Cybersecurity Blind Spots

Layer 1

The Entry Points

Points of contact are high-risk entry points into an org's data systems. Do you know who you're letting in?

- **Privileged access**

  Points of contact are high-risk entry points into an org's data systems. Do you know who you're letting in?

- **Personal devices**

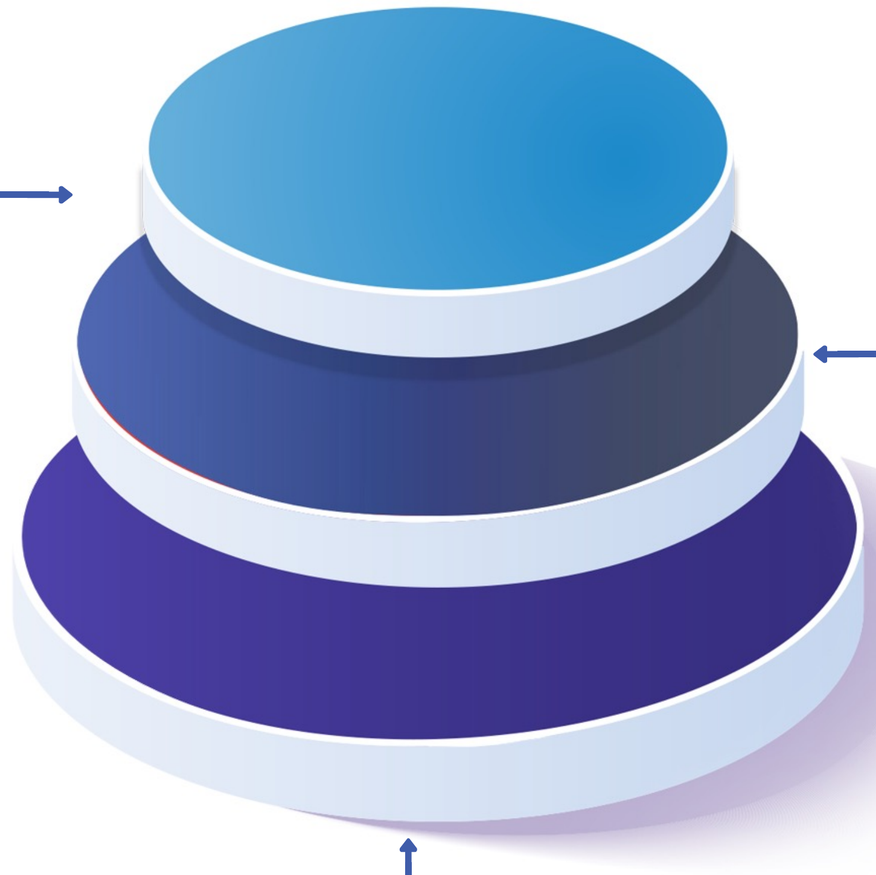
  An organizations' security controls aren't always extended to workers' personal devices, making them susceptible to cyberattacks.

- **Public networks**

  Public WiFi or unsecure networks increase likelihood of security breaches.

- **Third-parties**

  Collaboration tools, virtual meeting platforms, file sharing: organizations often rely on third-party applications, but these applications are prime targets for hackers looking for a way into company data or systems.



Layer 2

The Infrastructure

Tools and operations can make an organization more vulnerable. How well do you know your security system?

- **Operating systems**

  Outdated operating systems may be less resilient than new systems and unable to withstand cyberattacks.

- **Antivirus signatures**

  Today's malware is constantly changing, making it hard for signature-based security systems to keep up. Old antivirus signatures can't identify new threats.

- **VPNs and VDIs**

  Unpatched virtual private networks (VPNs) and inadequate virtual desktop infrastructures (VDIs) provide breaks in security which attackers can exploit.

- **SIEM tools**

  Not all security information and event management (SIEM) tools are created equal. Without essential functions like real-time insights, detailed analysis of endpoint activity, and immediate response to malicious behavior, you're limiting your view of critical areas throughout your organization's security systems.

Layer 3

The Oversight

Whether digital or human, security needs controls and monitors. Who's keeping an eye on your data?

- **Crisis management**

  Flooded with help requests and new threats to monitor, IT teams are overextended.

- **Endpoint controls**

  Anytime a device accesses your network, you're at risk. Proper endpoint controls (encryption, application control) are essential to prevent cyberattacks throughout your organization.

- **User awareness**

  A lack of cyber hygiene (privacy awareness, cybersecurity best practices) among employees and third-parties increases the likelihood of users falling victim to phishing scams and ransomware attacks.