Information Security Management

Chapter 9
Personnel & Security

Webster University
Scott Granneman

“I’ll take fifty percent efficiency
to get one hundred percent loyalty.”

-- Samuel Goldwyn (1882–1974),
US Film Producer

Upon completion of this chapter, you should be able to:

Identify the skills & requirements for InfoSec positions

Recognize the various
InfoSec professional certifications,
& identify which skills are encompassed by each

Understand & implement InfoSec constraints
on the general hiring processes

Understand the role of InfoSec in employee terminations

Describe the security practices used
to control employee behavior
& prevent misuse of information

InfoSec department
must be carefully structured
& staffed with
appropriately credentialed personnel

Proper procedures must be integrated
into all human resources activities,
including hiring, training, promotion,
& termination practices

Security technical & managerial skills face supply & demand cycles

To move the InfoSec discipline forward:

✓ General mgmt should learn qualifications for InfoSec positions & IT positions

✓ Upper mgmt should learn more about InfoSec budgetary & personnel needs

✓ IT & general mgmt must grant InfoSec function (& CISO) an appropriate level of influence & prestige

Qualifications & requirements

✓ Understand how organizations
are structured & operated

✓ Recognize that InfoSec is a management task
that cannot be handled with technology alone

✓ Work well with people in general, including users,
& communicate effectively using both
strong written & verbal communication skills

✓ Acknowledge the role of policy
in guiding security efforts

more … →

✓ Understand the essential role
of InfoSec education & training,
which helps make users part of the solution,
rather than part of the problem

✓ Perceive the threats facing an organization,
understand how these threats
can become transformed into attacks,
& safeguard the organization from InfoSec attacks

✓ Understand how technical controls
can be applied to solve specific InfoSec problems

✓ Demonstrate familiarity with
mainstream information technologies,
including DOS, Windows, Linux, & UNIX

✓ Understand IT & InfoSec terminology & concepts

Many InfoSec professionals enter the field
after having prior careers
in law enforcement or the military,
or careers in other IT areas,
such as networking, programming,
database administration,
or systems administration

Organizations can foster
greater professionalism
in the InfoSec discipline
by clearly defining their expectations
& establishing explicit position descriptions

FIGURE 10-1 Information Security Career Paths

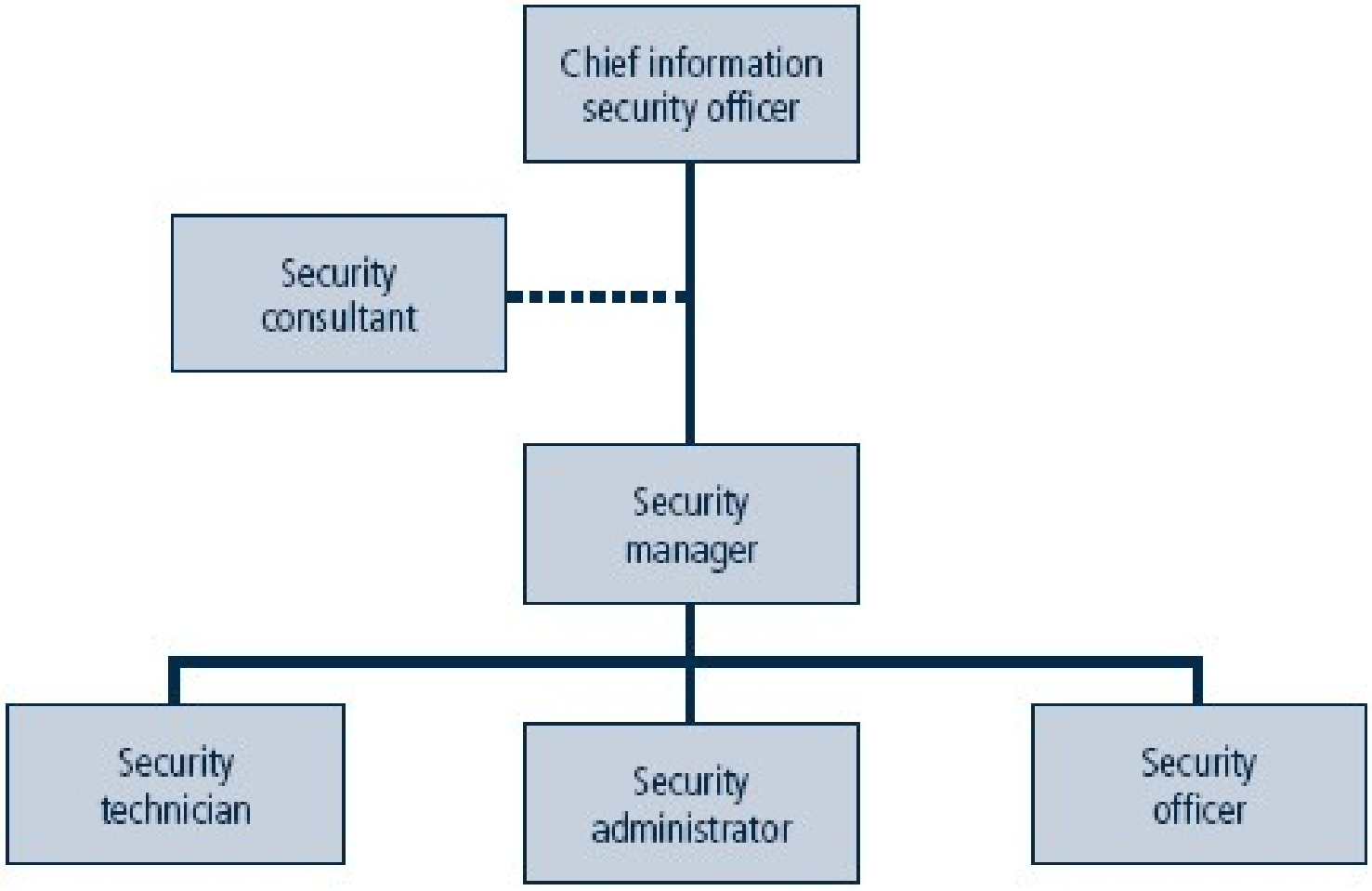

FIGURE 10-2 Possible Information Security Positions and Reporting Relationships

Chief InfoSec Officer (CISO)

CISO is typically considered
the top InfoSec officer
in the organization,
although the CISO is usually not
an executive-level position
& frequently reports to the CIO

Although these individuals
are business managers first
& technologists second,
they must be conversant
in all areas of InfoSec,
including technology, planning, & policy

Most common qualification for the CISO
is the Certified Information Systems
Security Professional (CISSP)

Graduate degree in criminal justice,
business, technology,
or another related field
is usually required as well

Candidate for this position
should have experience
as a security manager,
as well as in planning, policy, & budgets

Job Competencies for the CISO

✓ Maintains current & appropriate
body of knowledge necessary
to perform InfoSec management function

✓ Effectively applies
InfoSec management knowledge
to enhance security of open network
& associated systems & services

✓ Maintains working knowledge
of external legislative & regulatory initiatives

more … →

✓ Interprets & translates
requirements for implementation

✓ Develops appropriate InfoSec policies,
standards, guidelines, & procedures

✓ Works effectively with other
organization InfoSec personnel
& the committee process

✓ Provides meaningful input,
prepares effective presentations,
& communicates InfoSec objectives

more … →

✓ Participates in short- & long-term planning

✓ Monitors InfoSec program
compliance & effectiveness

✓ Works with committees
& management professionals
to accomplish InfoSec goals

✓ Coordinates & prioritizes activities
of the Office of InfoSec
in support of the organization’s mission

✓ Acts as a resource for matters of InfoSec

✓ Provides pertinent & useful information

more … →

✓ Oversees & conducts InfoSec reviews
& liaison visits to organizations

✓ Makes recommendations & reports
to Regional Practice Administration

✓ Coordinates & performs
reviews of contracts, projects, & proposals

✓ Assists information technology proponents
with standards compliance

✓ Conducts investigations of InfoSec violations
& computer crimes, & works effectively
with management & external law enforcement
to resolve these instances

more ... →

✓ Reviews instances of noncompliance
& works effectively & tactfully
to correct deficiencies

✓ Determines positions & personnel
necessary to accomplish InfoSec goals

✓ Requests positions, screens personnel,
& takes the lead
in the interviewing & hiring process

✓ Develops meaningful job descriptions

✓ Communicates expectations
& actively coaches personnel for success

more ... →

✓ Prioritizes & assigns tasks

✓ Reviews work performed

✓ Challenges staff to better themselves
& advance the level of service provided

✓ Provides meaningful feedback to staff
on an ongoing basis
& formally appraises performance annually

✓ Assists information technology proponents
with standards compliance

more … →

Security managers are accountable
for the day-to-day operation of InfoSec program

They accomplish objectives identified by the CISO
& resolve issues identified by the technicians

Security managers are often assigned
specific managerial duties by the CISO,
including policy development, risk assessment,
contingency planning,
& operational & tactical planning
for the security function

Management of technology requires
an understanding of the technology administered,
but not necessarily proficiency
in its configuration, operation, or fault resolution

Security Manager
Qualifications & Position Requirements

✓ Not uncommon for a security manager
to have a CISSP

✓ These individuals must have experience
in traditional business activities,
including budgeting, project management,
personnel management, & hiring & firing,
& they must be able to draft
middle- & lower-level policies
as well as standards & guidelines

✓ Several types of InfoSec managers exist,
& the people who fill these roles
tend to be much more specialized than CISOs

Security technicians are
technically qualified individuals who:

✓ Configure firewalls & IDSs

✓ Implement security software

✓ Diagnose & troubleshoot problems

✓ Coordinate with
systems & network administrators
to ensure that security technology
is properly implemented

Technician
Qualifications & Position Requirements

Technical qualifications & position requirements
for a security technician vary

Organizations typically prefer
expert, certified, proficient technicians

Job requirements usually include
some level of experience
with a particular hardware & software package

Sometimes familiarity with a particular technology
is enough to secure an applicant an interview

However, experience using the technology
is usually required

Many organizations rely to some extent
on recognizable professional certifications
to ascertain the level of proficiency
possessed by any given candidate

Many of the certification programs are relatively new

Precise value is not fully understood
by most hiring organizations

Certifying bodies work diligently
to educate their constituent communities
on the value & qualifications
of their certificate recipients

Employers struggle to match certifications
to position requirements,
while potential InfoSec workers try to determine
which certification programs will help in the job market

Certified Information Systems Security Professional (CISSP)

CISSP is considered most prestigious certification for security managers & CISOs

CISSP certification recognizes common body of knowledge (CBK) in InfoSec with 10 domains

- ✓ Access control systems & methodology
- ✓ Applications & systems development
- ✓ Business continuity planning
- ✓ Cryptography
- ✓ Law, investigation, & ethics
- ✓ Operations security
- ✓ Physical security
- ✓ Security architecture & models
- ✓ Security management practices
- ✓ Telecommunications, network, & Internet security

Systems Security Certified Practitioner (SSCP)

SSCP certification is more applicable to security manager

SSCP focuses “on practices, roles & responsibilities as defined by experts from major IS industries” & covers 7 domains:

- ✓ Access controls
- ✓ Administration
- ✓ Audit & monitoring
- ✓ Risk, response, & recovery
- ✓ Cryptography
- ✓ Data communications
- ✓ Malicious code/malware

Global Information Assurance Certification (GIAC)

SANS-sponsored technical security certification

GIAC certifications can be pursued independently or combined to earn a comprehensive certification called GIAC Security Engineer (GSE)

The individual GIAC certifications are:

- ✓ GIAC Security Essentials Certification (GSEC)
- ✓ GIAC Certified Firewall Analyst (GCFW)
- ✓ GIAC Certified Intrusion Analyst (GCIA)
- ✓ GIAC Certified Incident Handler (GCIH)
- ✓ GIAC Certified Windows Security Administrator (GCWN)
- ✓ GIAC Certified UNIX Security Administrator (GCUX)
- ✓ GIAC InfoSec Officer—Basic (GISO–Basic)
- ✓ GIAC Systems & Network Auditor (GSNA)
- ✓ GIAC Certified Forensic Analyst (GCFA)
- ✓ GIAC Security Leadership Certificate (GSLC)

Security Certified Program (SCP)

SCP offers two tracks:
Security Certified Network Professional (SCNP) &
the Security Certified Network Architect (SCNA)

Both designed for the security technician

more ... →

The SCNP track targets
firewalls & intrusion detection,
& requires 2 exams:

✓ Network Security Fundamentals (NSF)

✓ Network Defense & Countermeasures (NDC)

The SCNA program includes authentication areas,
including biometrics & PKI,
& equires two certification exams:

✓ PKI & Biometrics Concepts & Planning (PBC)

✓ PKI & Biometrics Implementation (PBI)

TruSecure ICSA Certified Security Associate (TICSA)

“Complementary to CISSP, as a stepping stone toward higher-level security management”

Examination is based on TruSecure methodology & TruSecure Six Categories of Risk:

- ✓ Electronic
- ✓ Malicious Code
- ✓ Physical
- ✓ Human
- ✓ Privacy
- ✓ Down time

TruSecure ICSA Certified Security Expert (TICSE)

TICSE candidate must demonstrate proficiency in:

- ✓ Firewall implementation
- ✓ Security policy formulation & implementation
- ✓ Risk analysis
- ✓ Attack method identification & solutions
- ✓ Bastion hosts & system hardening techniques
- ✓ Proxy server filtering properties
- ✓ VPN deployment
- ✓ Operating system security
- ✓ Applied cryptography (PGP, S/MIME, VPNs)
- ✓ Key management issues & solutions
- ✓ Incident response planning
- ✓ Biometrics
- ✓ Network & computer forensics

Security+

CompTIA certification
tests for security knowledge mastery
of an individual with
2 years on-the-job networking experience

Exam covers industry-wide topics including:

- ✓ General Security Concepts
- ✓ Communication Security
- ✓ Infrastructure Security
- ✓ Basics of Cryptography
- ✓ Operational/Organizational Security

Certified Information Systems Auditor (CISA)

Information Systems Audit & Control Association & Foundation (ISACA) touts the CISA as being appropriate for auditing, networking, & security professionals

Exam covers:

- ✓ IS audit process
- ✓ Management, planning, & organization of IS
- ✓ Technical infrastructure & operational practices
- ✓ Protection of information assets
- ✓ Disaster recovery & business continuity
- ✓ Business application system development, acquisition, implementation, & maintenance
- ✓ Business process evaluation & risk management

Certified InfoSec Manager (CISM)

Geared toward experienced InfoSec managers

Can assure executive management
that a candidate has
required background knowledge
needed for effective
security management & consulting

Exam covers:

✓ InfoSec Governance
✓ Risk Management
✓ InfoSec Program Management
✓ InfoSec Management
✓ Response Management

Certified Information Forensics Investigator (CIFI)

Under development by
InfoSec Forensics Association

Will evaluate expertise of those who work with law enforcement, & auditing

Body of knowledge includes:

- ✓ Countermeasures
- ✓ Auditing
- ✓ Incident response teams
- ✓ Law enforcement & investigation
- ✓ Traceback
- ✓ Tools & techniques

Certifications can be expensive

Most experienced professionals
find it difficult to do well on them
without at least some review

Most programs require
between 2 & 3 years
of work experience

Often structured to reward candidates
who have significant hands-on experience

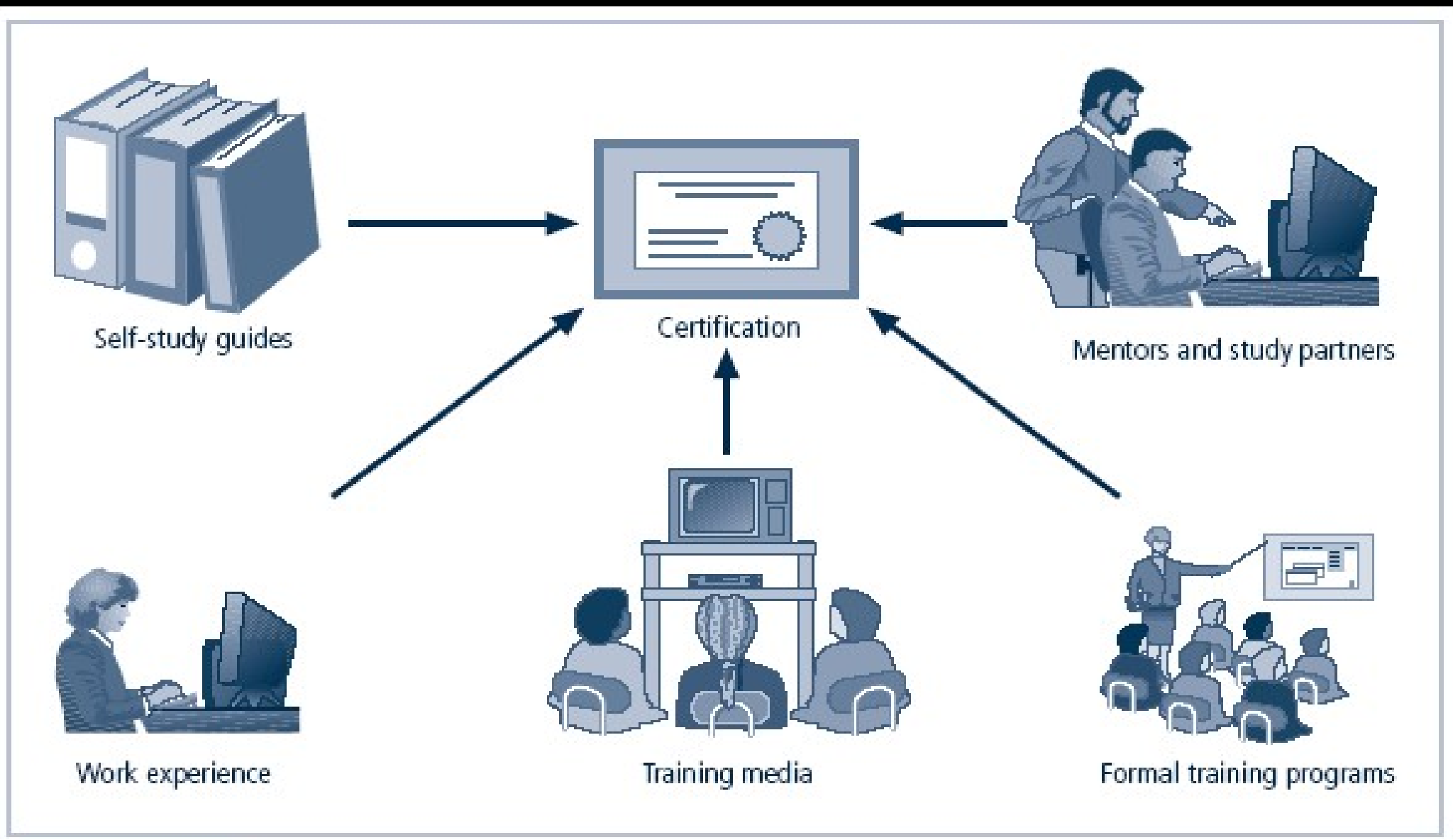

FIGURE 10-3 Preparing for Security Certification

Employment Policies & Practices

General management community of interest
should integrate solid InfoSec concepts
across organization's
employment policies & practices

Including InfoSec responsibilities
into every employee's job description
& subsequent performance reviews
can make an entire organization
take InfoSec more seriously

From InfoSec perspective,
hiring of employees
is laden with potential security pitfalls

CISO, in cooperation with CIO
& relevant InfoSec managers,
should establish a dialogue
with human resources personnel
so that InfoSec considerations
become part of the hiring process

Hiring Issues

Job Descriptions: organizations
that provide complete job descriptions
when advertising open positions
should omit elements of the job description
that describe access privileges

Interviews: InfoSec should advise HR
to limit information provided to candidates
on access rights of the position

When an interview includes a site visit,
tour should avoid secure & restricted sites

more … →

New Hire Orientation: new employees
should receive, as part of their orientation,
an extensive InfoSec briefing

On-the-Job Security Training:
organizations should conduct
periodic security awareness & training activities
to keep security at the forefront
of employees' minds
& minimize employee mistakes

Security Checks: background check
should be conducted
before organization extends an offer
to any candidate, regardless of job level

Common Background Checks

Identity checks: Personal identity validation

Education & credential checks:
Institutions attended,
degrees & certifications earned,
& certification status

Previous employment verification:
Where candidates worked, why they left,
what they did, & for how long

Reference checks: Validity of references
& integrity of reference sources

more … →

Worker’s compensation history:
Claims from worker’s compensation

Motor vehicle records: driving records,
suspensions, & other items
noted in the applicant’s public record

Drug history: drug screening & drug usage,
past & present

Medical history:
current & previous medical conditions,
usually associated with physical capability
to perform the work in the specified position

more … →

Credit history: credit problems,
financial problems, & bankruptcy

Civil court history:
involvement as the plaintiff or defendant
in civil suits

Criminal court history: criminal background,
arrests, convictions, & time served

Once a candidate has accepted a job offer,
the employment contract
becomes an important security instrument

It is important to have
these contracts & agreements in place
at the time of the hire

To heighten InfoSec awareness
& change workplace behavior,
organizations should incorporate
InfoSec components
into employee performance evaluations

Employees pay close attention
to job performance evaluations

Including InfoSec tasks in them
will motivate employees
to take more care
when performing these tasks

When an employee leaves an organization, the following tasks must be performed:

✓ Access to organization's systems must be disabled

✓ Former employee must return all removable media

✓ Former employee's hard drives must be secured

✓ File cabinet locks must be changed

✓ Office door locks must be changed

more … →

✓ Former employee’s keycard access
must be revoked

✓ Former employee’s personal effects
must be removed from the premises

✓ Former employee should be escorted
from the premises, once keys, keycards,
& other business property have been turned over

more … →

✓ Exit interview to remind employee
of any contractual obligations,
such as nondisclosure agreements,
& to obtain feedback
on the employee's tenure in the organization

✓ Two methods
for handling employee outprocessing,
depending on the employee's reasons for leaving:

1. Hostile departure

2. Friendly departure

Hostile Departure

Security cuts off all logical & keycard access
before employee is terminated

Employee reports for work
& is escorted into supervisor's office
to receive bad news

Individual is then escorted from the workplace
& informed that his personal property will be forwarded,
or is escorted to
his office, cubicle, or personal area
to collect personal effects under supervision

Once personal property has been gathered,
employee is asked to surrender
all keys, keycards, & other organizational
identification & access devices, PDAs, pagers, cell phones,
& all remaining company property,
& is then escorted from the building

Friendly Departure

Employee may have tendered notice
well in advance of actual departure date
which can make it much more difficult
for security to maintain positive control
over employee's access & information usage

Employee accounts are usually allowed
to continue with a new expiration date

Employee can come & go at will,
usually collects any belongings
& leaves without escort

Employee is asked to drop off
all organizational property before departing

In either circumstance,
offices & information used by departing employees
must be inventoried,
their files stored or destroyed,
& all property returned to organizational stores

Possible that departing employees
have collected & taken home information or assets
that could be valuable in their future jobs

Only by scrutinizing system logs
during transition period
& after employee has departed,
& sorting out authorized actions
from system misuse or information theft,
can the organization determine whether
a breach of policy or a loss of information
has occurred

There are various ways
of monitoring & controlling employees
to minimize their opportunities
to misuse information

Separation of duties is used
to make it difficult for an individual
to violate InfoSec
& breach the CIA of information

Two-man control requires
that 2 individuals review & approve
each other's work
before the task is considered complete

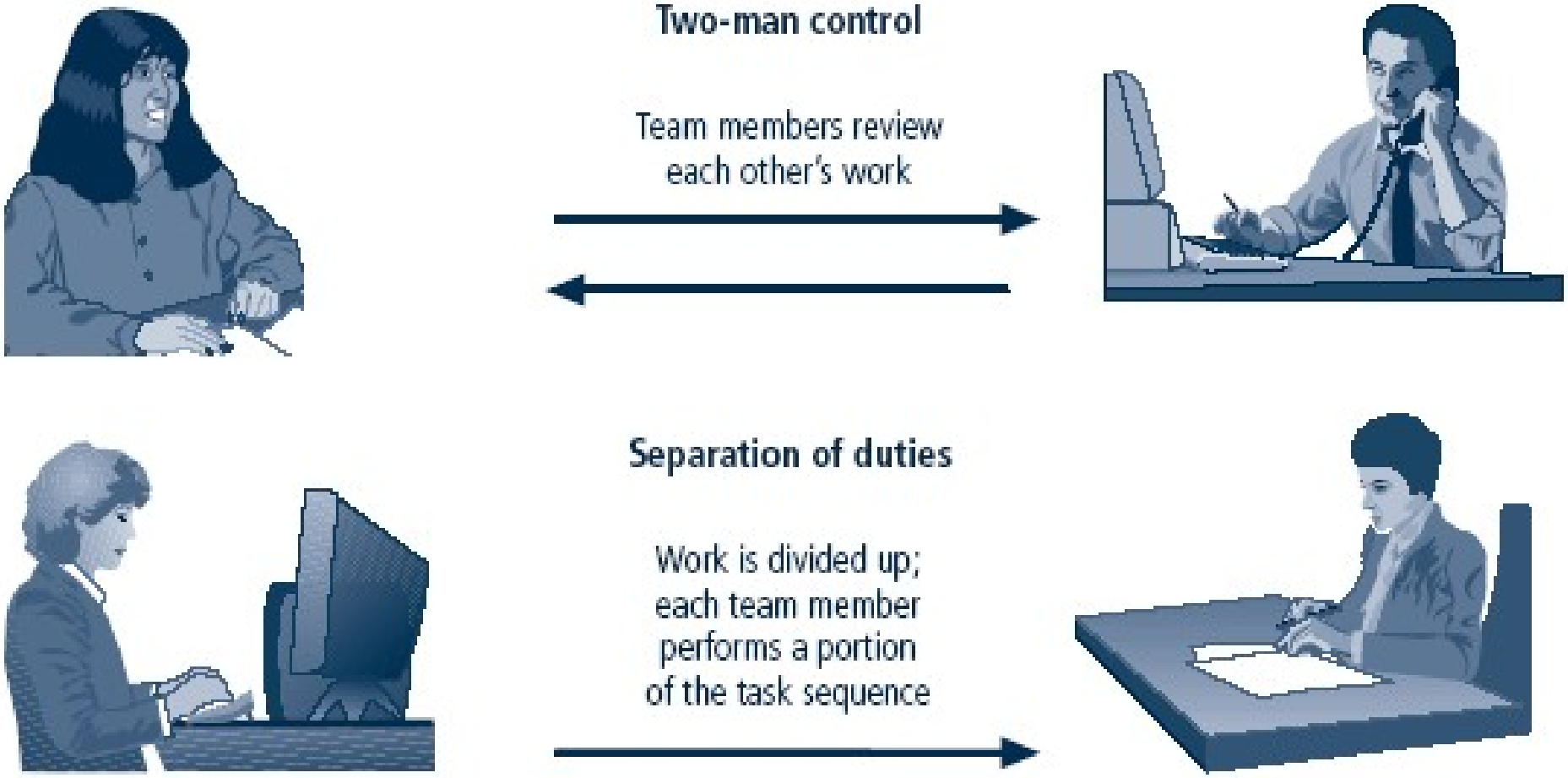

FIGURE 10-6 Personnel Security Controls

Job rotation

✓ Another control used to prevent personnel from misusing information assets

✓ Requires that every employee be able to perform the work of at least one other employee

Task rotation

✓ All critical tasks can be performed by multiple individuals

Both job rotation & task rotation ensure
that no one employee is performing actions
that cannot be knowledgeably reviewed
by another employee

For similar reasons,
each employee should be required
to take a mandatory vacation
of at least one week per year

Policy gives organization
a chance to perform a detailed review
of everyone's work

Finally, another important way
to minimize opportunities
for employee misuse information
is to limit access to information

Employees should be able to access
only the information they need
& only for the period required
to perform their tasks

This policy gives the organization a chance
to perform a detailed review of everyone's work

Organizations are required by law
to protect sensitive or personal
employee information,
including personally identifying facts
such as
employee addresses, phone numbers,
Social Security Numbers, medical conditions,
& even names & addresses of family members

This responsibility also extends to
customers, patients, & anyone with whom
the organization has business relationships

While personnel data is, in principle,
no different than other data
that InfoSec is expected to protect,
certainly more regulations
cover its protection

As a result, InfoSec procedures
should ensure that this data
receives at least the same level of protection
as other important data in the organization

Many individuals who are not employees
often have access
to sensitive organizational information

Relationships with individuals
in this category
should be carefully managed
to prevent threats
to information assets from materializing

Because temporary workers
are not employed by the organization
for which they are working,
they may not be subject
to contractual obligations or general policies
that govern other employees

Unless specified in contract,
temp agency may not be liable for losses
caused by its workers

From a security standpoint,
access to information for these individuals
should be limited to what is necessary
to perform their duties

While professional contractors may require access
to virtually all areas of the organization
to do their jobs,
service contractors usually need access
only to specific facilities, so they should not
be allowed to wander freely in & out of buildings

In a secure facility, all service contractors are escorted
from room to room & into & out of the facility

Any service agreements or contracts
should contain the following regulations:

✓ Facility requires 24 to 48 hours' notice
of a maintenance visit
✓ Facility requires all on-site personnel
to undergo background checks
✓ Facility requires advance notice for
cancellation or rescheduling of a maintenance visit

Consultants have their own
security requirements & contractual obligations

Should be handled like contract employees,
with special requirements,
such as information or facility access requirements,
being integrated into the contract
before they are given free access to the facility

In particular, security & technology consultants
must be prescreened, escorted, & subjected
to NDAs to protect the organization
from intentional or accidental
breaches of confidentiality

more ... →

Just because you pay security consultants,
it doesn’t mean that protecting your information
is their number one priority

Always remember to apply
the principle of least privilege
when working with consultants

Businesses sometimes engage
in strategic alliances with other organizations,
so as to exchange information, integrate systems,
or enjoy some other mutual advantage

A prior business agreement must specify
the levels of exposure that both organizations
are willing to tolerate

more ... →

If strategic partnership evolves
into an integration of the systems
of both companies,
competing groups may be provided
with information
that neither parent organization expected

Level of security of both systems
must be examined
before any physical integration takes place,
as system connection
means that vulnerability on one system
becomes vulnerability for all linked systems

Summary

Introduction

Staffing the Security Function

InfoSec Professional Credentials

Employment Policies & Practices

Thank you!

Scott Granneman