Figure 1—Cybersecurity Attack Vectors

Cyberattack Vector	Examples/Description	Objective	Problem Identifier
Malware	Virus, worm, trojan horse, spyware, rootkit software	Data theft, password stealer, network or system compromise	Antivirus software; intrusion detection system (IDS)
Phishing (includes spear phishing)	Deceptive malicious email that targets organizational users and uses attachments or malicious links to plant malware	Network or system access; data breach	User
Ransomware (includes doxing)[a]	Extortion (data are deleted or encrypted unless ransom is paid)	Blackmail for ransom	Ransomware announcement
Denial of service (DoS) (includes distributed DoS [DDoS])	Overwhelm network device or server to prevent access or usage	Network or system disruption	Network administrators via network monitoring system
Compromised, weak or stolen credentials	User login account and password	Data breach	Forensic investigation
Malicious insiders	Disgruntled employee who exposes private information	Revenge, embarrassment	Management, United States Computer Emergency Readiness Team (US-CERT)
Third- and fourth-party vendors	Suppliers, cybersecurity partners	Obtain competitive information	Network monitoring system; log management system
Missing or poor encryption	Data at rest, data in motion	Gain access to data	System assessment
Device misconfiguration	Servers, network devices, mobile computing devices	Obtain access to device and data	System assessment
Unpatched vulnerabilities	Servers, network devices, mobile computing devices	Obtain access to device and data	Patch management system
Structured Query Language (SQL) injections	Manipulate database servers to expose information	Gain access to data	Penetration tester
Cross-site scripting	Inject malicious code into a comment	Gain access to system, network and data	Penetration tester
Session hijacking	Intercepted session cookies	Gain access to data	User
Man-in-the-middle (MitM) attacks	Public Wi-Fi networks	Gain access to network	Intrusion prevention system (IPS)
Brute-force attack	Trial-and-error attempts to gain access to network or system	Gain access to system, network and data	Log management system