Asset Management

ASSET MANAGEMENT STRATEGIES allow organizations to be vigilant against cyber attacks. Today, hospitals are suffering cyber attacks that cause commotion and disrupt day-to-day patient care. The biggest vulnerabilities lie in the numerous networked medical devices these hospitals use. Unfortunately, many organizations, including medical facilities, are unable to identify or produce inventory documentation of the locations and virtual addresses of these devices. The caution is, "You cannot protect what you do not know you have." A cyber asset management inventory helps prevent cyber attacks.

Objective:

Analyze the benefits of cyber asset management strategies, including hardware and software inventories, patches, and cloud computing fundamentals, in helping to secure networks.

Key Terms:

APIs
assets
breach
cloud computing
Common Vulnerabilities and Exposures (CVE®)
critical enterprise documentation (CED)
elasticity
evergreen inventory
firmware
intent
IT asset
IT asset management program
logical network topology
network topology
patch
patch management
physical network topology
risk
risk assessment
risk management
scalability
software
threat
topology diagram
vulnerability

Cyber Asset Management Strategies

Assets are persons, structures, facilities, information and records, information technology systems and resources, materials, processes, relationships, or reputations that have value. [Adapted from NICCS (National Initiative for Cybersecurity Careers and Studies, U.S. Department of Homeland Security).] An **IT asset** is any company-owned information, system, or hardware used in the course of business activities. An **IT asset management program** is the maintenance of a complete organizational inventory listing without employees conducting a physical or manual count. It is an extensive data gathering of detailed software and hardware inventory. For example:

- Items that are known and inventoried can be included in an organization's cyber security documentation.
- Deploying inquiries into a network could return detailed information of all the devices registered on that network. This is one way of gathering the data. The other way of gathering the data without the help of software would be recording it by hand in a log.

HARDWARE AND SOFTWARE SYSTEMS INVENTORIES

Risk

Risk is "the potential for an unwanted or adverse outcome resulting from an incident, event, or occurrence, as determined by the likelihood that a particular threat will exploit a particular vulnerability, with the associated consequences."

Vulnerability is "a characteristic or specific weakness that renders an organization or asset (such as information or an information system) open to exploitation by a given threat or susceptible to a given hazard."

A **threat** is anything that has the potential to cause serious harm, exploiting vulnerabilities and/or adversely impacting an organization's assets. A threat may or may not happen, but it does have the potential to cause damage. Computer security threats include viruses, worms, spyware, adware, scareware, keyloggers, Trojans, phishing, cookies, etc.

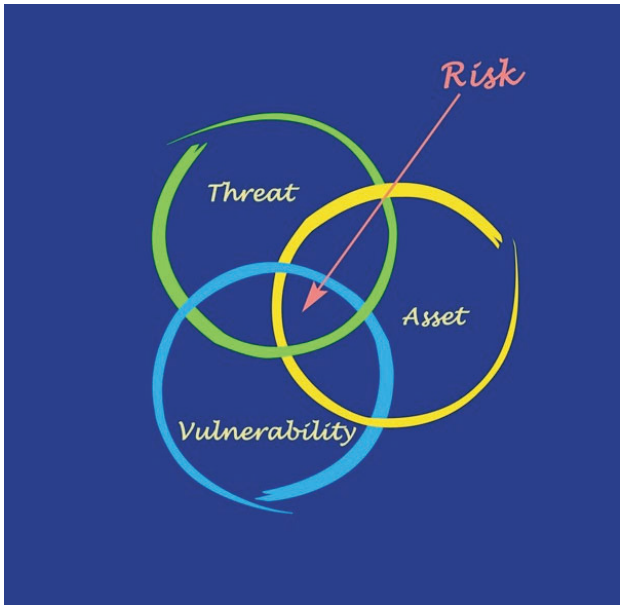

FIGURE 1. Risk is "the potential for an unwanted or adverse outcome resulting from an incident, event, or occurrence, as determined by the likelihood that a particular threat will exploit a particular vulnerability, with the associated consequences." [Source: NICCS.]

Risk assessment is "the product or process which collects information and assigns values to risks for the purpose of informing priorities, developing or comparing courses of action, and informing decision making."

Risk management is "the process of identifying, analyzing, assessing, and communicating risk and accepting, avoiding, transferring or controlling it to an acceptable-level considering associated costs and benefits of any actions taken." Life cycle schedules and replacement schedules are part of risk management.

[Source for all quoted definitions above: NICCS.]

Life Cycle Schedules

Maintaining hardware and software inventory schedules helps identify gaps between older systems and productivity life cycles. With these gaps identified, schedules can be created and tracked to allow for downtime when replacing systems.

Replacement Schedules

Replacing assets according to a schedule reduces the likelihood of a breach. A **breach** is an intrusion into an organization's network with intent to do harm. **Intent** is a state of mind or desire to achieve an objective. By following a replacement schedule, attention can be given to the activity of an older system as employees monitor the traffic to reduce the threat of an intruder that could potentially cost the organization significantly (dollars, reputation, lost clients, etc.).

Financial Benefits of Asset Management

When combining the effects of risk management and sound business operation, the result is almost always a financial benefit.

Asset Inventory Strategies

An **evergreen inventory** is a system to ensure that asset information is kept current. Recording all existing inventory categories is the first step. The next step is to conduct frequent audits (updates to the inventory). For example, personnel must be actively aware of their role within the company when a crisis occurs. Performing periodic scheduled audits helps ensure proper execution of the agreed-upon procedures. For example, hardware and software details, network and communications infrastructure details, mobile device details, and important paperwork and digital files details would appear on a cyber security asset inventory. Larger organizations may have additional requirements.

Hardware and Software Details

These include:

- Hardware location, model, purchase date, warranty information, etc.
- Software manufacturer, version, licensing and support contact information, etc.

Network and Communications Infrastructure Details

These include topology diagrams. The simplest type of topology is called point-to-point, which links two end points: telephone systems and computers connected to terminals use point-to-point topology. A **topology diagram** is a map of a company's infrastructure identifying physical locations and/or virtual addresses. Use of topology diagrams promotes efficient support and accurate recordkeeping (inventory). **Network topology** is the arrangement of a network, including its nodes and connecting lines. Network topologies have two geometries: physical (the geometric layout of workstations) and logical (signal).

Physical network topology is the configuration of cables, computers, and other peripherals. Physical layout diagrams include the following basic types as well as wireless:

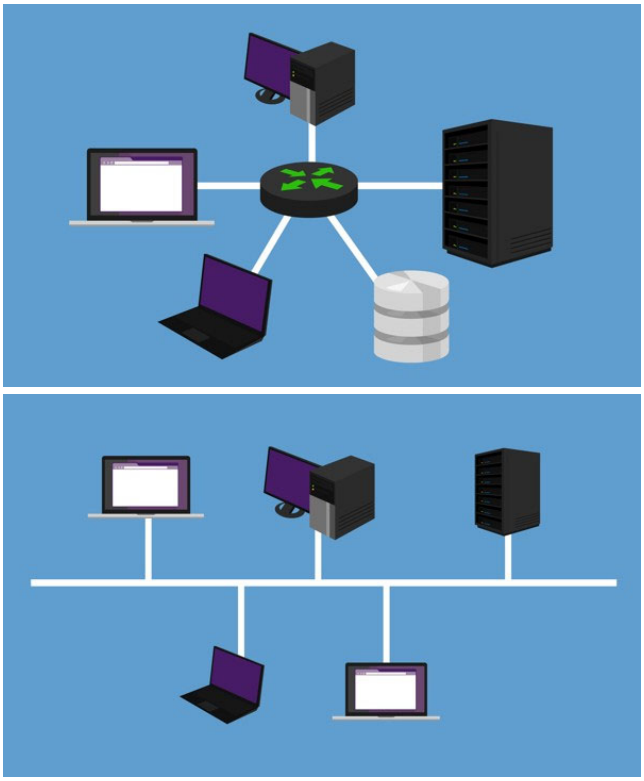

FIGURE 2. A topology diagram is a map of a company's infrastructure identifying physical locations and/or virtual addresses. Use of topology diagrams promotes efficient support and accurate recordkeeping (inventory). These two examples are simple local area network (LAN) diagrams: star and bus.

- *Bus*: Devices are all connected to the central cable (main wire) on a LAN, also called a backbone.
- *Mesh:* Devices are connected with many redundant interconnections between network nodes; often every node has a connection to every other node in the network.
- *Ring:* All nodes are connected in a closed loop; messages travel around the ring, and each node reads the messages addressed to it.
- *Star:* Devices are connected to a central computer, called a hub.
- *Tree:* This is a hybrid that combines features of bus and

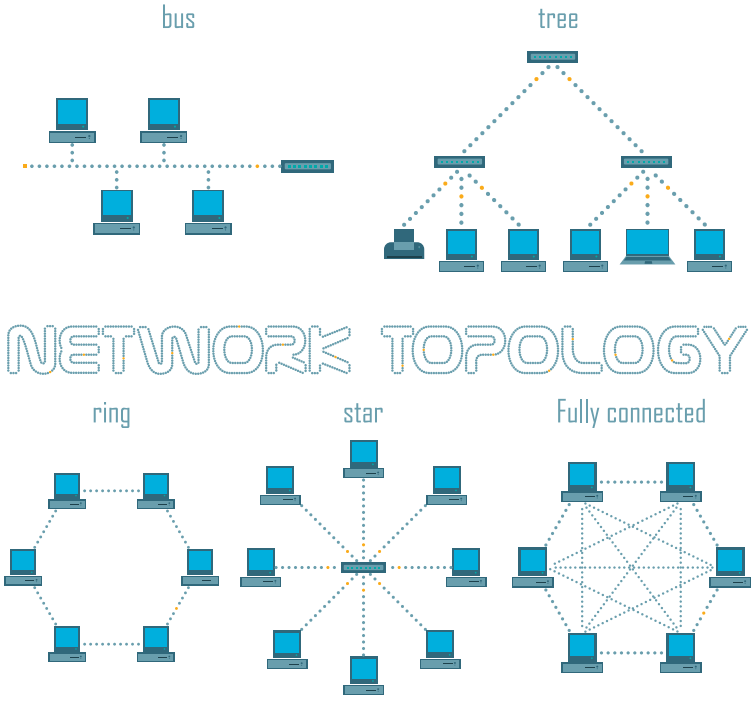

FIGURE 3. Network topology is the arrangement of a network, including its nodes and connecting lines. Network topologies have two geometries: physical (the geometric layout of workstations) and logical (signal). Topologies are part of an asset inventory.

star topologies; groups of star-configured networks are connected to a linear bus backbone cable.

Logical network topology is the way the signals act on the network media: the way data passes through the network from one device to the next regardless of the physical interconnection of the devices. For example, to communicate:

- Bus topology often uses Ethernet protocol.
- Bus or star topology often uses LocalTalk protocol.
- Ring topology often uses IBM's Token Ring protocol.

Mobile Device Details

- Device user, brand, model, device life cycle, etc.
- Mobile device contracts, monthly billing statements, data usage, etc.

Important Paperwork and Digital Files Details

Critical enterprise documentation (CED) [a.k.a. enterprise document management (EDM)] is a strategy for overseeing and managing the organization's important paperwork and digital files for easy retrieval in the event of a legal action or compliance audit. Other items that should be inventoried include:

- Closed circuit television and alarm systems
- Telephone circuits
- Facility equipment for IT services details

Requirements of Larger Organizations

A larger organization also requires inventories for the office environment, manufacturing facility, showroom, and IT support. Keeping the IT department "up and running" in the event of a cyber or natural disaster (tornado, hurricane, etc.) must be a priority. As such, documentation on electricity, heating/cooling, auxiliary power, etc., must also be up to date and part of the asset management inventory process.

PATCH SOFTWARE AND FIRMWARE

Patches

A **patch** is a piece of software composed of code inserted (patched) into an existing software program to fix a problem in the program. Patches are designed to update a computer program or its supporting data, to fix or improve it. They are often short-term fixes installed between full releases of a software package. **Patch management** is a systems management

practice that involves acquiring, testing, and installing multiple code changes to a computer system. According to the Technopedia website, patches are used to:

- Fix software bugs
- Install new drivers
- Address security vulnerabilities or threats
- Address software stability
- Upgrade software

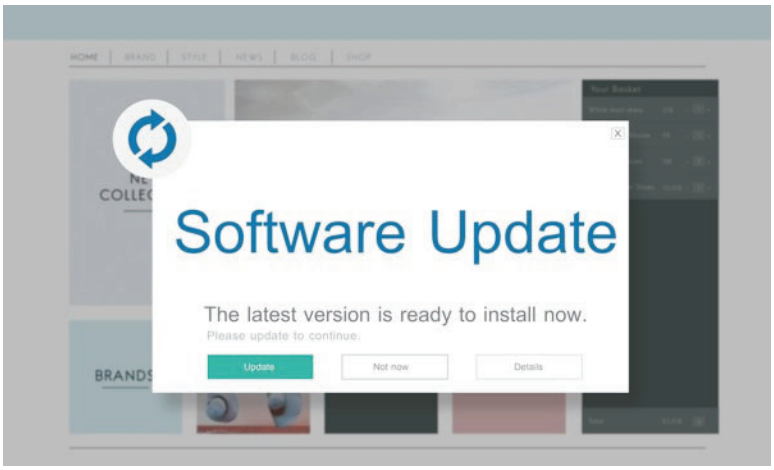

FIGURE 4. A patch is a piece of software composed of code inserted (patched) into an existing software program to fix a problem in the program. Patches are designed to update a computer program or its supporting data, to fix or improve it. They are often short-term fixes installed between full releases of a software package.

Software and Firmware

Software is removable programs and other operating information that a computer uses to run. Patches for software programs address vulnerabilities users may encounter.

Firmware is permanent programming installed into a read-only memory device that comprises the computer or network. Manufacturers of hardware deploy patches for their firmware because of a changing digital landscape. Firmware is a type of computer program that provides the low-level control for a device's specific hardware. It is held in memory devices, such as ROM, EPROM, or flash memory. Devices that contain firmware include embedded systems:

- Consumer appliances (remote control devices for televisions, on-board computers and sensors for automobiles, timing and control systems for clothes washers, etc.)
- Computers (including routers and firewalls)
- Computer peripherals (printers, scanners, cameras, USB flash drives)

The Patch Management Process

STEP 1: Vulnerability Assessment. Conducting an audit to expose security threats and vulnerable areas of the production environment is an initial action. Automated processes are often the way the need for a patch is discovered.

STEP 2: Patch Assessment. This step determines what threats the patch poses. If decisions indicate a patch needs to be installed, this ensures a secure process to acquire the patch. Downloading the patch can be a timely process. To maximize employee productivity, the acquisition and download of the patch are typically set to occur during a period of the day when employee system access is least necessary. Scheduling a convenient time for the patch helps ensures no downtime and no loss of employee productivity.

STEP 3: Patch Testing. Patches may react differently in varying technology environments. Testing the patch in a secure section of a network is recommended to determine how it would affect a specific configuration. Patch testing is a good opportunity to ensure that complemen-

tary and supplementary updates are performed so the patch is implemented with little inconvenience to the user.

STEP 4: Distribution. Once the patch is tested and approved and conflicts are known, it is distributed. Once a system restore/backup point is created, patch deployment should occur as timely as its relative urgency dictates. If it is not a priority, it can wait for the most suitable time.

STEP 5: Verification. Patch management verifies the success of the installation and purpose for the patch. Once it is determined that the system is protected and all impact of installing the patch is known, normal operating functions can resume.

STEP 6: Management of the Compliance. New patches must be added to the baseline system information to be considered normal operating procedures. Standard analysis resumes to determine any abnormalities, overlooked or new. Users can subscribe to any feed highlighting necessary updates or vulnerabilities. Should any other vulnerability exist, the patch management process begins again.

CLOUD COMPUTING SECURITY FUNDAMENTALS

Benefits of Cloud Computing

Cloud computing is a general term for the delivery of hosted services over the Internet. [Source: TechTarget website.] It is also described as having that data synced with other information over the web. (In contrast, storing data or running programs from a hard drive is the opposite of cloud computing.) It is a "model for enabling on-demand network access to a shared pool of configurable computing capabilities or resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." [Source: NICCS.] Most cloud computing is on a pay-for-use basis. Advantages include the following.

Shared resources enable options for delivery and storage.

Scalability is "an attribute (quality, characteristic, feature) that describes the ability of a process, network, software, or organization to grow and manage increased demand." [Source: Technopedia website.] Scalability is also described as the ability to handle a growing amount of work in a capable manner or the ability to be enlarged to accommodate that growth. It is also a sign of stability and competitiveness. For

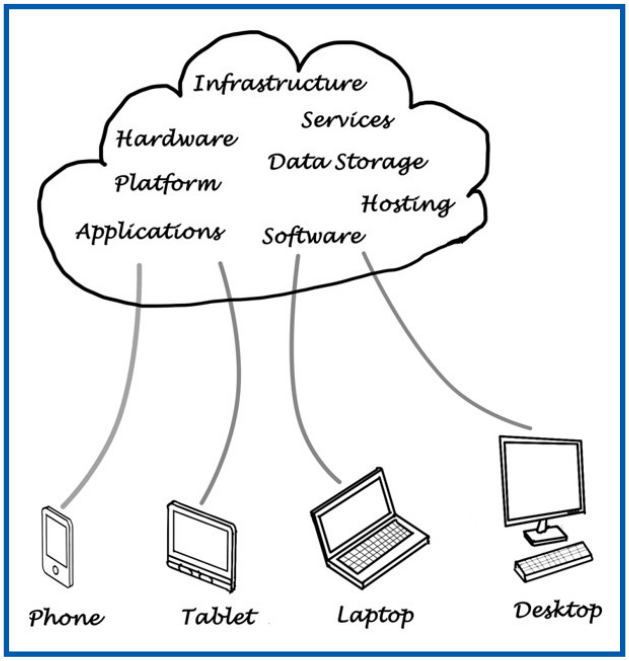

FIGURE 5. Cloud computing is a general term for the delivery of hosted services over the Internet. [Source: TechTarget website.] It is accessing data or programs over the Internet (or having that data synced with other information over the web). The opposite of cloud computing is storing data or running programs from a hard drive.

example, according to the Stack Overflow website, "If you can do something on a small database (say less than 1,000 records), a program that is highly scalable would work well on a small set as well as working well on a large set (say millions, or billions of records)." This is an important benefit in cloud computing because, as its popularity grows, it will need more space to operate, and it will need to provide more access to the users.

Elasticity is a type of horizontal scaling: it is "the degree to which a system is able to adapt to workload changes by provisioning and de-provisioning resources in an autonomic (involuntary) manner and…at each point in time the available resources match the current demand as closely as possible." [Source: Nikolas Herbst, Samuel Kounev, Ralf Reussner (2013), "Elasticity in Cloud Computing: What It Is, and What It Is Not" (PDF), *Proceedings of the 10th International Conference on Autonomic Computing (ICAC 2013), San Jose, CA, June 24–28*.] Elasticity allows users to quickly change the amount of cloud resources they need.

One pays only for the resources used. (Overpaying for access or storage for a service one is not using, via other methods and providers, is a monetary disadvantage to the user.)

The user regulates how many resources are needed and when it is time to increase usage. The user can control resource use.

Three Main Cloud Computing Categories

SaaS (Software as a Service)

SaaS is a category of cloud computing that is a software licensing and delivery model in which a third-party provider hosts applications and makes them available to customers over the Internet. It resides in the cloud, so it doesn't take up hard drive space of the user or space in the servers at a company. It is sometimes referred to as "on-demand software." In short, an organization that uses SaaS also eliminates the need to purchase and install hardware, provisioning and maintenance, and software licensing. The software is accessible to the audience for which it is intended from any web browser or cloud application. The consumer has no commitment to maintain the usability of the software. SaaS delivers many of the following types of business application software:

- Office suite
- Messaging
- Payroll
- CAD
- Accounting
- Invoicing
- Many types of customer and human resources packages

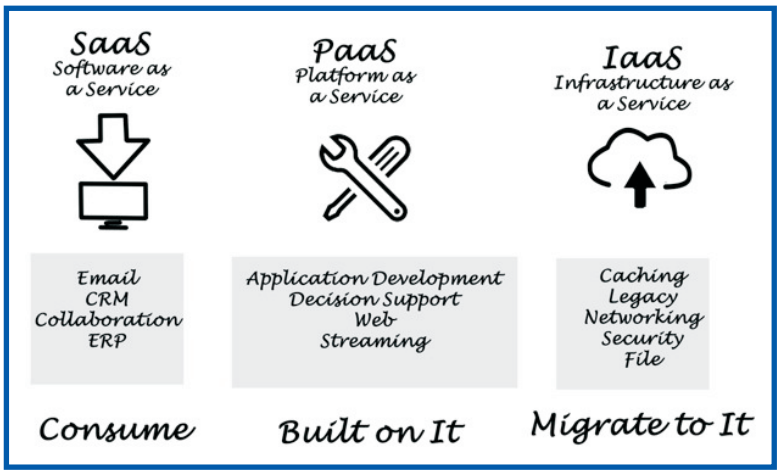

FIGURE 6. SaaS is a software licensing and delivery model in which a third-party provider hosts applications and makes them available to customers over the Internet. PaaS provides a "stage" for customers to develop, run, and manage applications without building and maintaining the infrastructure associated with developing and launching an app. IaaS provides virtualized computing resources (infrastructure) over the Internet, including the use of virtual machines and other resources.

PaaS (Platform as a Service)

PaaS is a category of cloud computing that provides a "stage" for customers to develop, run, and manage applications without building and maintaining the infrastructure associated with developing and launching an app. An advantage of PaaS is that the consumer needs only to maintain the applications the consumer created. There are three types of PaaS: public, private, and hybrid. PaaS was originally intended for applications on public cloud services before expanding to private and hybrid types.

IaaS (Infrastructure as a Service)

IaaS is a cloud computing service for subscribers that provides virtualized computing resources (infrastructure) over the Internet, including the use of virtual machines and other resources. It uses high-level APIs (application programming interfaces) that dereference: use a name, a reference, or a container instead of values to access such tools as physical computing resources, data partitioning, scaling, security, backup, etc. Some types of IaaS offer a range of services that accompany the infrastructure: billing, log access, load balancing, and clustering.

APIs are a set of subroutine definitions, protocols, and tools for building application software.

Subscribers have access to storage, networks, and other basic resources of the IaaS provider, to create their own software and potentially their own operating systems.

Subscribers' resources manage anything they deploy or create.

Regulations and International Identifiers

Cloud computing processes are largely dictated by the organizations that govern the industry, similar to the way in which HIPAA compliance law ensures that healthcare organizations maintain the privacy of medical records. Also, many school districts allow greater parental access to student records as mandated by the Family Educational Rights and Protection Act (FERPA). FERPA sets the cloud computing processes that the districts follow. As a result, school districts must use cloud computing in ways that maintain security while allowing certain parties access to sensitive information.

Common Vulnerabilities and Exposures (CVE®) is a list of common identifiers for publicly known cyber security vulnerabilities. CVE is an international cyber security community for which the Cyber Security Division of the U.S. Department of Homeland Security provides funding. CVE Identifiers, or "CVE IDs," which are assigned by CVE Numbering Authorities (CNA) from around the world, ensure confidence among parties when used to discuss or share information about a unique software or firmware vulnerability, provide a baseline for tool evaluation, and enable data exchange for cyber security automation. CVE is:

- One identifier for one vulnerability or exposure
- One standardized description for each vulnerability or exposure
- A dictionary rather than a database
- How disparate databases and tools can "speak" the same language

FURTHER EXPLORATION...

ONLINE CONNECTION:
The Common Vulnerabilities and Exposures (CVE®) Website

When visiting the CVE website, you'll see the tagline "The Standard for Information Security Vulnerability Names." Rest assured that CVE has much of the known information to keep your system safe. This site discusses what it takes to become an authorized CVE numbering authority and provides users and/or technology departments with downloadable content. The resources on the site are impressive.

If you would like to stay informed about CVE, you can follow its Twitter feed to provide up-to-the-minute information. Its social media option is a fantastic way to know about the latest threats and about known cyber security issues. You can see for yourself what a community of concerned individuals can do to protect the industry by visiting the CVE website at https://cve.mitre.org/.

CVE is an international cyber security community for which the Cyber Security Division of the U.S. Department of Homeland Security provides funding.

- The way to interoperability and better security coverage
- A basis for evaluation among services, tools, and databases
- Free for public download and use
- Industry-endorsed via the CVE Numbering Authorities, CVE Board, and numerous products and services that include CVE. [Source: CVE website at https://cve.mitre.org/about/.]

Summary:

Assets are persons, structures, facilities, information and records, information technology systems and resources, materials, processes, relationships, or reputations that have value. [Adapted from NICCS.] An IT asset management program is the maintenance of a complete organizational inventory listing without employees conducting a physical or manual count. It is an extensive data gathering of detailed software and hardware inventory.

Yet, you cannot protect what you do not know you own. The sheer number of networked devices is already unfathomable. Organizations are continually purchasing and replacing devices, and each one must be properly inventoried if the network is to be secure. It's only a matter of time, according to many sources within the IT industry, until all companies will be hacked. However, if companies / government

offices / businesses exercise due diligence in protecting their firms, such as creating an asset inventory, the damage can be minimal.

Network intrusions can be identified and quarantined before any damage is done. These are still considered hacks, but nothing needs to be compromised that creates a financial burden. To minimize significant threats, you need to know your inventory, keep current with updates, and secure your cloud infrastructure.

Checking Your Knowledge:

1. What is an asset? What is IT asset management?
2. How do asset inventories assist cyber security?
3. Compare and contrast software and firmware.
4. What is a patch? How is it used for software and firmware fixes?
5. Describe cloud computing. In what ways do you consider cloud computing to be a risk to your data and information?

Expanding Your Knowledge:

Read the article, "Hollywood Hospital Pays $17,000 in Bitcoin to Hackers; FBI Investigating," at http://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html. Learn how this California hospital was held ransom because of a hacker gaining access to its network devices. Seventeen thousand dollars in bitcoin totals just under $170 million dollars. This was no easy pill to swallow, but what other choice did the hospital have? When medical devices are held ransom, lives are at risk, and new patients are told to go elsewhere. Weak cyber security asset management affects the future of hospitals and other institutions. What would you recommend to this Hollywood hospital to recover and prevent future hacks?

Web Links:

13 Biggest Challenges When Moving Your Business to the Cloud
https://www.forbes.com/sites/forbestechcouncil/2017/06/05/13-biggest-challenges-when-moving-your-business-to-the-cloud/#325585719b0e

The Safety Net of an Asset Management System
https://pointofsale.com/2017111722035/Point-of-Sale-News/The-Safety-Net-of-an-Asset-Management-System.html