Preventive Information Assurance Tools o Content Filters o Cryptographic Protocols and Tools o Firewalls o Proxy Servers o Public Key Infrastructure o Virtual Private Networks Preventive Information Assurance Tools Content Filters o Content filters control the access of end users to portions of the Internet.Patch Management o Patch management requires performing planned and timely system patches to maintain operational efficiency and effectiveness, mitigate information security vulnerabilities, and maintain the stability of IT systems.Preventive Information Assurance Tools Network Intrusion Prevention System o NIPS can be problematic if they are configured incorrectly or if they are unable to detect legitimate changes to an organization 's network o As noted, they are preventive devices and can often automatically shut off traffic or redirect it based on the rules provided to it. This can cause unplanned outages and confusion if NIPS configuration and modification is not part of an organization 's change management and configuration management process.o The most successful implementations of content filters contain a process through which users can request web sites be unblocked after it has been analyzed to determine whether it should be opened for use Preventive Information Assurance Tools Cryptographic Protocols and Tools o Cryptography is a technique for hiding information by transforming it so that only authorized individuals can access it in its original form.Organizations may choose to use network intrusion detection systems (NIDSs) instead of NIPS because of the disruptions NIPS may create Preventive Information Assurance Tools Proxy Servers o Proxy servers act as an intermediary between clients and the Internet by allowing clients to make indirect connections to other network services through them.o Sources of change: o Alliances and partnerships o Business market demands o Competitive markets o Operational issues o Regulations changes Change Management and Configuration Management 2/2 o Configuration management controls hardware, software, and their associated documentation.Proxy servers can be configured to require authentication of the end user, restricting communication to a defined set of protocols, applying access control restrictions, and carrying out auditing and logging.Preventive Information Assurance Tools Network Intrusion Prevention System There are two types of network intrusion prevention systems: Content based used to detect attacks, the contents of the network packets are checked for distinctive sequences called signatures.The strongest VPN solutions use multifactor authentication and have their cryptography certified by independent parties such as the U.S. National Institute of Standards and Technology's Cryptographic Module Validation Program (CVMP).Content filters may be used to change employees' productivity and to increase an organization's information assurance profile by reducing user access to web sites that have no organizational value, improper content, or malicious code.SSL and TLS are preferred information security protocols in web environments, while IPSec protocols are preferred for implementing virtual private networks (VPNs).Additionally, firewalls are often multifunction devices that may also contain solutions for remote users to connect to an organization's intranet and web content filtering.PKI enables a secure method for exchanging confidential information over unsecured networks and is the de facto standard for implementing trust online.Preventive Information Assurance Controls Backup Change Management and Configuration Management IT Support Media Controls and Documentation Patch Management Backup o An organization should have a policy on what to back up (data, software, and hardware), when to back up (depending on the frequency of changes that occur), and how to back up

Summarized by © lakhasly.com

(the process of backup).o Examples of protocols that implement network services include Secure Sockets Layer (SSL), Transport Layer Security (TLS), and IP Security (IPSec) protocols.Proxy Vs VPN Preventive Information Assurance Tools Public Key Infrastructure o The use of public key infrastructure (PKI) implementation is growing worldwide.o A successful and effective patch management program combines well-defined processes, effective software, and training into a strategic program for assessing, obtaining, testing, and deploying patches.o Encryption techniques for hosts range from encryption of the entire hard disk, database encryption, selective folder (group of files) encryption, or individual file encryption.o Access control policies may be implemented in the firewall and are important for controlling information traffic and movement from public accessible networks to private networks but they are not solver for all problems.Preventive Information Assurance Tools Network Intrusion Prevention System oA network intrusion prevention system (NIPS) inspects network traffic based on organizational information assurance policy and configuration.Various types of VPN protocols are IPSec, SSL, Point-to-Point Tunneling Protocol (PPTP), and others.Organizations should be vigilant and do pre implementation research about key management and types of encryption algorithms used and their strengths before employing any VPN technology.o Note that there are limitations in firewalls because they can only inspect and filter the traffic that flows through them; they cannot protect from internal threats unless appropriately implemented.Preventive Information Assurance Tools Proxy Servers o Care should be used with proxy servers since they can be used to disguise sources of traffic (anonymized).Preventive Information Assurance Tools Public Key Infrastructure o A common way of associating public keys with their owners is to use digital certificates.In PKI, user credentials take the form of a digital certificate, think of it as an electronic passport.o One in five companies (19 per cent) that suffered a malicious data breach was infiltrated due to stolen or compromised credentials, increasing the average total cost of a breach for these companies by nearly $1 million to $4.77 million.Going out of favour due to the lowering in costs associated with disk-based backup o Cloud backup: This utilizing a service like Amazon Web Services to provide backup services versus an internal backup mechanism.Preventive Information Assurance Tools Cryptographic Protocols and Tools Preventive Information Assurance Tools Firewalls o Firewalls act as a primary control for information assurance technology.This system uses application content, behavior, and context, and not IP addresses or ports, to formulate decisions on access control.o A digital certificate is an electronic message that links a public key to the name of the owner in a secure way by using a trusted third party, known as a certificate authority (CA), that guarantees the relationship.o Certificates may be published and stored in public directories such as an LDAP server.Preventive Information Assurance Tools Virtual Private Networks o A virtual private network is a secure network that uses a public network (usually the Internet) to allow users to interconnect.A VPN provides costeffective solutions to organizations spread over wide areas.Although a firewall protects network assets, organizational systems will be at a higher risk of compromise if patch management is implemented inappropriately.o For example, a financial system will typically provide data to human resources and external business partners o Is the information synced or replicated across multiple servers?Organizations should track all changes to configuration items throughout the life cycle of the components and system with tracking records.Configuration management is closely related to asset

management it represents the detailed configuration information for each identified asset.Configuration is also closely related to contingency planning because restored systems must comply with configuration baseline standards.Cryptographic tools also provide confidentiality, integrity, and nonrepudiation protection as defined by the MSR model discussed earlier.o Firewalls are widely used throughout organizations; however, recently there has been an increase in the usage of personal firewalls.It may reduce the exploitation of a network with its capability to manage network packets and identify attacks.An anomaly –based NIPS may be used to prevent denial of service (DOS) attacks by monitoring and learning normal network behavior.Preventive Information Assurance Controls o Network and computing environments constantly change.o Disk backup: Because the storage is not linear, such as tape, individual files can be directly accessed allowing for faster recovery times.o The information security professional must make take care when reviewing the cloud backup provider contract ensuring that the backup provider meets all of the information security requirements for the business' information.These tools allow network administrators to block access selectively to certain types of web sites based on predefined local policy.The simplest form of a proxy server is called a gateway.With faster growth of e–commerce, e business, and e–government applications, the adoption of PKI has increased in recent years.Authentication using PKI technology means proving one's identity by proving knowledge of the associated private key (as indeed the owner of that private key).o IPSec uses the Internet Key Exchange (IKE) protocol to exchange certificates as part of the key exchange procedure.It uses cryptographic means (encryption) to provide secure communications on public networks.Various out–of the–box VPN solutions are readily available.Organizations need to ensure that proper mechanisms exist to complement the use of technology.The full suite of preventive information assurance mechanisms that can be used follows.It is thus critical that restoration and integrity tests are performed frequently.Change Management and Configuration Management 1/2 o If an organization is to remain competitive, it should be prepared to change continuously since the environment is not static.Common practices for an effective patch management include the following: standardized patch management policies, procedures, and tools.They may be implemented as hardware, software, or a combination of both. They exist at the host (desktop, user level) and the network or server level.PKI provides a secure electronic business environment.o According to Norton, the average recovery cost from a common data breach is estimated at $3.86 million.Human error was the cause of 23 per cent of breaches, and system glitches (25 per cent), were at an average total cost of $4.27 million.Types of storage options o Virtual machine snapshot: This type of backup makes a point in time copy of a virtual machine disk file.o Tape backup: Liner storage mechanism used for long–term archival storage.o Organizations should not implement configuration management without having a change management process in place.They can also be used to cache web content.The same Norton research found that it can take companies, on average, 196 days to identify a data breach.The backup process should be fully supported by the baseline process.o Backing up systems is important, but more important is the correct restoration of the backup.This can be used to restore a virtual machine to a particular point in time.It provides a higher capacity and speed than tape.All others are denied access since they cannot decrypt the information.Another good practice is to document each restoration step.Refer to Chapter 25 for more

information on backup and related matters.Questions you should ask your IT organization regarding the information's location o Is the information shared with multiple information systems?It is part of configuration management.o How is the information backed up?

Summarized by © lakhasly.com