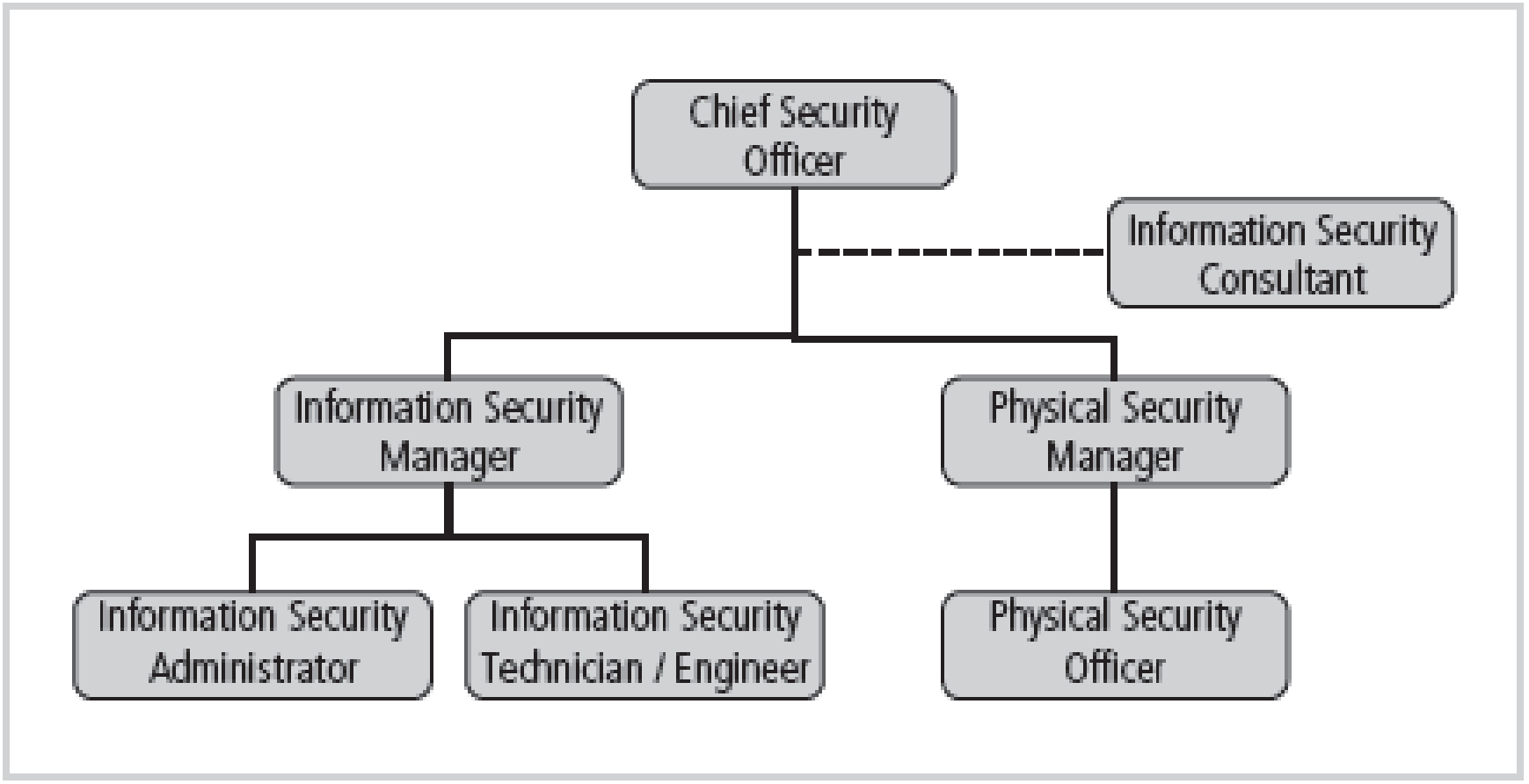
- **Entry into the information security profession**
- Many information security professionals enter the field through one of two career paths:
  1. Law enforcement and military
  2. Technical, working on security applications and processes
- Today, students select and tailor degree programs to prepare for work in information security
- Organizations can foster greater professionalism by matching candidates to clearly defined expectations and position descriptions

CAREER PATHS TO INFORMATION SECURITY POSITIONS



POSITIONS IN INFORMATION SECURITY

Use of standard job descriptions can increase degree of professionalism and improve the consistency of roles and responsibilities between organizations



CHIEF INFORMATION SECURITY OFFICER (CISO OR CSO)

- This position is typically considered the top information security officer in the organization.
- The CISO is usually not an executive-level position and frequently reports to the Chief Information Officer
- Manages the overall information security program
- Drafts or approves information security policies
- Works with the CIO on strategic plans
- Develops information security budgets
- Sets priorities for information security projects and technology
- Makes recruiting, hiring, and firing decisions or recommendations
- Acts as spokesperson for information security team
- Typical qualifications: A graduate degree in one of the following areas is also probably required: criminal justice, business, technology, or other related fields

POSITIONS IN INFORMATION SECURITY

- **Chief Security Officer (CSO)**
  - CISO's position may be combined with physical security responsibilities
  - Knowledgeable in both IS requirements and "guards, gates, and guns" approach to security
- **Security Manager**
  - Security managers are accountable for the day-to-day operation of the information security program.
  - They accomplish objectives as identified by the CISO and resolve issues identified by technicians
  - Typical qualifications: Not uncommon to have accreditation; ability to draft middle- and lower-level policies; standards and guidelines; budgeting, project management, and hiring and firing.
  - They must also be able to manage technicians, both in the assignment of tasks and the monitoring of activities.

POSITIONS IN INFORMATION SECURITY

- **Security Technician**
  - Technically qualified individuals tasked to configure security hardware and software
  - Tend to be specialized
  - Typical qualifications
    - Varied; organizations prefer expert, certified, proficient technician
    - Some experience with a particular hardware and software package
    - Actual experience in using a technology usually required
- **Advice for Information Security Professionals**
- As an information security professional:
  - Always remember: business before technology
  - Technology provides elegant solutions for some problems, but adds to difficulties for others
  - Never lose sight of goal: protection
  - Your education is never complete

EMPLOYMENT POLICIES AND PRACTICES

- Management should integrate solid information security concepts into organization's employment policies and practices
- Organization should make information security a documented part of every employee's job description
- From information security perspective, hiring of employees is a responsibility loaded with potential security pitfalls
- CISO and information security manager should provide human resources with information security input to personnel hiring guidelines
- **Job Descriptions**
  - Integrating information security perspectives into hiring process begins with reviewing and updating all job descriptions
  - Organization should avoid revealing access privileges to prospective employees when advertising open positions

EMPLOYMENT POLICIES AND PRACTICES

- **Interviews**
  - An opening within the information security department creates a unique opportunity for the security manager to educate HR on certifications, experience, and qualifications of a good candidate
  - Information security should advise HR to limit information provided to the candidate on the responsibilities and access rights the new hire would have
  - For organizations that include on-site visits as part of interviews, it's important to use caution when showing candidate around facility
- **Background Checks**
  - Investigation into a candidate's past
  - Should be conducted before organization extends offer to candidate
  - Background checks differ in level of detail and depth with which candidate is examined
  - May include identity check, education and credential check, previous employment verification, references check, worker's compensation history, motor vehicle records, drug history, credit history, and more

EMPLOYMENT POLICIES AND PRACTICES

- **Types of Background Checks**
  - **Identity checks**: Validation of identity and Social Security/NRIC number
  - **Education and credential checks**: Validation of institutions attended, degrees and certifications earned, and certification status
  - **Previous employment verification**: Validation of where candidates worked, why they left, what they did, and for how long
  - **Reference checks**: Validation of references and integrity of reference sources
  - **Worker's compensation history**: Investigation of claims from worker's compensation
  - **Motor vehicle records:** Investigation of driving records, suspensions, and DUIs (driving under the influence)
  - **Drug history:** Screening for drugs and drug usage, past and present
  - **Credit history**: Investigation of credit problems, financial problems, and bankruptcy

EMPLOYMENT POLICIES AND PRACTICES

- **Civil court history**: Investigation of involvement as the plaintiff or defendant in civil suits
- Criminal court history: Investigation of criminal background, arrests, convictions, and time served

- **Employment Contracts**
  - Once a candidate has accepted the job offer, employment contract becomes important security instrument
  - Many security policies require an employee to agree in writing
  - New employees should not be offered the position unless binding organizational policies are agreed to

- **New Hire Orientation**
  - New employees should receive extensive information security briefing on policies, procedures, levels of authorized access, training etc.
  - By the time employees start, they should be thoroughly briefed and ready to perform duties securely

EMPLOYMENT POLICIES AND PRACTICES

- **On-the-Job Security Training**
  - Organization should conduct periodic security awareness training
  - Security awareness training can minimize employee mistakes and is an important part of information security awareness mission
  - External and internal seminars also increase level of security awareness for all employees, particularly security employees
- **Evaluating Performance**
  - Organizations should incorporate information security components into employee performance evaluations
  - Employees pay close attention to job performance evaluations
  - If evaluations include information security tasks, employees are more motivated to perform these tasks at a satisfactory level
- **Termination**
  - When employee leaves organization, there are a number of security-related issues

EMPLOYMENT POLICIES AND PRACTICES

- Key is protection of all information to which employee had access
- Once cleared, the former employee should be escorted from premises
- Hostile departures include termination for cause, permanent downsizing, temporary lay-off, or some instances of quitting
  - Before employee is aware, all logical and keycard access is terminated
  - Employee collects all belongings and surrenders all keys, keycards, and other company property
  - Employee is then escorted out of the building
- Friendly departures include resignation, retirement, promotion, or relocation
  - Employee may be notified well in advance of departure date
  - More difficult for security to maintain positive control over employee's access and information usage
  - Employee access usually continues with new expiration date
  - Employees come and go at will, collect their own belongings, and leave on their own

EMPLOYMENT POLICIES AND PRACTICES

- Offices and information used by the employee must be inventoried; files stored or destroyed; and property returned to organizational stores
- Possible that employees foresee departure well in advance and begin collecting organizational information for their future employment
- Only by scrutinizing systems logs after employee has departed can organization determine if there has been a breach of policy or a loss of information
- If information has been copied or stolen, report an incident and follow the appropriate policy
- **Temporary Employees**
  - Hired by organization to serve in temporary position or to supplement existing workforce
  - Often not subject to contractual obligations or general policies; if temporary employees breach a policy or cause a problem, possible actions are limited
  - Access to information for temporary employees should be limited to that necessary to perform duties

Information disclosure agreements

Audit system use and storage

Changing of system access

Equipment inventory

Exit interview

Changing of locks

Termination activities

Source: © Tatiana Popova/www.Shutterstock.com, © wavebreakmedia/www.Shutterstock.com.

EMPLOYMENT POLICIES AND PRACTICES

- **Contract Employees**
  - Typically hired to perform specific services for organization
  - Host company often makes contract with parent organization rather than with individual for a particular task
  - In secure facility, all contract employees should be escorted from room to room, as well as into and out of facility
  - The need for restrictions or requirements to be negotiated into contract agreements when they are activated
- **Consultants**
  - Should be handled like contract employees, with special requirements for information or facility access integrated into contract
  - Security and technology consultants must be prescreened, escorted, and subjected to nondisclosure agreements to protect organization
  - Just because security consultant is paid, it doesn't make the protection of organization's information the consultant's number one priority

EMPLOYMENT POLICIES AND PRACTICES

- **Business Partners**
  - Businesses find themselves in strategic alliances with other organizations, desiring to exchange information or integrate systems
  - There must be meticulous, deliberate process of determining what information is to be exchanged, in what format, and to whom
  - Nondisclosure agreements and the level of security of both systems must be examined before any physical integration takes place
- **Privacy and the Security of Personnel Data**
  - Organizations required by law to protect sensitive or personal employee information
  - Includes employee addresses, phone numbers, Social Security/NRIC numbers, medical conditions, and family names and addresses
  - This responsibility also extends to customers, patients, and business relationships
  - The Personal Data Protection Act 2021 (PDPA) is the data protection law that governs the: Collection, Use, Disclosure, Handling of personal data

What is a Non-Disclosure Agreement?

A non-disclosure agreement (NDA) is a legally binding contract between a provider and recipient of confidential material, knowledge or information. It is an undertaking not to disclose such confidential information covered under the agreement.

What are Non-Compete Clauses?

Non-compete clauses are commonly found in employment contracts in Singapore.

Typically, a non-compete clause prevents **employees from plying their trade or skill or engaging in businesses** in certain markets and geographies for a certain period of time.

It may purport to exert control over an employee's actions during the employment period (e.g. to prevent moonlighting) and/or after the termination of the employment contract.

SECURITY INCIDENT RESPONSE

- **Some attacks inevitably succeed.**
  - Successful attacks are called incidents or compromises.
  - Security moves into the respond stage.

- **Response should be "reacting according to plan."**
  - Planning is critical.
  - A compromise is not the right time to think about what to do.
- **Major Incidents and CSIRTs**
  - Major incidents are incidents the on-duty security staff cannot handle.
  - Company must convene a **computer security incident response team** (CSIRT).
  - CSIRTs should include members of senior management, the firm's security staff, members of the IT staff, members of affected functional departments, and the firm's public relations and legal departments

COMPUTER SECURITY INCIDENT RESPONSE TEAM

- For large and medium-sized organizations, a computer security incident response team (CSIRT) is responsible for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services.

CSIRTs are responsible for:

- Rapidly detecting incidents
- Minimizing loss and destruction
- Mitigating the weaknesses that were exploited
- Restoring computing services

SECURITY INCIDENTS

"Any action that threatens one or more of the classic security services of confidentiality, integrity, availability, accountability, authenticity, and reliability in a system"

Unauthorized access to a system

- **Accessing information not authorized to see**
- **Passing information on to a person not authorized to see it**
- **Attempting to circumvent the access mechanisms**
- **Using another person's password and user id**

Unauthorized modification of information on the system

- **Attempting to corrupt information that may be of value**
- **Attempting to modify information without authority**
- **Processing information in an unauthorized manner**

DETECTING INCIDENT AND REPORTING

- Incidents may be detected by users or administration staff, and they should be reported
- Log analysis, Intrusion detection systems (IDS) and Intrusion prevention systems
- **Triage Function**

Goal:

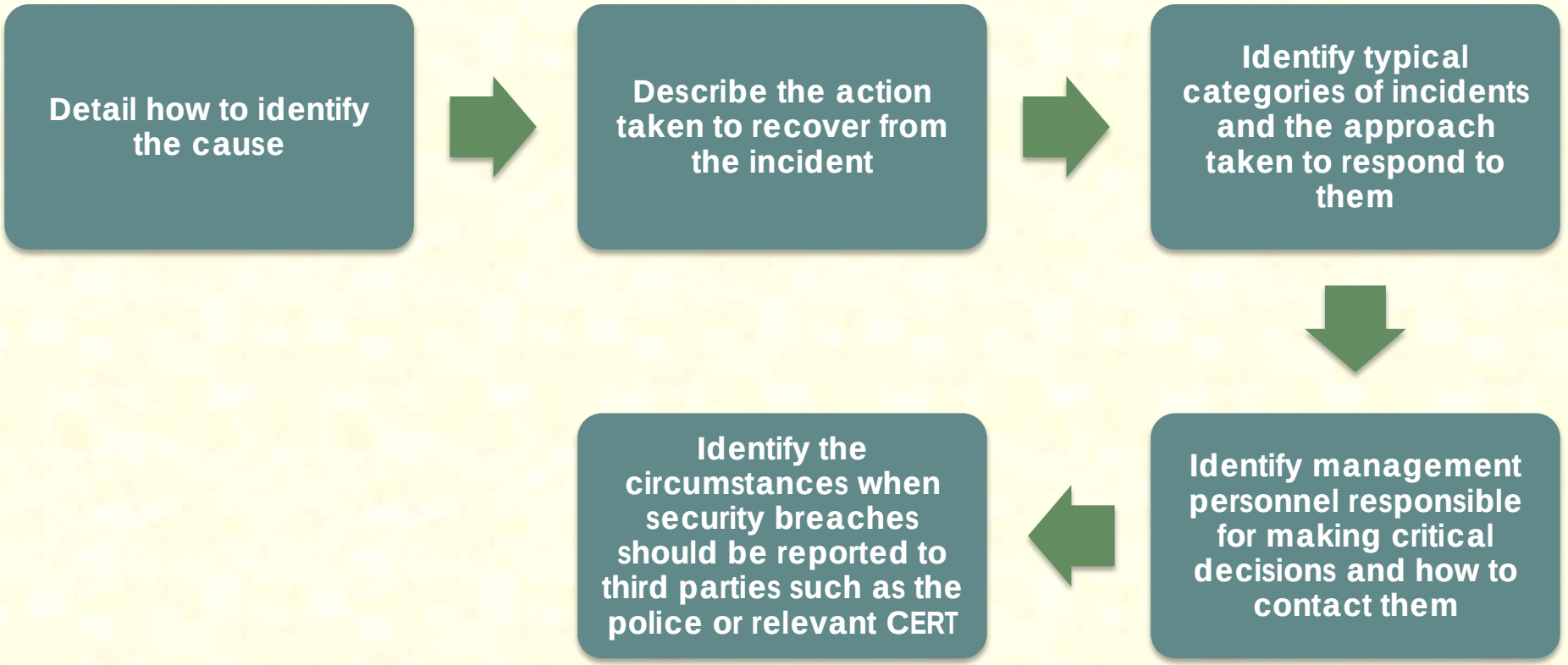
- Ensure that all information destined for the incident handling service is channeled through a single focal point
- Commonly achieved by advertising the triage function as the single point of contact for the whole incident handling service

Responds to incoming information by:

- Requesting additional information in order to categorize the incident
- Notifying the various parts of the enterprise or constituency about the vulnerability and shares information about how to fix or mitigate the vulnerability
- Identifies the incident as either new or part of an ongoing incident and passes this information on to the incident handling response function

RESPONDING TO INCIDENTS

- Must have documented procedures to respond to incidents
- Procedures should:



SECURITY INCIDENT RESPONSE

STAGES

- Detecting the attack
- Stopping the attack
- Repairing the damage
- Punishing the attacker

SECURITY INCIDENT RESPONSE

- **Disasters and Disaster Recovery**
  - Natural and humanly-made disasters
  - IT disaster recovery
    - Dedicated backup sites and transferring personnel or
    - Having two sites mutually back up each other
  - Business continuity recovery
    - Getting the whole firm back into operation
    - IT is only one concern

- **Rehearsals**
  - Incident response is responding according to plan.
  - Rehearsals are necessary for accuracy.
    - To find problems with the plan.
  - Rehearsals are necessary for response speed.
    - Time literally is money.

CASE STUDY: EQUIFAX

CASE STUDY: EQUIFAX: REALLY BIG DATA HACKED

EQUIFAX

- Equifax is a multinational credit reporting agency, founded in 1899 and headquartered in Atlanta, Georgia.
- Equifax holds the information of millions of consumers and businesses worldwide and sells both commercial credit reports and consumer credit reports to banks, insurance firms, and healthcare providers etc.
- Equifax also sells credit monitoring services, including credit fraud and identity theft prevention services.
- In the years leading up to the breach, Equifax had struggled with outdated cybersecurity policies and technology, which was highlighted during audit reports.
- In 2016, Equifax's website was hacked, resulting in the leak of 430,000 names, addresses, social security numbers, and other types of personal information.
- On 10 March 2017, personally identifying data of 147 millions of people was stolen from Equifax.
- Event began on 7th March 2017, when Apache publicized and provided a patch for Apache Struts, an easily exploitable software vulnerability.

EQUIFAX

- On March 8th, The Department of Homeland Security's US-CERT team responsible for disseminating information on cyber security threats, notified Equifax of the software flaw, and an alert was distributed to 400 employees by Equifax's Global Threats and Vulnerability Management (GTVM) team.
- On March 10th, hackers breached Equifax's networks by exploiting Apache Struts via Equifax's online dispute portal.
- On May 13th, attackers spread from the infected portal and gained access to other parts of Equifax's network.
- From May through July, hackers accessed multiple Equifax databases and extracted consumers' personal information. Stolen data included consumers' names, addresses, dates of birth, social security number, and credit card numbers.
- After learning of the breach, Equifax GVTM teams attempted and failed to locate Apache struts on servers and the inability to locate and patch Apache Struts can be attributed to the existing flaws in their cyber security policy.
- Equifax's security policy stated that vulnerabilities be patched within 48 hours of discovery, but the excuse given during the investigation was that "meeting this deadline impossible".

EQUIFAX

- The server was eventually patched 5 months after Equifax learned of the flaw.
- After failing to locate the application, IT and security took no further action to find Struts, and management did not check the vulnerability had been remediated.
- Equifax was criticized for everything ranging from their lax security to their bumbling response to the breach, and top executives were accused of corruption in the aftermath.
- The question is "who was behind the breach?" as this has serious implications for the global political landscape.
- Equifax held monthly GMTV meetings to discuss new vulnerabilities, but the status of the previous months' threats was often not discussed.
- For encryption, they needed digital certificate, however they had failed to renew one of their SSL certificates nearly for 10 months previously and the expired certificate wasn't discovered and renewed until July 29, 2019.
- Equifax publicized the breach, only on September 8, 2017, before executives sold company stock in early August, raising suspicions of corruption.

EQUIFAX

- The Equifax breach was investigated by several Federal authorities, including the FBI, related to the sale of $2 million of Equifax stock by executives after the discovery of the breach.
- Equifax faced lawsuits by both local and state governments and in 2019, former Chief information Officer Jun Ying was found guilty of insider trading and sentenced to four months in jail.
- Equifax manager Sudhakar Reddy Bonthu was also found guilty of insider trading and sentenced to 8 months of home confinement. No other Equifax employees faced arrest.
- In July of 2019, in a settlement, Equifax agreed to pay up to $700 million in fines and compensation for the 147 million affected individuals.
- Equifax was also required to pay up to $125 million in consumer compensation $175 million to states and $100 million to the civil penalties.
- Equifax spent $1.4 Billion on upgrading its security in the wake of the incident.

EQUIFAX

- **What are the lessons learned from the Equifax breach?**
- **Get the basics right**: No network is invulnerable. But Equifax was breached because it failed to patch a basic vulnerability, despite having procedures in place to make sure such patches were applied promptly.
- Huge amounts of data was exfiltrated unnoticed because someone neglected to renew a security certificate.
- Once the attackers were inside the perimeter, they were able to move from machine to machine and database to database. If they had been restricted to a single machine, the damage would've been much less.
- **Data governance is key:** users should only be given access to database content on a "need to know basis"; giving general access to any "trusted" users means that an attacker can seize control of those user accounts and run wild.
- Also, systems need to keep an eye out for weird behavior; the attackers executed up to 9,000 database queries very rapidly, which should've been a red flag.

DOES ANYONE WANT TO GET A BILLION DOLLAR?

- **IS IT POSSIBLE?**
- **YES**
- **HOW?**
- **STEAL ONLINE**
- **CAN ANYONE DO IT?**
- Well, it takes time, planning, manpower – and capitalizing on your target's vulnerabilities
- This is exactly what happened to BCB (Bangladesh Central Bank)
- It was the weekend of 5th February 2016 and due to Chinese new year, in Asia banks were closed for three days (Sunday, Saturday and Monday).
- Hackers manipulating the SWIFT system, which is used for world's interbank financial transfers.
- BCB mostly has around $39 billions to $40 billions in reserves, which are kept New York branch of the U.S. Federal Reserve.

- In BCB few people were sharing the same password, which was not very secure
- Attackers had penetrated BCB and had watched their operations for many months.
- Pretending to be the BCB, the thieves sent fake instructions over SWIFT to the New York Fed, asking for some funds to be transferred to bank accounts in Philippines, Sri Lanka and other parts of Asia.
- SWIFT usually notifies banks of transfers by sending the order to a bank's printers. But in this case, the attackers disabled the BCB's printers with a piece of malware.
- The security cameras in the banks were also disabled.
- On Monday, when BCB fixed its printer and received the notifications of the transfers, it was already too late, as the money had been sent.
- Hackers had tried to transfer $1 billon however due to spelling and formatting mistakes they were only able to transfer $81 millions to Manila casino system.
- In Manila, Philippines, workers at the Riza Commercial Banking Corporation allowed the attackers to open accounts using fake driving licenses; these accounts were then used to receive and traffic stolen funds.

- BCB managed to get Pan Asia Banking to cancel the $20 million that it had already received and reroute that money back to Bangladesh Bank's New York Fed account.
- The hackers apparently had indicated that at least one of the transfers should go to the Shalika Foundation, but they misspelled “foundation” as “fandation”, so it was stopped.
- Other transactions totaling $850 millions were stopped as they were sent to a company called “Jupiter”, which in USA federal reserve is listed as Iranian owned company under sanctions.
- So, what went wrong and how this sorts of attacks can be avoided?
- May things:
  - BCB Employee: Human error/careless, even some expert suggesting this as inside job
  - SWIFT: Some weaknesses, which has been rectified, however, no system is 100% secure and it can never be.
  - Phishing: Most likely the malware BCB was infected with was spread via shared USB.
  - International Laws: How thieves were allowed to open fake accounts, deposit money and closed it easily.

SUMMARY

- Positioning the information security function within organizations is very important
- Issues and concerns about staffing information security, should be considered carefully
- Professional credentials of information security professionals needs to be properly verified
- Organizational employment policies and practices related to successful information security need to be clearly specified and communicated
- Special security precautions for temporary employees should be in place
- Special requirements needed for the privacy of personnel data