6.3: Tools for Information Security

To ensure the confidentiality, integrity, and availability of information, organizations can choose from various tools. Each of these tools can be utilized as a part of an overall information-security policy, which will be discussed in the next section.

Authentication

The most common way to identify people is through physical appearance, but how do we identify someone sitting behind a computer screen or at the ATM? Tools for authentication are used to ensure that the person accessing the information is, indeed, who they present themselves to be.

Authentication can be accomplished by identifying someone through one or more of three factors: something they know, something they have, or something they are. For example, the most common form of authentication today is the user ID and password. In this case, the authentication is done by confirming something that the user knows (their ID and password). But this form of authentication is easy to compromise (see sidebar), and stronger forms of authentication are sometimes needed. Identifying someone only by something they have, such as a key or a card, can also be problematic. When that identifying token is lost or stolen, the identity can be easily stolen. The final factor, something you are, is much harder to compromise. This factor identifies a user through physical characteristics, such as an eye-scan or fingerprint. Identifying someone through their physical characteristics is called biometrics.

A more secure way to authenticate a user is to do multi-factor authentication. Combining two or more of the factors listed above makes it much more difficult for someone to misrepresent themselves. An example of this would be the use of an RSA SecurID token. The RSA device is something you have and will generate a new access code every sixty seconds. To log in to an information resource using the RSA device, you combine something you know, a four-digit PIN, with the device's code. The only way to properly authenticate is by both knowing the code and having the RSA device.

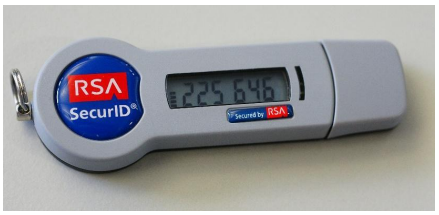

Figure 6.3.1: An RSA SecurID SID800 token with USB connector. Image by Alexander Klink is licensed CC BY

Access Control

Once a user has been authenticated, the next step is to ensure that they can access the appropriate information resources. This is done through the use of access control. Access control determines which users are authorized to read, modify, add, and/or delete information. Several different access control models exist. Here we will discuss two: the access control list (ACL) and role-based access control (RBAC).

For each information resource that an organization wishes to manage, a list of users who have the ability to take specific actions can be created. This is an access control list or ACL. For each user, specific capabilities are assigned, such as reading, writing, deleting, or adding. Only users with those capabilities are allowed to perform those functions. If a user is not on the list, they have no ability even to know that the information resource exists.

ACLs are simple to understand and maintain. However, they have several drawbacks. The primary drawback is that each information resource is managed separately. If a security administrator wanted to add or remove a user to a large set of information resources, it would not be easy. And as the number of users and resources increases, ACLs become harder to maintain. This has led to an improved method of access control, called role-based access control, or RBAC. With RBAC, instead of giving specific users access rights to an information resource, users are assigned to roles, and then those roles are assigned access. This allows the administrators to manage users and roles separately, simplifying administration and, by extension, improving security.

Access Control List

User	Read	Write	Add	Delete
jsmith	x			
rlee	x			
knguyen	x	x	x	x
mroberts	x	x		
manderson	x	x		

Role-Based Access Control

Role	Read	Write	Add	Delete
Reader	x			
Editor	x	x		
Administrato	x	x	x	x

Role Assignments

User	Role
jsmith	Reader
rlee	Reader
knguyen	Admin
mroberts	Editor
manderson	Editor

Figure 6.3.2 Comparison of ACL and RBAC. Image by David Bourgeois is licensed CC BY 4.0

Encryption

An organization often needs to transmit information over the Internet or transfer it on external media such as a USB. In these cases, even with proper authentication and access control, an unauthorized person can access the data. Encryption is a process of encoding data upon its transmission or storage so that only authorized individuals can read it. This encoding is accomplished by a computer program, which encodes the plain text that needs to be transmitted; then, the recipient receives the ciphertext and decodes it (decryption). For this to work, the sender and receiver need to agree on the method of encoding so that both parties can communicate properly. Both parties share the encryption key, enabling them to encode and decode each other's messages. This is called symmetric key encryption. This type of encryption is problematic because the key is available in two different places.

EMPLOYEE INFORMATION

Name: Employee ID:
Department: Employee Job Title:
Supervisor: Supervisor Job:

RATINGS

	Poor	Fair	Satisfactory	Good	Excellent
Job Knowledge—Understands duties, responsibilities, has ability to use materials needed, and has the level of proficiency required to accomplish the work.	☐	☐	☐	☐	☐
Comments					
Work Quality—Accuracy, thoroughness, dependability of results.	☐	☐	☐	☐	☐
Comments					
Attendance—Reports to work as scheduled. Follows established procedures for breaks. Notifies supervisor in advance of scheduling changes.	☐	☐	☐	☐	☐
Comments					
Initiative—Ability to be self-directed, efficient, creative, and resourceful. Assumes extra work on own initiative, adapts quickly to new responsibilities.	☐	☐	☐	☐	☐
Comments					
Work Attitude and Cooperation—Extent to which employee demonstrates a positive attitude, and promotes cooperation with supervisors, peers and others.	☐	☐	☐	☐	☐
Comments					
Dependability—Extent to which employee can be counted on to carry out instructions and fulfill job responsibilities accurately and efficiently.	☐	☐	☐	☐	☐
Comments					
Overall Rating					

Figure 6.3.3 Symmetric/private key encryption. Image by Phayzfaustyn is licensed CC0 1.0

An alternative to symmetric key encryption is public-key encryption. In public-key encryption, two keys are used: a public key and a private key. To send an encrypted message, you obtain the public key, encode the message, and send it. The recipient then uses the private key to decode it. The public key can be given to anyone who wishes to send the recipient a message. Each user needs one private key and one public key to secure messages. The private key is necessary to decrypt something sent with the public key.

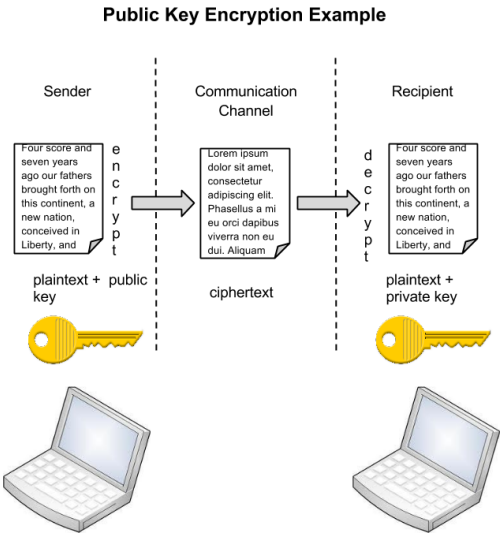

Figure 6.3.4 Public key encryption. Image by David Bourgeoi Ph.D. is licensed CC BY 4.0

Sidebar: Password Security

The security of a password depends on its strengths to guard against brute-force guesses. Strong passwords reduce overall breaches of security because it is harder for criminals to guess.

Password policies and technologies have evolved to combat security threats, from short to long passwords, from single-factor authentication to multi-factor authentications. Most companies now have specific requirements for users to create passwords and how they are authenticated.

Below are some of the more common policies that organizations should put in place.

- **Require complex passwords that make it hard to guess**. For example, a good password policy requires the use of a minimum of eight characters, and at least one upper-case letter, one special character, and one number.
- **Change passwords regularly**. Users must change their passwords regularly. Users should change their passwords every sixty to ninety days, ensuring that any passwords that might have been stolen or guessed will not be used against the company.
- **Train employees not to give away passwords**. One of the primary methods used to steal passwords is to figure them out by asking the users or administrators. Pretexting occurs when an attacker calls a helpdesk or security administrator and pretends to be a particular authorized user having trouble logging in. Then, by providing some personal information about the authorized user, the attacker convinces the security person to reset the password and tell him what it is. Another way that employees may be tricked into giving away passwords is through email phishing.
- **Train employees not to click on a link**. Phishing occurs when a user receives an email that looks as if it is from a trusted source, such as their bank or their employer. In the email, the user is asked to click a link and log in to a website that mimics the genuine website and enter their ID and password, which the attacker then captures.

Backups

Another essential tool for information security is a comprehensive backup plan for the entire organization. Not only should the data on the corporate servers be backed up, but individual computers used throughout the organization should also be backed up. A good backup plan should consist of several components.

- **A full understanding of the organizational information resources.** What information does the organization actually have? Where is it stored? Some data may be stored on the organization's servers, other data on users' hard drives, some in the cloud, and some on third-party sites. An organization should make a full inventory of all of the information that needs to be backed up and determine the best way to back it up.
- **Regular backups of all data**. The frequency of backups should be based on how important the data is to the company, combined with the company's ability to replace any data that is lost. Critical data should be backed up daily, while less critical data could be backed up weekly.
- **Offsite storage of backup data sets**. If all of the backup data is being stored in the same facility as the original copies of the data, then a single event, such as an earthquake, fire, or tornado, would take out both the original data and the backup! It is

essential that part of the backup plan is to store the data in an offsite location.
- **Test of data restoration**. Regularly, the backups should be put to the test by having some of the data restored. This will ensure that the process is working and will give the organization confidence in the backup plan.

Besides these considerations, organizations should also examine their operations to determine what effect downtime would have on their business. If their information technology were to be unavailable for any sustained period of time, how would it impact the business?

Additional concepts related to backup include the following:

- **Universal Power Supply (UPS)**. A UPS is a device that provides battery backup to critical components of the system, allowing them to stay online longer and/or allowing the IT staff to shut them down using proper procedures to prevent the data loss that might occur from a power failure.
- **Alternate or "hot" sites.** Some organizations choose to have an alternate site where their critical data replica is always kept up to date. When the primary site goes down, the alternate site is immediately brought online to experience little or no downtime.

As information has become a strategic asset, a whole industry has sprung up around the technologies necessary for implementing a proper backup strategy. A company can contract with a service provider to back up all of their data or purchase large amounts of online storage space and do it themselves. Most large businesses now use technologies such as storage area networks and archival systems.

Firewalls

Another method that an organization should use to increase security on its network is a firewall. A firewall can exist as hardware or software (or both). A hardware firewall is a device connected to the network and filters the packets based on a set of rules. A software firewall runs on the operating system and intercepts packets as they arrive at a computer. A firewall protects all company servers and computers by stopping packets from outside the organization's network that does not meet a strict set of criteria. A firewall may also be configured to restrict the flow of packets leaving the organization. This may be done to eliminate the possibility of employees watching YouTube videos or using Facebook from a company computer.

Some organizations may choose to implement multiple firewalls as part of their network security configuration, creating one or more sections of their partially secured network. This segment of the network is referred to as a DMZ, borrowing the term demilitarized zone from the military. It is where an organization may place resources that need broader access but still need to be secured.

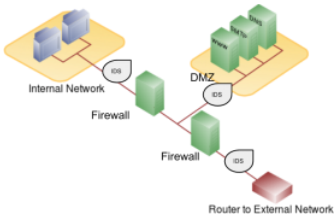

Figure 6.3.5 Network configuration with firewalls, IDS, and a DMZ. Image by David Bourgeois is licensed CC BY 4.0

Intrusion Detection Systems

Another device that can be placed on the network for security purposes is an intrusion detection system or IDS. An IDS does not add any additional security; instead, it provides the functionality to identify if the network is being attacked. An IDS can be configured to watch for specific types of activities and then alert security personnel if that activity occurs. An IDS also can log various types of traffic on the network for analysis later. An IDS is an essential part of any good security setup.

Physical Security

An organization can implement the best authentication scheme globally, develop the best access control, and install firewalls and intrusion prevention. Still, its security cannot be complete without the implementation of physical security. Physical security is the protection of the actual hardware and networking components that store and transmit information resources. To implement physical security, an organization must identify all of the vulnerable resources and ensure that these resources cannot be physically tampered with or stolen. These measures include the following.

- **Locked doors**: It may seem obvious, but all the security in the world is useless if an intruder can walk in and physically remove a computing device. High-value information assets should be secured in a location with limited access.
- **Physical intrusion detection**: High-value information assets should be monitored through the use of security cameras and other means to detect unauthorized access to the physical locations where they exist.
- **Secured equipment**: Devices should be locked down to prevent them from being stolen. One employee's hard drive could contain all of your customer information, so it must be secured.
- **Environmental monitoring**: An organization's servers and other high-value equipment should always be kept in a monitored room for temperature, humidity, and airflow. The risk of server failure rises when these factors go out of a specified range.
- **Employee training**: One of the most common ways thieves steal corporate information is to steal employee laptops while employees are traveling. Employees should be trained to secure their equipment whenever they are away from the office.

Security Policies

Besides the technical controls listed above, organizations also need to implement security policies as a form of administrative control. In fact, these policies should really be a starting point in developing an overall security plan. A good information-security policy lays out the guidelines for employee use of the information resources of the company. It provides the company recourse in the case that an employee violates a policy.

A security policy should be guided by the information security triad discussed above. It should lay out guidelines and processes for employees to follow to access all resources to maintain the three categories' integrity: confidentiality, integrity, and availability.

Policies require compliance and need to be enforceable; failure to comply with a policy will result in disciplinary action. SANS Institute's Information Security Policy Page (2020) lists many templates for different types of security policies. One example of a security policy is how remote access should be managed, which can be found here.

A security policy should also address any governmental or industry regulations that apply to the organization. For example, if the organization is a university, it must be aware of the Family Educational Rights and Privacy Act (FERPA), which restricts who has access to student information. Health care organizations are obligated to follow several regulations, such as the Health Insurance Portability and Accountability Act (HIPAA).

Mobile Security and Remote Work

Mobile devices like smartphones and laptops along with remote work capabilities introduce new security challenges for businesses. As mobile devices such as smartphones and tablets proliferate, organizations must be ready to address the unique security concerns that these devices use. One of the first questions an organization must consider is whether to allow mobile devices in the workplace.

Many employees already have these devices, so the question becomes: Should we allow employees to bring their own devices and use them as part of their employment activities? Or should we provide the devices to our employees? Creating a BYOD ("Bring Your Own Device") policy allows employees to integrate themselves more fully into their job and bring higher employee satisfaction and productivity. It may be virtually impossible to prevent employees from having their own smartphones or iPads in the workplace in many cases. If the organization provides the devices to its employees, it gains more control over the use of the devices, but it also exposes itself to the possibility of an administrative (and costly) mess.

Mobile devices can pose many unique security challenges to an organization. Probably one of the biggest concerns is the theft of intellectual property. It would be a straightforward process for an employee with malicious intent to connect a mobile device either to a computer via the USB port or wirelessly to the corporate network and download confidential data. It would also be easy to take a high-quality picture using a built-in camera secretly.

When an employee has permission to access and save company data on their device, a different security threat emerges: that device now becomes a target for thieves. Theft of mobile devices (in this case, including laptops) is one of the primary methods that data thieves use.

So, what can be done to secure mobile devices? It will start with a good policy regarding their use. Specific guidelines should include

- Mobile device management (MDM) software to configure security settings, encrypt data, remotely wipe lost devices, etc.
- Containerization to isolate and secure corporate data and apps separately from personal content.
- Multi-factor authentication and secure VPN for remote access.

- Policies requiring PIN/password protection, app blacklisting/whitelisting, and avoiding public WiFi.
- Securing cloud-based business apps and limiting employee BYOD usage if deemed high risk.

Besides policies, there are several different tools that an organization can use to mitigate some of these risks. For example, if a device is stolen or lost, geolocation software can help the organization find it. In some cases, it may even make sense to install remote data-removal software, which will remove data from a device if it becomes a security risk.

> **Note: Virtual Private Networks (VPN)**
>
> Using firewalls and other security technologies, organizations can effectively protect many of their information resources by making them invisible to the outside world. But what if an employee working from home requires access to some of these resources? What if a consultant is hired to work on the internal corporate network from a remote location? In these cases, a virtual private network (VPN) is called for.
>
> A VPN allows a user outside of a corporate network to detour around the firewall and access the internal network from the outside. A combination of software and security measures lets an organization allow limited access to its networks while at the same time ensuring overall security.

Usability

When looking to secure information resources, organizations must balance the need for security with users' need to access and use these resources effectively. If a system's security measures make it difficult to use, then users will find ways around the security, which may make the system more vulnerable than it would have been without the security measures! Take, for example, password policies. If the organization requires an extremely long password with several special characters, an employee may resort to writing it down and putting it in a drawer since it will be impossible to memorize.

Reference:

Security Policy Templates. Retrieved September 6, 2020, from SANS Institute's Information Security www.sans.org/information-security-policy/