Cyber Speak, Simplified:

Breaking Down Technically Complex Issues for Non-Technical People

Cybersecurity is hot on nearly everyone's mind, but how much does the average person really know? Although frequently discussed aspects of cybersecurity offer a straightforward and user-friendly gateway to the subject, they only scratch the surface of the multifaceted challenges within the domain. These foundational concepts, though easy to digest, often provide an incomplete perspective that fails to account for the nuances and ever-evolving landscape of cyber threats.

User awareness training is one of the most utilized cybersecurity measures. Nearly everyone has watched a cyber safety video and taken the subsequent quiz at least once. However, these measures only address a fraction of cyber vulnerabilities. In fact, data reveals these user awareness trainings account for about 10% of ransomware cases.

The majority of cyber threats, ones that can freeze entire networks and halt business operations, are driven by technical vulnerabilities. What is a technical vulnerability? It already sounds more complicated than "user awareness training," and it is – but defining and discussing technical vulnerabilities is critical to effectively countering the cyber threats.

A technical vulnerability is a vulnerable point within a system susceptible to intrusion by threat actors. Such systems include networks and computer software and hardware. These vulnerabilities are potential entry points for cyberattacks and underscore the importance of proactive security measures to safeguard digital assets and protect against unauthorized access.

Threat actors typically exploit three primary technical vulnerabilities:

- **Public Exposure Issues:**
  A network is like a fortress with multiple entry points. If your network has an open entry point unguarded on the public internet, threat actors can easily invade, often undetected. This intrusion can be a particularly significant issue when using Remote Desk Protocol (RDP). RDP allows users to remote in and control a computer over a network connection. If you have an issue that needs the assistance of IT, this is a great tool, but if you're on a public network, your trusted IT team is only one of many on a long list of entities – many malicious – that can access your network.

- **Software Vulnerabilities:**
  A software program is similar to a chain with many links. If there is a weak link in the chain, threat actors can put in little effort to break it and gain access to your system. Unpatched software is one of the most common weak links. Software companies frequently release updates to fix known security flaws and are closely monitored by the organization's IT team. Updates fortify a network's cybersecurity, but users often ignore these updates and don't install the new patches, leaving systems vulnerable to attack.

Misconfigured VPNs:
A Virtual Private Network (VPN) is like a secret tunnel that helps secure online communications anonymously and securely. When you use a VPN, your internet traffic is encrypted and routed through a secure server, making it nearly impossible for prying eyes to eavesdrop on your online activities. VPNs enhance your online privacy and safeguard sensitive information from potential threats. However, if a VPN is set up incorrectly, that secret tunnel is no longer a secret. Misconfigured VPNs become an unintentional invitation to threat actors looking for vulnerabilities to exploit within your network.

Misconfigured VPNs:
A Virtual Private Network (VPN) is like a secret tunnel that helps secure online communications anonymously and securely. When you use a VPN, your internet traffic is encrypted and routed through a secure server, making it nearly impossible for prying eyes to eavesdrop on your online activities. VPNs enhance your online privacy and safeguard sensitive information from potential threats. However, if a VPN is set up incorrectly, that secret tunnel is no longer a secret. Misconfigured VPNs become an unintentional invitation to threat actors looking for vulnerabilities to exploit within your network.

If these are the big three technical vulnerabilities, what are some optimal technical controls that have the potential to thwart these cyberattacks in the first place?

External Exposure Monitoring:
A software program is similar to a chain with many links. If there is a weak link in the chain, threat actors can put in little effort to break it and gain access to your system. Unpatched software is one of the most common weak links. Software companies frequently release updates to fix known security flaws and are closely monitored by the organization’s IT team. Updates fortify a network’s cybersecurity, but users often ignore these updates and don’t install the new patches, leaving systems vulnerable to attack.

Backups:
Think of data like a book. If someone steals or destroys your book, your backup is a spare copy hidden in a secret vault. But the true value of backups extends beyond just recovering from data loss. Backups offer peace of mind and control over your organization’s digital assets. Regular backups solidify fortified preparation in the event of unforeseen circumstances, whether it's a ransomware attack that encrypts your files or a hardware failure that renders your computer useless. There are many user-friendly backup solutions: external drives, cloud storage, or network-attached storage (NAS) devices. The key is to set up a reliable and consistent backup strategy to ensure your “digital book” is safe and recoverable.

While we can’t say that cybersecurity will ever be simple, we can help make it more digestible and accessible for your organization’s safety and continued success. Our advisors are highly specialized in the cyber sphere and keep a pulse on emerging trends and threat actors. We leverage our relationships with top insurance company partners, incident response teams, and other trusted partners to create solutions that align with your organization’s needs.

Connect with us to discover how we can help you thrive in the digital world.

INSGROUP
A BALDWIN RISK PARTNER

BRP
CYBER CENTER OF EXCELLENCE

This material has been prepared for informational purposes only. BRP Group, Inc. and its affiliates, do not provide tax, legal or accounting advice. Please consult with your own tax, legal or accounting professionals before engaging in any transaction.