DASHLANE

Essential Guide To Common Cybersecurity Terms

Make sense of jargon related to information technology, cybersecurity, cyber threats, Identity and Access Management, and password management.

Understanding the basics of cybersecurity

Understanding the basics of cybersecurity can help you make better decisions, yet navigating all that cybersecurity jargon can get confusing. Whether you have a small team of IT experts or none, this glossary should help you make sense of key terminology. To help guide you through the maze of jargon, we've included the most common terms related to IT, cybersecurity, cyber threats, identity and access management, and password managers.

But before we dive in, let's define cybersecurity and why it's important.

What it is: According to the U.S. Cybersecurity and Infrastructure Security Agency (CISA), cybersecurity is "the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information." Essentially, cybersecurity is your ability to prevent, protect, and defend your organization from cyberattacks.

Why you should care: As your organization relies more on digital technology, your tools create exposure to cyber threats. Cybercriminals may target smaller businesses not only for their valuable data but also as an entry point into larger organizations that these businesses are connected to as vendors and partners. Cybersecurity helps protect your organization's assets, including your people and your reputation, as well as minimize your business risks.

Section 1

Information technology (IT)

Blockchain

A distributed, unchangeable, typically public ledger or database that's shared among different computers in a peer-to-peer network for the purpose of recording transactions and tracking assets. Since there's no central authority, transactions are authenticated using cryptographic keys and then authorized (or validated) by the computer nodes.

BYOD (bring your own device)

The practice of employees using personal devices to connect to their corporate network and access work-related systems and applications, either with or without permission and oversight by the IT department.

Deprovisioning

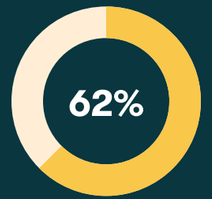
A part of the employment lifecycle that ensures your employees' access to IT systems and applications is revoked when they change roles or leave the company. Deprovisioning may involve changing access or deleting accounts and user identities altogether.

of surveyed organizations expect BYOD adoption to increase

(Source: Cybersecurity Insiders, "BYOD Security Report," 2021)

Integration

The ability to connect different systems, applications, and other IT resources seamlessly so they can work together as a cohesive unit. For software, the most common integration mechanism is APIs (application programming interfaces), an intermediary layer that sits between applications to enable them to communicate.

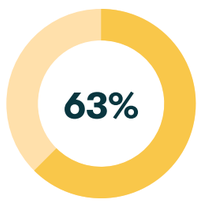


of surveyed organizations say their biggest BYOD security concern is data leakage or loss due to work device disposal or an employee separation

(Source: Cybersecurity Insiders, "BYOD Security Report," 2021)

IoT (Internet of Things)

A network of internet-enabled devices, machines, and other objects (often called smart or connected devices) that have unique identifiers (called UIDs), as well as embedded sensors, software, and processors that enable them to collect and exchange data with each other without requiring human interaction (called machine-to-machine or M2M communication). IoT subsets include IIoT (the Internet of Industrial Things) in the manufacturing and industrial sectors and IoMT (the Internet of Medical Things) in healthcare. A newer term is Internet of Everything (IoE), which in addition to "things" also includes people, processes, and data that are intelligently connected together.

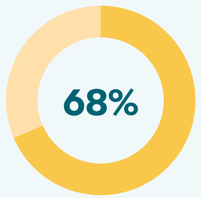


of surveyed organizations identify unmanaged IoT devices as their greatest risk to data loss

(Source: Ponemon Institute, "Cost of Insider Threats Global Report," 2022)

Provisioning
The process of deploying and configuring IT infrastructure and resources, ranging from networks and servers to user accounts. For employee access, provisioning includes steps such as creating new user accounts and configuring access based on established policies.

SaaS (software-as-a-service)
Web-based software and applications delivered through the cloud rather than installed locally on each device. Typically, SaaS services require subscription on a “pay-as-you-go” basis and include regular updates from the vendor.



of organizations with 500 employees or less report having shadow IT

(Source: Productiv, “The State of SaaS Sprawl,” 2022)

Small businesses have an average of 242 SaaS applications

(Source: Productiv, “The State of SaaS Sprawl,” 2022)

Shadow IT
Employee use of IT resources—from devices and applications to services and systems—without the IT department’s permission and knowledge. Any unsanctioned use of technology, whether on personal or corporate devices, is considered shadow IT.

Sync
Short for synchronizing, the process of copying data from one device to another, so the same information is available consistently on multiple devices. In the case of SaaS, the data typically syncs automatically through the cloud so that you can access your account and information from anywhere.

Useful resources

- **Blog** Is My Smart Fridge Listening to Me? And Other Concerns
- **Blog** What is the Internet of Things and How Safe Is It?
- **Blog** How Admins Can Simplify Provisioning
- **Blog** Shadow IT: How to Mitigate Risks with a Password Manager

Section 2

Cybersecurity

Cloud security

The combination of processes, policies, procedures, tools, and controls your organization uses to protect its cloud-based assets, such as data and applications. Cloud security examples include:

- Security tools such as password managers
- Security policies that restrict user access to sensitive data
- Controls such as encrypting data stored in the cloud

Cyber insurance

A business insurance product that protects against financial losses stemming from a cybersecurity incident or data breach. While coverage varies, common cyber policies address areas such as business interruption, forensic investigations, and regulatory defense and fines.

Cybersecurity posture

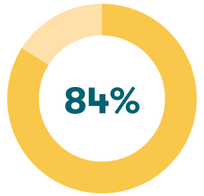
Your organization's overall ability and capability to prevent, defend against, and recover from cyber threats. The posture is the status of your company's total defenses, including security solutions and practices.

Data privacy

The area concerning how your organization collects, uses, stores, shares, and manages the data of individuals, including employees and customers. Many nations, local governments, and industries have some form of data privacy regulations, from the General Data Protection Rule (GDPR) in the European Union to the Personal Protection Information Law (PIPL) in China.

Decryption

The process of converting encrypted data back into its original format. Decryption requires the right decoding tools, such as keys, passwords, or codes.



of surveyed security professionals believe an attack will start with the endpoint

(Source: Dark Reading, "Battle for the Endpoint," 2021)

Encryption

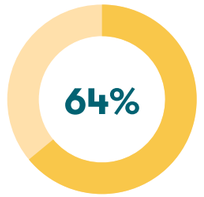
The process of scrambling data ("plaintext") into an unreadable format ("cypher text") to protect it from unauthorized access. Encryption standards vary based on the encryption purpose, whether that's to store data online or send a secure email. One of the most commonly used methods is the Advanced Encryption Standard, or AES, with AES-256 as the strongest cipher currently available.

Endpoint

Any computing device, such as a desktop, mobile device, server, or IoT device, that connects to your company's network. Endpoint security is a top priority for many organizations because threat actors often target endpoints as the initial entry point into the network.

PII (personally identifiable information)

Any data that allows an individual to be identified, directly or indirectly, such as their name, date of birth, address, government identification number, phone number, and biometrics (such as fingerprints, facial recognition, or iris recognition). PII is very valuable for cybercriminals because they can use it for fraud schemes, phishing, and other nefarious purposes.



of surveyed companies had cyber insurance policies in 2022, up from 58% in 2020

(Source: Hiscox, "Cyber Readiness Report," 2022)

Security audit

A systematic process for evaluating your cybersecurity posture, including assessing policies, procedures, and security tools. Audits help you discover security weaknesses and vulnerabilities so you can take the necessary measures to close those gaps.

Security stack

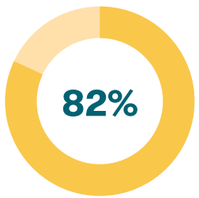
The multiple layers of cybersecurity tools that your organization has in place to detect, respond to, and recover from cyber threats. The layers range from the infrastructure and hardware all the way up to applications and users.

VPN (virtual private network)

An app or software that creates an encrypted connection over the internet from your device or network. When you use an unsecured connection, such as a public WiFi hotspot, a VPN protects the information that you transmit from the prying eyes of a hacker.

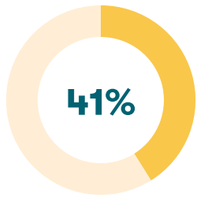
Zero-knowledge architecture

A security principle that grants you—and no one else—access to your data. The data is encrypted locally on your device, and access requires a password or another form of authentication.



of surveyed organizations with 1,000 employees or fewer identify security as their top cloud challenge

(Source: Flexera, "State of the Cloud Report," 2022)



of surveyed organizations have deployed zero-trust security architecture

(Source: IBM, "Cost of a Data Breach Report," 2022)

Zero-trust security

A cybersecurity approach based on the idea that no connection can be trusted implicitly, regardless of where it originates. In a zero-trust model, every user and device must be dynamically authenticated and their access continuously authorized and validated. For example, if you're trying to log into your corporate network, zero-trust security would require authentication before you can access a resource, whether you're logging in from your corporate office or from home.

Useful resources

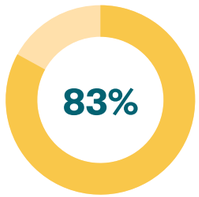
- **Blog Guide** Our Guide to Data Privacy
- **Blog** What Is Encryption?
- **Blog** How to Conduct Your Own Internal Security Audit
- **Blog** Is Your Work Laptop Secure?
- **Blog** What is a VPN and Why Should I Use One?

Section 3

Cyber threats

Attack surface and attack vector
An attack vector is a method or path that a cyberattacker uses to get entry into your organization's network or systems. Examples include malware, compromised logins, and phishing. The sum of all the possible entry points and vulnerabilities comprises the attack surface.

Backdoor
A method for bypassing built-in security mechanisms to gain access to a system. Backdoors may be authorized (for example, for troubleshooting purposes) or unauthorized (for example, created by a cybercriminal).



of surveyed organizations experienced more than one data breach within the past year

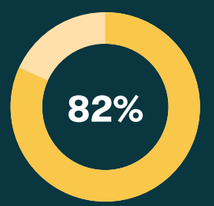
(Source: IBM Security, "Cost of a Data Breach Report 2022," 2022)

Breach
A cybersecurity incident that results in unauthorized access to data, applications, a network, or another protected IT system as a result of bypassed security protocols. A data breach, specifically, is a security incident that results in the confirmed disclosure of sensitive data—such as PII, logins, or intellectual property—to an unauthorized party.

Brute force attack
A series of trial-and-error attempts to crack a password by using an exhaustive number of character combinations, including common passwords, typically executed with automated tools.

Command and control (a.k.a. C2 or C&C)
A technique (or set of tools and infrastructure) threat actors use to establish communication with a compromised system, gain complete control, and execute malicious actions such as extracting data or launching an attack. For example, after a device is infected with malware, it will "call home" to the C2 to receive further instructions, such as controlling the system remotely.

Compromised
An account, password, or system that's vulnerable due to unauthorized access or exposure. For example, a compromised account is an account that had its logins stolen or leaked on the dark web or has insecure access protocols such as a weak or default password and no 2FA.



of breaches involve the human element

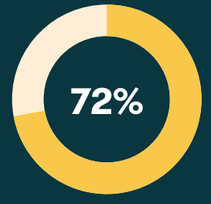
(Source: Verizon, "Data Breach Investigations Report," 2022)

Cyber threat

An adverse action, event, or circumstance that can impact your organization's operations, people, and assets through unauthorized access to information systems, disclosure of sensitive information, disruption, and other impacts. Examples include malware, social engineering, unpatched software, and weak logins.

Cyberattack

An attempt to gain unauthorized access to computer systems through cyberspace for malicious purposes such as stealing sensitive information, controlling a computing environment, disabling systems, or compromising data or system integrity.



of surveyed organizations experienced an increase in the volume, complexity, and/or impact of cyberattacks in 2021, compared to 37% the previous year

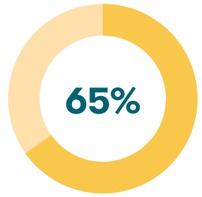
(Source: Sophos, "The State of Ransomware 2022," April 2022)

Dark web

A section of the world wide web that's hidden from search engines and can only be accessed with specialized, anonymous browsers, most commonly Tor. Also called the darknet, this space is home to various black markets, including cybercriminal services and compromised digital assets such as logins.

As of 2022, more than 24 billion credentials have been exposed by threat actors, a 65% increase from 2020

(Source: Digital Shadows, "Account Takeover in 2022," 2022)



Data leak

The unauthorized sharing of data from within your organization (either intentionally, such as through a disgruntled employee, or unintentionally, such as through accidental sharing or a misconfigured database); can also refer to cybercriminals sharing data on the dark web.

Hack

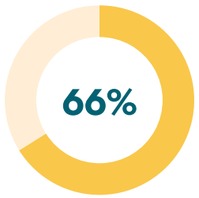
An intentional attack to gain unauthorized access to a device, server, or another protected IT resource. The purpose of a hack is to compromise the system's availability, integrity, or confidentiality.

Phishing and ransomware are the top two root causes of data breaches

(Source: Identity Theft Resource Center, "Q1 2022 Data Breach Analysis," 2022)

Keystroke logging (or keylogging)

The recording of every keystroke users make on a device. This recording is done using tracking software or hardware. Keylogging can be malicious (such as bad actors trying to steal your organization's data) or legitimate (such as you monitoring your employees for a specific company purpose).



of surveyed organizations were hit with ransomware in 2021, compared to 37% the previous year

(Source: Sophos, "The State of Ransomware 2022," April 2022)

Malware

Malicious, intrusive software designed to damage or interfere with a system's normal functions, such as damaging a computer or stealing data. Viruses, spyware, and ransomware are some malware examples.

Phishing

A fake communication, such as an email or text message, that appears to come from a trustworthy sender in an attempt to lure you into revealing sensitive data or compromising a system.

In the first quarter of 2022, the number of phishing attacks exceeded 1 million for the first time. The previous record was 888,585, reached in the fourth quarter of 2021.

(Source: APWG, "Phishing Activity Trends Report," 1st quarter 2022)

Ransomware

A type of malware that encrypts files on a device, blocking access to the data and related systems. In the past couple of years, ransomware operators have been using so-called double-extortion schemes, stealing the data before encrypting it and threatening to leak it if the victim doesn't pay the ransom.

Social engineering

Manipulation techniques exploiting human behaviors and weaknesses in an attempt to coerce individuals to take a specific action, such as divulging sensitive information, sending money, or circumventing security protocols.

Useful resources

- E-book A Business Guide to Data Breaches and Hacks
- Blog What the Hack Is a Brute Force Attack?
- Blog What Is the Dark Web?
- Blog What the Hack Is Malware?
- E-book Phishing 101
- Blog 6 Cybersecurity Threats that Lead to Business Breaches and Hacks

Section 4

Identity and Access Management

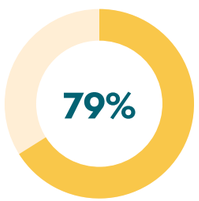
2FA

A security process for providing two different authentication factors before you can access an account or system. Also referred to as two-step verification, 2FA requires verification factors from two of these categories:

- Something you know (like your password or PIN)
- Something you have (like your smartphone or a fob)
- Something you are (like your fingerprint or voice)

IAM (Identity and Access Management)

A set of technologies, policies, and processes that helps your organization centrally manage user roles and activity and enforce security policies. IAM solutions serve four main purposes: authentication, authorization, user management, and central user repository.



of surveyed organizations reported using 2FA in 2021, up from 53% two years earlier

(Source: Duo, "The 2021 State of the Auth Report," 2021)

MFA (multi-factor authentication)

A security process, similar to 2FA, that requires at least two authentication factors for granting access. MFA and 2FA are often used interchangeably; the primary difference between them is that MFA may have three or more verification steps.

SCIM (system of cross-domain identity management)

An open standard protocol that allows IT systems or domains to exchange user identity information. SCIM is commonly used to automate user provisioning.

SSL (secure socket layer)

A protocol for encrypting information sent over the internet. SSL is commonly used on websites to encrypt the connection between the browser and the web server.

SSO (single sign-on)

A user authentication method that allows your employees to log in with one set of credentials to access multiple accounts. SSO often integrates with a password manager and other IAM tools to simplify logins.

Token

A physical or digital device that you need to access a protected IT resource like an app. Tokens, such as physical fobs or digital codes, are commonly used for 2-factor authentication (2FA) or multifactor authentication (MFA).

Only around half of the apps employees routinely use are behind single sign-on (SSO)

(Source: BusinessWire, Less than Half of Company SaaS Applications Are Regularly Used by Employees, 2022)

Useful resources

- **Blog** A Beginner's Guide to Two-Factor Authentication
- **White Paper** Identity and Access Management 101
- **Blog** SSO Technology Overview & Integration With Dashlane

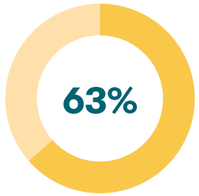
Section 5

Password management

Autofill
A password manager feature that automatically populates websites with the information you have stored in your password manager, such as your personal details, logins, and payment cards.

Dark web insights
A password manager feature that scans billions of records on the dark web for any leaked data and alerts employees when their information is involved in data leaks. Many dark web insights tools also explain simple actions for remediating such threats.

Dark web monitoring
A password manager feature that provides IT admins with a dashboard where they can access real-time insights and alerts about security breaches and other vulnerabilities facing employees in their organization.



of employees admit to using the same passwords for multiple work accounts

(Source: Visual Objects: "Cybersecurity Topics: Employees & Cyber Defense," 2020)

FIDO-based authentication
An open standard developed by the FIDO Alliance that enables the replacement of password-only logins with secure and fast login methods, such as biometrics and security keys.

Master password
A private key that encrypts all the data you store in your password manager and is required for granting access to that data.

Passkey
A security feature that replaces passwords and uses a unique pair of cryptographic keys for an app or website. Considered a next-generation login technology, passkeys are more resistant to threats such as phishing.

Password generator
A password manager feature for automatically and securely generating random, strong, unique passwords that can be customized to meet a website's requirements. Most password managers offer this feature.

Password health
An indicator of your overall password security, typically shown as a score. The score is calculated based on the number of weak, reused, or compromised passwords you have across your accounts.

Increased usage of a password manager was the top change organizations implemented as a result of hybrid work

(Source: Dashlane, "The Future of Secure Work for People + Organizations," 2022)

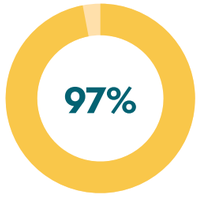
Password manager
A software application that stores all your logins in a secure location. Many password manager apps (also known as password keepers) offer multiple features, such as the ability to create long, random, unique passwords automatically; syncing all your logins across your devices; and autofilling your logins on websites.

Password policy
A set of best practices and rules related to password use that your organization has established for business accounts. A password policy includes guidelines for password strength, secure password sharing, and password management.

Secure note
A password manager feature for securely saving private information, such as WiFi passwords and apartment codes.

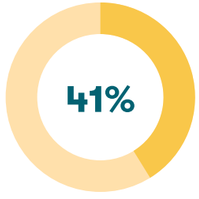
Secure sharing
A password manager feature for safely sharing private information stored in your password manager app, such as passwords and secure notes, with specific people.

Security vault
A secure, encrypted location for storing data, which could include anything from passwords and encryption keys to sensitive files and other information.



of surveyed IT leaders and 52% of employees believe their organization needs a password manager

(Source: Dashlane, "The Future of Secure Work for People + Organizations," 2022)



of surveyed organizations require a password manager

(Source: Dashlane, "The Future of Secure Work for People + Organizations," 2022)

Useful resources

- **Blog** Is a Passwordless Future on the Way? What You Should Know About FIDO-Based Authentication
- **Blog** 5 Must-Haves in a Password Manager for Business
- **Blog** Creating a Password Policy Your Employees Will Actually Follow
- **Report** The Future of Secure Work for People + Organizations

What's next

Learning the basics of cybersecurity is the first step in protecting your business. With that knowledge under your belt, your next step is to understand what cybersecurity tools are available to you and how they work.

Read our e-book, "The Employee Guide to How Password Managers Work," to learn how a password manager can help defend your organization—and your people—against some of today's biggest cyber threats.

Alphabetical index

DASHLANE

About Dashlane

Dashlane offers businesses a password management solution that is as easy to use as it is secure. Admins can easily onboard, offboard, and manage their employees with the assurance that company data is safe. And employees can enjoy a way to manage their work and personal accounts that's already loved by millions. Our team in Paris, New York, and Lisbon is united by our passion for improving the digital experience and the belief that with the right tools, we can help everyone realize the promise of the internet. Dashlane has empowered over 15 million users and over 20,000 organizations in 180 countries to dash across the internet without compromising on security.

dashlane.com

LinkedIn

Twitter

Instagram

Blog

Reddit