

Ministry of SaskBuilds and Procurement
Information Technology Division, Cybersecurity and Risk Management Branch

Overview

This document provides plain language definitions for terms and phrases you may encounter when receiving communications or reviewing documentation from the Cybersecurity and Risk Management (CSRM) Branch. If you have questions or feedback, contact the CSRM Branch at: SBPITInformationSecurityBranch@cgi.sk.ca

Cyber Threat Communications Definitions

The following definitions are for words and phrases you may encounter while reading a cyber threat communication sent by the Cybersecurity and Risk Management Branch. Understanding these words and phrases can help you stay vigilant and protect Government's sensitive information and your personal information.

Cloud Security Issues: Risks associated with storing data online, such as unauthorized access, data breaches and loss of data due to incorrectly configured systems or solutions or malicious attacks.

Deepfake: A type of video or audio file that has been digitally altered to make it look or sound like someone else is doing or saying something they never actually did. Attackers will use deepfakes of someone in authority to have a user volunteer sensitive information such as corporate/government credit card numbers or banking information.

Denial of Service Attacks: When attackers overwhelm a website or online service with too much traffic, causing it to crash and become unavailable.

Insider Threats: Risks posed by people within your organization, like employees or contractors, who misuse their access to data for malicious purposes.

Internet of Things (IoT) Vulnerabilities: Security weaknesses in connected devices like smart home gadgets, which can be exploited by attackers to gain access to your network.

Malware: Short for "malicious software," this includes viruses, worms, and trojans that can damage your computer, steal information or spy on your activities.

Man-in-the-Middle Attacks: When attackers intercept and alter communication between you and someone else without you knowing, often to steal information or add harmful content.

Password Attacks: Attempts to steal your passwords. This can happen in a number of ways, like guessing, using software to crack them or tricking you into revealing them.

Information Security Glossary

Ministry of SaskBuilds and Procurement

Information Technology Division, Cybersecurity and Risk Management Branch

Phishing: This is when attackers trick you into giving away personal information, like passwords or credit card numbers, by pretending to be someone you trust, usually through fake emails or websites.

There are several different types of Phishing:

- **Clone Phishing:** Attackers create a nearly identical copy of a legitimate email that you've received before, but with malicious links or attachments.
- **HTTPS Phishing:** Attackers create fake websites that appear secure (using HTTPS) to trick you into entering sensitive information.
- **Pharming:** This redirects you from a legitimate website to a fake one without you knowing, often through malicious code on your computer.
- **Pop-up Phishing:** Attackers use pop-up windows on legitimate websites to ask for personal information.
- **Search Engine Phishing:** Attackers create fake websites that appear in search engine results, hoping you'll click on them and enter personal information.
- **Smishing:** This uses SMS (text messages) to trick you into providing personal information or clicking on malicious links.
- **Social Media Phishing:** Attackers use social media platforms to trick you into revealing personal information or clicking on malicious links.
- **Spear Phishing:** This targets specific individuals or organizations. Attackers often gather personal information about the target to make the attack more convincing.
- **Vishing:** Short for "voice phishing," this involves phone calls where attackers pretend to be someone trustworthy to steal personal information.
- **Whaling:** This targets high-profile individuals like executives or celebrities, often with highly personalized messages.

Ransomware: A type of malicious software that locks you out of your computer or files until you pay a ransom to the attacker.

Social Engineering: Techniques used by attackers to manipulate you into revealing confidential information. This can include phishing, phone calls or in-person tricks.

Website Spoofing: Website spoofing is a scam used by cyber criminals where they create a copy of a real website to fool you into giving them your personal information.

Information Security Glossary

Ministry of SaskBuilds and Procurement

Information Technology Division, Cybersecurity and Risk Management Branch

Information Security Glossary

The following definitions are for common words and phrases you may encounter while reviewing cybersecurity documentation such as policies, standards, guidelines and other supporting documentation.

Access Control: Rules and methods to decide who can see or use IT systems and data.

Access Control List: A list that tells a system which users can access certain IT systems and data and what they can do with them.

Advanced Encryption Standard (AES): A widely used method for converting data and information into a code (encrypting) to keep it secure.

AES-256: Advanced Encryption Standard-256 is an extra secure way to convert data and information into a code (encrypting) to keep it safe.

Application: A software program that helps users do specific tasks.

Asset: Anything that is valuable to the Government of Saskatchewan, like data, software and hardware.

Audit: A review or examination of records and activities to ensure they comply with policies and regulations.

Audit Log: A record of events or actions taken on a system, used for tracking and analysis.

Authentication: The process of verifying someone's identity before allowing them access to systems and data.

Authorization: The process of giving someone permission to access IT systems and data or do actions.

Availability: Ensuring that systems, data and other IT services are accessible when needed.

Backup: A copy of data stored separately to restore the original in case it is lost or damaged.

Biometric: Unique physical characteristics, like fingerprints or facial recognition, that can be used to prove someone's identity or authenticate them.

Chain of Custody: The documented process that shows the control, transfer and analysis of evidence.

Cloud Security Issues: Risks associated with storing data online, such as unauthorized access, data breaches and loss of data due to incorrectly configured systems or solutions or malicious attacks.

Information Security Glossary

Ministry of SaskBuilds and Procurement

Information Technology Division, Cybersecurity and Risk Management Branch

Commercial-off-the-Shelf (COTS):	Ready-made software and other products that are ready to buy and use and don't need to be modified.
Confidentiality:	Ensuring that information is only accessible to those authorized to see it.
Control:	A measure or measures taken to manage risks and protect IT systems and data.
Countermeasure:	Actions or devices designed to prevent or reduce security threats.
Cryptographic Algorithm:	A way to encrypt and decrypt information into and out of unreadable code to keep it secure.
Cryptographic Key:	A piece of information used to encrypt and decrypt information into and out of an unreadable code to keep it secure.
Cryptography:	The practice of securing information by transforming it into an unreadable format.
Deepfake:	A type of video or audio file that has been digitally altered to make it look or sound like someone else is doing or saying something they never actually did. Attackers will use deepfakes of someone in authority to have a user volunteer sensitive information such as corporate/government credit card numbers or banking information.
Denial of Service (DoS) Attack:	When attackers overwhelm a website or online service with too much traffic, causing it to crash and become unavailable.
Detailed Infrastructure Design:	A comprehensive technical plan for the setup of a system or network.
Digital Signature:	An electronic signature that verifies a message or document is authentic.
Disaster Recovery Plan:	A documented strategy for recovering IT systems and data after a disaster.
Egress Filtering:	Monitoring and controlling outgoing network traffic to prevent data leaks.
Electronic Messaging Services:	IT services that allow the exchange of messages electronically, like email or instant messaging.
Electronic Storage Media:	Devices that are used to store digital data, like hard drives, USB sticks, CDs and DVDs.
Electronic Security Perimeter:	The boundary that separates secure areas of a network from unsecured areas.
Employee:	A person who works for an organization.
Encryption:	The process of converting information into an unreadable code to prevent unauthorized access.

Information Security Glossary

Ministry of SaskBuilds and Procurement

Information Technology Division, Cybersecurity and Risk Management Branch

Event: An occurrence or action that can be tracked and recorded.

FIPS: Stands for Federal Information Processing Standards.

FIPS 140-2 Validated: Refers to *Federal Information Processing Standards Publication 140-2*, which is an industry standard for verifying that cryptographic modules meet specific security requirements.

Firewall: A security system that monitors and controls incoming and outgoing network traffic.

Government Records: Documents and information created or received by government agencies.

Identification: The process of recognizing and verifying a person's identity — that they are who they say they are.

Identity: The unique characteristics and information that define a person or entity.

Identity Management: The process of managing user identities and their access to systems and data.

Incident: An event that disrupts normal operations or poses a security threat.

Information Owner: An individual (in possession and/or control of the information) who is responsible for managing and protecting specific information.

Information Processing Facilities: Physical locations where information is processed and managed.

Information Security: Protecting information from unauthorized access, use, disclosure, disruption, modification or destruction.

Information Security Event: Anything that has happened that may affect the safety of data.

Information Security Incident: A confirmed event that compromises the security of information.

Information System: A system for collecting, storing, processing and distributing information like Government's human resource system, online learning systems and network storage systems.

Injury: Harm or damage to a person or property.

Insider Threats: Risks posed by people within your organization, like employees or contractors, who misuse their access to data for malicious purposes.

Integrity: Ensuring that information is accurate and has not been tampered with.

Information Security Glossary

Ministry of SaskBuilds and Procurement

Information Technology Division, Cybersecurity and Risk Management Branch

Intellectual Property: Creations of the mind, like inventions, literary works and designs, that are legally protected.

Internet of Things (IoT) Vulnerabilities: Security weaknesses in connected devices like smart home gadgets, which can be exploited by attackers to gain access to your network.

Intrusion: Unauthorized access to a system or network.

Intrusion Detection: Identifying and responding to unauthorized access or attacks on a system.

Key Management: The process of handling cryptographic keys, including their creation, storage, and distribution.

Least Privilege: Giving users the minimum level of access they need to do their tasks.

Local Admin: A user with administrative privileges on a local computer or network.

Malicious Code: Software designed to harm or exploit systems, like viruses or worms.

Malware: Short for "malicious software," this includes viruses, worms, and trojans that can damage your computer, steal information or spy on your activities.

Man-in-the-Middle Attacks: When attackers intercept and alter communication between you and someone else without your knowing, often to steal information or add harmful content.

Media: Devices or materials used to store data, like hard drives, CDs, DVDs or USB drives.

Media Sanitization: The process of securely erasing data from media like hard drives, USB drives and other storage devices.

Mobile Device: A portable electronic device, like a smartphone or tablet.

Monitoring: Continuously watching systems or networks to detect and respond to issues.

Multifactor Authentication (MFA): Also known as MFA or 2FA, this uses multiple methods to verify a user is who they say they are. Examples include a password and a fingerprint or a code from a trusted device.

Need-to-Know: Restricting access to information only to those who need it to perform their duties.

Network: A group of interconnected computers and devices that share IT systems, data and information.

Network Security Zone: Sections of a network with different security levels and controls.

Information Security Glossary

Ministry of SaskBuilds and Procurement

Information Technology Division, Cybersecurity and Risk Management Branch

Network Segregation:	Dividing a network into smaller parts to improve security.
Network Service Agreement:	A contract that defines the services and responsibilities between a network provider and a customer.
Non-repudiation:	Ensuring that a person cannot deny the authenticity of their actions or communications.
Password Attacks:	Attempts to steal your passwords. This can happen in a number of ways, like guessing, using software to crack them or tricking you into revealing them.
Personal Health Information (PHI):	Information about an individual's health status, care or payment for healthcare.
Personal Information (PI):	Information that can identify an individual, like name, address or social insurance number.
Phishing	This is when attackers trick you into giving away personal information, like passwords or credit card numbers, by pretending to be someone you trust, usually through fake emails or websites.
Portable Storage Device:	A small gadget for your saved data that you can bring with you, like a USB drive.
Privacy Impact Assessment (PIA):	An analysis to identify and mitigate risks to private data in a project or system.
Privilege:	Special rights or permissions granted to a user or system.
Privileged User:	User with special access rights and permissions, often with administrative capabilities.
Ransomware:	A type of malicious software that locks you out of your computer or files until you pay a ransom to the attacker.
Record:	A documented piece of information, often stored for reference or legal purposes.
Remote Access:	The ability to access a computer or network from a distant location.
Removable Media:	Storage devices that can be easily removed from a computer, like CDs or USB drives.
Risk:	The potential for loss or damage when a threat exploits a vulnerability.
Risk Analysis:	The process of identifying and evaluating the potential for loss or damage.
Risk Assessment:	The overall process of identification, analysis and evaluation for potential loss or damage.

Information Security Glossary

Ministry of SaskBuilds and Procurement

Information Technology Division, Cybersecurity and Risk Management Branch

Security Control:	Measures implemented to protect systems and information.
Security Incident:	An event that compromises the security of information or systems.
Security Posture:	The overall status of an organization's system and network security.
Security Weakness:	A flaw or vulnerability that could be exploited to compromise security.
Service Owners:	Individuals responsible for delivering and managing specific IT services.
Social Engineering:	Techniques used by attackers to manipulate you into revealing confidential information. This can include phishing, phone calls or in-person tricks.
Spyware:	Malicious software that secretly monitors and collects information from a user's device.
Statement of Sensitivity (SOS):	A document that outlines the sensitivity of data, usually within an information system.
Telework:	Working remotely, often from home, using telecommunications technology like phones, networks, virtual private network (VPN), information technology systems.
Threat:	Anything that can cause harm to systems, networks or information.
Threat and Risk Assessment (TRA):	A process to identify threats and evaluate the risks they pose.
Trojans:	Named after the Trojan Horse from Greek mythology, these are malicious programs that disguise themselves as legitimate software. Once installed, they can make it easier for attackers to access systems, steal data or cause other harm, often without the user realizing it.
Trusted Path:	A secure communication channel that ensures data integrity and confidentiality.
Uninterruptible Power Supply (UPS):	A device that provides backup power to systems in case of a power outage.
User ID:	The first half of your login information that you are assigned to access systems and data.
Virtual Private Network (VPN):	A secure connection over the internet that protects data and privacy.
Virus:	Malicious software that can replicate itself and spread to other systems.
Vulnerability:	A weakness in a system that can be exploited by threats.

Information Security Glossary

Ministry of SaskBuilds and Procurement

Information Technology Division, Cybersecurity and Risk Management Branch

Vulnerability Assessment: The process of identifying and evaluating weaknesses in a system.

Website Spoofing: Website spoofing is a scam used by cyber criminals where they create a copy of a real website to fool you into giving them your personal information.

Worms: These are malicious programs that can spread themselves from one computer to another without any human action. They often exploit vulnerabilities in software to replicate and spread across networks, causing damage or stealing information.
