RANSOMWARE PROTECTION CHECKLIST

82% of ransomware attacks target small businesses.
It can be difficult to know how to protect your organization without a detailed plan in place.

BCS365

1. PROTECT YOUR EMAIL | Ransomware attacks often start with a phishing email to capture admin or user credentials.

1a	**BLOCK PHISHING ATTACKS** Attackers use social engineering tactics to bypass traditional email security. Use an email security solution that includes AI-enabled phishing and account takeover protection, as well as alerts when malicious activities are detected.	☐
1b	**TRAIN USERS** Your users are your last line of defense against phishing attacks. Training needs to be an ongoing effort, as attacks often become more sophisticated over time.	☐
1c	**IMPLEMENT REMEDIATION** Email attacks that evade email security and land in users' inboxes need to be addressed quickly. Choose an email security solution that enables proactive threat discovery and automates remediation.	☐

2. SECURE YOUR APPLICATIONS | Attackers hack your web applications to gain access to your data.

2a	**PROTECT WEB APPLICATIONS** Applications often have open vulnerabilities that can be exploited to gain access to your data. Use an application security solution that defends against web application vulnerabilities such as OWASP Top 10, zero-day and brute force attacks.	☐
2b	**PROTECT ACCESS TO APPLICATIONS** For internal applications, you should only allow access for authorized users and devices. Choose a zero trust access solution that enables role based access, multi-factor authentication and continuous verification of user and device identity.	☐
2c	**PREVENT LATERAL MOVEMENT ON YOUR NETWORK** If attackers gain access to your network, they often attempt to move laterally to find and infect data sources. You need a network firewall that protects both your on-prem and cloud networks with network segmentation and advanced security services.	☐

888-886-5767 sales@BCS365.com BCS365.com

RANSOMWARE PROTECTION CHECKLIST

3. BACK UP YOUR DATA | Attackers encrypt your data and demand ransom.

3a	**BLOCK PHISHING ATTACKS** Attackers use social engineering tactics to bypass traditional email security. Use an email security solution that includes AI-enabled phishing and account takeover protection, as well as alerts when malicious activities are detected.	☐
3b	**TRAIN USERS** Your users are your last line of defense against phishing attacks. Training needs to be an ongoing effort, as attacks often become more sophisticated over time.	☐
3c	**IMPLEMENT REMEDIATION** Email attacks that evade email security and land in users' inboxes need to be addressed quickly. Choose an email security solution that enables proactive threat discovery and automates remediation.	☐

OTHER RECOMMENDATIONS

- **PATCHING** | Make sure software is patched and up to date. Attackers look for known vulnerabilities first, so don't make it easy for them.
- **PASSWORD SECURITY** | Enforce strong passwords. Many recent attacks were successful due to weak passwords and ineffective password management practices.
- **MULTIFACTOR AUTHENTICATION** | Consider requiring a phone app or text based second factor authentication for all applications and resources. This is very useful in preventing brute-force login attempts.

BUILD YOUR RANSOMWARE PLAN TODAY

BCS365.com/Contact

BCS365®

888-886-5767 sales@BCS365.com BCS365.com