By upholding a strong cybersecurity posture, you can minimize your company’s digital exposures and safeguard your operations against potential losses. **By upholding a strong cybersecurity posture, you can minimize your company’s digital exposures and safeguard your operations against potential losses.**

**Common Threat Vectors**

In the realm of cybersecurity, a threat vector refers to any avenue or method a cybercriminal can leverage to infiltrate a target’s network, system, or device. In other words, threat vectors serve as pathways for cybercriminals to conduct their attacks. Here are some common threat vectors:

1. **Social engineering and phishing scams**—Social engineering entails a cybercriminal utilizing deceptive communication and other manipulation tactics to lure targets into sharing sensitive information or providing unauthorized access to their systems. One of the most prevalent social engineering methods is phishing, which involves sending emails or texts that appear to be from legitimate sources but contain malicious links or attachments.

2. **Malware and ransomware**—Malware is any software designed to perform a malicious action, such as stealing financial data, accessing sensitive data, or taking control of a device.

3. **Identity-based attacks**—Identity-based attacks aim to exploit vulnerabilities in an individual’s identity before gaining access to their systems.

4. **End-of-life (EOL) software management**—When software reaches the end of its life, manufacturers discontinue technical support and upgrades for this technology. As a result, EOL software generally contains additional vulnerabilities that can be exploited in cyberattacks. It’s imperative to address these issues with an end-of-life plan to ensure security.

5. **Multifactor authentication (MFA)**—MFA encompasses a hybrid approach to safeguarding networks and systems, requiring users to provide two or more credentials (e.g., a password and a security question) to confirm their identity before gaining access. This extra layer of security can prevent cybercriminals from easily unlocking and infiltrating accounts.

6. **Endpoint detection and response (EDR)**—EDR solutions can provide continuous monitoring capabilities and enhance overall visibility into network and system activities, allowing for improved threat identification and remediation. Key features of EDR solutions include data triage; contextualized threat hunting; and malicious activity detection and containment.

7. **Patch management**—Patch management is the process of applying security patches to address vulnerabilities. This is essential because it helps prevent cybercriminals from exploiting weaknesses in software or systems.

8. **Distributed denial-of-service (DDoS) attacks**—DDoS attacks are a common form of cyber-attack in which criminals send an excess of requests to overwhelm a target’s network or system, forcing it to shut down. These attacks usually utilize large groups of internet-connected devices (also called botnets) to send a surge of traffic. This is achieved by sending a surfeit of requests that exceed the capacity of the service or system, forcing it to shut down.

9. **End-of-life (EOL) software management**—When software reaches the end of its life, manufacturers discontinue technical support and upgrades for this technology. As a result, EOL software generally contains additional vulnerabilities that can be exploited in cyberattacks. It’s imperative to address these issues with an end-of-life plan to ensure security.

10. **Multifactor authentication (MFA)**—MFA encompasses a hybrid approach to safeguarding networks and systems, requiring users to provide two or more credentials (e.g., a password and a security question) to confirm their identity before gaining access. This extra layer of security can prevent cybercriminals from easily unlocking and infiltrating accounts.

**Key Controls to Better Your Cybersecurity Posture**

It’s important to implement control measures to protect your business against various threat vectors and uphold a solid cybersecurity posture. Consider the following key controls for your business:

1. **Employee education and training**—Training employees on cybersecurity best practices can help prevent them from unwittingly exposing your business to threats. This includes awareness training on social engineering and phishing scams, as well as regular updates on the latest threats.

2. **End-of-life (EOL) software management**—When software reaches the end of its life, manufacturers discontinue technical support and upgrades for this technology. As a result, EOL software generally contains additional vulnerabilities that can be exploited in cyberattacks. It’s imperative to address these issues with an end-of-life plan to ensure security.

3. **Multifactor authentication (MFA)**—MFA encompasses a hybrid approach to safeguarding networks and systems, requiring users to provide two or more credentials (e.g., a password and a security question) to confirm their identity before gaining access. This extra layer of security can prevent cybercriminals from easily unlocking and infiltrating accounts.

4. **Endpoint detection and response (EDR)**—EDR solutions can provide continuous monitoring capabilities and enhance overall visibility into network and system activities, allowing for improved threat identification and remediation. Key features of EDR solutions include data triage; contextualized threat hunting; and malicious activity detection and containment.

5. **Patch management**—Patch management is the process of applying security patches to address vulnerabilities. This is essential because it helps prevent cybercriminals from exploiting weaknesses in software or systems.

6. **Distributed denial-of-service (DDoS) attacks**—DDoS attacks are a common form of cyber-attack in which criminals send an excess of requests to overwhelm a target’s network or system, forcing it to shut down. These attacks usually utilize large groups of internet-connected devices (also called botnets) to send a surge of traffic. This is achieved by sending a surfeit of requests that exceed the capacity of the service or system, forcing it to shut down.

7. **End-of-life (EOL) software management**—When software reaches the end of its life, manufacturers discontinue technical support and upgrades for this technology. As a result, EOL software generally contains additional vulnerabilities that can be exploited in cyberattacks. It’s imperative to address these issues with an end-of-life plan to ensure security.

8. **Multifactor authentication (MFA)**—MFA encompasses a hybrid approach to safeguarding networks and systems, requiring users to provide two or more credentials (e.g., a password and a security question) to confirm their identity before gaining access. This extra layer of security can prevent cybercriminals from easily unlocking and infiltrating accounts.

9. **Endpoint detection and response (EDR)**—EDR solutions can provide continuous monitoring capabilities and enhance overall visibility into network and system activities, allowing for improved threat identification and remediation. Key features of EDR solutions include data triage; contextualized threat hunting; and malicious activity detection and containment.

10. **Patch management**—Patch management is the process of applying security patches to address vulnerabilities. This is essential because it helps prevent cybercriminals from exploiting weaknesses in software or systems.