**Cybersecurity Methods**

**Section: Examine Cybersecurity Methods**

To effectively safeguard our organisation against modern cyber threats, it is imperative to adopt a layered and strategic approach to cybersecurity. Below are five essential methods that integrate both technical and organisational principles to strengthen our overall security posture.

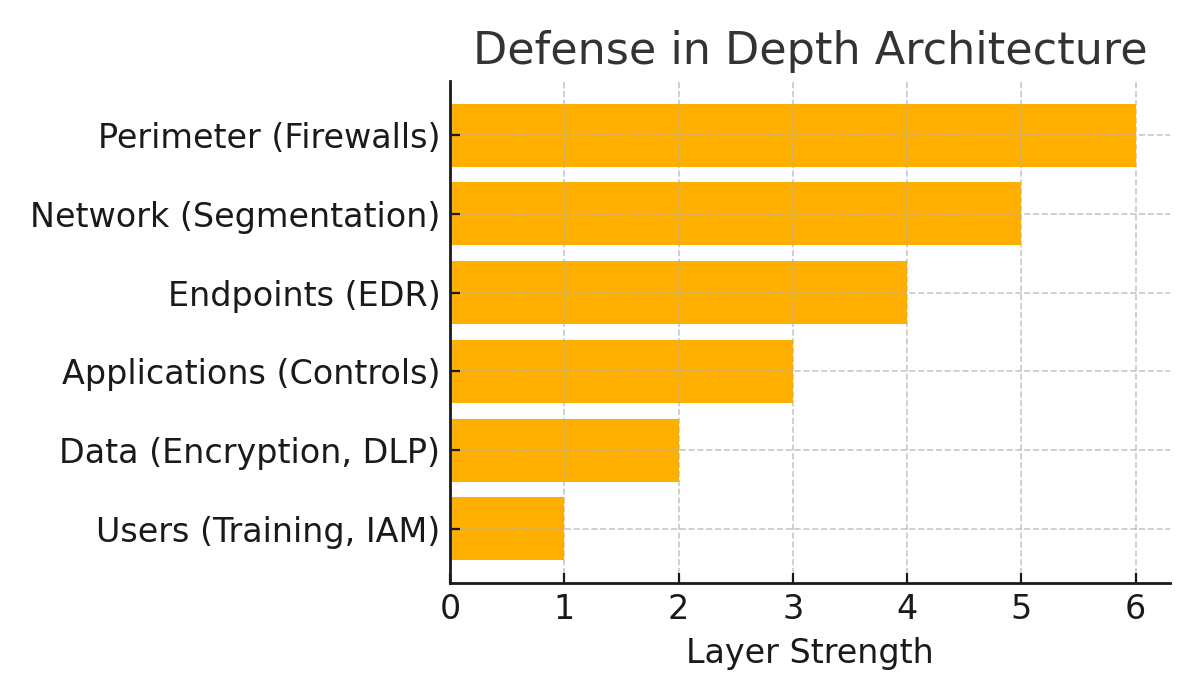
1. **Defense in Depth Architecture**  
   Deploy multiple layers of security controls across various points in the IT environment. From network perimeter defenses like firewalls to endpoint protection and user education, this architecture ensures redundancy and containment, reducing single points of failure.
2. **Continuous Security Testing (DevSecOps)**  
   Integrate security practices into every stage of the software development lifecycle. Automated security scans in CI/CD pipelines catch vulnerabilities early, fostering collaboration between developers, operations, and security teams.
3. **Identity and Access Management (IAM) with Zero Trust**  
   Restrict access based on verified identities and roles. With Zero Trust, access is never assumed and always verified using MFA and least privilege principles, enforced technically and supported by governance policies.
4. **Security Information and Event Management (SIEM)**  
   Collect and correlate logs across the network to detect anomalies and enable incident response. Its effectiveness depends on organisational structures—teams must manage alerts, tune rules, and handle real-time monitoring.
5. **Risk-Based Vulnerability Management**  
   Prioritise vulnerabilities based on risk severity rather than treating all equally. Technical tools identify exposures, while business context determines remediation priorities, aligning technical findings with organisational impact.

**User Consultation and Business Process Impact**  
Before implementing any cybersecurity method, engage in user consultation and conduct a business process impact assessment to align changes with workflows, reduce operational friction, and increase adoption. For example, IAM with Zero Trust requires assessing how access restrictions affect productivity and defining roles accurately to prevent disruptions. Similarly, deploying SIEM must consider alert fatigue and ensure teams receive adequate training.

**Selected Security Solution Topics**  
To address additional governance and technical enhancements, the following topics are selected with practical application examples:  
- **Separation of Privileges:** Enforce role-based access by mapping out critical duties; for example, finance team members can approve requests but require a second-level manager sign‑off to execute payments, reducing insider risk.  
- **Biometrics:** Integrate fingerprint recognition at workstation login; for example, employees authenticate via fingerprint scanners to access confidential systems, minimizing password fatigue and tailgating risks.  
- **AI-Driven Security Solutions:** Deploy machine learning models to analyze user behavior; for example, the system auto‑flags anomalous access patterns and initiates automated threat hunting, accelerating incident response.

- Digital Identity: Implement federated identity management systems; for example, employees use single sign‑on (SSO) across business applications, improving security and user experience.

- Blockchain‑Driven Security Assurance: Use blockchain to create immutable audit logs; for example, key transactions and access events are recorded on a private ledger to ensure tamper‑proof forensics.

**Figure 1. Defense in Depth Architecture**.  
  
Defense in Depth Diagram  
*Note. Adapted from NIST SP 800-160 and KnowBe4 (2023).*

**References**  
KnowBe4. (2023). *2023 Phishing by Industry Benchmarking Report*. https://www.knowbe4.com/  
National Institute of Standards and Technology. (2020). *Framework for Improving Critical Infrastructure Cybersecurity (NIST SP 800‑53 Rev. 5)*. https://nvlpubs.nist.gov  
Ross, R., McEvilley, M., & Oren, J. (2016). *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems* (NIST SP 800‑160). https://nvlpubs.nist.gov  
ThreatCop. (2022). *Top 5 Cyberattacks and Security Breaches Due to Human Error*. https://threatcop.com/blog/top-5-cyber-attacks-and-security-breaches-due-to-human-error/  
Williams, P. A. H. (2019). The human firewall: Cybersecurity awareness and education. *Computers & Security, 87*, 101580.