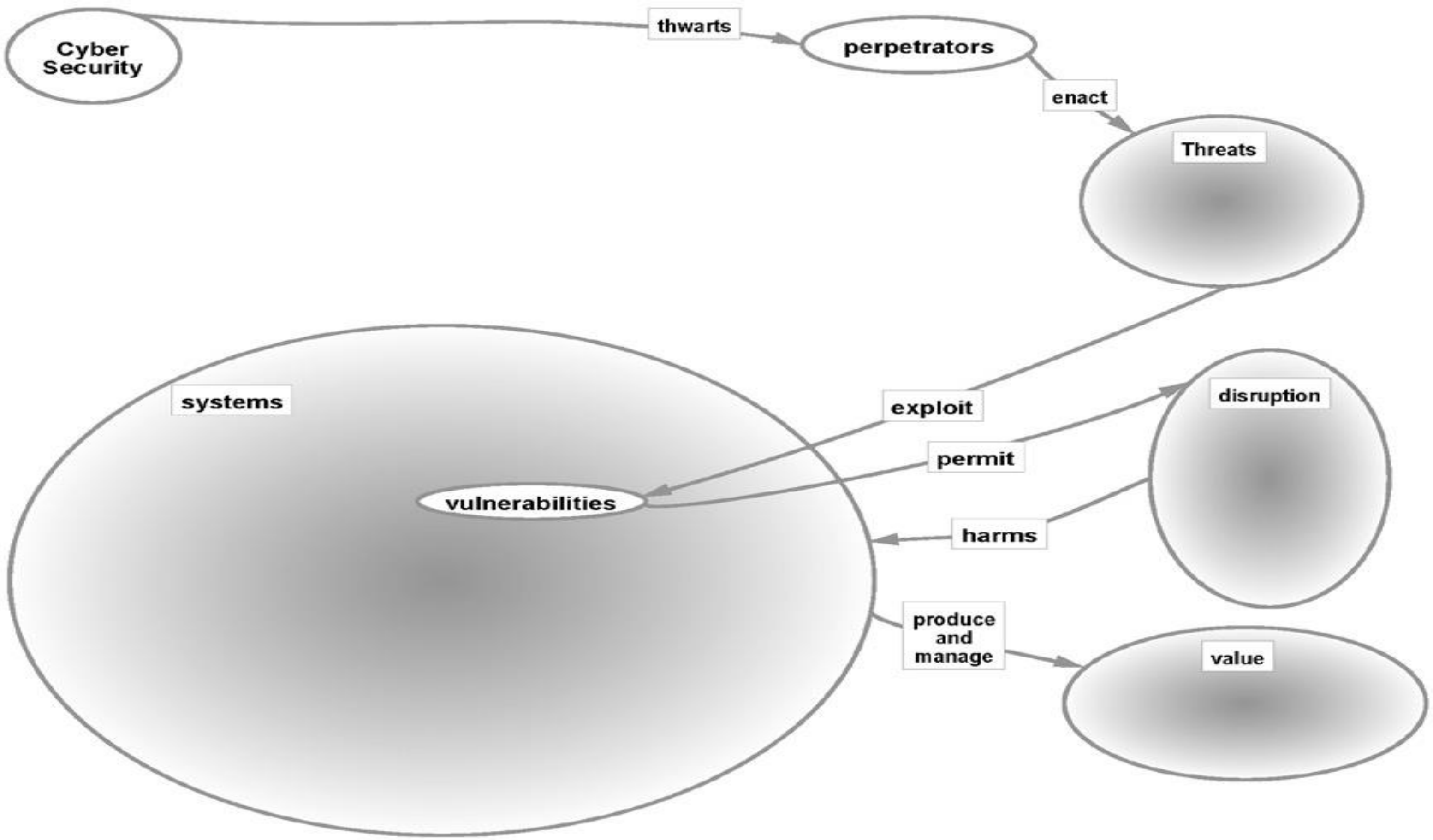
# UNIT-2

# Cyber Security Objectives

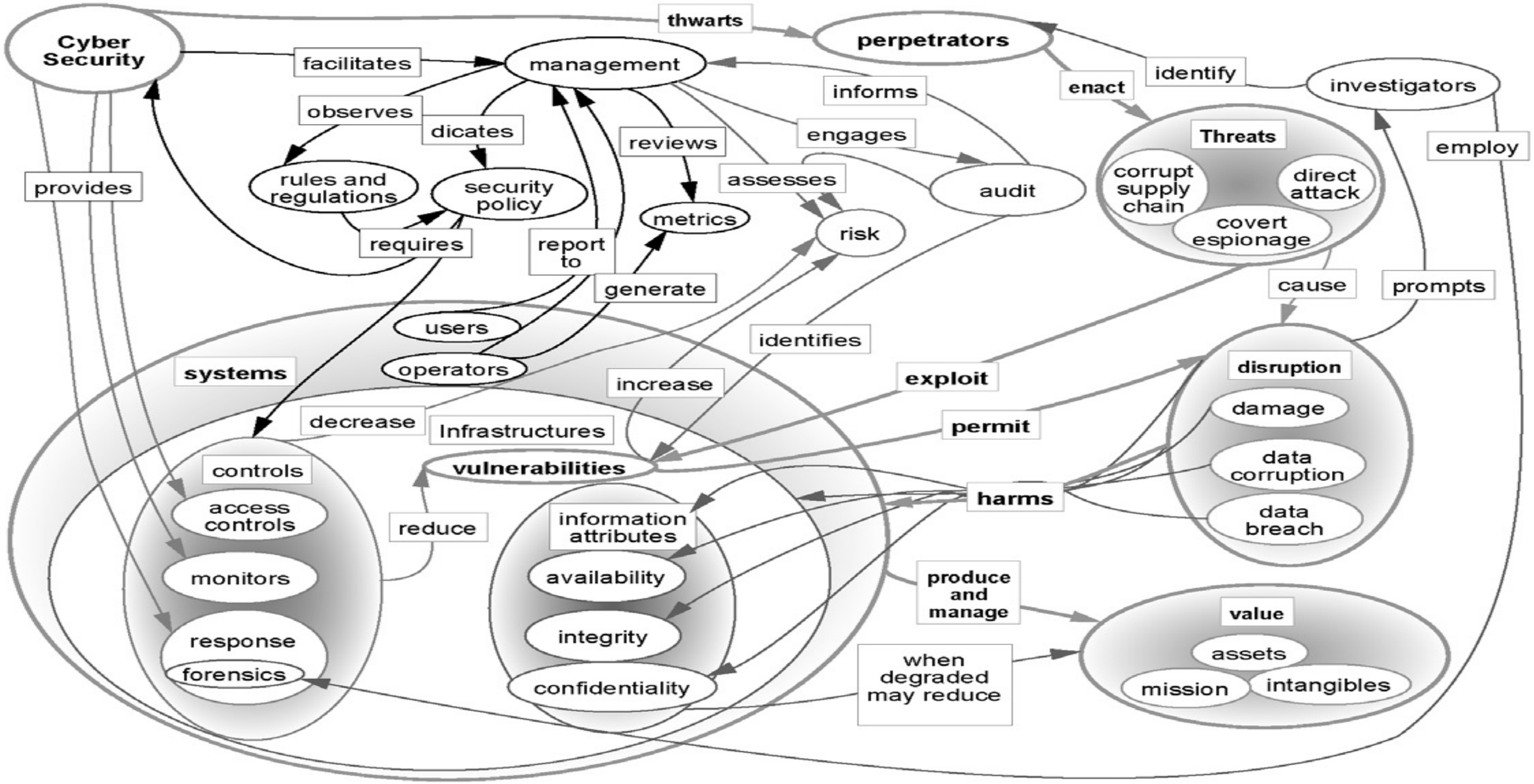
- Measurement is the process of mapping from the empirical world to theformal, relational world.
- Combinations of measures corresponding to an elusive attribute are considered derived measures and are subject to interpretation in the context of an abstract model of the thing to be measured (ISO/IEC 2007).
- *Metrics* is a generic term that refers to the set ofmeasures that characterize a given field.
- Cyber security is not the direct object of measurement, nor a well-enough-understood attribute of a system to easily define derived measures or metrics.
- So those engaged in cyber security metrics are measuring other things and drawing conclusions about security goal achievement from them.
- this challenge has spawned a field of study called security metrics (Jaquith and Geer 2005).
- Metrics in physical security traditionally have concentrated on the ability of a system to meet the goal of withstanding a design basis threat (DBt)
- A DBt describes characteristics of the most powerful andinnovative adversary that it is realistic to expect to protect against.
- Adopting a DBt approach to security implies that the strength of security protection required by a system should be calculated with respect to atechnical specification of how it is likely to be attacked.
- If the DBt is a force of 20 people with access to explosives of a given type, then the strength of the physical barriers to unauthorized entry must withstand the ton of force that these 20 people could physically bring into system contact.
- To achieve this:
- Barrier protection mate- rials are specified, threat delay and response systems are designed, and validation tests are conducted accordingly.

Security systemigram mainstay.



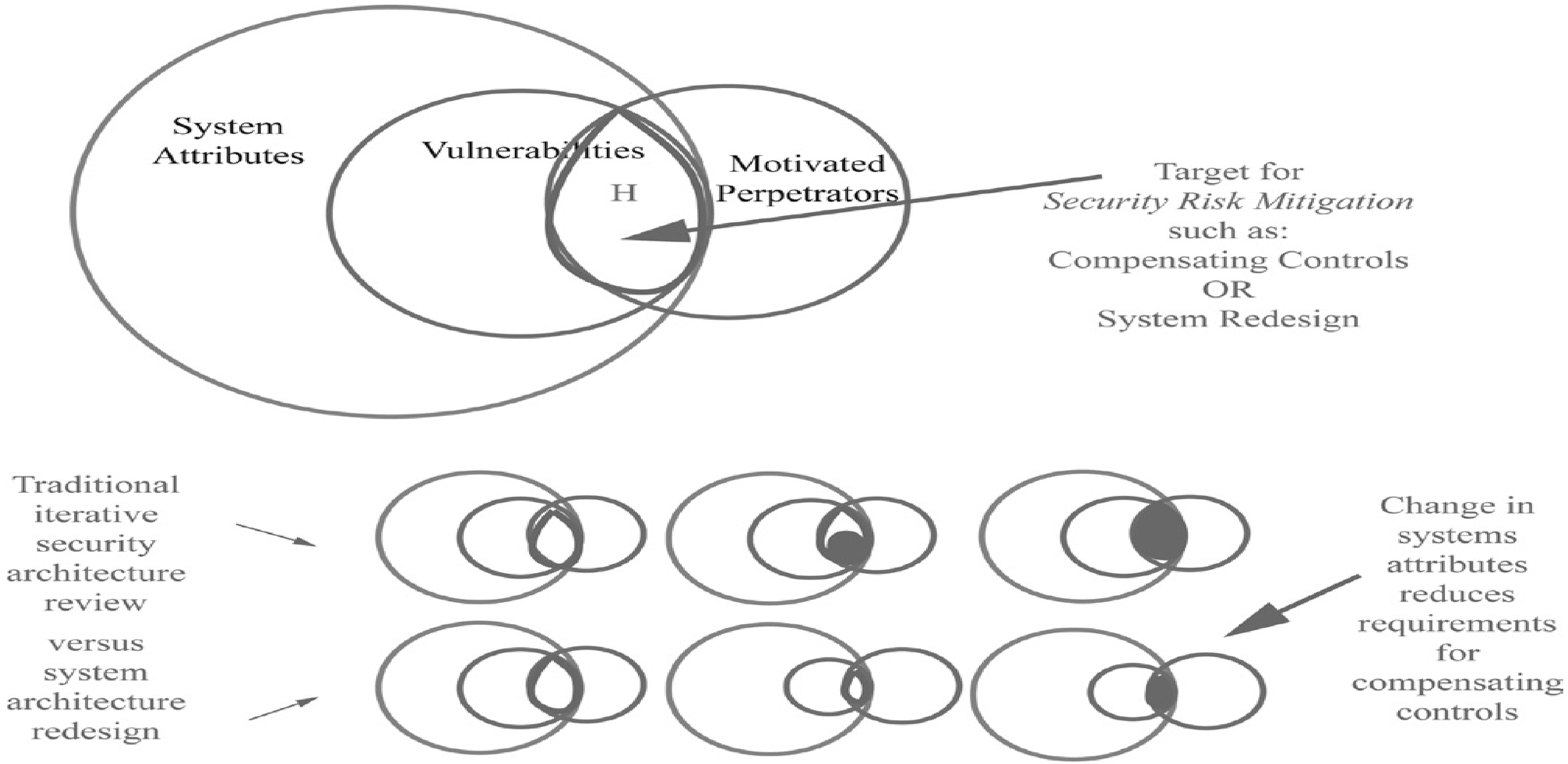
- In cyber security, the terms perpetrator, threat, exploit, and vulnerability are terms of the trade, their meaning is distinct and interrelated.
- a perpetrator is an individual or entity.
- threat is a potential action that may or may not be committed by a perpetrator.
- An exploit refers to the technical details that comprise an attack.
- A vulnerability is a system characteristic that allows an exploit to succeed.
- the mainstay of the systemigram of Figure 3.1 is read as, “Security thwarts perpetrators who enact threats that exploit system vulnerabilities to cause damage that adversely impacts value”
- As each type of system vulnerability reached the stage of security community awareness, a corresponding set of security countermeasure technologies came to the market, and became part of an ever-increasing number of best practice recommendations.
- Countermeasures were applied to vulnerable system components, and threats to systems were assumed to be covered by the aggregated result of implementing all of them.

# Full security systemigram.



- Illustrates the difference between this traditional approach to security architecture and a more holistic, system-level approach.
- It depicts vulnerable attributes of a system as a subset of system attributes, and perpetrator targets as a subset of the system’s vulnerable attributes.
- traditionally, security engineering has attacked this problem with security-specific components, dero these are often labeled “compensating controls,” which is a technical term in the auditthat refers to management controls that are devised because the system itself has no controls that would minimize damage were the vulnerability to be exploited.
- Boltons are by definition work-arounds that are not part of the system itself, Such as Firewalls.
- the lowerpart of Figure 3.3 illustrates the contrast between a bolt-on approach to solving security problems and a security design approach that instead isexpected to alter system-level attributes to eliminate or reduce vulnerability.

# Bolt-on versus design



Target for *Security Risk Mitigation* such as: Compensating Controls OR System Redesign

Traditional iterative security architecture review

versus system architecture redesign

Change in systems attributes reduces requirements for compensating controls

Area of vulnerability is either reduced, or covered with security-specific bolt-ons.

# Example of cyber security metrics.

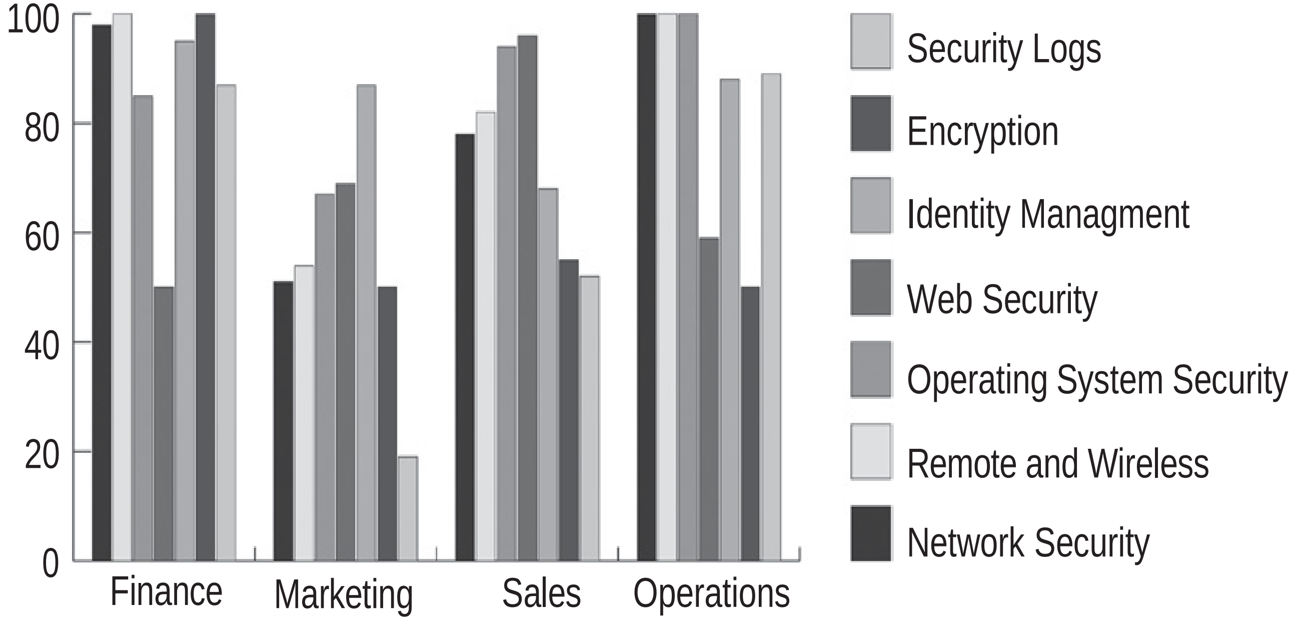


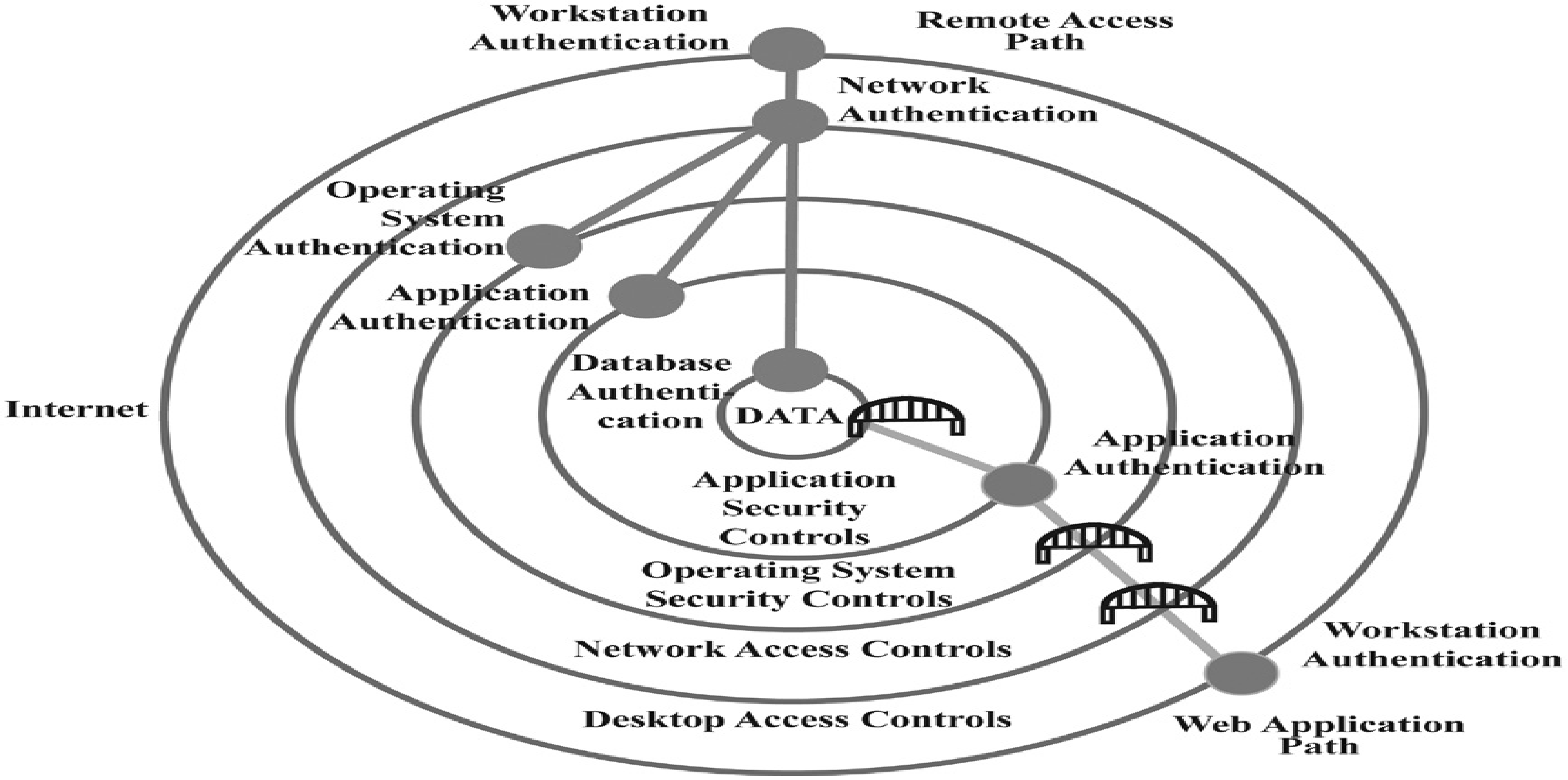
**Figure 3.4** Example of cyber security metrics.

# Security Management Goals

- All information Security measures try to agree at least one goals
- Protection of confidentiality of data
- Preserve integrity of data
- Promote the availability of data

- Security programs that are motivated by regulatory compliance are not specifically designed to achieve organizational goals for security, but instead are designed to demonstrate compliance with security management standards.
- the standards themselves have become de facto security metrics taxonomies that cross organizational borders.
- Practitioners are often advised to organize their metrics around the requirements in security management standards against which they may expect to be audited (Herrmann 2007; Jaquith 2007).
- there is even an international standard for using the security management standards to create security metrics (ISO/ IEC 2009b).
- the disadvantage to this type of approach to security management is that details of standards compliance are seen as isolated technology configurations to be mapped to a pre-established scorecard.
- None of these standards comprise a generally accepted method of directly measur ing security in terms of achievement in thwarting threats (King 2010).
- For example, individuals who have changed jobs sometimes measure the security at the old and new firms in terms based on the degree of difficulty for them to access important data and information, both locally and remotely.
- Like they may identify the number of passwords they have to use from their desktops at home to access customer data in the office, and decide that the firm that makes them use more authentication factors is more secure.
- *Term as defense in depth.*
- Figure 3.5 shows this type of layered-defense depiction of system security.

A layered defense


Workstation Authentication
Remote Access Path
Network Authentication
Operating System Authentication
Application Authentication
Database Authentication
DATA
Internet
Application Authentication
Application Security Controls
Operating System Security Controls
Network Access Controls
Desktop Access Controls
Workstation Authentication
Web Application Path

- Figure 3.5 provides a layered perspective on a typical network.
- It has multiple security “layers,” as described in thecentral lower part of the diagram.
- At the top of the diagram, the “Remote Access” user is illustrated as being required to authenticate a workstation, which may or may not be controlled by the enterprise. the user then authenticates via the Internet to the enterprise network.
- From the network access point, the remote user can directly authenticate to any of the other layers in the internal network.
- this is why remote access typically requires a higher level of security, because once on the internal network, there are a variety of choices for platform access.

# Web Applications Path

- In the case of the web application, the existence of the layers does not actually constitute defense in depth. this is because such Internet accessible applications are usually accessible with just one log-in.
- A user then can access the application without authenticating to the network because the firewall allows anyone on the Internet to have directaccess to the login screen of the application on the web server.
- Once within the application, the data authentication layer is not presented to the user; the application automatically connects to it on behalf of the user.
- Bridges Are used to depict through the layers that the remote user would have to authenticate to pass, but the application user does not. Hence, to apply the term defense in depth tothis case would be a misnomer.
- Figure 3.6, it is recommended that security metrics be raised to consider business-level requirements for security.
- However, there is an issue with this approach. It is that there is currently no convergence around a *single* organizational management structure for security, so there can be no corresponding authoritative business-levelsecurity metrics taxonomy.
- Instead, there has been a great deal of consensus around standards for security process (ISO/IEC 2005; ISO/IEC 2005; ISACA 2007; ISF 2007; Ross, Katzke et al. 2007).
- the NIST report also suggested a classification of security metrics into leading, concurrent, and lagging indicators of security effectiveness.
- An example of a leading indicator is a positive assessment of the security of a system thatis about to be deployed.
- Concurrent indicators are technical target metricsthat show whether security was currently configured correctly or not.
- Lagging indicators would be discovery of past security incidents due to inadequate security requirements definition, or failures in maintaining specified configurations.

- If the goal is to know the current state of system security, concurrent indicators would make better metrics.
- Recommendations for security metrics often suggest a hierarchical metrics structure where business process security metrics are at the top.
- the next level includes support process metrics like information secu- rity management, business risk management, and technology products andservices.
- Each leaf-level measure is combined with its peers to provide an aggregation measure that deter- mines the metric above them in the hierarchy.
- the average percentage target goals achieved in each subset for the four business areas would be called the “Product Security” and “Service Security” metrics, respectively.
- the average of those two would be the “technology Security”metric.
- this method of measurement is still verification that the design for security was implemented (or not) as planned, rather than validation that the top-level security goals are met via the process of decomposition and measures of leaf performance.

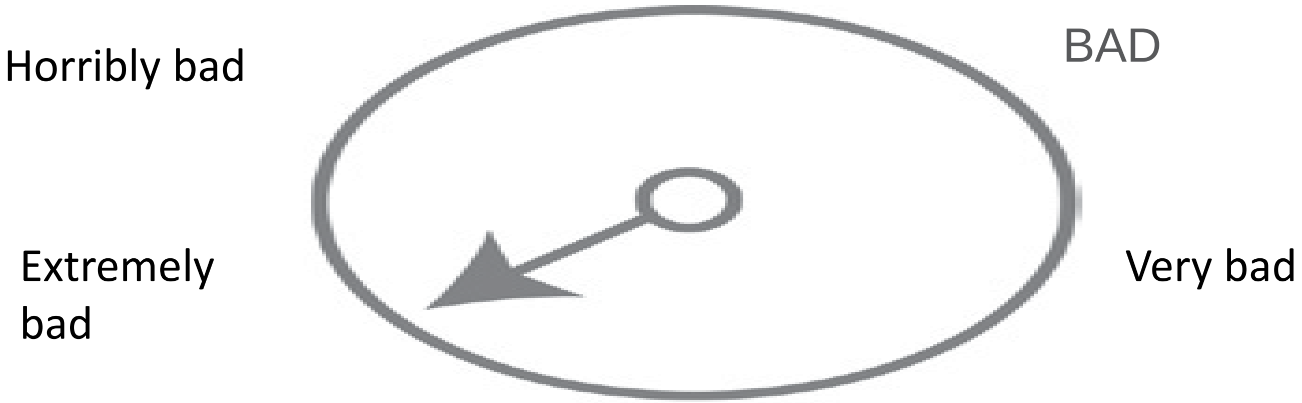
# Counting Vulnerabilities

- In computer system, vulnerability is a weakness which can be exploited by threat actor, such as an actors, to perform unauthorized action within the system.
- To Exploit vulnerability Attackers must have at least one tool or technique that can connect to a system weakness.in this frame vulnerability is also known as attack surface.
- Vulnerability management is a cyclic practice of identifying, classifying, remediating and mitigating vulnerability. This practice generally referred to as software vulnerability of computing system.
- A Security Risk is often incorrectly classified as a vulnerability.
- The window of vulnerability is the time from when the security hole was introduced in deployed software, to when access was removed, a security fix was available/deployed, or the attackers was disabled-Zero Day attack.
- A notable exception to technology management approach to security metrices, though still one does not directly measures security, is vulnerability and threat focus.
- This is the enumeration of system vulnerability and misuse techniques.
- NIST and MITRE encouraged a consortium of security product vendors and practitioners to contribute to an endlessly growing repository of structured data describing known software vulnerabilities in a project known as the National vulnerability Database (NVD)

- the first *Common Vulnerability Enumeration* (CVE) waspublished in 1997 (MITRE ongoing).
- this provided some standard by whichsecurity protection efforts would be judged to be effective by providing a “to-fix” list.
- Just listing the vulnerabilities that allowed malware to work did not address the concern that malware had to be identified in order for it to be eradicated,
- in 2004, the CVE was followed with a *Common Malware Enumeration*(CME) that catalogs malware that exploits vulnerabilities.
- This facilitates the development of automated methods to detect and eradicate malware.
- the MITRE NVD data was extended in 2006 to include the *Common Weakness Enumeration* (CWE), which is a list of software developmentmistakes that are made frequently and commonly result in vulnerabilities.
- An example of a specific issue would be the identification of a softwaresecurity flaw that appears on the “Never-Events” list.
- the list is a metaphorical reference to the National Quality Forum’s (NQF) medical Never- Events list.
- that list includes medical mistakes that are serious, largely preventable, and of concern to both the public and health- care providers for the purpose of public accountability such as leaving asurgical instrument in a patient.
- the software integrity version of the Never- Events list is the list of the top 25 mistakes software developers make that introduce security flaws.
- *SQL Injection* in the metric example for this category refers to one of those never-events.
- An SQL-injection mistake allows database commands to be entered by web page users in such a way that the users have the ability to execute arbitrarydatabase queries that provide them with information that the application is not designed to allow them to access.
- SQL injections is a code injection technique that might destroy database.
- SQL injections is most common web hacking technique.
- SQL injections is a placement of malicious code in SQL Statement via web page input.

- the metric is the number of applications that allow SQL injection tooccur.
- to cover the possibility that some system access feature may have been intended, but nevertheless introduces a security vulnerability.
- in 2009, NIST introduced a *Common Misuse Scoring System*, which provides a method to measure the severity of software “trust” flaws by correlating them with estimates of negative impact.
- All types of vulnerabilities in the NVD are used to create security metrics by using them as a checklist and checking a technology environment tosee if they exist.
- this database is also used by security software vendors used to create a set of test cases for vulnerabilities against which securitysoftware should be effective.
- these are not only anti-malware vendors, butvendors of software vulnerability testing software.
- . Penetration tests of the type used by malicious hackers (also known as “black hats” in reference to old Western movies where the heroes always wore white hats) are designed by cyber security analysts (“white hats”) to exploit any and all of the vulnerabilities in the NVD.
- they are automated so they can be run from a console. the security metric is usually the inverse of the percentage of machines in inventory that test positive for any of the vulnerabilities in the database.
- If a stated security goal is to have no known vulnerabilities, this type of test may seem to provide a good cyber security metric.
- these metrics will necessarily miss the zero-day attack, and so, if a complete technology inventory test for all the known NVD vulnerabilities was passed with flying colors, then this would not mean that the system was secure.
- It could simply mean that *if* the system had security bugs and flaws, those bugs andflaws were not yet identified.
- As one software security expert puts it, they are a *badness-ometer* (McGraw 2006). As illustrated in Figure 3.7, these types of measures can provide evidence that security is bad, but there is no number on the scale that would show security is good.

Security badness-ometer. *Source*: McGraw (2006).



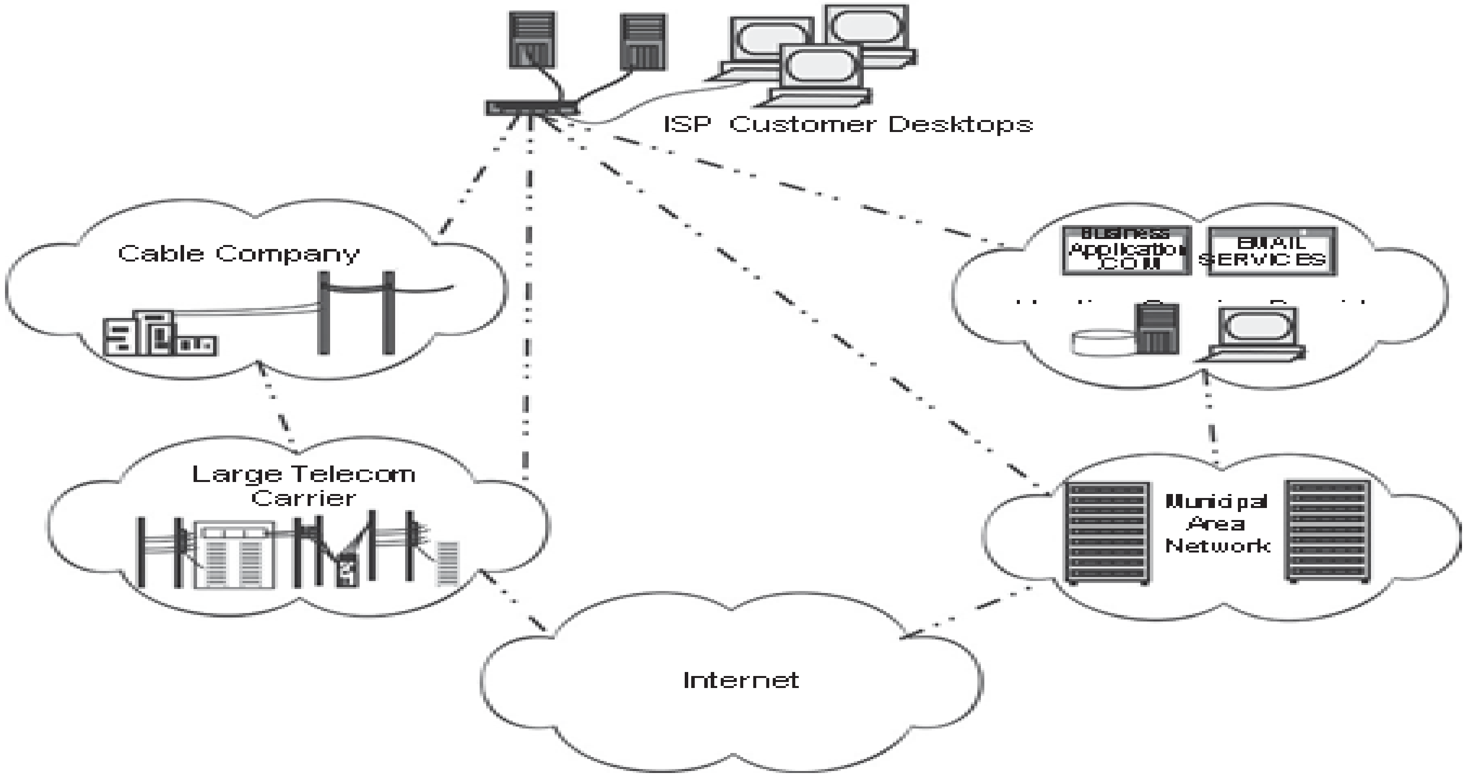
# Security Frameworks

- Goals for cyber security, and methods to achieve those goals, will vary considerably with the framework within which cyber components operate.
- e-commerce systems generically as a frame- work in order to contrast it with other types of frameworks.
- so we first chose e-commerce systems and then follow with two at opposite ends of the spectrum for illustration purposes: ICSs and personal mobile devices.

# e-Commerce Systems

- e-Commerce systems are Internet-facing systems that allow facilitative transactions. the word itself is short for of the now obvious adjective, “electronic,” as in “electronic commerce.”
- e-Commerce has matured to the point where many retailers only exist online, and many brands are only available via online stores and businesses.
- In addition to traditional customer-to-business relationships (C2B), e-Commerce also includes business-to-business (B2B) transactions conducted between manufacturers, suppliers, distributors, and retail stores.
- e-Commerce systems are called “Internet facing” because they are designed to be directly reached by any other system on the Internet.
- In order to be Internet facing, a system must be connected to an Internet service provider (ISP).
- ISP is a generic term for different types of companies that provide Internet connectivity services.
- they may be a local cable company, a large telecommunications carrier, a municipal network operator, or a web hosting service provider.
- the common element of the service is that network traffic between the customer and the Internet traverses the ISP.

# e-Commerce system environment

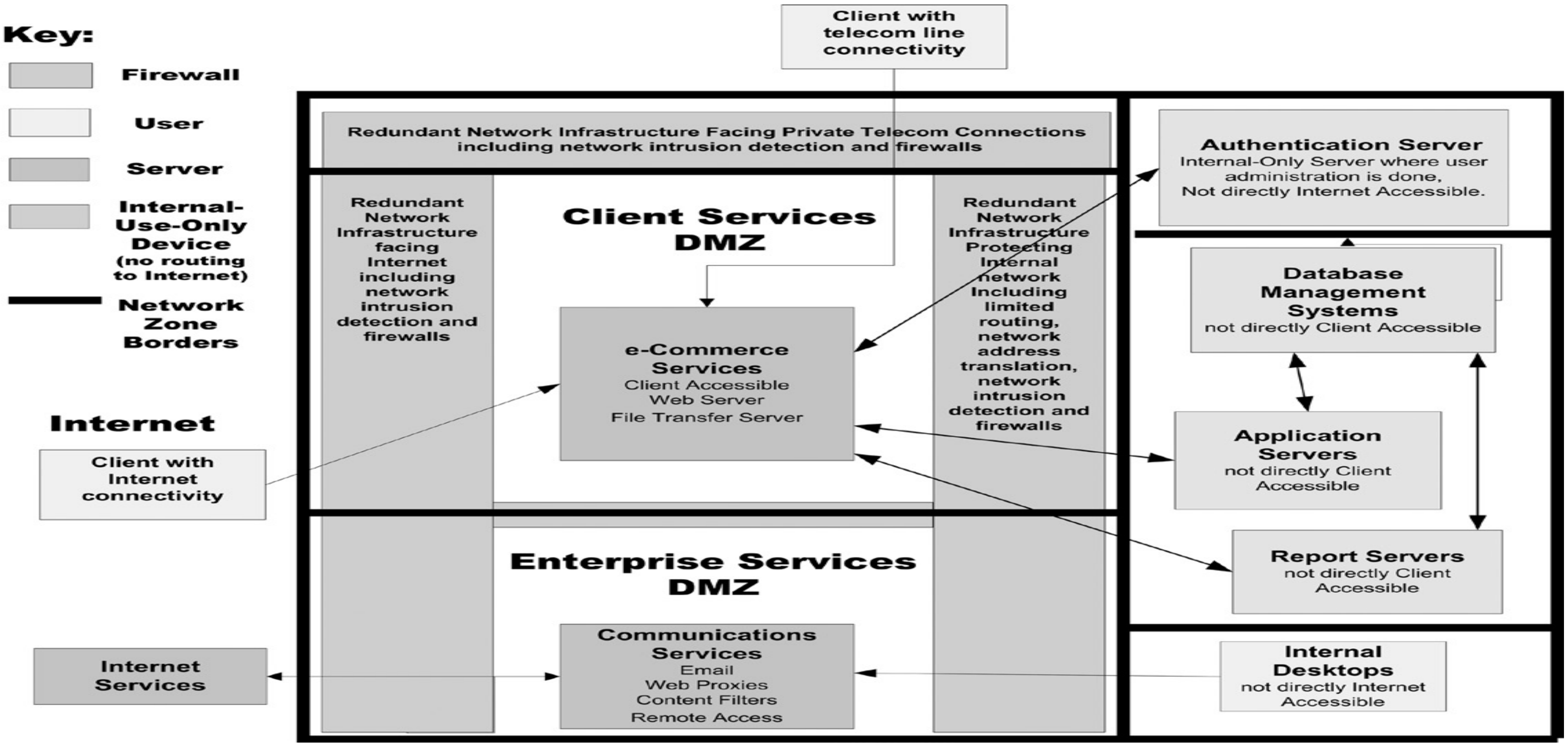


- Illustrates a few alternate ISP connections in the context of the Internet as a whole.
- Because of the large numbers of systems that must be represented in any diagram of the Internet, the Internet itself is depicted in Network diagrams as a cloud.
- the cloud symbol has been in use since the 1970s and in no way is meant to refer to the subset of Internet services that today utilize the word “cloud” as a marketing term.
- the connection from the customer to the hosting service provider is not itself a direct Internet connection. Rather, it is facilitated by a telephone line, cable, or wireless link that becomes a conduit to the Internet through the hosting provider network.
- this line is typically leased from a large telecommunications carrier, but that carrier is not the ISP for the customer; the hosting service provider connects the customer to the Internet via their own relationship with a telecommunications carrier.
- Where a hosting service provider and a client have offices in the same building, they may just arrange for a wire to connect their equipment through a wall or ceiling duct.
- the diagram is meant to illustrate that there is no single type of company that provides Internet service.
- Different companies will offer different types of services, including cyber security services, to its customers.
- Some types of cyber security services, such as denial of service attack mitigation, may only be possible to perform as an add-on to a carrier service.
- Others, such as mail spam filtering, may only be possible to perform as an add-on to a hosting service.
- Hence, the way a system connects to the Internet may constrain its options for cyber security.
- Once Internet is connectivity established, a typical e-commerce system will follow the general architecture of Figure 3.9.

- there will be firewalls between the enterprise border and any external network.
- All computers that face the Internet will be enclosed within an isolated network zone.
- Any security-critical system will be connected to an internal network zone with no direct routing to external networks.
- user desktops will also typically be segregated into their own network zone.
- various security technologies will be placed at network zone interfaces to facilitate tasks such as remote access to the internal network, intrusion detection, and communications monitoring.
- Different companies will offer different types of services, including cyber security services, to its customers.
- Some types of cyber security services, such as denial of service attack mitigation, may only be possible to perform as an add-on to a carrier service.
- Others, such as mail spam filtering, may only be possible to perform as an add-on to a hosting service.
- Hence, the way a system connects to the Internet may constrain its options for cyber security.
- Once Internet is connectivity established, a typical e-commerce system will follow the general architecture of Figure 3.9.

- there will be firewalls between the enterprise border and any external network.
- All computers that face the Internet will be enclosed within an isolated network zone.
- Any security-critical system will be connected to an internal network zone with no direct routing to external networks.
- user desktops will also typically be segregated into their own network zone.
- various security technologies will be placed at network zone interfaces to facilitate tasks such as remote access to the internal network, intrusion detection, and communications monitoring.

# e-Commerce system architecture.



**Key:**

Firewall

User

Server

Internal-Use-Only Device (no routing to Internet)

Network Zone Borders

**Internet**

Client with Internet connectivity

Internet Services

Client with telecom line connectivity

Redundant Network Infrastructure Facing Private Telecom Connections including network intrusion detection and firewalls

Redundant Network Infrastructure facing Internet including network intrusion detection and firewalls

**Client Services DMZ**

**e-Commerce Services**
Client Accessible
Web Server
File Transfer Server

Redundant Network Infrastructure Protecting Internal network Including limited routing, network address translation, network intrusion detection and firewalls

**Enterprise Services DMZ**

**Communications Services**
Email
Web Proxies
Content Filters
Remote Access

**Authentication Server**
Internal-Only Server where user administration is done,
Not directly Internet Accessible.

**Database Management Systems**
not directly Client Accessible

**Application Servers**
not directly Client Accessible

**Report Servers**
not directly Client Accessible

**Internal Desktops**
not directly Internet Accessible

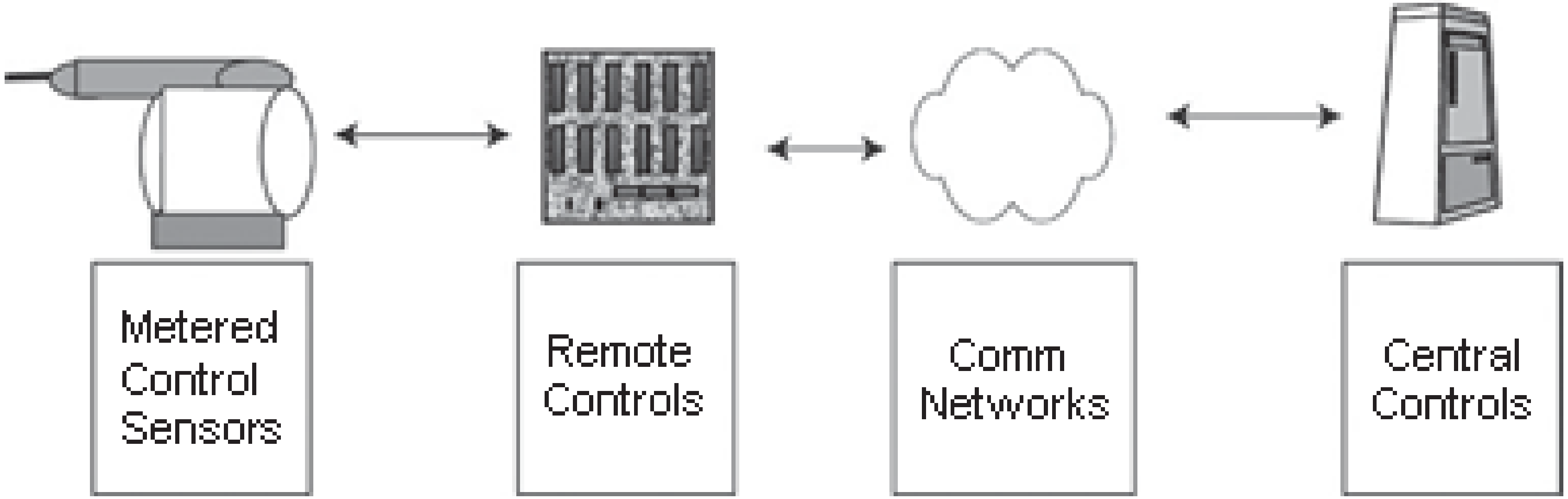
- It is also the case that providers of frequently used website features, such as store locators or news releases, will allow their software to be used for free in return for being able to advertise to the customers of the original vendor's site.
- Scenarios where the user experiences a composite of e-commerce websites are sometimes referred to as mashups.
- A mashup is a website wherein multiple companies' e-commerce services are combined into a single web page under the heading of a single e-commerce vendor.
- the purpose of an e-commerce system is usually to provide continuous transactions for customers on Internet-facing servers, while simultaneously facilitating the business transactions received from the Internet with robust and reliable transaction execution. Security features that facilitate this purpose include, but are not limited to:
- **System redundancy**—if one system goes down, another takes its place.
- **System diversity**—if one system is vulnerable to an attack in progress, transactions it supports can be supported with alternative technology.
- **System integrity**—systems are not changed unless there is a well-defined and tested plan to maintain service continuity while the system under- goes change.
- **transaction accountability**—counterparties are identified in a manner that does not allow them to repudiate their activity on the e-commerce site.
- that these four security features, if accomplished, would be sufficient to support an overall goal of transaction security.
- validation rather than verification metrics.
- validation of security goals requires measurements of the system in the context of its operation rather than measures of the system conformance to security specification.
- It has been our observation that everyone's first instinct in proposing security validation metrics is to measure successful attacks or intrusions.

- For example, in the book, *How to Measure Anything*, the author suggests that security goals be measured by the absence of successful virus attacks.
- the process described in the book is to start with what you know, structure that knowledge, identify what you would like to know, and use the structured data you have to reduce uncertainty concerning your object of measure.
- the suggested metric of “absence of successful virus attacks” suffers the fatal flaw that it measures progress toward a goal by the absence of an event rather than by any positive indicator that the goal is met.
- using this approach, a system that is rarely attacked will be judged to be more secure than another simply because its security has not often been tested.

## Industrial Control Systems

- ICSs operate the industrial infrastructures worldwide including electric power, water, oil/gas, pipelines, chemicals, mining, pharmaceuticals, transportation, and manufacturing.
- ICSs measure, control, and provide a view of the physical process ICSs monitor sensors and automatically move physical machinery such as levers, valves, and conveyor belts. When most people think of cyberspace, they think of Internet-enabled applications and corresponding information technology (It).
- ICSs also utilize advanced communication capabilities and are networked to improve process efficiency, productivity, regulatory compliance, and safety.
- When an ICS does not operate properly, it can result in impacts ranging from minor to catastrophic. Consequently, there is a critical need to ensure that electronic impacts do not cause, or enable, operation of ICSs.
- A typical ICS is composed of a control center that will house the human–machine interface (HMI), that is, the operator displays.
- these are generally Windows-based workstations. Other typical components of an ICS control center include Supervisory Control and Data Acquisition (SCADA) and Distributed Control Systems (DCSs).
- the control center communicates to the remote field devices over communication networks using proprietary communication protocols.

# Industrial control system framework



Metered Control Sensors

Remote Controls

Comm Networks

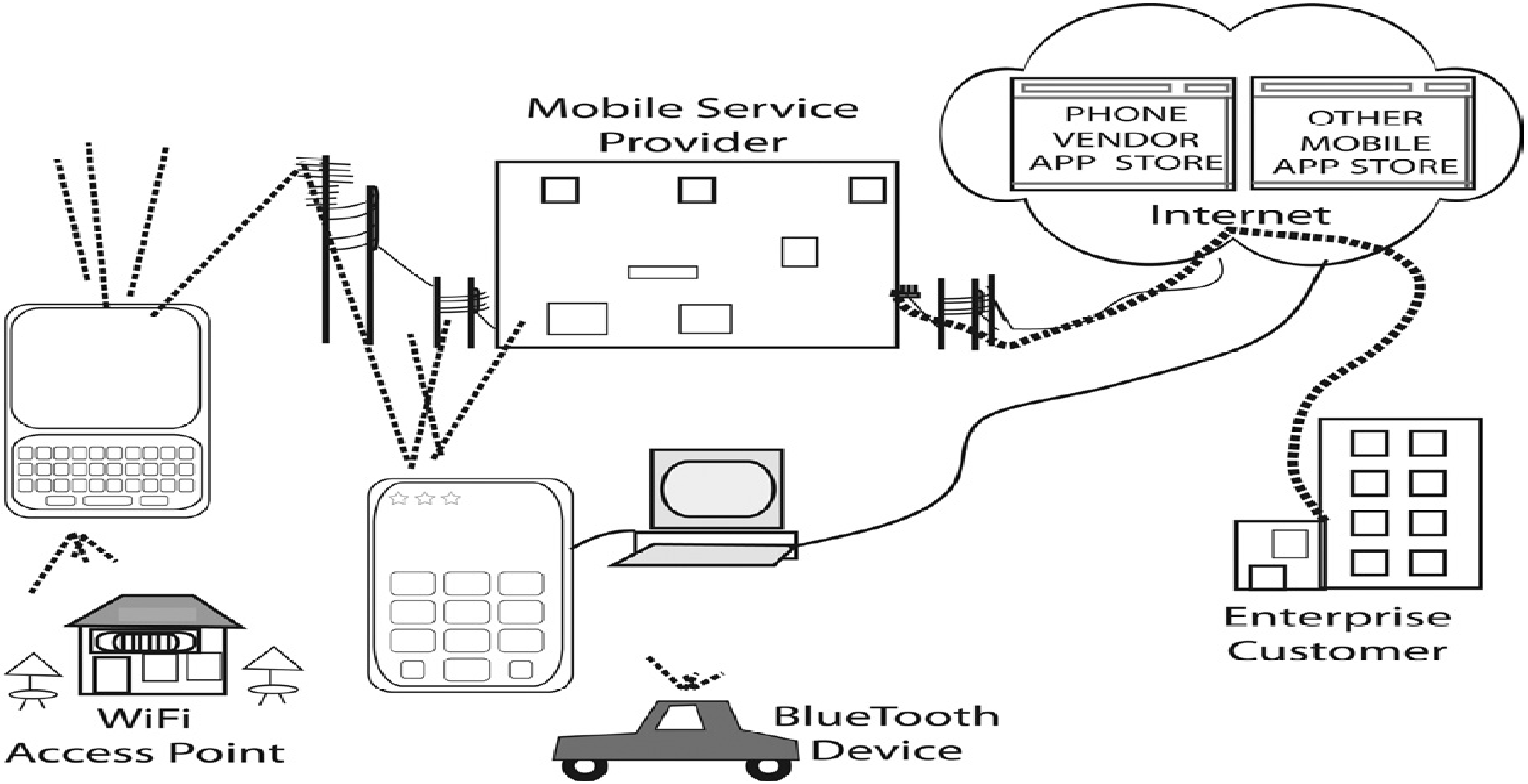
Central Controls

- the control center generally communicates to a remote control device such as a remote terminal unit (Rtu) or directly to a controller such as programmable logic controller (PLC) or an intelligent electronic device.
- the PLC or IED communicates via serial, Ethernet, micro-wave, spread spectrum radio, and a variety of other communication protocols.
- the communication is received by sensors, gathering measurements of pressure, temperature, flow, current, voltage, motor speed, chemical composition, or other physical phenomena, to determine when and if final elements such as valves, motors, and switches need to be actuated if the system requirements change or if the system is out specification.
- Generally, these changes are made automatically with the changes sent back to the operator of the control center.

# Personal Mobile Devices

- mobile devices are designed to allow the mobile carrier service providers to control the device.
- Mobile operating systems are in some sense tethered to the mobile carrier and unable to fulfill their purpose without it.
- this is why the mobile carrier has more interest in ensuring that the configuration of the device can be accessed remotely than in providing the user control over its content.
- For example, some device operating systems may have configurable security settings that allow an administrator to disallow installation of applications, but allow installation of applications from the corporate server.
- Figure 3.12 illustrates mobile phone connectivity.
- Phones signal cell towers, which relay the signals to equipment that identifies the transmitting device and allocates land-based telecommunications bandwidth to the mobile device based on the tower operator's agreements with the mobile carrier who administers the phone

# Mobile device system framework



Where device configuration is administered via the cell service, administration occurs from computers in the mobile carrier’s data centers.

they identify the device that is connected and send it data and commands that update the software on the device.

Note that this administration process uses part of the same bandwidth that is reserved for cell service itself, and mobile carriers do not charge the customer for the service time spent updating software.

keeps mobile carrier updates to a minimum and thus may actually delay the implementation of security patches if they become available during times of peak mobile service requirements. Security features that facilitate these goals include, though are not limited to:

- Possession—the phone number associated with the device is not transferable without permission of the owner.
- Reliability—transmissions sent by one user are received by the specified recipients.
- Connectivity—the system is available to transmit and receive.
- Confidentiality—mobile users expect that data transmissions will not be intercepted by parties other than those with whom they specifically choose to communicate.

# Guidance for Decision Makers

## Tone at the Top

- informative is because many of today’s information security controls were firstestablished as standards by the Electronic Data Processing Auditor’s Association (EDPAA, now the Information Systems Audit and Control Association, ISACA) (Bayuk 2005).
- accounting profession’s mantra concerning the integrity of financial management applies across the board to cyber security management. Thatis: “*the tone is set at the top*” (COSO 2009).
- In the domainof cyber security, policy is a documented enterprise agreement on cyber security goals and objectives, and tone is the level of commitment thatmanagement has toward that documented policy and corresponding enforcement measures.
- There is no single right way for a decision maker to make sure peopleare really understanding and following cyber security policy.
- The way a manager behaves toward issues of importance to cyber security policy will set the tone for the enterprise.
- Adjustments in both strategy and policy must be customized to the evolving requirements of the organization, which means cumulatively they point to where formal policy should evolve.
- Cyber security planning: Technology risk management.
- Aim of cybersecurity is to minimize risks.
- cyber security strategy must be a mainstream part of business, system, or mission planning, not a subcomponent of a technology-only function.
- For example, it is not uncommon for a technology department that has no set security strategy to set unreasonably hard standards for user-selected pass-words, while sharing administrative passwords among themselves via email.

- A decision maker will often count on an information security profes- sional to shepherd cyber security policy (e.g., a Chief Information Security Officer, or “CISO”), ensuring it remains effective and relevant. If it is not relevant, the void will doubtless be filled with what some security profes- sionals call “*security theater*.”
- Security theater is created when security concerns within the business prompt action, but the action is more visible than effective.
- Security theater does not actually prevent anything bad from happening. It just creates the illusion that security is in place.
- For example, in a building that has experienced a recent rash of thefts, a guard is installed behind a desk in the lobby of a building, and told to ask for identification, but anyone with any kind of laminated card with a name and photo on it can get in.

# Policy as a Project

- cyber security is managed as a program, the program structure provides organization, strategy, and operational process to maintain activities in support of cyber security.
- Where security is viewed as part of, or integrated with, other business or mission goals, it becomes evident that the strategy to achieve security objectives cannot be a stand- alone project, but must be part of a larger program.
- an enterprise management structure, the cyber security program will be a set of inter- related discrete projects and combined with processes managed in a coor- dinated way to obtain benefits and control not available from managing them individually.
- Policy is an extremely important component of strategy execution because it is used to communicate desired outcomes.
- Even if an executive issues only one policy statement, that statement will be interpreted in the context of other plans, objectives, and operational environments that complete an organization’s cyber security posture.

# Gantt chart

Task:

Articulate Cyber Security Strategy

Articulate Cyber Security Risks

Assemble Stakeholder Review

TeamDraft Cybersecurity Policy

Review Risks and Cybersecurity Policy

DraftSpecify Verification and Validation

Metrics Iterate Draft and Review

Process

Accept Policy as Documented

Conspicuously Approve Policy

Monitor Policy Implementation

Process Monitor Changes in Cyber

Security Risks
*Repeat as required*

Resourses:

Executive Decision

MakerCISO
Executive Decision Maker

CISO

Stakeholder Review Team

Executive Decision
Maker andStakeholder
Review Team

Stakeholder Review

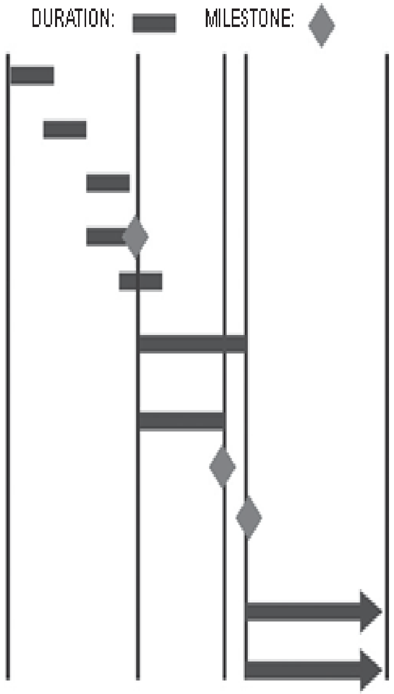
Team and CISO

Stakeholder Review

Team
Executive Decision Maker

Executive Decision
Maker and Stakeholder
Review Team and CISO

CISO



# Cyber Security Management

- a Chief Security Office
- Chief Information Security Office.
- These offices generally are skilled in the tools and tech- niques necessary to enforce security policy, but often do not have the understanding of business or mission that would be required to establishone.
- the team an executive needs to determine security policy is the same team convened to create other important strategic objectives.

**Arriving at Goals**

- To begin the process of developing cyber security policy, executives may ask themselves:
- What assets need to be in place to maintain operations? Which are the "crown jewels?" Are these changing and/or evolving with our long-term business plans?
- What cyberspace infrastructure houses or impacts our most critical assets?
- Do we have any information that should be kept from general circulation? If so:
- What criteria would we use to release it to someone within theorganization?
- What criteria would we use to release it to someone outside theorganization?
- If someone with access to it left the organization, should it still beprotected?
- Do we participate in socio-technical networks with communities who are hostile to our interests? Are we subject to cyber threats simply frombeing a bystander within a larger community?

Detailed questions can be probed with the help of a cyber security task force composed of operations, financial, and technology staff.

cyber liabilities.

- Have we protected our company in contracts with vendors.
- What is our risk exposure of technology or business operation failures at our vendors and service providers.
- overall financial impact of mishandling communications with our key stakeholders following a cyber security event? Have we budgeted for a cyber security event.

From these types of questions:

- An information classification system can be developed (e.g., customer info, financial info, and marketing info).
- merge classifications into a hierarchical taxonomy.
- A strategy to protect a business process should also protect regulatory-specified information , but the opposite is rarely true.
- Once a cyber security policy serves the needs of the business, a simple internal audit should confirm that it also meets the needs of the regulators, or identify a gap that can be closed in a way compatible with the agreed-upon business security requirements.

- Sample cyber security goals are:
- Make operations safe from hackers.
- Make it extremely hard to steal information stored on physical assets without insider collaboration.
- Always detect cyber-space-enabled asset fraud or theft.
- 100% achievable.
- Cyber security policy statements should be phrased in a language native to the same team of executive decision makers that set cyber security goals.

Sample cyber security policy statements based on the three sample goals above might be:

- Critical program information includes the software, systems configurations, documentation, and test generation methods for all business applications, and these include electronically enabled controls for mechanical equipment. The integrity of all critical program information shall be maintained.
- Physical access to all information assets shall be restricted to those required to operate them via job functions. Any physical device capable of storing information that is small enough to be portable shall be centrally encrypted with keys that do not leave the internal network.
- Where any asset is capable of being disbursed via online mechanisms, the software controlling the disbursement shall require end-to-end non- repudiation using physical, geographical, and logical authentication, authorization, and robust delivery verification

## Cyber Security Documentation

- policy awareness is a necessary step to complete after policy development and before implementation.
- security standards, operating procedures, and guidelines are also often issued in conjunction with policy to demonstrate how compliance with a given policy may be achieved.
- Procedures are documented step-by-step implementation instructions that a technician may follow in order to be successful in implementing policy and standards.
- Used to train new technicians on the mechanics of configuring the technology.
- Procedures therefore must be written at a much lower level of detail than policies or standards, and they must fully explain how to operate technology.
- Guidelines are the most general type of security document.
- CISOs documented cyber security policy.
- Cyber security specialists often act as trusted advisors to executive decision makers, but are not as well-versed on overall organizational mission as the executives who would be expected to create cyber security strategy.
- Cyber security specialists usually advise on matters of cyber security technology and implementation while leaving the organizational goals that form the basis of the policy to executive decision makers.

# Using the Catalog

- In a physical security environment, each significant social, economic, institutional, and political segment of the community has a number of potential resources that can be brought to bear (NCPI 2001).
- Cybersecurity policies are not implemented in complete sense.
- in order to coordinate response, one first needs an ability to detect cyber attacks, access to intelligence with which to analyze them, and a method and means of response.
- An individual organization may lay plans to coordinate its own response, but for response to cross all communities of interest, more coordinated policies are required on common fronts.
- Policy should not only address goals, but also identify key barriers to goal achievement and anticipate resistance to change.
- The resistance may come from sources both internal and external to the organization.
- Those with experience in accountability for security measures well understand that security policy is often used as a shield against change.
- a true enterprise strategist will see security policy as a flexible tool with which to achieve objectives, not as a barrier or disincentive to innovation.

# The Catalog Approach

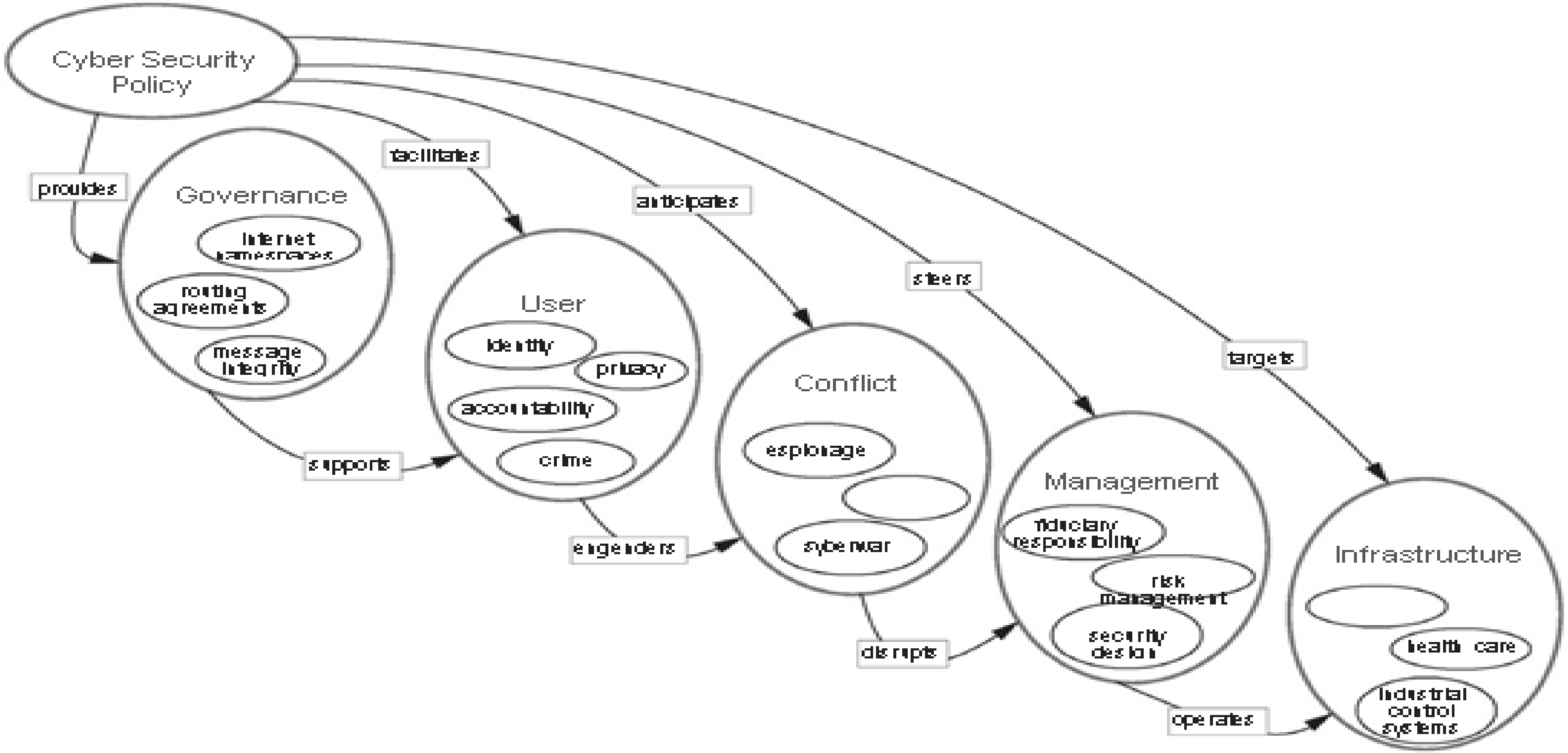
- The full spectrum of issues that may one day be laid before cyber security policy decision makers would be similarly long.
- A listing of all cyber security policy issues is not feasible to attempt because it is the type of list that would be out of date as soon as it was done.
- a catalog approach provides structure for classification and examples of cyber secu-rity policy issues.

The primary reason for listing and explaining a set of issues:

- to introduce and explain the foundations of concepts that frequently recur in cyber security policy debates.
- A secondary reason for presenting a catalog is to impress the reader with the variety and breadth of the field of cyber security policy.
- A third reason is to include enough detail in the explanation of cyber security policy issues for decision makers to recognize how the consequence of a given policy may affect their enterprise, whether or not it is a policy they themselves adopt, or a policy that has been adopted by others.
- The process of listing the issues and the corresponding discussion among authors while contributing to the list altered the taxonomy several times.
- Root cause analysis of cyber security incidents, as in any root cause analysis exercise, will produce two types of causes: events and conditions.
- Events are the proximate causes, and conditions are the situations that allowed the event to occur.
- ▪ Events are by nature unpredictable and difficult to control. But conditions that allow events in cyberspace to become security issues may be controlled with policy.

- Concentration on conditions rather than events led to the current taxonomy for the catalog of cyber security policy issues.
- Cyber policy issues faced by individual agencies and organizations seem hopelessly complicated in isolation, but in the context of the issues faced globally, sense can be made of the individual organization's choices in the context of the cyber-enabled community.
- a solid understanding of cyber security policy issues suggests potential solutions not only for the organization, but provides a solid foundation for the organization to lobby for choices made by others that affect them.
- For example, nearly everyone who uses cyberspace is affected by mechanisms that govern the allocation of Internet domain names and numbers.
- But only those who have been affected to the extent that policy choices in this domain have facilitated incidents that cause negative impact to their enterprise have likely investigated these issues.
- Even then, the investigation is typically into how Internet governance works, rather than how it could work if policy was different.
- From the Catalog's clear presentation of the issues related to Internet Governance, it is apparent that no matter how many lawyers one has, all domains will continue to be subject to threats of impersonation unless several policies are changed globally.
- five aspects of cyber security policy goals:
    1. Cyber Governance Issues
    2. Cyber User Issues
    3. Cyber Conflict Issues
    4. Cyber Management Issues
    5. Cyber Infrastructure Issues

# Cyber security policy taxonomy



- ***Cyber Governance*** is concerned with issues relating to Internet operation and its continued utility and feasibility.
- The resolution of issues in the governance arena undoubtedly will heavily influence the e-commerce environment, which is how most users are exposed to cyber security policy issues.
- ***Cyber Users*** are concerned with the stability of cyberspace as a platform upon which to conduct business, as well as their own personal expectations for Internet communication. Cyber security policy issues decided in that arena may have downstream consequences, both intended and unintended, on *Cyber Conflict* between political factions and nation- states.
- ***Cyber Management*** **policies** in some sense form a baseline of due care with respect to security, although each industry will face issues of unique concern. Hence, we provide examples of *Cyber Infrastructure* issues.
- foster an understanding of the various types of policy issues in order to prompt recognition that they are separate and distinct.
- For example, most cyber governance issues may be resolved independent of user issues, though some may constrain the policy choices made on behalf of users.
- Also, the resolution of user privacy issues may limit choices or introduce constraints in alterna- tives for cyber policy concerning cyber conflict issues.

# Catalog Format

- Each section of the Catalog follows a uniform format.
- Each section begins with an overview of the issues of interest for that section.
- . The overview is meant to shed light on cyber security policy concerns and introduce a taxonomy for the issues within the general section heading.
- Each item in the taxonomy will have its own subsection introductory description.
- These descriptions are followed by a categorization of cyber security policy issues that illustrate the concerns of the subsection and may include examples of events that illustrate major cyberspace developments and corresponding security impact.
- The opening discussion in each subsection is followed by a table that lists specific examples of cyber security policy issues.
- Each policy statement in a tabular list is enhanced with both explanation and opinions that indicate why cyber security policy constituents may be concerned about the issuance of executive mandates with respect to the issue.
- Readers should also keep in mind that cyber security policy that makes sense for one organization does not necessarily make sense for any other, and two organizations with inconsistent internal cyber security policies may nevertheless coexist in harmony.
- the reasons why a statement may stir controversy are presented in the form of virtual constitu- ent opinions.

- There are at least two reasons for controversy cited for each policy statement.
- the reasons for controversy reveal that there are often more than two sides to a cyber security policy debate.
- all issues and corresponding literature have surfaced in published information security standards, government directives, or academic literature.
- executives today are faced with responsibility for creating their own organizational cyber strategy and cyber security policy statements.
- These reasons for controversy are highlighted solely to enhance awareness of debates in progress while encouraging development of new opinions on the issue.
- In line with the objective of providing a comprehensive guide to cyber security policy issues for executive decision makers, an attempt has been made to phrase the cyber security policy issues in such a manner that an executive in the domain sees the consequences of mandating these statements as policy within their own sphere of organizational control.
- The members of the list have been grouped by subject of concern to the corresponding domain in order for an executive to quickly get a sense of how cyber security policy issues within a given domain may be related to each other.
- The adoption of one may entail the adoption of another, or it may conflict with the opportunity to adopt another.

- The catalog approach is intended to ensure that policy issues are captured systematically and without prejudice toward one overarching global strategy to accomplish any given organization’s objective for the utilization of cyberspace.
- A key goal of the Catalog is to provide well-articulated constituent opinions with respect to each policy statement.
- These opinions are clearly demarcated from the explanation of the policy issue itself, as the explanation is intended to be fact-based. Inclusion of a policy statement in this document in no way implies endorsement.
- A reason for controversy with respect to a policy statement is not highlighted as either a pro or a con.
- Though they may be grouped by category or similarity of opinion, reasons for controversy are not listed in any purposeful order.
- all policies are subject to unanticipated, as opposed to unintended, consequences.
- Unanticipated consequences are inherently unknown and so will not be listed.
- By contrast, unintended consequences may be anticipated, though they are not certain to occur.
- an unintended consequence carries a likelihood value that is subject to opinion.
- If unintended consequences are included in the catalog in the context of a policy statement, they will be listed as opinions, that is, as reasons for controversy.

# Cyber Security Policy Taxonomy

1. **Cyber Governance Issues**
    1. Net Neutrality
    2. Internet Names and Numbers
    3. Copyrights and Trademarks
    4. Email and Messaging
2. **Cyber Conflict Issues**
    1. Intellectual Property Theft
    2. Cyber Espionage
    3. Cyber Sabotage
    4. Cyber Warfare
3. **Cyber Management Issues**
    1. Fiduciary Responsibility
    2. Risk Management
    3. Professional Certification
    4. Supply Chain
    5. Security Principles
    6. Research and Development
4. **Cyber Infrastructure Issues**
    1. Banking and Finance
    2. Health Care
    3. Industrial Control Systems

**5.Cyber User Issues**

1. Malvertising
2. Impersonation
3. Appropriate Use
4. Cyber Crime
5. Geolocation
6. Privacy

- The original domain sub- sections for the Catalog were loosely modeled on the U.S. Department of Homeland Security Critical Infrastructure domains.