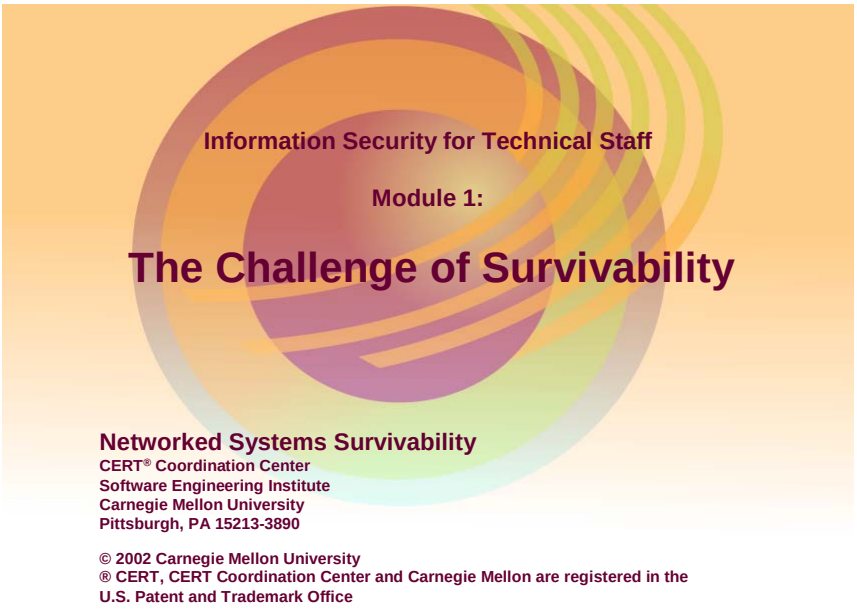
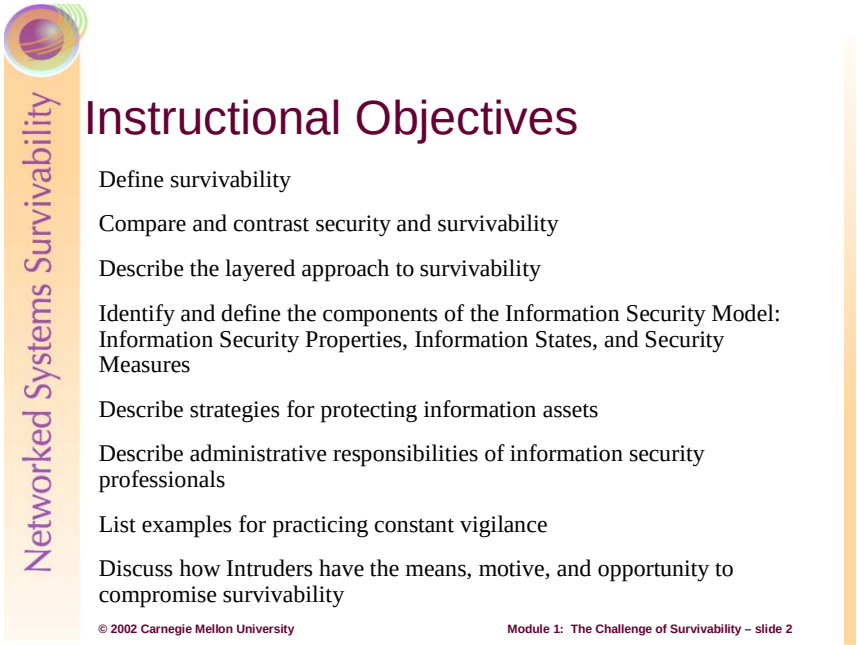
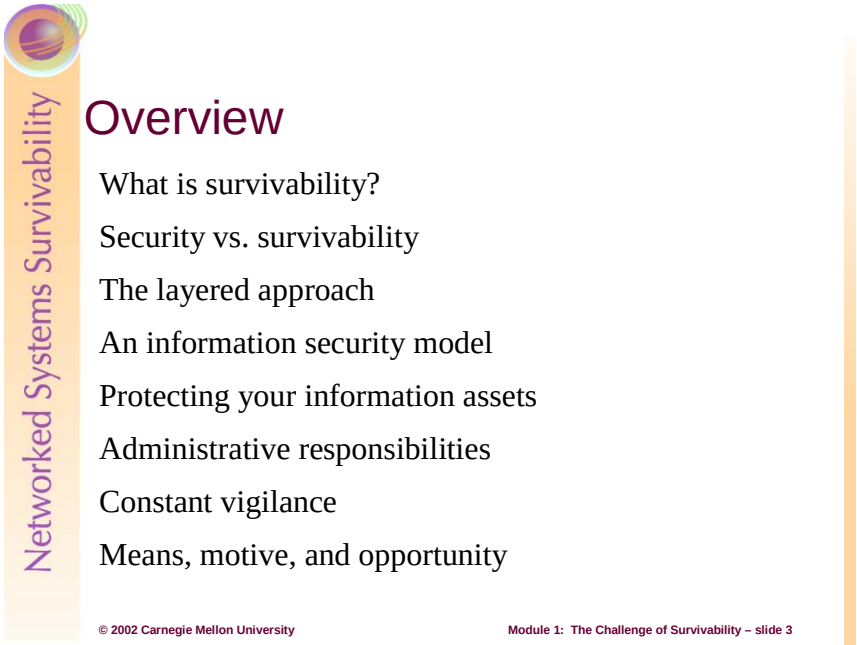


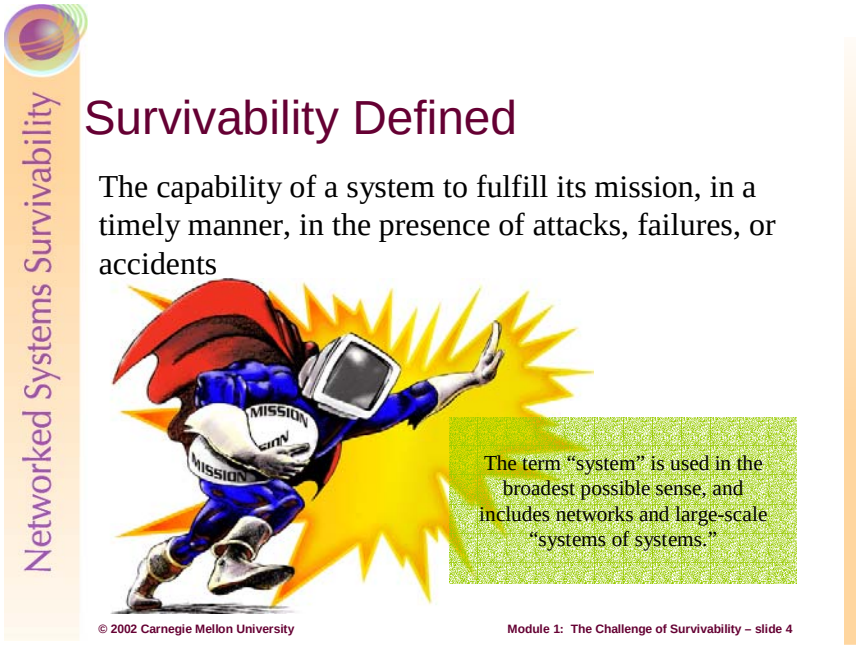
This module serves to introduce the student to the notion of survivable systems and thereafter focuses on Information Security as a component of Survivability.



After completing this module, the students will be able to do the above.



These are the topics that will be covered in this module.

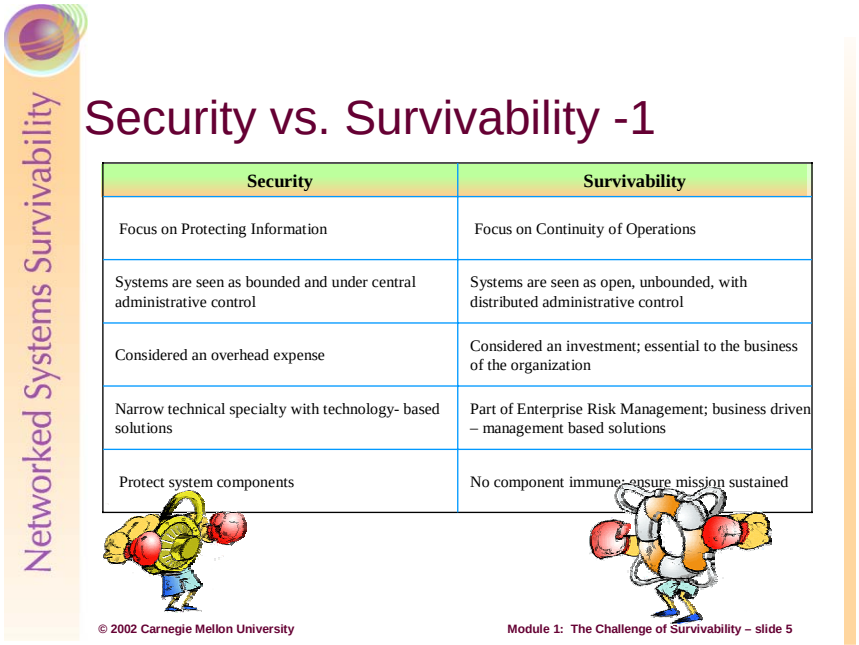


In recent years, there have been dramatic changes in the character of security problems, in their technical and business contexts, and in the goals and purposes of their stakeholders. As a consequence, many of the assumptions underlying traditional security technologies are no longer valid. Failure to recognize the depth and breadth of these changes combined prevents effective solutions to modern security problems. Survivability provides a new technical and business perspective on security, which is essential to our search for solutions. Moreover, our survivability approach expands the view of security from a narrow technical specialty, accessible only to security experts, towards a risk-management perspective that requires the participation of an organization as a whole (executive management, security experts, application domain experts, and other stakeholders) to protect mission-critical systems from cyber-attacks, failures, and accidents [Lipson 99].

Other important definitions:

Information systems security (INFOSEC and/or ISS): [The] protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats. [ANST]

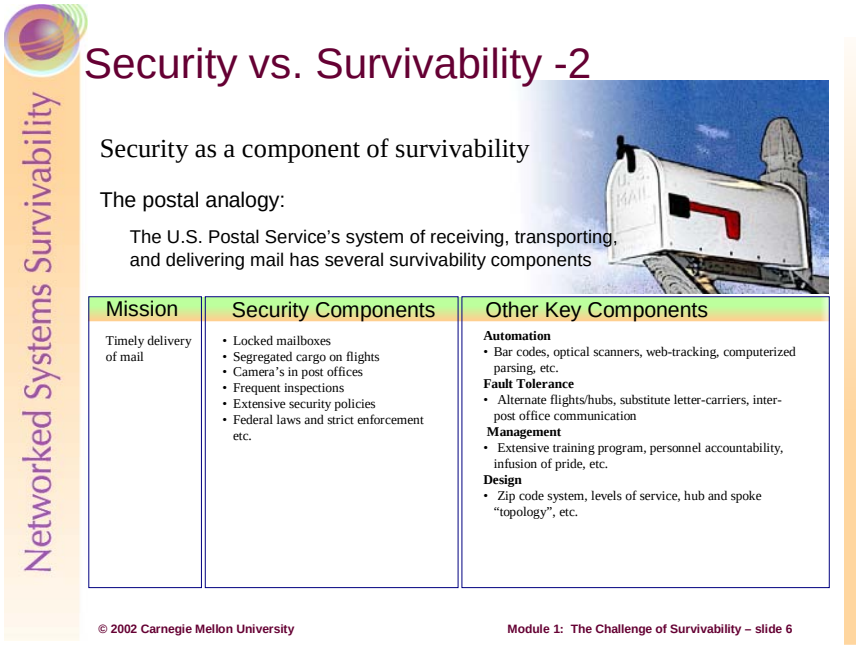
Information assurance: Information operations (IO) that protect and defend information and information systems (IS) by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. [ANST]



Survivability is an emerging discipline that blends computer security with business risk management for the purpose of protecting highly distributed information services and assets. A fundamental assumption is that no system is totally immune to attacks, accidents, or failures. Therefore, the focus of this new discipline is not only to thwart computer intruders, but also to ensure that mission-critical functions are sustained and a (situation-dependent) essential set of services is delivered, despite the presence of cyber-attacks. Improving survivability in the presence of cyber-attacks also improves the capacity to survive accidents and system failures that are not malicious in nature.

Traditional computer security is a highly specialized discipline that seeks to thwart intruders through technical means that are largely independent of the domain of the application or system being protected. Firewalls, cryptography, access control, authentication, and other mechanisms used in computer security are meant to protect an underlying application in much the same way regardless of the specific application being protected. In contrast, survivability has a very sharp mission focus, and is more akin to risk management. Ultimately it is the mission that must survive, not any particular component of the system or even the system itself. The mission must go on even if an attack causes significant damage to or even destruction of the system that supports the mission. It is the shift toward risk management, an approach that is highly intertwined with the mission-specific features of the application being protected, that is the most radical paradigm shift that is occurring as the new discipline of information survivability continues to emerge.

Survivability solutions are best understood as risk management strategies that first depend on an intimate knowledge of the mission being protected. The mission focus expands survivability solutions beyond purely independent ("one size fits all") technical solutions, even if those solutions are broad-based and extend beyond traditional computer security to include fault tolerance, reliability, usability, and so forth [Lipson 99].



The U.S. Postal Service's (USPS) system is analogous to large-scale, complex Information Technology (IT) systems and data networks. In this case, we're attempting to accomplish the mission of delivering mail in a timely manner. There are many risks associated with this, i.e. loss/theft of mail, slow transport and delivery, etc. The USPS applies numerous solutions as synergistic survivability components.

Security is critical to sustaining the mission in this analogy. Physical security is implemented by having locked mailboxes and cargo containers on commercial flights as well as secure sorting and storage rooms in post offices that are inaccessible to the general public. Personnel security is implemented by having cameras in post office sorting rooms and by conducting announced and unannounced inspections of post office operations. Organizational security is implemented by enforcing extensive policies and procedures on how mail is to be securely handled. Federal laws give teeth to all security measures by inflicting stiff consequences on violators while also serving as a deterrent.

Automation sustains the mission by streamlining operations and reducing the chance of human error. Bar codes and high-speed optical scanning are implemented at all regional hubs (and most post offices as well) and improve the accuracy and efficiency of routing mail. This system has been modernized continually and now has direct connectivity to the USPS web site <http://www.usps.com/>, enabling customers to track their mail online. While technology provides great benefit to the mission of the USPS, it cannot solve all problems or mitigate all risks or potential failures. Again it is part of a larger survivability construct.

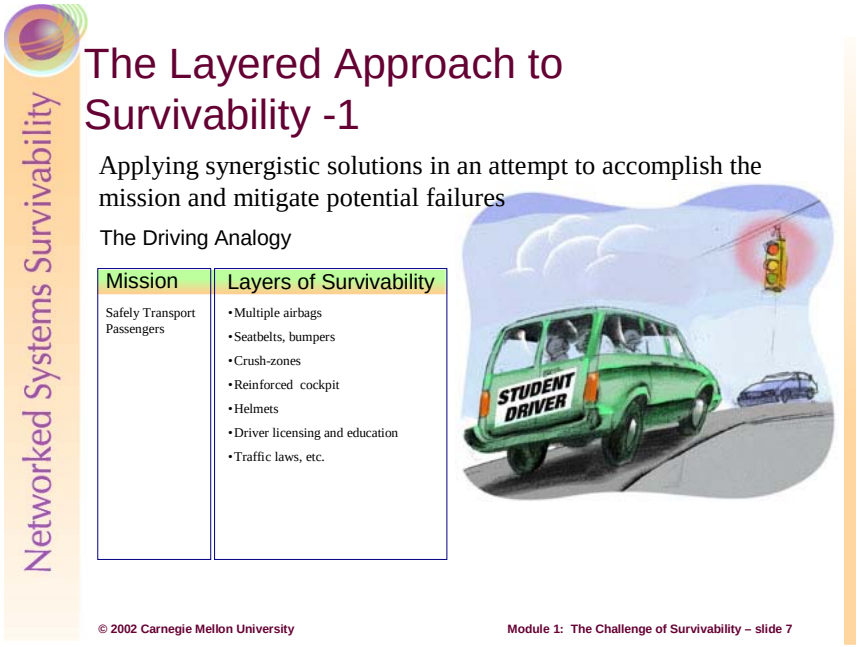
Fault Tolerance attempts to eliminate single points of failure and can also provide a degree of redundancy and fail-over in the system. If a fully loaded plane cannot fly due to mechanical problems, the system can accommodate this by using another plane, carrier, or means of transport. If your postman is sick, you'll still receive your mail that day. If your letter arrives at the wrong community post office, USPS personnel will re-route it to the correct one.

The Management structure of the USPS ensures that all members are properly trained. It has mature rating and evaluation programs and corrective measures that effectively provide for personnel accountability. It also has had great success in instilling pride in its employees—they don't want to lose letters because it hurts the reputation of the USPS as an organization and also

hurts their customers. Tradition has been nurtured and maintained and has helped to ensure a motivated workforce.

The Design of the system is essential to its success. Zip codes make routing and transport logical (much the same way as IP routing does), and they allow for scalability. There are many levels of service customers can choose. If speed is important, they can choose overnight express mail—although it comes at a cost. If guaranteed delivery is critical, than a patron can choose registered mail, which operates on an unbroken chain of receipts and constant physical security. It is so trustworthy, the U.S. military routinely sends classified documents (up to Secret) via registered mail. Customers can even pay an extra 50 cents and track their Christmas packages via the Internet. The mail system operates in a logical hub-and-spoke topology. When you mail a letter across the country, it goes first to your local hub (your community post office) then it's routed to a regional hub. From the regional hub, it's transported to the destination regional hub. The letter is then sent to the destination community post office and finally out to the spoke—the person's house to which you were mailing the letter in the first place. This topology has checks built into the system at all stages of transport and allows for reliable, fast, efficient, and inexpensive service.

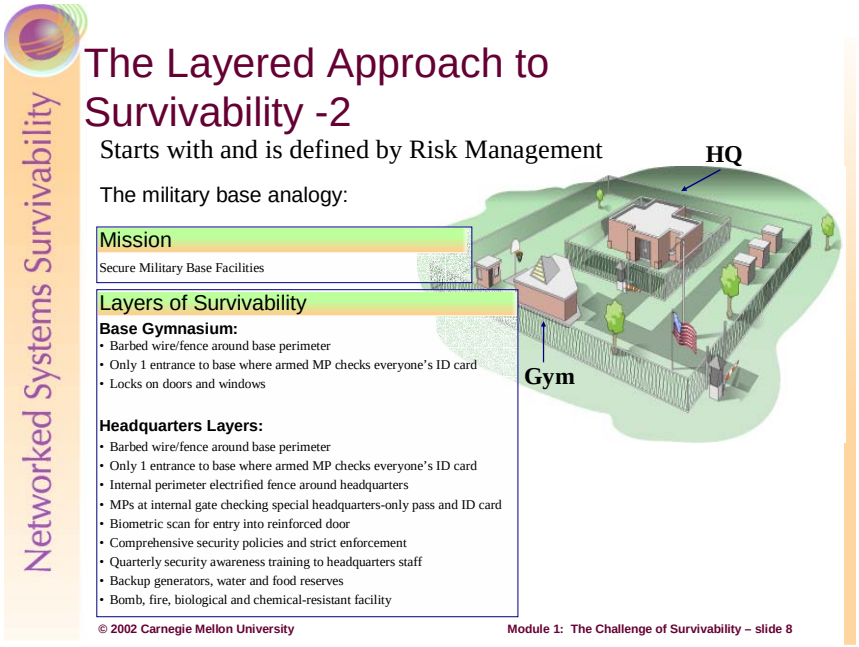
All of these survivability components are synergistic, working together to sustain the mission. IT systems and data networks have many of the same characteristics, problems, and challenges. Security is a crucial part of maintaining a survivable system; however, it will not be effective in the absence of other symbiotic solutions. Implementing survivability components based on prudent risk management conclusions can help achieve and sustain the mission of the organization.



This is a more simple analogy that reinforces the concept of Survivability. Applying multiple survivability measures increase the likelihood of mission accomplishment while reducing the chance of failure. These measures are applied as a holistic system, not numerous, stand-alone pieces. For example, the airbags in a car work in conjunction with the seatbelt system. If passengers are not wearing their seatbelts and are in a serious accident, it is unlikely that they will escape uninjured solely as a result of the airbags deploying.

Here is another analogy that further illustrates this paradigm:

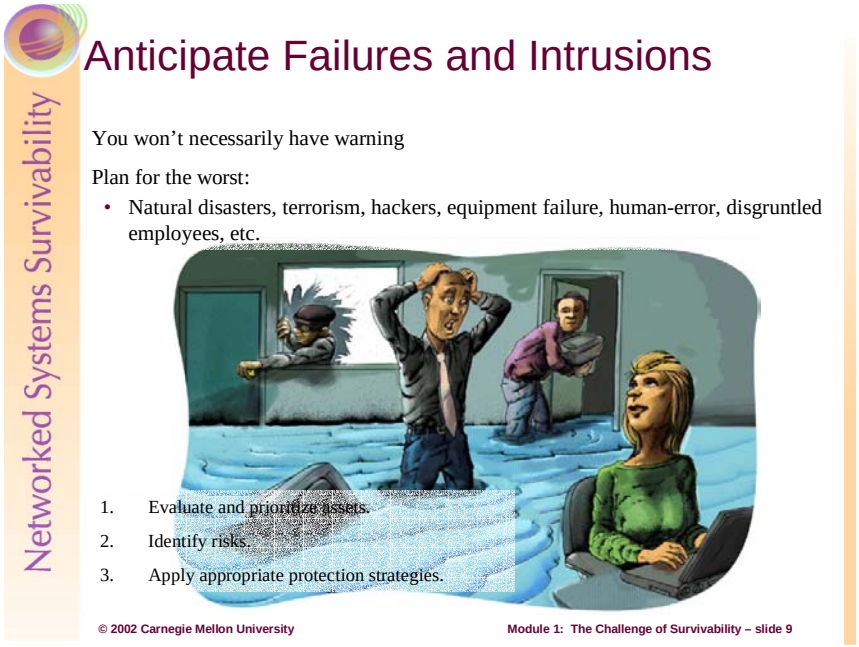
Consider the analogy of a village farmer with the mission of supplying food to a village. The farmer may have a fence around the crops to keep out deer, rabbits, and other intruders (traditional security). The farmer may have an irrigation system to be used in the event of insufficient rainfall (redundancy). He or she may plant a variety of crops so that even if environmental conditions (e.g., pests) adversely affect one crop, others will survive (diversity). All of this is well and good. But even if all the crops fail and no food is grown, the mission can still succeed if the farmer has an alternate strategy based on the mission of providing food — *not* necessarily growing food using the local ecosystem. If the crops fail, the farmer may turn to hunting or fishing to provide the life-sustaining mission fulfillment that fellow villagers depend upon. Is hunting a security, reliability, or fault tolerance strategy? No — it is outside the system for growing food. This is a risk management strategy that can be formulated only with an intimate understanding of the mission that must survive. Detailed technical expertise on fence-building, or even agriculture, is helpful but inadequate compared to strategies based on an intimate knowledge of the mission requirements [Lipson 99].



This analogy focuses on Risk Management and its importance to Survivability. Before you can apply appropriate survivability measures to an asset, you must evaluate its importance to the mission of the organization, and then identify risks associated with that asset. After the risks have been articulated, appropriate survivability measures are set in place.

In this analogy, the base gymnasium is of less importance to the overall mission of the military organization on the base. Because of this, relatively few survivability measures have been applied to mitigate the risk of intrusion.

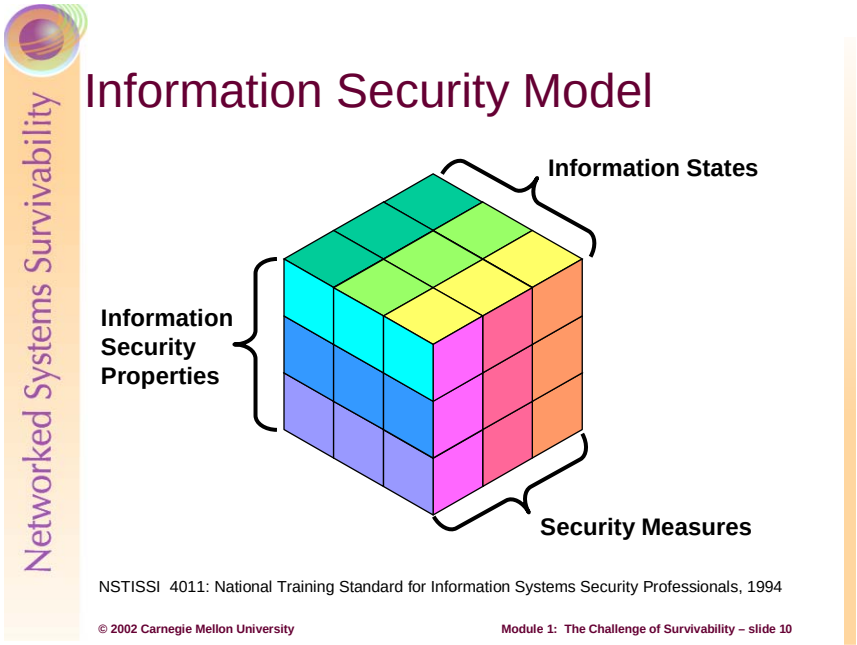
In contrast, the headquarters is considered to be the most vital building on the military base. It's central to all operations in both peacetime and during war. Because of this, it has much higher and more varied risks associated with it and therefore has many layers of survivability measures applied. Additionally, the complexity of these measures is far greater than the complexity of the measures for the gym and, because of this, the overall investment for the headquarters is greater.



Many businesses have contingency plans for dealing with business interruptions caused by natural disasters or accidents. Although the majority of cyber-attacks are relatively minor in nature, a cyber-attack on an organization's critical networked information systems has the potential to cause severe and prolonged business disruption, whether the business has been targeted specifically or is a random victim of a broad-based attack. If a cyber-attack disrupts critical business functions and interrupts the essential services that customers depend upon, then the survival of the business itself is at risk. An example would be the Web services offered by major banks. If a bank's home page were to be defaced as part of a cyber-attack, it would very likely decrease the confidence that patrons have in the bank's ability to safeguard their money. These patrons may decide to move their money elsewhere. Therefore, relatively benign attacks (from an operational stand-point) can cause significant damage to the overall business survivability of an organization.

One significant difference between disruptions caused by natural disasters and those caused by cyber-attacks (besides the notion of an intelligent adversary behind a cyber-attack) is that with a natural disaster there is a customer expectation of diminished service. A business disruption caused by a cyber-attack will likely be seen by a company's customers as a sign of incompetence. Unless the cyber-attack is widespread and well publicized, no customer sympathy will be forthcoming [Lipson 99].

While this course will tend to focus on the security component of survivability, it is essential that survivability be treated holistically when managing IT systems and information assets. Sustaining the mission of the organization is, after all, the primary motivation for investing in survivability components in the first place—not just protecting systems from intruders.



The security of information systems can be characterized in a variety of ways. The model depicted above, adapted from the National Training Standard for Information Systems Security Professionals [NST 94], characterizes information security in three dimensions:

Information Security Properties

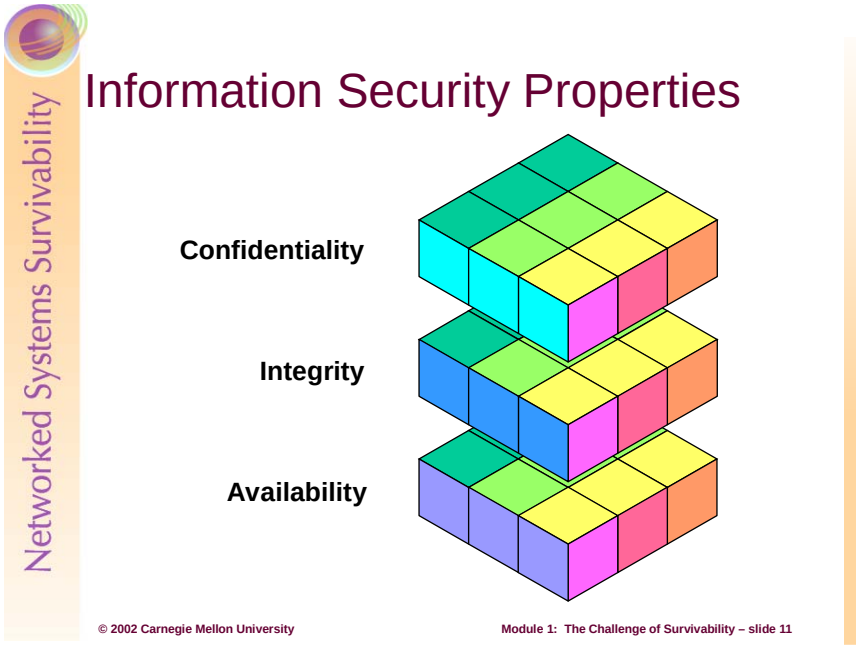
It's generally accepted that Information Security contains three properties: Confidentiality, Integrity, and Availability. These properties (defined later) may have different priorities based on the mission of the organization. For example, a Financial Institution with an Internet banking/investing capability will likely be most concerned with the confidentiality of its information. In contrast, an Internet Search Engine (like Google.com) will likely be most concerned with protecting the availability of its information.

Information States

Information is not a static entity. It exists in processing (i.e. RAM), storage (i.e. on disk), and transmission (i.e. on the wire). Therefore, it must be safeguarded appropriately in each.

Security Measures

Organizations must apply security measures in order to effectively mitigate risk to their information assets.



The goal of information security is to sustain and defend three critical security properties of information: *confidentiality*, *integrity*, and *availability*.

Confidentiality refers to assurance that information can be read and interpreted only by persons and processes explicitly authorized to do so. Protecting confidentiality involves implementing procedures and measures to prevent malicious and accidental disclosure of information to unauthorized readers. Information that could be considered confidential is commonly called *sensitive* information.

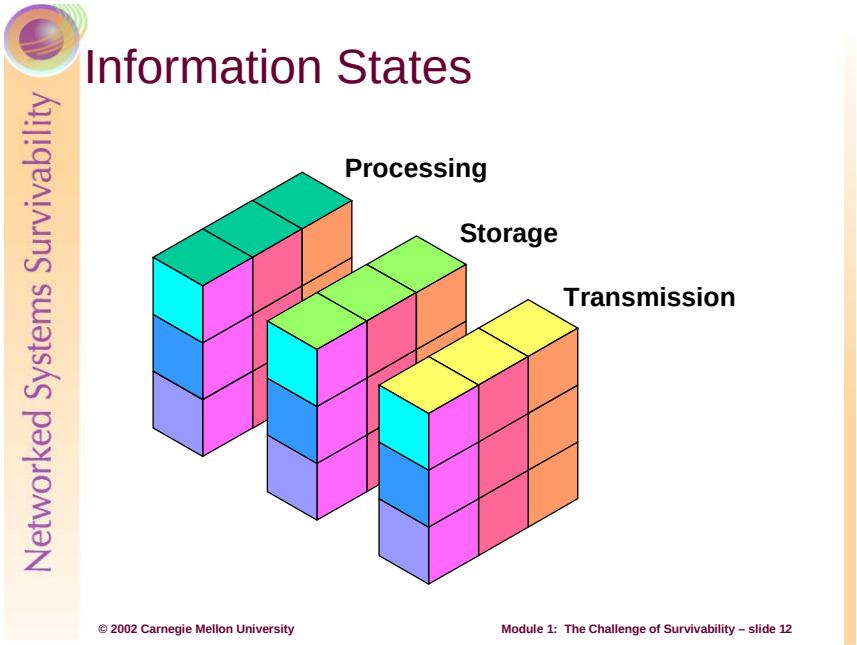
> Example: protecting email content from being read by anyone other than the intended addressees

Integrity of information is about assurance that information remains intact, correct, and authentic. Protecting the integrity involves preventing and detecting unauthorized creation, modification, or destruction of information.

> Example: implementing measures to verify that email content was not modified in transit

Availability refers to assurance that authorized users can access and work with information assets, resources, and systems when needed, with sufficient response and performance. Protecting availability involves measures to sustain accessibility to information in spite of possible sources of interference, including system failures and deliberate attempts to obstruct availability.

> Example: access to and throughput of email service



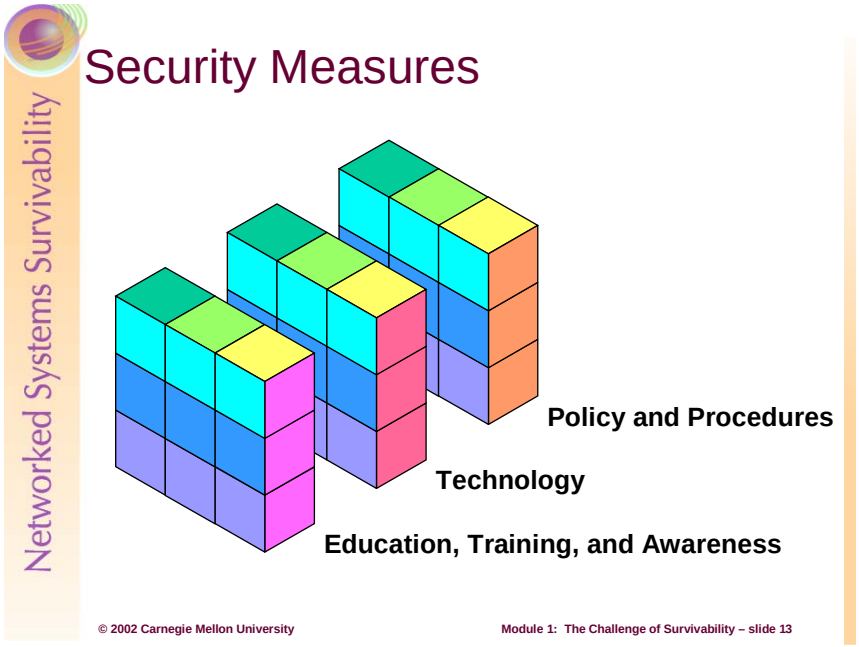
For the purposes of this model, information states refer to *where* in the information systems environment the information to be protected may be found. At any given moment, information may be accessible in an information system's local memory (*processing*), recorded on some form of physical media (*storage*), and in transit as it is being delivered from one place to another within and between systems (*transmission*).

The confidentiality, integrity, and availability of information must be protected consistently in all of these states. For example, the content of a confidential document composed by a user must be protected against unauthorized access while the document is:

- In the random access memory (RAM) of the workstation as the user is editing it
- On the workstation or file server's disk after the user saves the document
- In transit over networks when the user sends it to an authorized reader via email, including the memory and storage of all intervening systems encountered during delivery (e.g., routers, mail servers)
- In RAM of the recipient's workstation as he or she is reading it
- On a disk of the recipient's workstation or mail server if it is retained

Security of discarded media and output:

The proper disposal of confidential information is also of critical importance. If media or other output (e.g., printouts, slides) on which confidential information was written is not completely erased or destroyed, an unauthorized reader may be able to salvage the content from discarded materials (aka "dumpster diving"). Backup media such as tapes CD/DVD, etc, need to be treated with the same amount of care—critical information is most likely stored on this media. Therefore, careful planning should be conducted to facilitate proper disposal.

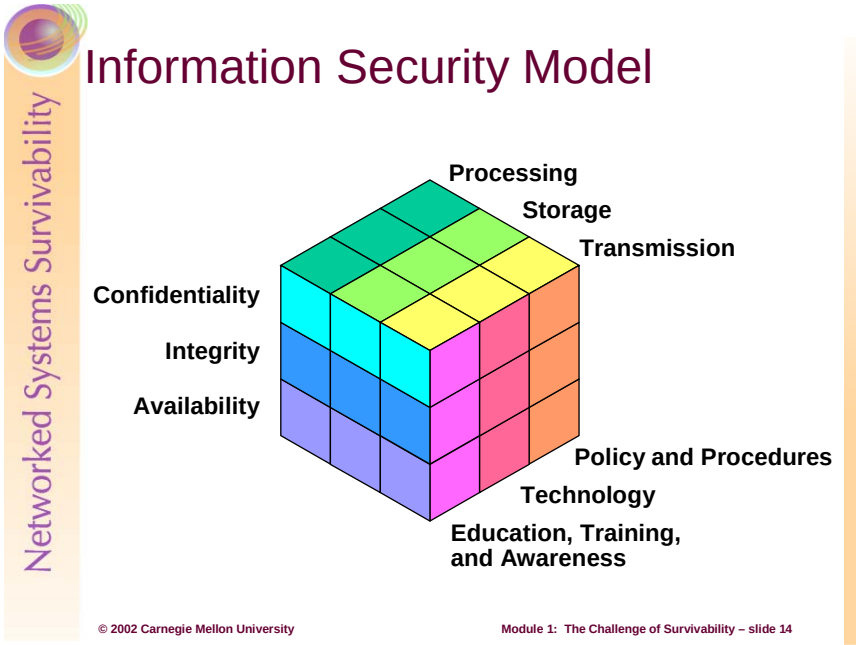


Measures to implement and sustain information security involve policy and procedures, technology, and the knowledge and abilities of system and network administrators and users.

Information security policies define the organization's rules and expectations regarding access, protection, and accountability of information assets and resources. Procedures include methods for proper handling of sensitive information, and instructions for what to do in the event of an information security incident.

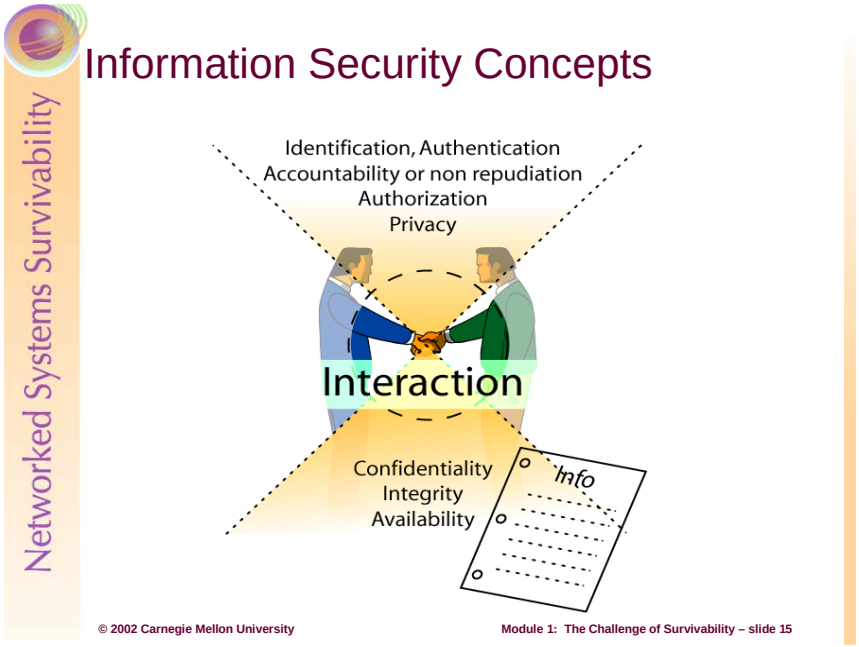
To help enforce information security policies, defend against information system vulnerabilities and threats, and facilitate quick response when information security incidents occur, appropriate technology must be securely configured, deployed and maintained. Examples include network firewalls, file system access controls, system and network monitoring tools, and user authentication technologies.

Administrators and users of information systems must understand their responsibilities for information security, and execute appropriate procedures to sustain and improve the security of information assets and resources. As conditions change, users and administrators must remain informed and be ready to act appropriately to safeguard information security.



This model of information security emphasizes the need to sustain the confidentiality, integrity, and availability of information assets and resources in every state that the information could be found in a networked information systems environment. It is important to note that the concept of storage includes any media on which information can be recorded, including printed output. Secure handling of output media containing sensitive information requires that it be completely erased or destroyed before final disposal.

Organizations must develop policies and procedures that govern access, use, modification, transmission, and disposal of information. To defend and enforce information assets and resources, appropriate technologies must be securely configured and deployed. System and network administrators and users must be well informed regarding their information security responsibilities and be able to apply appropriate procedures to safeguard the security of information.



How is information considered to be secure?

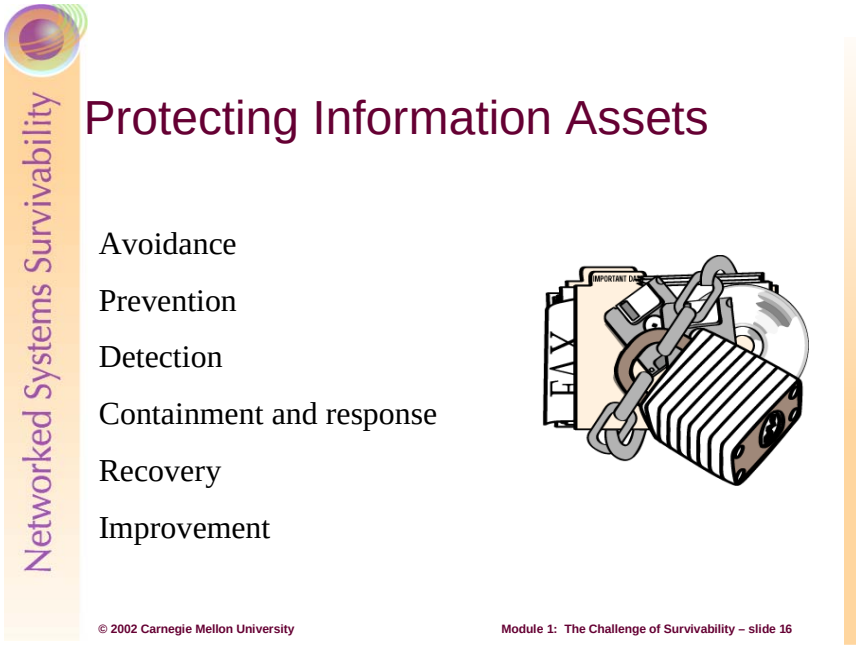
The properties of Confidentiality, Integrity, and Availability are at the foundation of what it means for information to be secure. As information is shared, there exists another layer of issues that we must be concerned with:

- **Identification**: refers to the unique properties of users that separate them from others and the means in which these users claim their identities on a system. Usernames are common means of identification. This is tightly linked with authentication.
- **Authentication**: is the process of proving that you are who you say you are—establishing proof of identity. This can be achieved through passwords, smart cards, biometrics, etc.
- **Accountability**: is a system's ability to determine the actions and behavior of a single individual within a system, and to identify that particular individual. It is what binds these actions to users. Audit trails and logs are used for this. This is very tightly linked with nonrepudiation.
- **Nonrepudiation**: is the mechanism that keeps an individual from denying that they did something. For example, if a customer places an order and a nonrepudiation security service is not built in to the system, the customer could deny ever making that purchase. Nonrepudiation services provide a means of proving that a transaction occurred, whether it's an online purchase or an email message that was sent or received. Digital signature can be used for nonrepudiation.
- **Authorization**: is the rights and permissions granted to an individual (or process) which enable access to a computer resource. Once a user is authenticated, authorization levels determine the extent of the system rights that are available to that user.
- **Privacy**: is the level of confidentiality and privacy protection that a user (or process) is given in a system. This is often an important component of security controls. Privacy not only guarantees the fundamental tenet of confidentiality of an organization's data, but also guarantees the data's level of privacy, which is being used by the operator. [Krutz 2001]

If any of these higher layer properties are compromised you lose CIA as a whole. The key to mitigating this is to securely manage the interactions. This can be accomplished through various means, including, but not limited to:

- Strong Authentication mechanisms, i.e. Kerberos, Radius, etc.
- Data Encryption, i.e. IPSEC, Encrypting File System, PGP, etc.
- Secure/thorough administrative practices, i.e. access controls, permissions/rights, integrity checking systems, etc.
- Secure architectural design, i.e. limiting unnecessary services, security perimeters, etc.

These implementations will be covered in detail later in this course.



A comprehensive approach to implementing and sustaining information security can include the following strategies and practices:

Avoidance: A desirable strategy for improving security is to avoid configurations that present unnecessary opportunities for problems to occur. For example, if users of systems on a particular network do not require direct access to external networks, and inbound connections are forbidden, then there is no reason to connect the network to external networks in the first place.

Prevention: Prevention refers to the implementation of measures and controls to minimize the possibility of security problems occurring. For example, it may be necessary to store different kinds of data on a common file server. To prevent unauthorized access to each kind of data, access controls should permit users to see only those kinds of data for which they have permission to do so.

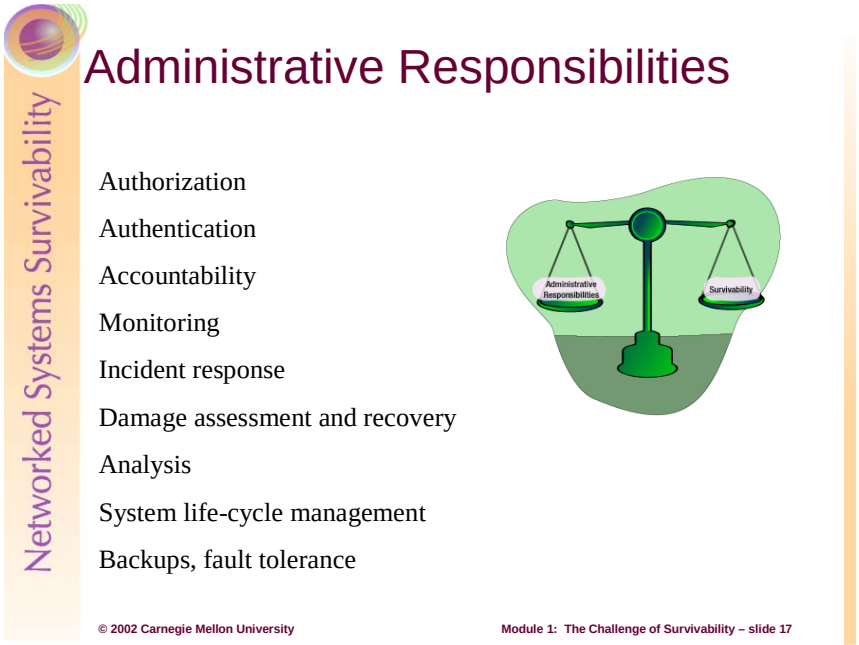
Detection: Despite all efforts to prevent unauthorized access to information assets and resources, security incidents are bound to occur. It is therefore necessary to implement measures to detect possible information security problems when they occur. For example, it may be appropriate for you to deploy network traffic monitors to alert you to unauthorized connection attempts to your networked systems.

Containment and Response: When information security incidents do occur, you will have to work quickly to contain the damage and respond to prevent further unauthorized activity. Preparation and practice in handling security incidents is an essential part of maintaining readiness to respond when incidents occur.

Recovery: When system failures and security incidents occur, you will need to have resources and data backups available to restore your data, systems, networks, and security infrastructure to a "known-good" state. This means that preparation and ongoing effort must be applied in advance to back up data and systems.

Improvement: New threats to the security of information and information systems are discovered every day. Intruders actively seek ways to infiltrate systems in search of information and resources. As a result, it is necessary to engage in a continuous effort to sustain and improve the security of the networked information systems under your administrative control. As security

incidents occur, lessons learned help to identify areas in need of improvement. Staying up-to-date regarding newly discovered problems and the means to mitigate them are essential elements of a continuous security improvement process.



To ensure information security, system and network administrators enable and implement secure means for the following activities:

Authorization: Within your organization, information security policies and management directives specify who is permitted to access which information assets and resources, and the conditions under which that access is permitted. To aid in enforcing these rules, you implement data access controls, user privilege configurations, quotas, network traffic filters, and a variety of other software and hardware controls that represent the rules for authorized access.

Authentication: For controls to be effective, you need ways to verify the identity of users accessing information assets and resources. User credentials are typically represented by one or more of the following:

- Something they *know*, e.g., a password or pass phrase
- Something they *have*, e.g., a physical access key or identity card
- Something they *are*, e.g., fingerprints, retinal or thermal patterns, DNA

The data used to authenticate user credentials must also be reliable and protected against modification. For example, you need to strictly protect access to a host system's password data against unauthorized viewing, copying, or modification.

Accountability: You need to ensure that appropriate auditing, logs, and revision histories are captured, as they may be necessary to investigate the nature and means of unauthorized activities, and the damage incurred. Such records may also be required if you are called upon to defend actions taken to respond to information security incidents, and as evidence in proceedings to prosecute violators.

Monitoring: To identify possible intrusions as soon as possible, you'll need to monitor system and network activities and changes made to sensitive files. Automated monitoring systems may be configured to alert system and network administrators to unusual or unexpected activity or changes.

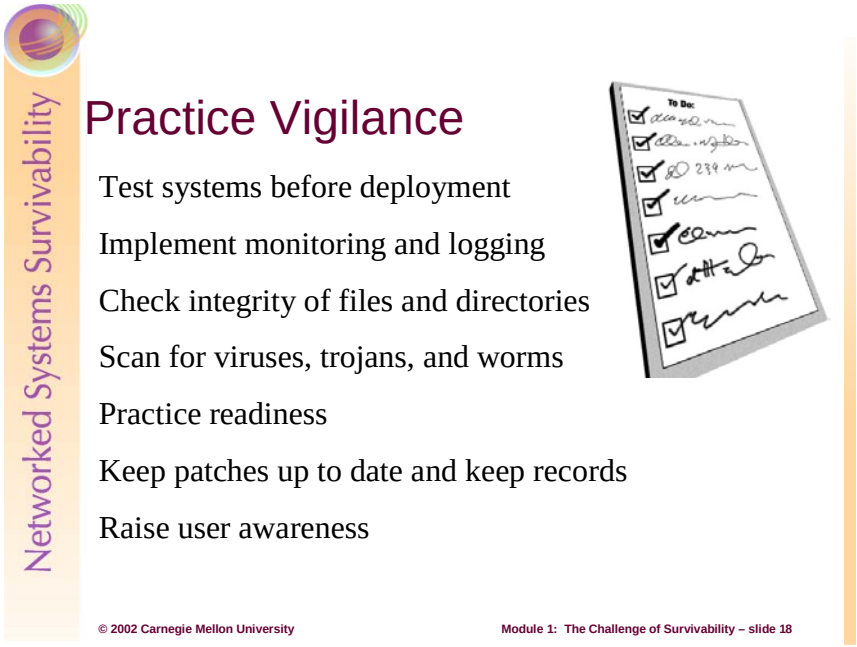
Response to information security incidents: When information security incidents occur, you may be called upon to use your technical knowledge and skills, and experience with the affected systems, to respond.

Damage assessment and recovery: Following the initial response to an information security incident or system failure, you may be called upon to assess the damage incurred, and to plan and implement steps to recover affected systems and data.

Analysis and implementation of security improvements: As your organization's information security requirements change over time, and as needs arise following information security incidents, it is likely that you will be expected to participate in planning and implementing new technology, configurations, and procedures to improve information security.

System and software deployment, upkeep, and retirement: Ongoing maintenance and upkeep of systems, software and configurations are essential to sustain information security over time. As new information security flaws are discovered, you will need to apply patches and updates to prevent exploitation of the flaws by intruders. In addition, as systems are retired from service, it is necessary to ensure that any associated media do not retain any sensitive information prior to disposal.

Backups and Fault Tolerance: To enable recovery in the event of system failures and information security incidents, secure, regular backups of the information contained on systems are essential. To maximize availability of critical system services in spite of failure, compromise, or necessary interruptions for maintenance, it is common practice to have "hot spares" of such critical systems available to take their place when needed. You may also want to implement other fault tolerant and fail-over techniques (like clustering) that allow critical systems to compute-through some levels of failure with little or no notice by users. Finally, ensure that your backups represent "good" data; that is to say, don't restore backups that contain the Trojan horse that corrupted your production system in the first place.



Prepare, replicate, and test systems in an isolated, physically secure environment.
Systems and software are typically at their most vulnerable during initial installation and configuration. In addition, changes to configurations and new technologies may have unforeseen side effects that can affect the security of systems and networks in a production environment. It is therefore imperative that initial installation, replication, and testing of systems and components are conducted in a physically secure environment isolated from all production and public networks. As you may know, this can be a difficult task for many organizations due to resource limitations. Therefore, it is advisable to use virtual machine environments and load simulators in an attempt to re-create the production environment for the purpose of testing. If you are involved in a network operating system (NOS) upgrade, you should prepare contingency plans for reverting to the old NOS (if you run into major problems)—as testing major upgrades outside of the production environment may be impossible.

Deploy secure system, network, and application logging and monitoring capabilities.
To support detection, investigation, and prosecution of intrusion attempts, and to sustain confidence in the security measures that you've deployed, it is often necessary to log and monitor system and network activity. The data that such logs and monitors collect are themselves sensitive, since they describe the operations and activities of your organization. Log and monitor data, as well as the tools used to process and analyze such data, must be collected, transmitted, stored, and disposed of with the same degree of care as confidential, proprietary information.

Regularly review logs for signs of intrusion.
The logging of system and network activities is of little use if no one ever looks at the logs. In addition, if the period between reviews of the logs is too long, the volume and complexity of the logged information may be too cumbersome to manage, and signs of intrusion may go unnoticed until significant damage has already occurred. If you review your logs frequently (at least on a daily basis), their value as a means of intrusion detection is enhanced. In addition, automated tools to monitor logs for specific signs of unauthorized activity can be configured to work with alerting mechanisms (e.g., e-mail, pagers) to draw immediate attention to severe signs of trouble.

Look for unexpected changes to directories and files.
On a regular basis, check critical system and proprietary data files for unexpected changes. For files that are not expected to change often (e.g., system and service configuration files), you can use software such as Tripwire or other integrity checking tools to watch for changes in file and directory contents and attributes.

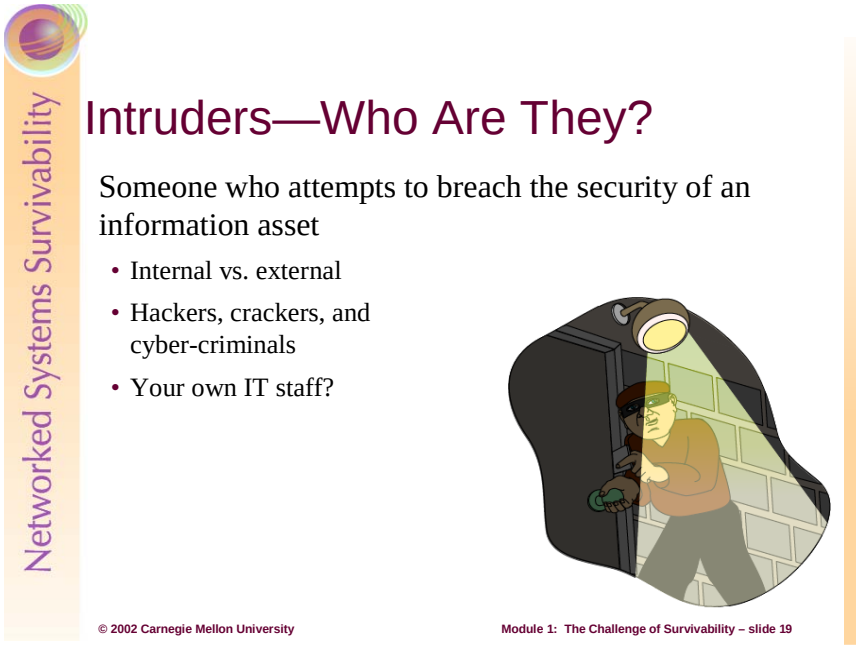
Regularly scan for viruses.
Install virus monitoring and scanning software on all user workstations, and require regular scanning for viruses whenever external data or programs are received. Additionally, it is highly recommended that all file servers and email servers be scanned for viruses as part of their normal operations.

Maintain and practice readiness to respond to security incidents.
In addition to establishing procedures for where to go, who to contact, and what to do in the event of an information security incident, it is important to periodically practice information security procedures with personnel to maintain readiness. Since incidents can occur in a matter of seconds, time is of the essence. By practicing response procedures, you can significantly decrease the amount of time it takes to detect and contain an intrusion.

Keep systems, software, and configurations up-to-date regarding security.
New vulnerabilities are discovered and exploited every day. For the systems, network components, and software used in your organization, it is important to stay abreast of reports regarding vulnerabilities and their solutions. Applicable security patches and workarounds should be applied and deployed as soon as possible. Changes in your organization's information security policy will also have consequences on existing security measures and controls. In addition, changes in personnel and their authority and responsibility will affect ownership, access, and restrictions regarding information assets and resources. To avoid inappropriate access to information and systems, review and revise existing access controls on a regular basis. It is very important to record which systems have been patched against particular vulnerabilities. Additionally, organizations should record who applied the patch and when it was done.

Actively raise user and management awareness regarding information security.
To defend and sustain support for information security, you'll need to keep managers and system users aware of information security issues. If personnel are not made aware of threats and signs of intrusion, they will be unable to recognize them when they occur.

Consider, for example, an email worm. You as the administrator should inform your users of its characteristics ahead of time (if possible), and then ask managers to hold those who open the infected file (out of negligence) accountable.



Intruders aren't always wily hackers on the other side of the country. Often times it's an employee who tries to access restricted information assets (i.e., human resources files) or a temporary contractor or subcontractor that has been granted access to sensitive data. However, there is a trend that intruders from outside of your network are becoming increasingly active. The following is excerpted from the 2001 CSI/FBI Computer Crime and Security Survey:

Conventional wisdom says "80% of computer security problems are due to insiders, 20% are due to outsiders." There are people who cling to this axiom as if some Galileo had just suggested that the Earth might actually be round. But for the fourth year in a row, more respondents (70%) cited their Internet connection as a frequent point of attack than cited their internal systems as a frequent point of attack (31%). Indeed, the number of those citing their Internet connection as a frequent point of attack has been rising, while the number of those reporting both dial-up remote access and their own internal systems as a frequent point of attack have been declining. Clearly, the threat from the outside is increasing dramatically and has been doing so for several years. But is the threat from the inside actually decreasing? It would be premature and dangerous to assume so [CSI 01].

This document goes on to describe several high-profile cases of Insider incidents and how vulnerable many organizations still are. In the highly distributed applications and Internet-based systems of today, there is little distinction between insiders and outsiders. Everyone who chooses to connect to the Internet is an insider, whether they are known to a particular subsystem or not. This characteristic is derived from the desire, and modern necessity, for connectivity. Companies cannot survive in highly competitive industries without easy and rapid access to their customers, suppliers, and partners [Lipson 99].

There are some "recognized" definitions for hackers, crackers, and cyber-criminals; however, these are becoming blurred as this kind of activity has increased. So to keep it simple here are the definitions we use:

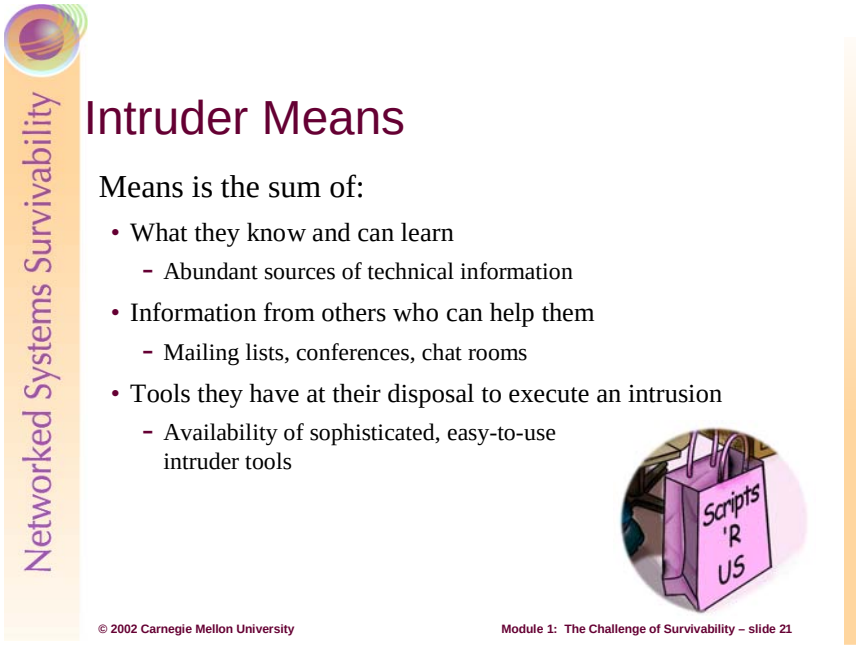
Hackers: Individuals more interested in probing systems and networks for their own enjoyment and curiosity rather than actually causing harm.

Crackers: Individuals who attempt to maliciously altar systems for their benefit. For example: web site defacements or breaking license codes for games, applications, and web sites.

Cyber-Criminals: Attempt to conduct large-scale crime online, i.e., credit card theft/scams, Internet drug sales, corporate blackmail.

It is commonplace in many organizations to institute a "fortress" model when addressing security. They invest considerable resources on perimeter defense, intrusion detection, and network monitoring systems, and yet leave much of the internal network under-protected. One of the biggest threats to security of an organization is its own Information Technology staff. Very often these individuals have complete access to all of the critical information assets of an organization, including intellectual property and critical business intelligence, like IPOs, mergers, and acquisitions. It is vital therefore that appropriate measures be taken to mitigate this risk based on the criticality of the information asset. Extensive personnel screening, compartmentalization of responsibilities, and access controls are some of the steps that organizations have taken toward this end. Do you know all of the access and privileges that your IT staff currently has?

We've all seen television police dramas where the detectives nab the criminal by determining who has the means, a motive, and the opportunity to commit a crime. They ask questions such as, "Did the suspect have the means to commit the crime? Did they have something to gain? Did they have the opportunity to carry out the crime?" Intruders involved in cyber attacks will normally possess these same three characteristics [Rogers 00].

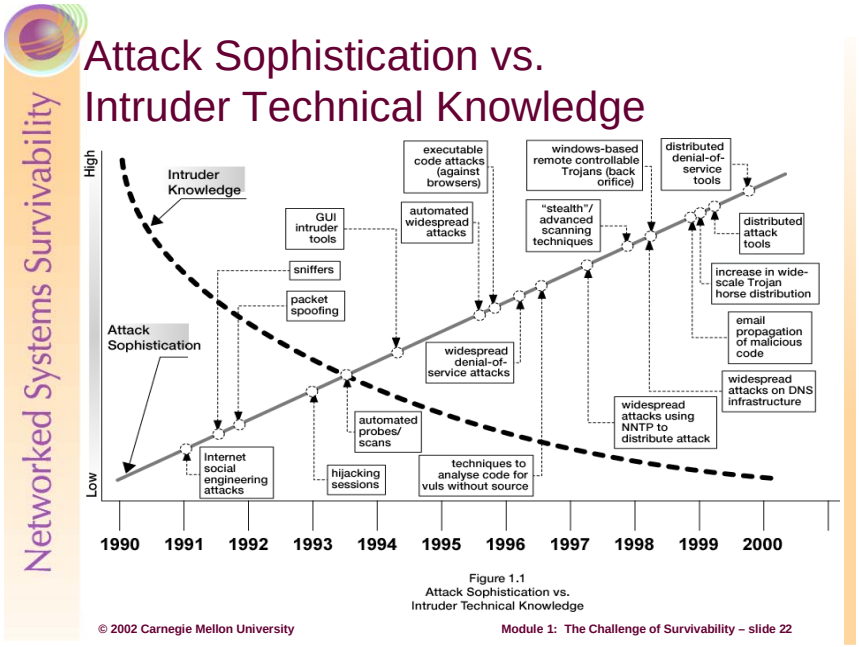


Means

The means for attacking computer systems has changed over the years. Ten years ago, intruders attacked computer systems primarily "by hand." For example, they tried to guess passwords by brute-force techniques such as repeatedly trying to login to an account by using a dictionary of passwords. They also used social engineering methods to trick people into revealing passwords. Today, there are tools that encrypt dictionary words and their variations (such as replacing the letter "o" with the digit "0") and compare them to the encrypted password.

The level of sophistication of intrusion tools has become high and is getting higher. Intruders have harnessed the power of the Internet itself, building automated tools to coordinate large-scale attacks involving hundreds of hosts aimed at Internet sites. These tools are well documented and are freely available on the Internet. Members of the intruder community share programs and improve on each other's work.

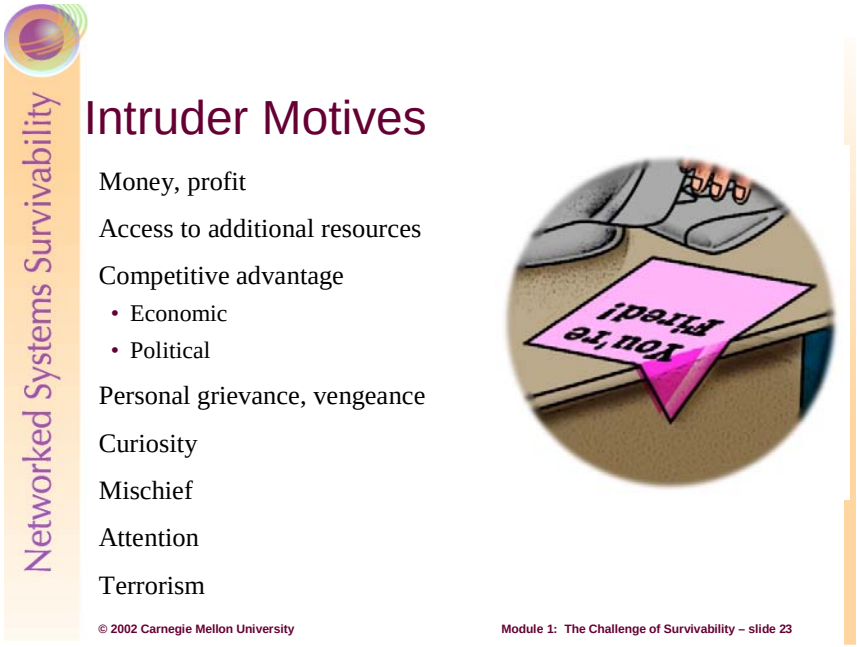
Sophisticated tools have given birth to a class of script kiddies, intruders who use tools to break into computer systems although they lack the knowledge to craft the tools themselves or even to understand the nuances of their inner workings. There have been reports of break-ins where the script kiddies used a sophisticated tool to gain access to one operating system but then typed commands that work only on another operating system [Rogers 00].



The level of knowledge required by intruders is getting steadily lower, yet their ability to perpetrate sophisticated attacks against the survivability of systems has increased.

Contributing factors include

- Explosion of computer and Internet availability
- Increase in broadband availability in residential areas
- Low priority of security for software developers
- Difficulty patching vulnerabilities on all systems
- Graphical user interface (GUI) based tools that exploit known software vulnerabilities
- Availability of Malware (Malicious Software) authoring/editing tools
- Introduction of tools that attempt to exploit multiple vulnerabilities, i.e. Nimda



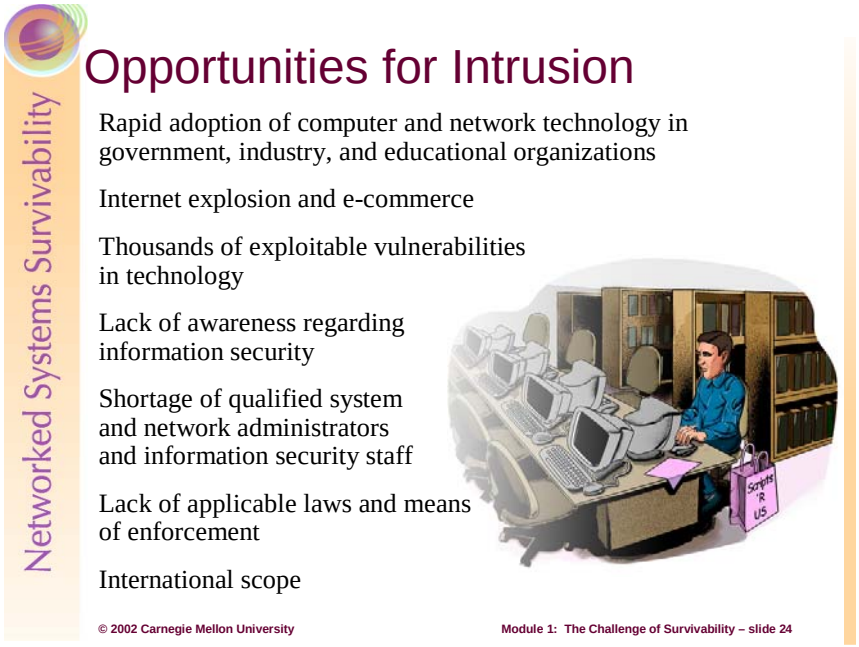
Motive

Motives for computer attacks have evolved just as the means have. In the early years of the Internet (then called the ARPAnet), there were no .com sites, only government and university research information. In 1981 only 213 computers were connected to the Internet. The small network made it easy for researchers at diverse locations to cooperate on work to their mutual benefit. There was a collegial atmosphere of sharing among people who either knew each other or knew of each other.

Contrast that to today's Internet. The January 2000 Internet Domain Survey reports that .com sites make up more than one-third of the Internet, which as of now, has passed the 100-million computers mark. You can find nearly everything on the Internet today: proprietary information about companies and people, corporate strategic plans, access to financial resources, and most commercial products.

Computer power has increased from the days of the VAX-11/780 with its 1 MIPS (million instructions per second) processing power, to 2Ghz (gigahertz) Pentium IV processors, producing 3,792 MIPS. As a result, attackers can steal processing power without the knowledge of the computer owner.

Long gone are the days of users and administrators knowing and trusting each other. Users on the Internet are anonymous, and their number grows daily. The atmosphere is not collegial, and trust is neither automatic nor always warranted [Rogers 00].



Opportunities

Opportunities for computer attacks are readily available for two reasons: the number of vulnerable systems on the Internet and the ease of connecting to the Internet. Ten years ago, there were about 300,000 hosts on the then ARPAnet; today there are over 100 million. Even if the same percentage of vulnerable hosts exists, that's over 300 times the number of vulnerable hosts today.

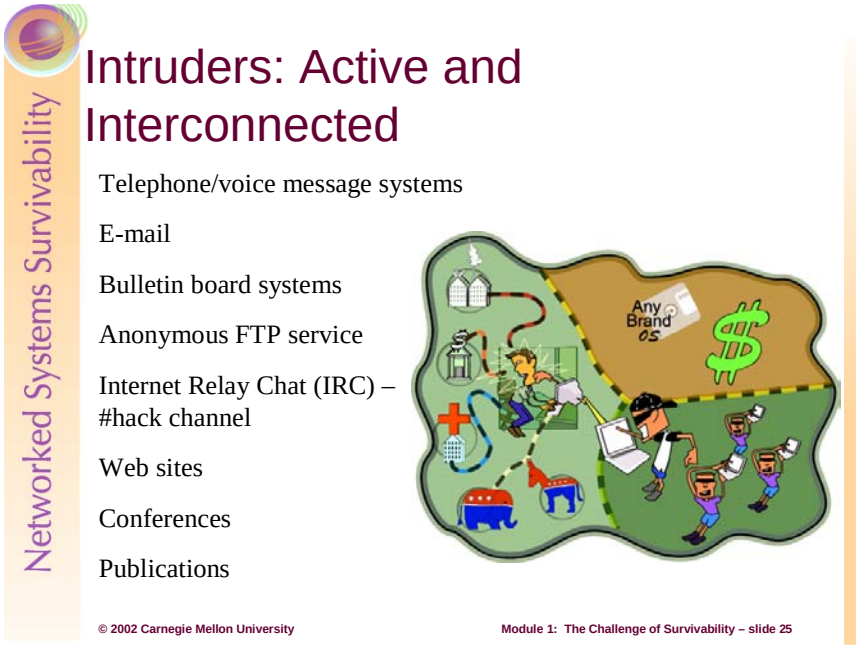
The number of computers on the Internet and the difficulty of configuring them securely mean that attackers have more chances of finding a way into systems than they did a decade ago. Along with low-cost (or no cost) Internet access, computers are inexpensive and the price is dropping. This means that more attackers can afford both the computer and Internet access needed for an attack.

Also, there are many more opportunities for computer access. Some libraries provide free Internet access. These Internet access points are a convenience and a helpful service, but they are also an opportunity to commit a crime, and are readily available to anyone so inclined.

Whatever the motive - money, curiosity, politics, power - this is all it takes to commit a crime on the Internet:

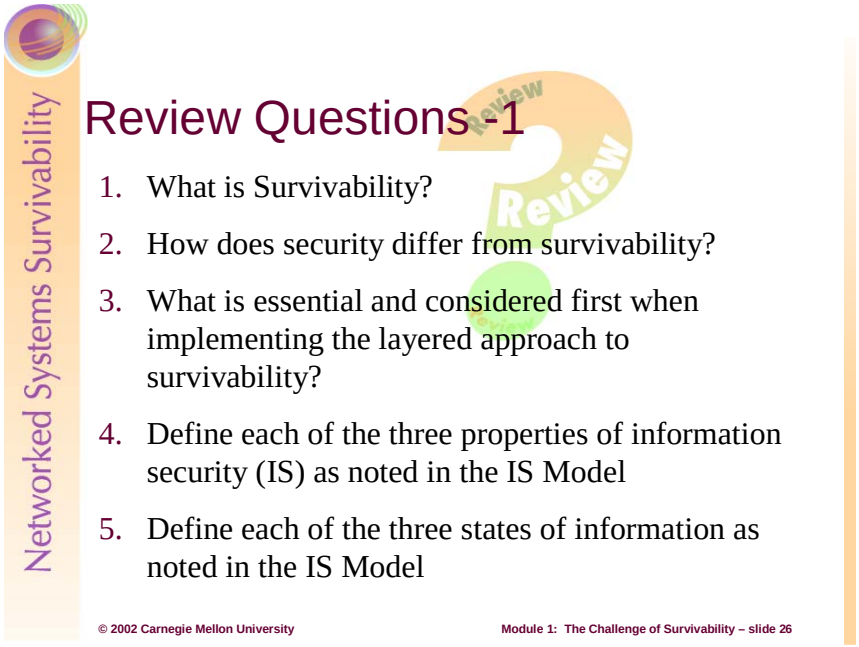
- Means – The tools are there, nicely catalogued and ready to go.
- Motives – With so much on the Internet, motives are there.
- Opportunity – There are many, many access points to the Internet, most inexpensive, some free.

Intrusions are going to happen; it's inevitable. Administrators, their managers, and senior executives all need to know what they're up against so that they are better equipped to deal with attacks and be aware of what intruders are doing. Because attack techniques and tools are constantly changing, we must maintain constant vigilance [Rogers 00].

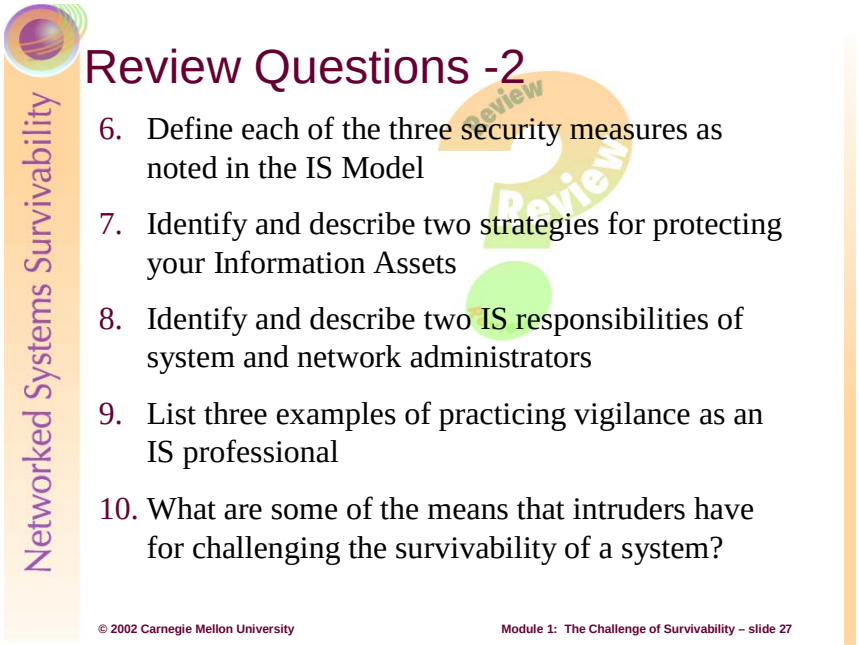


Just a few minutes of research on your favorite Internet search engine quickly shows how popular hacking has become. Intruders have a number of methods for exchanging information—most of these are available from the privacy of there own home, or even a public library. Hacking conferences such as *Def Con* draw thousands of participants including information security professionals and consultants, members of law enforcement, curious wanabees, script kiddies, as well as presenters from around the globe. The publication *2600 The Hacker Quarterly* has been in publication since January 1987 and has thousands of subscribers.

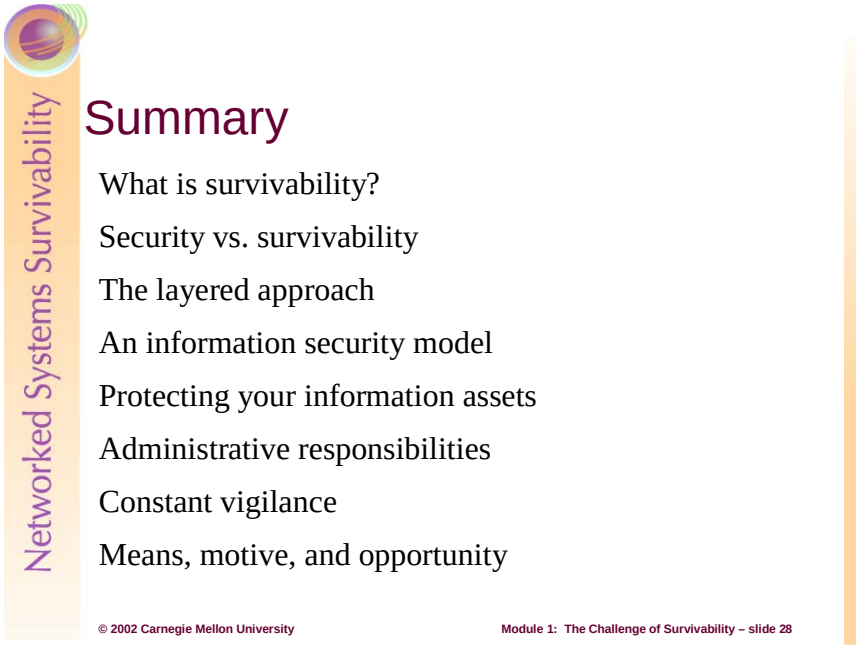
There are literally thousands of Intruder web sites that offer advice and easy-to-use tool-kits and scripts—many of these supported by surprisingly good documentation. Examples of some of the more infamous tools are Back Orifice (aka BO) authored by the Cult of the Dead Cow group and L0phtCrack authored by members of the L0pht-hackers turned information security professionals. The bottom line is: as the Internet community grows, so will the population of Intruders.



1. Answer: Survivability is the capability of a system to fulfill its mission, in a timely manner, in the presence of attacks, failures, or accidents
2. Answer: Security is a component of Survivability, and is concerned with ensuring that information has the properties of confidentiality, integrity, and availability
3. Answer: Risk Management
4. Answer: *Confidentiality* refers to assurance that information can be read and interpreted only by persons and processes explicitly authorized to do so. *Integrity* of information is the assurance that information remains intact, correct, and authentic. *Availability* refers to assurance that authorized users can access and work with information assets, resources, and systems when needed, with sufficient response and performance.
5. Answer: *Processing* refers to data that exists in local memory on a system. *Storage* refers to data that exists on physical media (i.e. a disk drive) or other non-volatile mediums. *Transmission* refers to data that is currently being transported on a network (i.e. on the wire).



6. Answer: *Policy and Procedures* are rules or expectations that seek to define desired behavior (i.e. Acceptable Use Policy). *Technology* is one means of attempting to enforce your policies and procedures (i.e. Web Filtering Software). *Education, Training, and Awareness* are essential because uninformed administrators and users can present a security risk in and of themselves.
7. Answer: *Prevention* is an attempt to implement security measures that proactively minimize the possibility of security problems from occurring. *Detection* is implemented such that administrators will notice security incidents when they (inevitably) occur.
8. Answer: *Monitoring* must be conducted by administrators so that suspicious network and system activity can be analyzed and then acted upon. *Backups and Fault Tolerance* help to ensure the availability of information.
9. Answer: *Scan for Viruses, Review Logs*, and *Conduct File/Directory Integrity Checking*.
10. Answer: Availability of Sophisticated Intrusion Tools, Accessibility to information concerning vulnerabilities and exploits.



Bibliography:

[Allen 01] Allen, Julia. *The CERT Guide to System and Network Security Practices*. Boston, MA: Addison-Wesley, 2001.

[ANST] American National Standard for Telecommunications - *Telecom Glossary 2000* Available at: http://www.its.bldrdoc.gov/projects/t1glossary2000/

[CSI 01] Power, Richard. *2001 CSI/FBI Computer Crime and Security Survey*. Computer Security Issues and Trends; Vol. VII, No.1, Spring 2001. Available at: http://www.gocsi.com/prelea/000321.html

[Krutz 2001] Krutz, Ronald L and Vines, Russell D. *The CISSP Prep Guide*. New York, NY. Wiley Computer Publishing, 2001.

[Lipson 99] Lipson, Howard and Fisher, David. *Survivability - A New Technical and*

Business Perspective on Security. Proceedings of the 1999 New Security Paradigms Workshop, September 22-24, 1999, Caledon Hills, Ontario, Canada. Available at: http://www.cert.org/archive/pdf/busperspec.pdf

[NST 94] National Security Telecommunications and Information Systems Security Committee. *NSTISSI 4011: National Training Standard for Information Systems Security Professionals*. Available at: http://www.nstissc.gov/Assets/pdf/4011.pdf

[Rogers 00] Rogers, Lawrence. *Means, Motive, and Opportunity*. Infosec Outlook; June 2000 Volume 1, Issue 3. Available at: http://www.cert.org/infosec-outlook/infosec_1-3.html#trends