LAYERED CYBERSECURITY GUIDE

elevITy
A GORDON FLESCH COMPANY

SECURITY ASSESSMENT
Assess the unique threat environment your business faces, based on the type of work you engage in, and Internet and network exposure.

EMAIL POLICIES & FILTERS
Email remains the most vulnerable threat vector. Reduce spam to increase productivity and limit your exposure to attacks via email.

PASSWORDS
Apply security policies on your network. Policies should include limits for USB file access, enabling enhanced password policies, and limiting user access.

SECURITY AWARENESS
Teach your staff basic data security, offer web-based training solutions, and implement security policies to help limit exposure to phishing and malware.

Did You Know?

64%

of companies have experienced web-based attacks.

ADVANCED ENDPOINT SECURITY
Protect your computers and data from malware, viruses, and cyber-attacks with advanced endpoint security software.

MULTI-FACTOR AUTHENTICATION
Multi-Factor Authentication adds an additional layer of protection to ensure that even if your password is stolen, your data stays protected.

COMPUTER UPDATES
Vendors are continually issuing patches and updates which are critically important to protect your computers from the latest known attacks

DARK WEB RESEARCH
Tools can be used to monitor the Dark Web, which is the Internet's black market where cybercriminals can buy and sell stolen data.

SIEM/LOG MANAGEMENT
Security Incident & Event Management (SIEM) software reviews event and security logs to protect against threats and to meet compliance requirements.

WEB GATEWAY SECURITY
Cloud based security detects web and email threats and blocks them on your network before they reach the user.

MOBILE DEVICE SECURITY
Mobile device security monitors and limits exposure from employees' phones and devices, which are often not managed or protected by security software.

FIREWALL
Intrusion Detection and Intrusion Prevention features can work in conjunction with SIEM systems to identify and mitigate emerging risks.

ENCRYPTION
Employ industry-standard encryption to protect communications and data when in transit or stored on networked systems.

BACKUP
Backup systems should be continually running so that in the event of a cyberattack a business can quickly restore systems.

CYBER INSURANCE
Cyber insurance policies can ensure that in the event of a breach or attack, a business will be protected from losses and liabilities. Elevity recommends that you discuss a Cyber Insurance policy with your agent.

CYBERSECURITY SERVICE RECOMMENDATIONS

The following products and services are designed to provide multiple layers of security within your network. No computer system is unhackable; but the more layers of cybersecurity protection between your systems and threat actors, the more difficult it will be to break into a computer network. Due to the growing threat of cyberattack, we recommend the following:

	Included	Add	Decline
Schedule a **Vulnerability Assessment** of my network __/__/__			
Upgrade/Add **SPAM Protection** for ____ users			
Add **Password Security** and reasonable **Group Policies** to our network			
Provide **Security Awareness Training** for our staff			
Upgrade our existing antivirus to **Advanced Endpoint Security**			
Add **Multi-Factor Authentication** to our systems			
Provide timely **Security Updates** and **Patch Management** to our network			
Upgrade our **Firewall** to include **Advanced Threat Protection**			
Add encryption services to our ☐ **Laptops** ☐ **Mobile Devices** ☐ **Email**			
Upgrade backup services to include ☐ **Cloud** ☐ **Local** ☐ **Offline**			
Add **Web Security Gateway** and **DNS Filter Security** to out account			
Deploy **Security Incident and Event Management (SIEM)** on our network			
Add **Mobile Device Security** to **All Company Owned** devices			

Elevity Customer Date

Elevity IT Consultant Date

elevITy
A GORDON FLESCH COMPANY