中國文化大學推廣教育部
SCHOOL OF CONTINUING EDUCATION
CHINESE CULTURE UNIVERSITY

Cybersecurity Governance

Allen Y. Chang
Graduate School of Information Management
Chinese Culture University, SCE
2023/9/15

The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards—and even then I have my doubts.

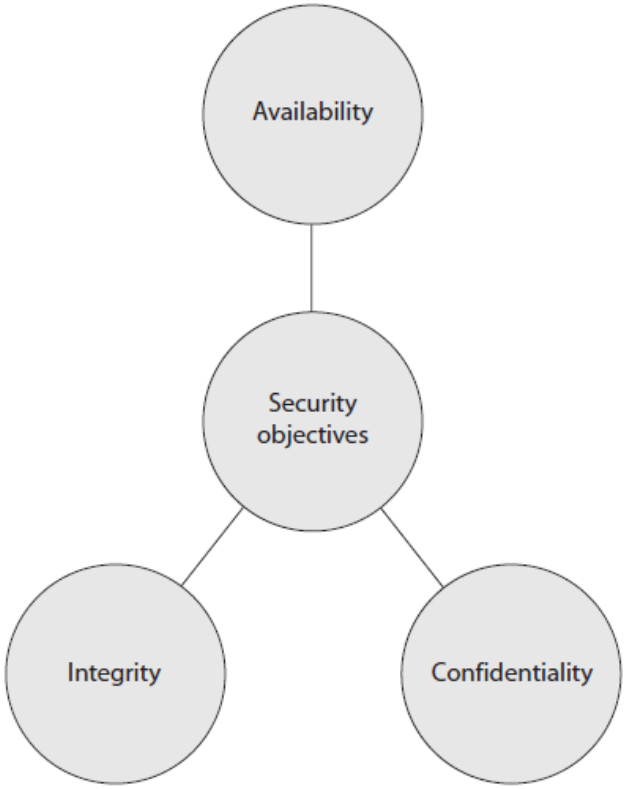
—Eugene H. Spafford

Outline

- Fundamental cybersecurity concepts and terms
- Security governance Principles
- Security policies, standards procedures, and guidelines
- Personnel security
- Security awareness, education, and training programs

Fundamental cybersecurity concepts and terms

- Cybersecurity professionals' efforts are ultimately focused on the protection of our information systems
- These systems consist of people, processes, and technologies designed to operate on information
- To protect them means to ensure the confidentiality, integrity, and availability (the CIA triad) of all assets in our information systems as well as the authenticity and nonrepudiation of tasks performed in them



Confidentiality

- *Confidentiality* means keeping unauthorized entities (be they people or processes) from gaining access to information assets
- It ensures that the necessary level of secrecy is enforced at each junction of data processing and prevents unauthorized disclosure
- Confidentiality can be provided by
  - ✓ Encrypting data as it is stored and transmitted
  - ✓ Enforcing strict access control and data classification
  - ✓ Training personnel on the proper data protection procedures

Confidentiality (cont.)

- Attackers can thwart confidentiality mechanisms by
  - ✓ Network monitoring
  - ✓ Shoulder surfing
  - ✓ Stealing credentials
  - ✓ Breaking encryption schemes
  - ✓ Social engineering
- *Shoulder surfing* is when a person looks over another person's shoulder and watches their keystrokes or views data as it appears on a computer screen
- *Social engineering* is when one person tricks another person into sharing confidential information
- Any one-to-one communication medium can be used to perform *social engineering attacks*

Integrity

- *Integrity* means that an asset is free from unauthorized alterations
- For example, orders placed by customers on your online store, you should not be able to increase the price of any items in those orders after they have been purchased
- Environments that enforce and provide this attribute of security ensure that attackers, or mistakes by users, do not compromise the integrity of systems or data
- Authorized users can also affect a system or its data's integrity by mistake
- For example, a user with a full hard drive may unwittingly delete a configuration file under the mistaken assumption that deleting a file must be okay because the user doesn't remember ever using it

Integrity (cont.)

- A user may insert incorrect values into a data-processing application that ends up charging a customer $3,000 instead of $300
- Security should streamline users' capabilities and give them only certain choices and functionality, so errors become less common and less devastating
- System-critical files should be restricted from viewing and access by users
- Applications should provide mechanisms that check for valid and reasonable input values
- Databases should let only authorized individuals modify data,
- Data in transit should be protected by encryption or other mechanisms

Availability

- *Availability* protection ensures reliable and timely access to data and resources to authorized individuals
- Network devices, computers, and applications should provide adequate functionality to perform in a predictable manner with an acceptable level of performance
- They should be able to recover from disruptions in a secure and quick fashion, so productivity is not negatively affected
- Necessary protection mechanisms must be in place to protect against inside and outside threats that could affect the availability and productivity of all business-processing components

Availability (cont.)

- Networks have many pieces that must stay up and running (routers, switches, proxies, firewalls, and so on)
- Software has many components that must be executing in a healthy manner (operating system, applications, antimalware software, and so forth)
- An organization's operations can potentially be negatively affected by
  - ✓ Environmental aspects (such as fire, flood, HVAC issues, or electrical problems)
  - ✓ Natural disasters
  - ✓ Physical theft or attacks

Authenticity

- *Authenticity* protections ensure we can trust that something comes from its claimed source
- This concept is at the heart of authentication, which establishes that an entity trying to log into a system is really who it claims to be
- Authenticity in information systems is almost always provided through cryptographic means
- As an example, when you connect to your bank's website, the connection should be encrypted using Transport Layer Security (TLS), which in turn uses your bank's digital certificate to authenticate to your browser that it truly is that bank on the other end and not an impostor

Nonrepudiation

- While authenticity establishes that an entity is who it claims to be at a particular point in time, it doesn't really provide historical proof of what that entity did or agreed to
  - ✓ For example, suppose Bob logs into his bank and then applies for a loan.
  - ✓ He doesn't read the fine print until later, at which point he decides he doesn't like the terms of the transaction
  - ✓ So he calls up the bank to say he never signed the contract and to please make it go away.
- Although the session was authenticated, Bob could claim that he walked away from his computer while logged into the bank's website, that his cat walked over the keyboard and stepped on enter, executing the transaction, and that Bob never intended to sign the loan application.
- It was the cat. Sadly, his claim could hold up in court

Nonrepudiation (cont.)

- *Nonrepudiation* means that someone cannot disavow being the source of a given action
  - For example, suppose Bob's bank had implemented a procedure for loan applications that required him to "sign" the application by entering his personal identification number (PIN)
  - Now the whole cat defense falls apart unless Bob could prove he trained his cat to enter PINs
- Most commonly, nonrepudiation is provided through the use of digital signatures
- Just like your physical signature on a piece of paper certifies that you either authored it or agree to whatever is written on it (e.g., a contract), the digital version attests to your sending an e-mail, writing software, or agreeing to a contract
- Digital signatures are cryptographic products that, just like an old-fashioned physical signature, can be used for a variety of purposes.

Balanced Security

- In reality, when information security is considered, it is commonly only through the lens of keeping secrets secret (confidentiality)
- The integrity and availability threats tend to be overlooked and only dealt with after they are properly compromised
- Some assets have a critical confidentiality requirement (e.g., company trade secrets)
- Some assets have critical integrity requirements (e.g., financial transaction values)
- Some assets have critical availability requirements (e.g., e-commerce web servers)
- Many people understand the concepts of the CIA triad, but may not fully appreciate the complexity of implementing the necessary controls to provide all the protection these concepts cover

Components of CIA controls

- The following provides a *short* list of some of these controls and how they map to the components of the CIA triad

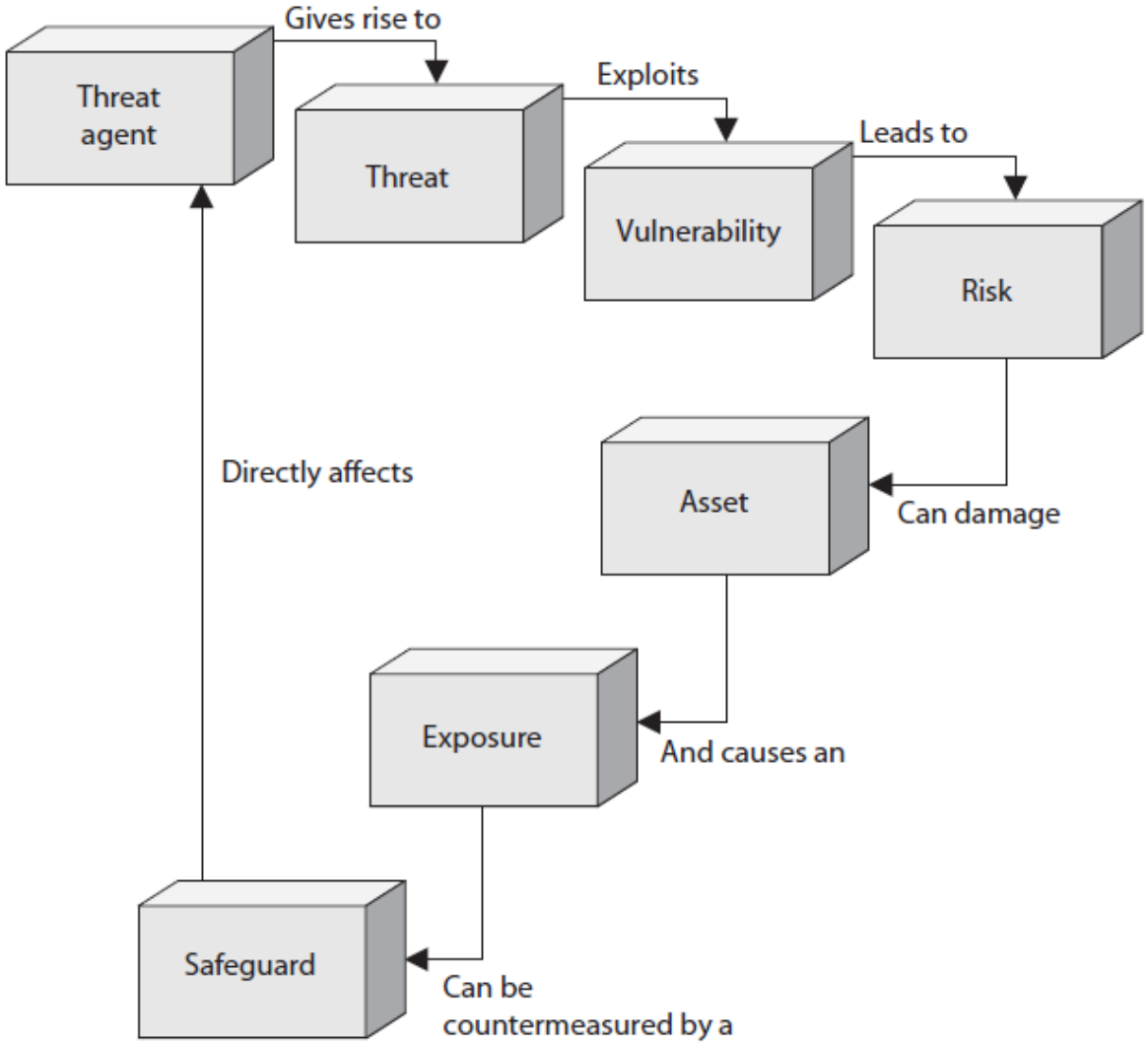
- **Availability:**
  - ✓ Redundant array of independent disks (RAID)
  - ✓ Clustering
  - ✓ Load balancing
  - ✓ Redundant data and power lines
  - ✓ Software and data backups
  - ✓ Disk shadowing
  - ✓ Co-location and offsite facilities
  - ✓ Rollback functions
  - ✓ Failover configurations

List of CIA components (cont.)

- **Integrity:**
  - ✓ Hashing (data integrity)
  - ✓ Configuration management (system integrity)
  - ✓ Change control (process integrity)
  - ✓ Access control (physical and technical)
  - ✓ Software digital signing
  - ✓ Transmission cyclic redundancy check (CRC) functions

- **Confidentiality:**
  - ✓ Encryption for data at rest (whole disk, database encryption)
  - ✓ Encryption for data in transit (IPSec, TLS, PPTP, SSH, described in Chapter 4)
  - ✓ Access control (physical and technical)

Relationship among different security concepts



Other Security Terms

- A *vulnerability* is a weakness in a system that allows a threat source to compromise its security
- A vulnerability can be a software, hardware, procedural, or human weakness that can be exploited
- A vulnerability may be
  - ✓ A service running on a server
  - ✓ unpatched applications or operating systems
  - ✓ An unrestricted wireless access point
  - ✓ An open port on a firewall
  - ✓ Lax physical security that allows anyone to enter a server room
  - ✓ Unenforced password management on servers and workstations

Other Security Terms (cont.)

- A *threat* is any potential danger that is associated with the exploitation of a vulnerability
- If the threat is that someone will identify a specific vulnerability and use it against the organization or individual, then the entity that takes advantage of a vulnerability is referred to as a *threat agent* (or *threat actor*)
- A threat agent could be
  - ✓ an intruder accessing the network through a port on the firewall
  - ✓ a process accessing data in a way that violates the security policy
  - ✓ an employee circumventing controls in order to copy files to a medium that could expose confidential information

Other Security Terms (cont.)

- A *risk* is the likelihood of a threat source exploiting a vulnerability and the corresponding business impact
  - If a firewall has several ports open, there is a higher likelihood that an intruder will use one to access the network in an unauthorized method
  - If users are not educated on processes and procedures, there is a higher likelihood that an employee will make an unintentional mistake that may destroy data
  - If an intrusion detection system (IDS) is not implemented on a network, there is a higher likelihood an attack will go unnoticed until it is too late.
- Risk ties the vulnerability, threat, and likelihood of exploitation to the resulting business impact.

Other Security Terms (cont.)

- An *exposure* is an instance of being exposed to losses
- A vulnerability exposes an organization to possible damages
- If password management is lax and password rules are not enforced, the organization is exposed to the possibility of having users' passwords compromised and used in an unauthorized manner
- If an organization does not have its wiring inspected and does not put proactive fire prevention steps into place, it exposes itself to potentially devastating fires

Control / Countermeasure / Safeguard

- A *control*, or *countermeasure*, is put into place to mitigate (reduce) the potential risk
- A countermeasure may be
  - ✓ a software configuration
  - ✓ a hardware device
  - ✓ a procedure that eliminates a vulnerability
  - ✓ a procedure reduces the likelihood a threat agent will be able to exploit a vulnerability
- Examples of countermeasures include
  - ✓ strong password management
  - ✓ firewalls
  - ✓ a security guard
  - ✓ access control mechanisms
  - ✓ encryption
  - ✓ security awareness training

Security governance Principles

- *Security governance* is a framework that supports the security goals of an organization being set and expressed by senior management, communicated throughout the different levels of the organization, and consistently applied and assessed
- Security governance grants power to the entities who need to implement and enforce security and provides a way to verify the performance of these necessary security activities
- Senior management not only needs to set the direction of security but also needs a way to be able to view and understand how their directives are being met or not being met
- Let's compare two companies
- Company A has an effective security governance program in place and Company B does not

Company A vs Company B

- To the untrained eye it would seem as though Companies A and B are equal in their security practices because they both have
  - ✓ security policies, procedures, and standards in place
  - ✓ the same security technology controls (firewalls, endpoint detection, identity management, and so on)
  - ✓ defined security roles
  - ✓ security awareness training
- You may think, “These two companies are on the ball and quite evolved in their security programs.”
- But if you look closer, you will see some critical differences

Security Governance Program: A Comparison of Two Companies

Company A	Company B
Board members understand that information security is critical to the company and demand to be updated quarterly on security performance and breaches.	Board members do not understand that information security is in their realm of responsibility and focus solely on corporate governance and profits.
The chief executive officer (CEO), chief financial officer (CFO), chief information officer (CIO), chief information security officer (CISO), and business unit managers participate in a risk management committee that meets each month, and information security is always one topic on the agenda to review.	The CEO, CFO, and business unit managers feel as though information security is the responsibility of the CIO, CISO, and IT department and do not get involved.
Executive management sets an acceptable risk level that is the basis for the company's security policies and all security activities.	The CISO copied some boilerplate security policies, inserted his company's name, and had the CEO sign them.
Executive management holds business unit managers responsible for carrying out risk management activities for their specific business units.	All security activity takes place within the security department; thus, security works within a silo and is not integrated throughout the organization.

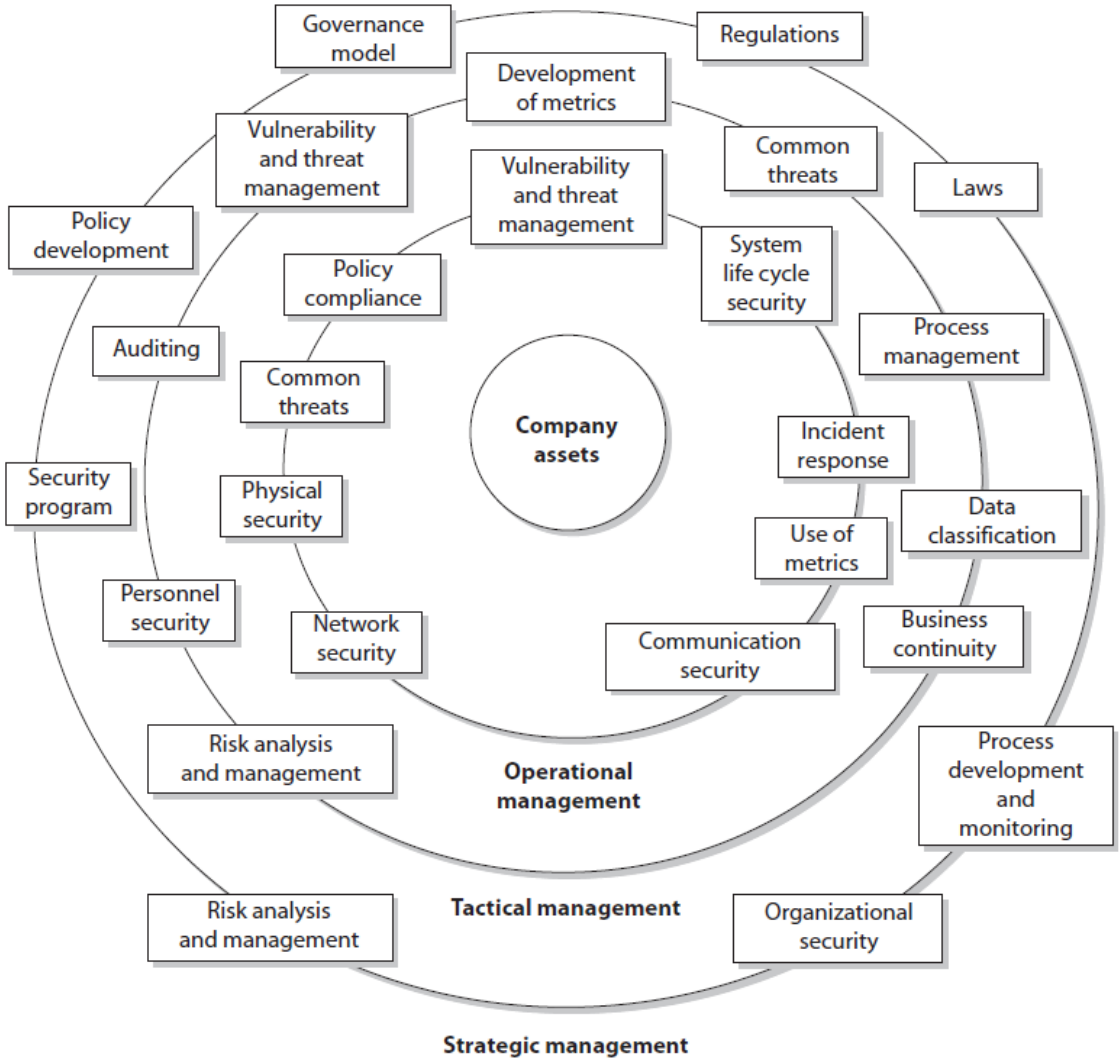
Security Governance Program: A Comparison of Two Companies (cont.)

Company A	Company B
Critical business processes are documented along with the risks that are inherent at the different steps within the business processes.	Business processes are not documented and not analyzed for potential risks that can affect operations, productivity, and profitability.
Employees are held accountable for any security breaches they participate in, either maliciously or accidentally.	Policies and standards are developed, but no enforcement or accountability practices have been envisioned or deployed.
Security products, managed services, and consulting services are purchased and deployed in an informed manner. They are also constantly reviewed to ensure they are cost-effective.	Security products, managed services, and consulting services are purchased and deployed without any real research or performance metrics to determine the return on investment or effectiveness.
The organization is continuing to review its processes, including security, with the goal of continued improvement.	The organization does not analyze its performance for improvement, but continually marches forward and makes similar mistakes over and over again.

Security governance in the real world

- Security governance is typically implemented as a formal cybersecurity program or an information security management system (ISMS)
- It is a collection of policies, procedures, baselines, and standards that an organization puts in place to make sure that its security efforts are aligned with business needs, streamlined, and effective, and that no security controls are missing

A complete security program



Aligning Security to Business Strategy

- An *enterprise security architecture (ESA)* is a subset of an enterprise architecture
- ESA implements an information security strategy
- ESA consists of layers of solutions, processes, and procedures and the way they are linked across an enterprise strategically, tactically, and operationally
- ESA is a comprehensive and rigorous method for describing the structure and behavior of all the components that make up a holistic ISMS
- The main reason to develop an ESA is to ensure that security efforts align with business practices in a standardized and cost-effective manner

*ESA *NOT* in place*

- How do you know if an organization does not have an enterprise security architecture in place?
- If the answer is "yes" to most of the following questions, this type of architecture is *NOT* in place:
  - ✓ Does security take place in silos throughout the organization?
  - ✓ Is there a continual disconnect between senior management and the security staff?
  - ✓ Are redundant products purchased for different departments for overlapping security needs?
  - ✓ Is the security program made up of mainly policies without actual implementation and enforcement?
  - ✓ When a user's access requirements increase because of business needs, does the network administrator just modify the access controls without the user manager's documented approval?

*ESA *NOT* in place (cont.)*

- ✓ When a new product is being rolled out, do unexpected interoperability issues pop up that require more time and money to fix?
- ✓ Do many "one-off" efforts take place instead of following standardized procedures when security issues arise?
- ✓ Are the business unit managers unaware of their security responsibilities and how their responsibilities map to legal and regulatory requirements?
- ✓ Is "sensitive data" defined in a policy, but the necessary controls are not fully implemented and monitored?
- ✓ Are stovepipe (point) solutions implemented instead of enterprise-wide solutions?

*ESA *NOT* in place (cont.)*

- ✓ Are the same expensive mistakes continuing to take place?
- ✓ Is security governance currently unavailable because the enterprise is not viewed or monitored in a standardized and holistic manner?
- ✓ Are business decisions being made without taking security into account?
- ✓ Are security personnel usually putting out fires with no real time to look at and develop strategic approaches?
- ✓ Are some business units engaged in security efforts that other business units know nothing about?

SABSA

- A helpful tool for aligning an organization's security architecture with its business strategy is the *Sherwood Applied Business Security Architecture (SABSA)*
- SABSA is a layered framework, with its first layer describing the business context within which the security architecture must exist
- Each layer of the framework decreases in abstraction and increases in detail, so it builds upon the others and moves from policy to practical implementation of technology and solutions
- The idea is to provide a chain of traceability through the levels of
  - ✓ contextual
  - ✓ conceptual
  - ✓ logical
  - ✓ physical
  - ✓ component
  - ✓ operational

SABSA Architecture Framework

	Assets (What)	Motivation (Why)	Process (How)	People (Who)	Location (Where)	Time (When)
Contextual	The business	Business risk model	Business process model	Business organization and relationships	Business geography	Business time dependencies
Conceptual	Business attributes profile	Control objectives	Security strategies and architectural layering	Security entity model and trust framework	Security domain model	Security-related lifetimes and deadlines
Logical	Business information model	Security policies	Security services	Entity schema and privilege profiles	Security domain definitions and associations	Security processing cycle
Physical	Business data model	Security rules, practices, and procedures	Security mechanisms	Users, applications, and user interface	Platform and network infrastructure	Control structure execution
Component	Detailed data structures	Security standards	Security products and tools	Identities, functions, actions, and ACLs	Processes, nodes, addresses, and protocols	Security step timing and sequencing
Operational	Assurance of operation continuity	Operation risk management	Security service management and support	Application and user management and support	Security of sites, networks, and platforms	Security operations schedule

Q&A of SABSA Framework

- The following outlines the questions that are to be asked and answered at each level of the framework:
  - ***What* are you trying to do at this layer?** The assets to be protected by your security architecture.
  - ***Why* are you doing it?** The motivation for wanting to apply security, expressed in the terms of this layer.
  - ***How* are you trying to do it?** The functions needed to achieve security at this layer.
  - ***Who* is involved?** The people and organizational aspects of security at this layer.
  - ***Where* are you doing it?** The locations where you apply your security, relevant to this layer.
  - ***When* are you doing it?** The time-related aspects of security relevant to this layer.

Framework & Methodology

- SABSA is a framework and methodology for enterprise security architecture and service management
- Since SABSA is a *framework*, this means it provides a structure for individual architectures to be built from
- Since SABSA is a *methodology* also, this means it provides the processes to follow to build and maintain this architecture
- SABSA provides a life-cycle model so that the architecture can be constantly monitored and improved upon over time

Strategic alignment

- *Strategic alignment* means the business drivers and the regulatory and legal requirements are being met by the enterprise security architecture
- Security efforts must provide and support an environment that allows an organization to not only survive, but thrive
- The security industry has grown up from the technical and engineering world, not the business world
- In many organizations, while the IT security personnel and business personnel might be located physically close to each other, they are commonly worlds apart in how they see the same organization they work in
- Technology is only a tool that supports a business; it is not the business itself

Business Enablement

- When looking at the *business enablement* requirement of the enterprise security architecture, we need to remind ourselves that each organization exists for one or more specific business purposes
  - ✓ Publicly traded companies are in the business of increasing shareholder value
  - ✓ Nonprofit organizations are in the business of furthering a specific set of causes
  - ✓ Government organizations are in the business of providing services to their citizens
- Companies and organizations do not exist for the sole purpose of being secure
- Security cannot stand in the way of business processes, but should be implemented to better enable them

Business Enablement (cont.)

- Business enablement means the core business processes are integrated into the security operating model—they are standards based and follow a risk tolerance criteria
- Let's say a company's accountants have figured out that if they allow the customer service and support staff to work from home, the company would save a lot of money on office rent, utilities, and overhead—plus, the company's insurance would be cheaper
- The company could move into this new model with the use of virtual private networks (VPNs), firewalls, content filtering, and so on

Business Enablement (cont.)

- Security enables the company to move to this different working model by providing the necessary protection mechanisms
- If a financial institution wants to enable its customers to view bank account information and carry out money transfers online, it can offer this service if the correct security mechanisms are put in place (access control, authentication, secure connections, etc.)
- Security should help the organization thrive by providing the mechanisms to do new things safely

Process enhancement

- *Process enhancement* can be quite beneficial to an organization if it takes advantage of this capability when it is presented to it
- Many times, these processes are viewed through the eyeglasses of security, because that's the reason for the activity, but this is a perfect chance to enhance and improve upon the same processes to increase productivity
- When you look at many business processes taking place in all types of organizations, you commonly find a duplication of efforts, manual steps that can be easily automated, or ways to streamline and reduce time and effort that are involved in certain tasks.
- This is commonly referred to as *process reengineering*

Organizational Processes

- The processes we just covered are regular day-to-day ones.
- There are other processes that happen less frequently but may have a much more significant impact on the security posture of the organization:
  - ✓ **Mergers and Acquisitions**
  - ✓ **Divestitures**
  - ✓ **Governance Committees**

Mergers and acquisitions

- As companies grow, they often acquire new capabilities (e.g., markets, products, and intellectual property) by merging with another company or outright acquiring it
- *Mergers and acquisitions (M&A)* always take place for business reasons, but they almost always have significant cybersecurity implications
- Think of it this way: your company didn't acquire only the business assets of that other company it just purchased; it also acquired its security program and all the baggage that may come with it
- Suppose that during the M&A process you discover that the company that your company is acquiring has a significant but previously unknown data breach

Mergers and acquisitions (cont.)

- This is exactly what happened in 2017 when Verizon acquired Yahoo! and discovered that the latter had experienced two massive security breaches
- The acquisition went forward, but at a price that was $350 million lower than originally agreed
- One of the ways in which companies protect themselves during a merger or acquisition is by conducting extensive audits of the company they are about to merge with or acquire
- There are many service providers who now offer *compromise assessments*, which are in-depth technical examinations of a company's information systems to determine whether an undocumented compromise is ongoing or has happened in the past
- Another approach is to conduct an audit of the ISMS, which is more focused on policies, procedures, and controls

Divestiture

- A *divestiture*, on the other hand, is when your company sells off (or otherwise gets rid of) a part of itself
- There are many reasons why a company may want to divest itself of a business asset, such as having a business unit that is not profitable or no longer well aligned with the overarching strategy
- For cybersecurity professionals, a divestiture is when we have to answer tough questions from the buyer, and an M&A is when we are the ones asking the tough questions of someone else. They are two sides to the same coin.
- If your company is divesting assets for whose security you are responsible, you will probably work closely with the business and legal teams to identify any problem areas that might reduce the value of the assets being sold

Divestiture (cont.)

- For example, if there are any significant vulnerabilities in those assets, you may want to apply controls to mitigate the related risks
- If you discover a compromise, you want to eradicate it and recover from it aggressively
- A less obvious cybersecurity implication of divestiture is the need to segment the part or parts of the ISMS that involve the asset(s) in question
- Whoever is acquiring the assets will want to know what those are, and maybe even test them at a technical level
- You need to be prepared to be audited without revealing any proprietary or confidential information in the process
- Be sure to keep your legal team close to ensure you are responsive to what is required of you, but nothing else

Governance Committee

- The organizational processes we've described so far (M&A and divestitures) are triggered by a business decision to either acquire or get rid of some set of assets
- There is another key process that is ongoing in many organizations with mature cybersecurity practices
- A *governance committee* is a standing body whose purpose is to review the structures and practices of the organization and report its findings to the board of directors
- While it may sound a bit scary to have such a committee watching over everything you do, they can actually be your allies by shining a light on the tough issues that you cannot solve by yourself without help from the board
- It is important for you to know who is who in your organization and who can help get what you need to ensure a secure environment

Organizational Roles and Responsibilities

- Senior management and other levels of management understand the vision of the organization, the business goals, and the objectives
- The next layer down is the functional management, whose members understand how their individual departments work, what roles individuals play within the organization, and how security affects their department directly
- The next layers are operational managers and staff. These layers are closer to the actual operations of the organization
- They know detailed information about the technical and procedural requirements, the systems, and how the systems are used.

Organizational Roles and Responsibilities (cont.)

- The employees at these layers understand how security mechanisms integrate into systems, how to configure them, and how they affect daily productivity
- Every layer offers different insight into what type of role security plays within an organization
- Each layer should have input into the best security practices, procedures, and chosen controls to ensure the agreed-upon security level provides the necessary amount of protection without negatively affecting the company's productivity

Organizational Roles and Responsibilities (cont.)

- Although each layer is important to the overall security of an organization, some specific roles must be clearly defined
- Individuals who work in smaller environments (where everyone must wear several hats) may get overwhelmed with the number of roles presented next
- Many commercial businesses do not have this level of structure in their security teams, but many large companies, government agencies, and military units do
- What you need to understand are the responsibilities that must be assigned and whether they are assigned to just a few people or to a large security team

Organizational Roles and Responsibilities (cont.)

- These roles include:
  - ✓ executive management
  - ✓ security officer
  - ✓ data owner
  - ✓ data custodian
  - ✓ system owner
  - ✓ security administrator
  - ✓ supervisor (user manager)
  - ✓ change control analyst
  - ✓ data analyst
  - ✓ user
  - ✓ auditor
  - ✓ the guy who gets everyone coffee

Security policies, standards procedures, and guidelines

- Computers and the information processed on them usually have a direct relationship with a company's critical missions and objectives
- Because of this level of importance, senior management should make protecting these items a high priority and provide the necessary support, funds, time, and resources to ensure that systems, networks, and information are protected in the most logical and cost-effective manner possible
- It is important to make sure everyone is consistent regarding security at a level that meets the needs of the organization
- For a company's security plan to be successful, it must start at the top level and be useful and functional at every single level within the organization

Security Program

- A security program contains all the pieces necessary to provide overall protection to an organization and lays out a long-term security strategy
- A security program's documentation should be made up of security policies, procedures, standards, guidelines, and baselines
- Security policies, standards, guidelines, procedures, and baselines must be developed with a realistic view to be most effective
- It is important that an organization's security does not just look good on paper, but in action also

Security Policy

- A *security policy* is an overall general statement produced by senior management (or a selected policy board or committee) that dictates what role security plays within the organization
- A security policy can be an organizational policy, an issue-specific policy, or a system-specific policy
- In an *organizational security policy*, management establishes
  - ✓ how a security program will be set up
  - ✓ lays out the program's goals
  - ✓ assigns responsibilities
  - ✓ shows the strategic and tactical value of security
  - ✓ outlines how enforcement should be carried out

Organizational Security Policy

- This policy must address applicable laws, regulations, and liability issues and how they are to be satisfied
- The organizational security policy provides scope and direction for all future security activities within the organization
- It also describes the amount of risk senior management is willing to accept
- An organization will have many policies, and they should be set up in a hierarchical manner
- The organizational (master) security policy is at the highest level, with policies underneath it that address security issues specifically
- These are referred to as issue-specific policies

Issue-specific Policy

- An *issue-specific policy*, also called a *functional policy*
- Addresses specific security issues that management feels need more detailed explanation and attention to make sure a comprehensive structure is built and all employees understand how they are to comply with these security issues
- For example, an organization may choose to have an e-mail security policy
- The e-mail security policy outlines what management can and cannot do with employees' e-mail messages for monitoring purposes
- Specifies which e-mail functionality employees can or cannot use
- The e-mail security policy also addresses specific privacy issues

Issue-specific Policy (cont.)

- **Organizational policy:**
  - ✓ Acceptable use policy
  - ✓ Risk management policy
  - ✓ Vulnerability management policy
  - ✓ Data protection policy
  - ✓ Access control policy
  - ✓ Business continuity policy
  - ✓ Log aggregation and auditing policy
  - ✓ Personnel security policy
  - ✓ Physical security policy
  - ✓ Secure application development policy
  - ✓ Change control policy
  - ✓ E-mail policy
  - ✓ Incident response policy

System-specific Policy

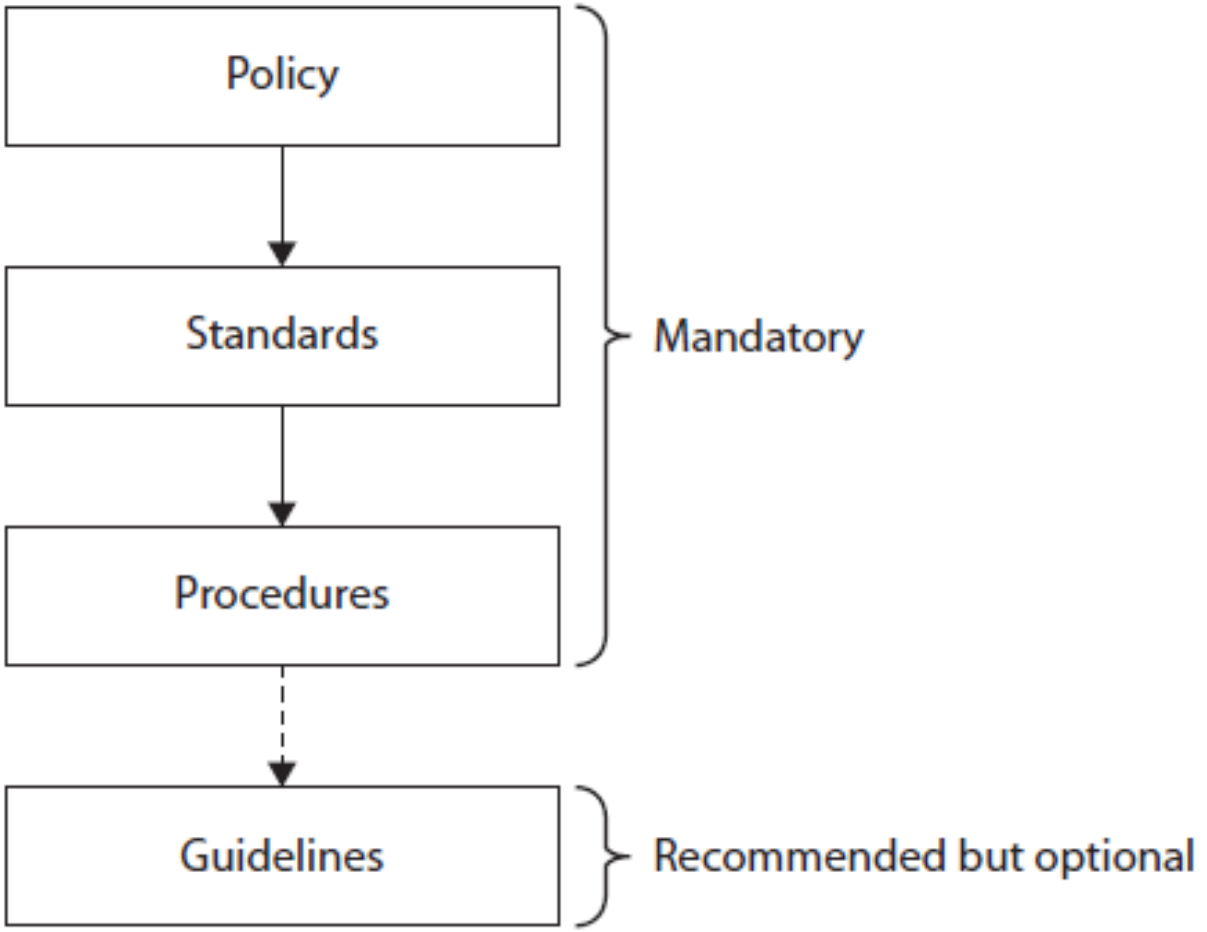
- A *system-specific policy* presents the management's decisions that are specific to the actual computers, networks, and applications
- An organization may have a system-specific policy outlining
  - ✓ how a database containing sensitive information should be protected
  - ✓ who can have access
  - ✓ how auditing should take place
- It may also have a system-specific policy outlining
  - ✓ how laptops should be locked down and managed
- This policy type is directed to one or a group of similar systems and outlines how they should be protected
- Much more granularity is needed to actually support the policy, and this happens with the use of procedures, standards, guidelines, and baselines

Standards

- *Standards* refer to mandatory activities, actions, or rules
- Standards describe specific requirements that allow us to meet our policy goals
- Standards are unambiguous, detailed, and measurable
- Organizational security standards may specify how hardware and software products are to be used
- Can also be used to indicate expected user behavior
- Provide a means to ensure that specific technologies, applications, parameters, and procedures are implemented in a uniform (standardized) manner across the organization
- Organizational standards may require that all employees use a specific smart card as their access control token, that its certificate expire after 12 months, and that it be locked after three unsuccessful attempts to enter a personal identification number (PIN)

Policy, Standard, Procedure and Guideline

- Policies are implemented through standards, procedures, and guidelines.



Baselines

- The term *baseline* refers to a point in time that is used as a comparison for future changes
- Once risks have been mitigated and security put in place, a baseline is formally reviewed and agreed upon, after which all further comparisons and development are measured against it
- A baseline results in a consistent reference point
- Baselines are also used to define the minimum level of protection required
- In security, specific baselines can be defined per system type, which indicates the necessary settings and the level of protection being provided
- For example, a company may stipulate that all accounting systems must meet an Evaluation Assurance Level (EAL) 4 baseline

Guidelines

- *Guidelines* are recommended actions and operational guides to users, IT staff, operations staff, and others when a specific standard does not apply
- Guidelines can also be used as a recommended way to achieve specific standards when those do apply
- Guidelines can deal with the methodologies of technology, personnel, or physical security
- Life is full of gray areas, and guidelines can be used as a reference during those times
- Whereas standards are specific mandatory rules, guidelines are general approaches that provide the necessary flexibility for unforeseen circumstances

Procedures

- *Procedures* are detailed step-by-step tasks that should be performed to achieve a certain goal
- Many organizations have written procedures on
  - ✓ how to install operating systems
  - ✓ configure security mechanisms
  - ✓ implement access control lists
  - ✓ set up new user accounts
  - ✓ assign computer privileges
  - ✓ audit activities
  - ✓ destroy material
  - ✓ report incidents
  - ✓ and much more….
- Procedures are considered the lowest level in the documentation chain and provide detailed steps for configuration and installation issues

Implementation Example

- Let's walk through an implementation example
- A corporation's security *policy* indicates that confidential information should be properly protected
- Policy states the issue in very broad and general terms
- A supporting *standard* mandates that all customer information held in databases must be encrypted with the Advanced Encryption Standard (AES) algorithm while it is stored and that it cannot be transmitted over the Internet unless IPSec encryption technology is used
- The standard indicates what type of protection is required and provides another level of granularity and explanation

Implementation Example (cont.)

- The supporting *procedures* explain exactly how to implement the AES and IPSec technologies
- *Guidelines* cover how to handle cases when data is accidentally corrupted or compromised during transmission.
- Once the software and devices are configured as outlined in the procedures, this is considered the *baseline* that must always be maintained
- All of these work together to provide a company with a security structure
- Unfortunately, security policies, standards, procedures, baselines, and guidelines often are written because an auditor instructed a company to document these items, but then they are placed on a file server and are not shared, explained, or used. To be useful, they must be put into action

Review

- The objectives of security are to provide confidentiality, integrity, availability, authenticity, and nonrepudiation.
- Confidentiality means keeping unauthorized entities (be they people or processes) from gaining access to information assets.
- Integrity means that keep an asset is free from unauthorized alterations.
- Availability protection ensures reliability and timely access to data and resources to authorized individuals.
- Authenticity protections ensure we can trust that something comes from its claimed source.
- Nonrepudiation, which is closely related to authenticity, means that someone cannot disavow being the source of a given action.

Review (cont.)

- A vulnerability is a weakness in a system that allows a threat source to compromise its security.
- A threat is any potential danger that is associated with the exploitation of a vulnerability.
- A threat source (or threat agent, or threat actor) is any entity that can exploit a vulnerability.
- A risk is the likelihood of a threat source exploiting a vulnerability and the corresponding business impact.
- A control, or countermeasure, is put into place to mitigate (reduce) the potential risk.
- Security governance is a framework that provides oversight, accountability, and compliance.

Review (cont.)

- An information security management system (ISMS) is a collection of policies, procedures, baselines, and standards that an organization puts in place to make sure that its security efforts are aligned with business needs, streamlined, and effective and that no security controls are missing.
- An enterprise security architecture (ESA) implements an information security strategy and consists of layers of solutions, processes, and procedures and the way they are linked across an enterprise strategically, tactically, and operationally.
- An ESA should tie in strategic alignment, business enablement, process enhancement, and security effectiveness.
- Senior management always carries the ultimate responsibility for the organization.

Review (cont.)

- Security governance is a framework that supports the security goals of an organization being set and expressed by senior management, communicated throughout the different levels of the organization, and consistently applied and assessed.
- A security policy is a statement by management dictating the role security plays in the organization.
- Standards are documents that describe specific requirements that are compulsory in nature and support the organization's security policies.
- A baseline is a minimum level of security.
- Guidelines are recommendations and general approaches that provide advice and flexibility.
- Procedures are detailed step-by-step tasks that should be performed to achieve a certain goal.