sirkit
MAKING IT EASY

IT Terms Guide

We've put together this guide to round up essential IT terms in one place. The following guide will provide a reference guide to commonly used IT terms and touch on their importance. We hope that this guide will make your life a little easier as you research IT topics. This guide is for anyone that is looking to expand their knowledge of IT and IT terminology. We will be covering the following:

- Multi-Factor Authentication
- Cybersecurity Awareness Staff Training
- Password Policies
- Backups
- Patches and Automatic Updates
- Device Encryption
- Cybersecurity Insurance
- Password Managers
- Endpoint Protection (anti-virus, anti-malware, and anti-ransomware)
- Next-Gen Firewalls
- Zero-Day Security Risks
- Incident Response Plans
- Mobile Device Management (MDM)
- Active Monitoring

We hope that you find the following guide helpful. If you have any questions, feel free to reach out to us. We will be happy to assist you.

Contact Us Now

Multi-Factor Authentication

Multi-Factor Authentication (MFA) is one of the essential parts of a cybersecurity policy and should be used in every business. MFA introduces a secondary verification step while logging in that blocks 99.9% of identity-based attacks. When MFA is active, a random code or prompt (push notification) is sent to your mobile device to confirm your identity. MFA can be used for people without mobile phones, too, by utilizing hardware tokens like Yubikeys. Even if a malicious party knows your credentials, MFA stops them.

For more information, check out our article on Multi-Factor Authentication here.

Cybersecurity Awareness Staff Training

Malicious actors often take advantage of ignorance, rather than technical vulnerabilities, to compromise businesses. For example, 88% of all data breaches are caused by human error. Therefore, one of the most effective steps to protect your business is cybersecurity awareness training. Cybersecurity awareness training, also referred to as security awareness training, is when an organization formally educates its employees on cyber threats. Sessions usually focus on how to identify cyber threats, existing cyber threats, and preventative measures. Providing your team with cybersecurity training will:

A) Teach staff to spot fraudulent e-mails, such as phishing e-mails
B) Teach staff how to operate safely in a technology environment
C) Significantly lower your risk of a breach

Cybersecurity training is a proven approach to reduce organizational risk.
Training should include topics like:

- Phishing attacks
- Social engineering and impersonation
- Removable media (e.g., USB keys)
- Passwords
- Physical security
- Mobile device security
- Working remotely
- Public WiFi
- Cloud security
- Social media
- Internet use
- E-mail use

Password Policies

A password policy is a simple way to enhance your company's security. A password policy is a formal set of rules governing the use of passwords at an organizational level. It allows for organizations to enforce security policies to reduce the risk of a breach. In addition, a password policy makes it much more difficult for 3rd parties to compromise accounts and ensures your team adheres to strict standards when implemented correctly. For example, did you know that a 10-character password that contains only numbers can be breached instantly?

All passwords should be strong. That means requiring minimum length, complexity, minimum/maximum password age, and allowing for account lockout rules. These rules are especially critical when multi-factor authentication (MFA) is not used.

To learn more about password policies, check out our blog here.

Backups

All businesses should have automated backups to protect critical information and systems. The backup process creates copies of data on a physical disk or cloud server. Ideally, servers should be backed up locally and then sent offsite to a trusted cloud partner. A cloud-to-cloud backup service should be utilized to protect SaaS or cloud services like Office 365. Never assume SaaS or cloud services are protected by the vendor hosting them.

You can learn more about offsite backups in our article here.

Patches and Automatic Updates

Keeping programs and software up to date is extremely important for security purposes. 60% of breach victims were compromised due to unpatched software vulnerabilities. Businesses should keep all network-connected systems up to date, including computers, servers, firewalls, phone systems, surveillance systems, and even thermostats. Everything on a network should be monitored and patched, and automatic updates should be enabled where possible.

Device Encryption

Encryption is a process that makes data unreadable by a third party. An example is the program Bitlocker. Encryption should be enforced on computers, servers, and mobile devices. When used correctly, a 3rd party cannot read the data even if they have the physical device in their possession.

If you lose a device that had users' personally identifiable information (PII) on it, you may be required to report it to the government. An exception to this, however, is if this device is encrypted. Encrypted devices are far less likely to be breached; therefore, reporting may not be required. However, you will have to be able to prove that the device was encrypted.

Cybersecurity Insurance

Cybersecurity insurance is an essential part of any business continuity plan and offers protection against potential claims resulting from a data breach. It also protects against financial loss, as well as providing business interruption coverage. To learn more about cybersecurity insurance, you can check out our article here.

Effective late 2021, insurance companies expect specific minimum cybersecurity measures to be in place to qualify for coverage. To learn more about this, check out our article here.

Password Managers

A password manager is a program that securely stores passwords for numerous systems to prevent you from having to remember them all. Creating abstract, long, or complex passwords becomes easier if users no longer worry about remembering their passwords. A password manager makes this easy by generating secure passwords for you and storing them for later use. Therefore, a Password Manager will enhance security for your organization.

We use and recommend LastPass as a password security solution.

Endpoint Protection (anti-virus, anti-malware, and anti-ransomware)

Endpoint protection (also known as endpoint security) is a modern name for anti-virus software, although most programs now offer additional protection against malware, spyware, viruses, and ransomware.

In 2021 there were approximately 560,000 instances of new malware detected per day, showing the need for modern endpoint protection.

Not all endpoint protection is equal, and they all provide different levels of protection from various threats. Therefore, it's essential to ensure that your endpoint security protects against viruses, malware, and ransomware.

Next-Gen Firewalls

Next-Generation firewalls (NGFW) are the modern standard that every business should have in place to protect itself. Next-Gen firewalls go beyond conventional firewalls by offering application awareness. They can identify which applications are in-use by analyzing network or internet traffic sent through them. Next-Gen firewalls provide various security services that defend against real-time attacks, malicious activity, or even employees misusing resources while on the job (e.g., pornography or illegal downloads).

Next-Gen firewalls include features like:

- Intrusion Prevention (IPS)
  - Stops a malicious actor from exploiting a known vulnerability
- Application Control
  - Blocks risky or unwanted applications from being used by staff

- Identity Awareness – for both users and groups
  - Helps identifies users and monitor their usage
- Advanced Threat Protection
  - Identifies when a user or device is trying to “call home” (communicate externally) to a malicious actor. Hackers will sometimes send out installation files or scripts to try and get onto remote systems. If they are successful, the software they managed to get on will “call home” for instructions.
- Web-Filtering
  - Block access to websites based on classification (e.g., pornography)
- QoS/Bandwidth Management
  - Can be used to limit or prioritize speed for a user, group, or service
- Sandbox Explosion and Antivirus Inspection
  - Tests incoming files before the user is permitted to use or open them

Zero-Day Security Risks

Zero-Day Security Risks are brand new security vulnerabilities discovered “in the wild.” The concept is that you must act immediately and should take ‘zero days’ to fix it because of the extraordinarily high risk. If left unpatched, you are exposed, and 3rd parties can leverage the vulnerability to breach your systems.

Incident Response Plans

Incident Response Plans can also be known as Disaster Recovery Plans. These plans are predetermined instructions to follow should an incident occur and ensure that they are handled consistently. Without a good plan in place, essential steps will likely be missed, and it could leave you open to additional incidents in the future.

A typical response plan might include:

- The scope of the incident (when, how, length of time)
- The appropriate response
- Who is going to take care of it
- What they are going to do
- What is the interim solution
- Who to notify
- How to make sure it doesn’t happen again

Mobile Device Management (MDM)

Mobile device management is the ability for an organization to secure and centrally manage devices using a program such as Microsoft Intune. MDM allows you to monitor, configure, and wipe devices remotely. In addition, MDM will enable companies to fully manage corporate data on users' devices, allowing for more secure bring your own device (BYOD) policies. For example, if a staff member leaves the company, you can clear your data off any managed device with a click of a button.

Active Monitoring

Active Monitoring is a process that monitors computers and networks for specific criteria. For example, an alert might be sent to the administrator when a user is low on space or if something is misconfigured. Active Monitoring can also alert the administrator in the case of an unusual user or network activity.

Monitoring your equipment is a critical service that helps you understand when an incident occurs, when equipment is falling behind, who equipment is assigned to, and much more. Without real-time information about your systems, it's unlikely you will be able to respond to an incident before it's too late.

Return to top