CYBERSECURITY ESSENTIALS

IN FIVE EASY STEPS

1. Multi-Factor Authentication (MFA)

A cyber attack often starts with stealing a username and password. With MFA, a bad actor needs more than just credentials to access an organizations network or critical data. MFA is a quick and easy way to add an essential layer of security—EO Advisor recently dedicated a whole article to MFA.

2. Password Complexity

Hackers use brute force computing power to try millions of passwords in a matter of minutes. More complicated passwords explode the demands on a brute force attack exponentially. Billions of possible password solutions are much better than millions. Incredibly, simple passwords remain a major vulnerability today.

3. Vulnerability Scanning and Remediation

This is software that conducts a detailed scan of servers, workstations, and network equipment, searching for vulnerabilities. The scans identify possible vulnerabilities such as out-of-date software, blank passwords (i.e., for printer configuration), and general misconfigurations that can create a back door for hackers. Digital Defense provides high value for organizations looking to up their game.

4. Security Awareness Training

Phishing is very sophisticated. Smart employees make mistakes. The US government estimates that 85% of cyberattacks begin with phishing. Formal training using an independent 3rd party like KnowBe4 provides a safe way to educate team members about phishing attacks. Explaining the problem is not sufficient. Software that generates fake phishing attacks uncovers employee lapses and provides immediate feedback in a safe context. This training technique makes a critical difference.

5. User Permissions (The Principle of Least Privilege)

Not everyone needs access to everything. Not everyone needs access to everything. Universal access is easier to administer, but it makes life easy for hackers to move through the entire network. For example, hacking a new employee in the HR department can let a bad actor worm their way into a server where financial accounting data is stored. Exercising the practice of Least Privilege provides a roadblock that can stop a hacker from gaining access to everything.