

# Savvy Cybersecurity<sup>®</sup>

## Business Protection

### Checklist

# 2021

**Randall A. Luebke, RFC, RMA, CMP, CWPP**  
**President**  
**Lifetime Paradigm, Inc.**  
260 Newport Center Drive  
Ste 100  
Newport Beach, CA 92660  
800-810-1736  
Info@LifetimeParadigm.com  
www.LifetimeParadigm.com



Use the following topics and questions to guide a cybersecurity discussion with your security professionals and management team. The goal is to share information, identify problems and strengths, and take action.

#### Ask your IT or Security Professional:

##### CYBERSECURITY PLANS

- Do we have a written information security policy?
- Do we conduct periodic reviews to identify security threats and vulnerabilities to our system?
- Do we have a written plan of action if we do suffer a cybersecurity attack?
- How do we protect ourselves from ransomware?
- What do you think is the most serious cybersecurity threat our business faces?

##### DATA PROTECTION

- Do we have a regular backup system in place?
- Where is our customer data housed on the network and how is it protected versus other locations?
- How do we control the transfer of customer data?
- Who has access to download customer data?
- Is our data encrypted?
- How is our communication encrypted?
- How do we protect customer information?
- What is our policy for aging out old data?
- How do we track computers and devices and the data they hold?
- How is mission critical data warehoused offsite?

##### NETWORK/CONNECTION

- Who connects to our networks from the outside and how do we manage?
- How do we monitor for unauthorized users or devices on the network?
- How restrictive is our firewall for inbound communication and access?
- Does our firewall have proxying services, antivirus gateway services, and intrusion detection and prevention services?
- What endpoint security do we have in place?
- Do we conduct vulnerability scans of the network?
- Do we have the ability to know we have an active attacker in our network?

##### DEVICES

- Do we have an inventory of all physical devices and systems within the company?
- Are all devices used in the company running antivirus software?
- How do we ensure all devices are running up-to-date software?
- Are our routers secure and are they running the most up-to-date firmware?

##### EMPLOYEE POLICIES

- Do we limit employee access to only networks, systems, files, and programs that they need for their job?
- What kind of employee cybersecurity training do we have?
- What is our policy for employees working or accessing work data on their personal devices?
- Do we offer employees a VPN for working remotely?
- What is our password policy?

##### THIRD PARTY POLICIES

- Do any third parties have access to our data?
- How do we vet the security of third party companies we use?
- Do we discuss cybersecurity risks and responsibilities when going into contract with other companies?

## Ask your CFO:

### FRAUD PREVENTION

- Do we have a two-step verification policy for wire transfers?
- Are we alerted anytime a charge or withdrawal is made from our accounts?
- Does our business insurance cover cybersecurity incidents?
- Do we have a PIN on our mobile phone accounts?
- How often do we check our business credit report?
- What type of security do we have on our bank accounts and credit cards?
- Do we receive email notifications when any change to our business registration is made online?
- How do we store personal employee information?

## Ask your employees:

### KNOWLEDGE

- Do you know the key ways to identify a phishing email message?
- Do you understand the link between hacking and updating software on your computers and devices?
- Do you understand the cybersecurity risks associated with accessing your email and other work data from an unsecured wireless connection?
- How do you protect any personal device that also contains business data and contacts?
- What is our policy on discarding digital and physical documents containing private customer or business information?

## GLOSSARY

**Account takeover attack-** The process of using an existing account to commit a fraud. Example: Your mobile phone account is taken over by hackers.

**Advanced persistent threat (APT)-** A long-term attack targeted on a specific person or institution. Over time, a hacker gains access to various parts of the network through malware or security holes.

**Distributed Denial of Service (DDoS)-** A type of attack that uses compromised devices to push traffic to a single website or system. The increase in traffic causes the system to shut down.

**Encryption-** The process of concealing messages or information so only others with permission can read them. Encryption creates a private tunnel for information and data to travel through.

**Endpoint security-** A security system used to secure a network accessed by remote wireless devices. The system secures the devices to block potential entry points to the network.

**Firewall-** A part of a computer system or network that's designed to monitor inbound and outbound communication between your device, other devices, and the Internet.

**Firmware-** Permanent software that has been programmed into a device, such as a wireless router.

**IP address-** A set of unique numbers assigned to every device connected to the Internet.

**Keylogger-** Malicious software or a physical device that records the keys that you hit on the keyboard. This is used to gain private information such as usernames and passwords.

**Malware-** Malicious software—such as Trojans, worms, and viruses—designed to interfere with a computer's normal functioning.

**Phishing/Spear phishing-** A scam by which email users are duped into revealing personal, confidential, or monetary information or downloading malware by clicking on a malicious link or attachment. Spear phishing is when these messages are directed at a particular business or person.

**Proxy server-** A software intermediary that intercepts and inspects data between an external network (the Internet) and an internal, private network. A proxy server prevents outsiders from directly accessing internal information.

**Ransomware-** A type of malware used by hackers that encrypts the victim's data and demands payment for the decryption key.

**Social engineering-** The process of manipulating people into giving up confidential information or breaking security procedures by appealing to human emotions.

**Two-step verification-** A two-stage process to verify your identity when trying to access an online account. It requires "something you know" and "something you have."

**Virtual Private Network (VPN)-** A network technology that creates a private encrypted Internet tunnel using a public Internet connection.

Investment Advisory Services are offered through Lifetime Financial, Inc., a Registered Investment Advisory. Insurance and other financial products and services are offered through Lifetime Paradigm, Inc. or Lifetime Paradigm Insurance Services. Neither Lifetime Financial, Inc. nor Lifetime Paradigm, Inc., or its associates and subsidiaries provide any specific tax or legal advice. Only guidance is provided in these areas. For specific recommendations please consult with a qualified, licensed Advisor. Past performance is no guarantee of future results. Your results can and will vary. Investments are subject to risk, including market and interest rate fluctuations. Investors can and do lose money and, unless otherwise noted, they are not guaranteed. Information provided is for educational purposes only and is not intended for the sale or purchase of any specific securities product, service or investment strategy. **BE SURE TO FIRST CONSULT WITH A QUALIFIED FINANCIAL ADVISER, TAX PROFESSIONAL, OR ATTORNEY BEFORE IMPLEMENTING ANY STRATEGY OR RECOMMENDATION DISCUSSED HEREIN.**