access one

Cyber criminals are more innovative and savvy than ever before, making it critical for businesses to have a strong cyber security program in place. Use this checklist to see if your cyber security program meets the challenge of modern security threats.

Security Awareness of Staff

Effective cyber security begins with a high level of awareness among your employees. A strong security awareness training program includes a number of elements, which we list here.

Written Policies

Written policies should be in place for all of the following:

- □ Bring your own device
- □ Remote access
- □ Clean desk policy
- □ Email
- □ Software installation
- □ Wireless
- □ Data destruction
- □ Password policies
- □ Social engineering
- □ Ethics
- □ Acceptable use

Security Awareness Training Controls

Critical elements of security awareness training include:

- □ Phishing
- □ Ransomware
- □ Incident response

Vulnerability Assessments

You'll better understand your security strengths and weaknesses and where your areas of highest risk are after a vulnerability assessment. These are typically conducted twice a year for any business in a regulated industry and quarterly for those requiring PCI compliance.

- □ Prioritization of risks and remediation
- □ Third-party suppliers
- □ Physical security (key fobs, locks, alarms, etc.)
- □ Compliance attestation
- □ Cloud infrastructure
- □ Applications
- □ Internal and external assessment perspectives
- □ Secure configurations

Compliance

Many organizations must adhere to regulatory frameworks. For businesses in regulated industries, compliance is a key consideration in creating a security program.

- □ HIPAA
- □ GDPR
- □ Control frameworks
- □ PCI DSS
- □ NYCRR
- □ Risk management frameworks
- □ CCPA
- □ Cyber security frameworks

Threat Detection

Detecting potential threats before they cause problems is an important element of any cyber security program.

- □ Log correlation
- □ Dark web monitoring
- □ Log retention
- □ Anomaly detection

Backup and Disaster Recovery

Whether caused by human error or a natural event, disasters happen. Be prepared with a thorough backup and disaster recovery plan.

- □ File level backup
- □ Disaster recovery
- □ Incident response and disaster recovery runbook
- □ Disk image backups
- □ Business continuity
- □ Replication
- □ Archival

Email Security

Malicious actors often make their way into a system through something as simple as an email. Your security program should include protection of your email system.

- □ Email backup and archival
- □ Attachment sandboxing
- □ Spam protection
- □ eDiscovery
- □ Link protection
- □ Social engineering
- □ Data leakage protection (DLP)
- □ Email firewall / security gateway

Endpoint & Server Security

A vulnerability assessment will automatically flag the absence of certain necessary endpoint and server security measures.

- □ Advanced malware protection (AMP)
- □ DNS protection
- □ Third-party patch management (Adobe, Chrome, Java, etc.)
- □ Mobile device management
- □ Windows updates
- □ Asset management (warranty and lifecycle)

Authentication

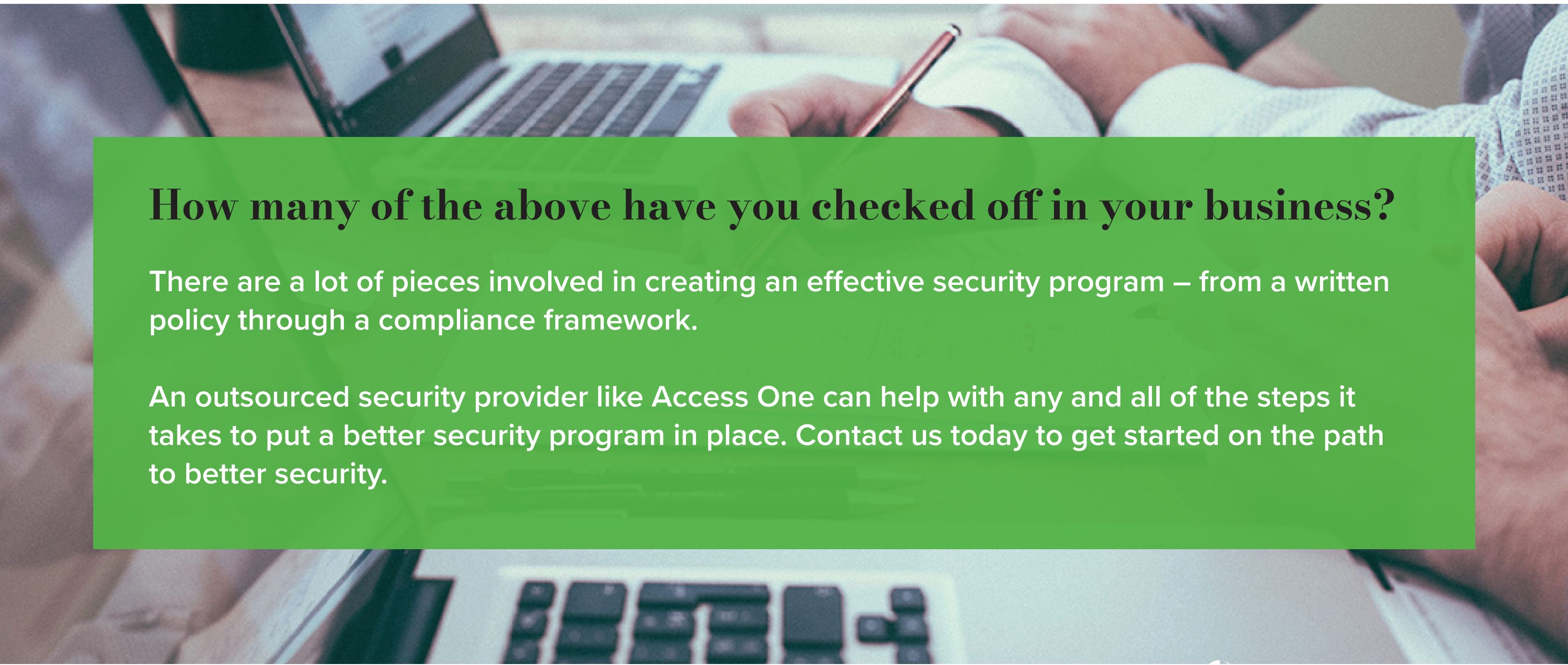
A basic security measure to have in place is authentication that goes beyond simply creating a strong password.

- □ RADIUS
- □ MFA
- □ AD
- □ TFA

Next Generation Firewall

Stay ahead of cyber criminals that work tirelessly to breach your systems and keep them locked out with a next generation firewall.

- □ Intrusion detection and prevention
- □ Content filtering
- □ Application layer security
- □ Advanced malware protection (AMP)
- □ VPN



How many of the above have you checked off in your business?

There are a lot of pieces involved in creating an effective security program – from a written policy through a compliance framework.

An outsourced security provider like Access One can help with any and all of the steps it takes to put a better security program in place. Contact us today to get started on the path to better security.