Corporate Account Takeover

Data Security Self-Assessment

Inventory the data controls you have in place. Evaluate different types of security procedures and think about whether they make sense for the type of information you maintain, the format in which it is maintained, the likelihood that someone might try to steal the information, and the harm that would result if the information was disclosed. Make sure to consider all data, including employee payroll information.

Step 1: Use the checklists below to assess whether the security measures you are taking are adequate.

Type of Data You Collect, Store and/or Transmit	Yes	No
Customer/Client Names	☐	☐
Employee Names	☐	☐
Mailing Addresses	☐	☐
Physical Addresses	☐	☐
Phone Numbers	☐	☐
Email Addresses	☐	☐
Account Numbers	☐	☐
Invoice Numbers	☐	☐
Social Security Numbers	☐	☐
Dates of Birth	☐	☐
Driver's License Numbers	☐	☐
Business ID Numbers	☐	☐
Types & Amounts of Transactions	☐	☐
Other Protected Information	☐	☐

Methods of Storage Used by Your Company	Yes	No
Paper *(employee files, customer files, invoices, order requests, contracts, contact lists, etc.)*	☐	☐
Email *(messages, contact lists, calendar entries)*	☐	☐
Databases/Spreadsheets *(accounting software, invoicing software, reconcilements, etc.)*	☐	☐
Electronic Documents *(financial reports, business plans, contracts, etc.)*	☐	☐
Payroll Files *(payroll software, ACH origination files)*	☐	☐
Online/Cloud File Storage *(iCloud, Amazon Cloud Drive, Google Drive, Dropbox, etc.)*	☐	☐

Physical & Electronic Storage Sites	Yes	No
Desk Drawers	☐	☐
Filing Cabinets	☐	☐
Mail Room	☐	☐
Home Office(s)	☐	☐
Desktop Computers	☐	☐
Laptops	☐	☐
Mobile Devices: phones, tablets, etc.	☐	☐
USB/Thumb Drives	☐	☐
CDs/DVDs	☐	☐
Other Storage Devices	☐	☐

Desktop/Laptop Computer Used for ACH Origination	Yes	No
Does it connect to an internal, protected network?	☐	☐
Does the data leave the office/internal network?	☐	☐
Is it accessible off-site?	☐	☐
Does it access the Internet or email accounts?	☐	☐
Who has access?		

Other Desktop Computers	Yes	No
Do they connect to an internal, protected network?	☐	☐
Does the data leave the office/internal network?	☐	☐
Is it accessible off-site?	☐	☐
Does it access the Internet or email accounts?	☐	☐
Who has access?		

Laptops	Yes	No
Do they connect to an internal, protected network?	☐	☐
Does the data leave the office/internal network?	☐	☐
Is it accessible off-site?	☐	☐
Does it access the Internet or email accounts?	☐	☐
Who has access?		

Internal Network Servers	Yes	No
Do they connect to an internal, protected network?	☐	☐
Does the data leave the office/internal network?	☐	☐
Is it accessible off-site?	☐	☐
Does it access the Internet or email accounts?	☐	☐
Who has access?		

Mobile Phones	Yes	No
Do they connect to an internal, protected network?	☐	☐
Does the data leave the office/internal network?	☐	☐
Is it accessible off-site?	☐	☐
Does it access the Internet or email accounts?	☐	☐
Who has access?		

Tablets	Yes	No
Do they connect to an internal, protected network?	☐	☐
Does the data leave the office/internal network?	☐	☐
Is it accessible off-site?	☐	☐
Does it access the Internet or email accounts?	☐	☐
Who has access?		

USB Drives	Yes	No
Do they connect to an internal, protected network?	☐	☐
Does the data leave the office/internal network?	☐	☐
Is it accessible off-site?	☐	☐
Does it access the Internet or email accounts?	☐	☐
Who has access?		

CDs/DVDs	Yes	No
Do they connect to an internal, protected network?	☐	☐
Does the data leave the office/internal network?	☐	☐
Is it accessible off-site?	☐	☐
Does it access the Internet or email accounts?	☐	☐
Who has access?		

Other Devices	Yes	No
Do they connect to an internal, protected network?	☐	☐
Does the data leave the office/internal network?	☐	☐
Is it accessible off-site?	☐	☐
Does it access the Internet or email accounts?	☐	☐
Who has access?		
Describe the types of devices:		

Controls/Protection	Yes	No	If Yes, How?
Computer operating systems have all current updates and patches on all machines?	☐	☐	
Computers have all security devices (firewalls, anti-virus, anti-malware) activated and up-to-date?	☐	☐	
Data encryption in place?	☐	☐	
Electronic data is automatically backed up and can be restored in the event of human error, system failure, or natural disaster?	☐	☐	
Anti-Phishing protections in place?	☐	☐	
You and your employees know how to recognize and avoid phishing emails that may be received via business or personal email accounts?	☐	☐	
Malware protections in place against internal network entry via:			
Business email accounts	☐	☐	
The Internet *(web browsers, web-based email)*	☐	☐	
Portable storage devices (USB drives, iPods/Phones) cannot be connected to endpoint machines and download sensitive data without authorization?	☐	☐	

Step 2: For each item under Controls/Protections that is checked "no," develop a plan to implement a solution.

This document is for informational purposes and is not intended to provide legal advice. The guidance included is not an exhaustive list of actions, and security threats change constantly.