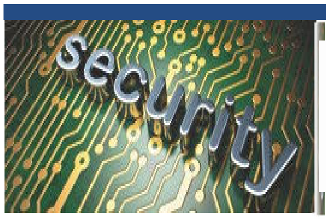

SIX AND GEVING INSURANCE, INC.

Cyber Self Assessment

Glatfelter Healthcare Practice℠
A Division of Glatfelter Insurance Group

According to *Protecting Personal Information – A Guide for Business*[1] a sound data security plan is built on **five key principles:**

1. ***Take stock.*** Know what personal information you have in your files and on your computers.
2. ***Scale down.*** Keep only what you need for your business.
3. ***Lock it.*** Protect the information that you keep.
4. ***Pitch it.*** Properly dispose of what you no longer need.
5. ***Plan ahead.*** Create a plan to respond to security.

This self-assessment tool was developed using the concepts outlined in the Federal Trade Commission booklet "Protecting Personal Information – A Guide for Business[2]. It can be used to help identify areas where a data security plan could be improved.

Item	Yes	No	Not Applicable/Comments
Take Stock			
1. Has an inventory been completed of all computers, laptops, mobile devices, flash drives, disks, home computers, digital copiers and other equipment to find out where sensitive data is stored?	□	□	
2. Has a tracking system for sensitive personal information been set up?	□	□	
Does it include:			
a. Who sends sensitive personal information the business	□	□	
b. How the business receives personal information	□	□	
c. What kind of information is collected at each entry point	□	□	
d. Where the collected information is kept	□	□	
e. Who has—or could have—access to the information	□	□	
Scale Down			
1. Is there a legitimate business need for all sensitive personally identifying information collected?	□	□	
a. Is there a process in place to destroy this information when it is no longer necessary?	□	□	
2. If you collect Social Security numbers, is it necessary (i.e. reporting employee taxes)?	□	□	
a. Can an employee or customer identification number be used instead?	□	□	
3. Are electronically printed credit and debit card receipts truncated (shortened)?	□	□	
4. Is there a policy in place to retain customer credit card information only where there is a business need for it?	□	□	
a. Is there a process in place to destroy this information when it is no longer necessary?	□	□	
5. For information that is kept due to business reasons or to comply with the law, is there a written records retention policy to identify:			
a. What information must be kept?	□	□	
b. How to secure it?	□	□	
c. How long to keep it?	□	□	
d. How to dispose of it securely when it is no longer needed?	□	□	

Item	Yes	No	Not Applicable/Comments
Lock It			
Effective data security plans deal with four key elements:			
1. Physical security	□	□	
2. Electronic security	□	□	
3. Employee training	□	□	
4. Security practices of contractors and service providers	□	□	
Physical Security			
1. Are paper documents or files, as well as CDs, floppy disks, zip drives, tapes and backups containing personally identifiable information, stored in a locked room or in a locked file cabinet?	□	□	
2. Is access limited to employees with a legitimate business need?	□	□	
3. Is there a procedure for controlling who has access (i.e. key control)?	□	□	
4. Are the following requirements in place?			
a. Are files containing personally identifiable information kept in locked file cabinets except when an employee is working on the file?	□	□	
b. Do employees secure sensitive papers when they are away from their workstations?	□	□	
c. Do employees put files away, log off their computers and lock their file cabinets and office doors at the end of the day?	□	□	
5. Is the building access controlled?	□	□	
6. Are employees informed what to do and whom to call if they see an unfamiliar person on the premises?	□	□	
7. If sensitive information is shipped using outside carriers or contractors, is the information encrypted and an inventory of the information being shipped kept?	□	□	
8. Is an overnight shipping service used that allows for tracking of the delivery?	□	□	
9. Are devices that collect sensitive information (i.e. PIN pads) secured so that identity thieves can't tamper with them?	□	□	
a. Have these devices been inventoried to ensure that they have not been switched?	□	□	

Item	Yes	No	Not Applicable/Comments
Electronic Security			
General Network Security			
1. Have the computers and servers where sensitive personal information is stored been identified?	□	□	
2. Have all connections to the computers where sensitive information is stored been identified? (These may include the Internet, electronic cash registers, computers at branch offices, computers used by service providers to support network, digital copiers and wireless devices like smartphones, tablets or inventory scanners.)	□	□	
3. Has the vulnerability of each connection been assessed to commonly known or reasonably foreseeable attacks? (Depending on circumstances, appropriate assessments may range from having knowledgeable employees run off-the-shelf security software to having an independent professional conduct a full-scale security audit.)	□	□	
4. Is only essential sensitive consumer data stored on computers with an Internet connection?	□	□	
5. Has consideration been given to the following:			
a. Encrypting sensitive information that is sent to third parties over public networks (like the Internet)?	□	□	
b. Encrypting sensitive information that is stored on computer networks (or on disks or portable storage devices used by employees)?	□	□	
c. Encrypting email transmissions within the business if they contain personally identifying information?	□	□	
6. Are up-to-date anti-virus and anti-spyware programs run regularly on individual computers and servers on the network?	□	□	
7. Is there a process in place to check expert websites (such as www.sans.org) and software vendors' websites regularly for alerts about new vulnerabilities and implement policies for installing vendor-approved patches to correct problems?	□	□	
8. Are there restrictions to employees' ability to download unauthorized software? (Software downloaded to devices that connect to the network – computers, smartphones and tablets – could be used to distribute malware.)	□	□	
9. Is there a process to scan computers on the network to identify and profile the operating system and open network services?	□	□	
a. If there are unneeded services found, are they disabled to help prevent hacks or other potential security problems?	□	□	
10. Is Secure Sockets Layer (SSL) or another secure connections used when credit card information or other sensitive financial data is received or transmitted?	□	□	

Item	Yes	No	Not Applicable/Comments
Password Management			
1. Are there requirements for passwords?	□	□	
If yes:			
a. Are there requirements to help assure that employees use “strong” passwords?	□	□	
b. Do the rules require a mix of letters, numbers and characters?	□	□	
c. Are passwords required to be different than an employee’s username?	□	□	
d. Is there a process in place requiring frequent changes in passwords?	□	□	
2. Is there a policy in place prohibiting employees from sharing their passwords or posting them near their workstations?	□	□	
3. Are password-activated screen savers used to lock employee computers after a period of inactivity?	□	□	
4. Does the system lock out users who don’t enter the correct password within a designated number of log-on attempts?	□	□	
5. Have employees been warned about possible calls from identity thieves attempting to deceive them into giving out their passwords by impersonating members of your IT staff?	□	□	
Mobile Device Security (laptops, cell phones, tablets, etc.)			
1. Is the use of mobile devices restricted to employees who need them to perform their jobs?	□	□	
2. Has an assessment been done to determine whether sensitive information really needs to be stored on a mobile device? (If not, delete it with a wiping program that overwrites data on the device.)	□	□	
3. Have employees been informed of the importance of storing mobile devices in a secure place?	□	□	
4. Have employees been trained to be mindful of mobile device security when travelling?	□	□	
5. Has consideration been given to allowing users only to access sensitive information, but not to store the information, on their devices?	□	□	
6. Have mobile devices containing sensitive data been encrypted and configured so users can’t download any software or change the security settings without approval from the company’s IT specialists?	□	□	
7. Has consideration been given to adding an auto-destroy function so data on a device that is reported stolen will be destroyed when the thief uses it to try to get on the Internet?	□	□	

Item	Yes	No	Not Applicable/Comments
Firewalls			
1. Is there a firewall in place to protect computers from hacker attacks while it is connected to the Internet?	□	□	
2. Has installation of a border firewall where the network connects to the Internet been considered?	□	□	
3. Has consideration been given to using additional firewalls to protect computers with sensitive information?	□	□	
Wireless and Remote Access			
1. Have wireless devices like smartphones, tablets or inventory scanners or cell phones that connect to the computer network or transmit sensitive information been identified?	□	□	
2. Has consideration been given to limiting who can use a wireless connection to access the computer network?	□	□	
3. Has encryption been considered to make it more difficult for an intruder to read the content on the network?	□	□	
4. Do you use a VPN when accessing company resources on a pubic Wi-Fi?	□	□	
Digital Copiers			
1. Have steps been taken to protect the data on the hard drive of digital copiers?	□	□	
2. Have the following safeguards been considered?			
a. Is IT involved in the purchase to help assess data security?	□	□	
b. Are security features of the copier being used?	□	□	
c. Is the entire hard drive being securely overwritten at least once a month?	□	□	
d. Is the hard drive removed and destroyed when disposing of a copier?	□	□	
• If not, has the data on the hard drive been overwritten?	□	□	
Detecting Breaches			
1. Do you have an intrusion detection system on the network?	□	□	
a. Is it updated frequently to address new types of hacking?	□	□	
2. Is a central log file of security-related information maintained to monitor activity on the network to help spot and respond to attacks?	□	□	
3. Do you monitor incoming traffic for signs that someone is trying to hack in?	□	□	
4. Is outgoing traffic monitored for signs of a data breach?	□	□	
5. Is there a breach response plan in place?	□	□	
a. Is the breach response practiced on a regular basis?	□	□	
b. Does the plan address data loss due to ransomware attacks?	□	□	

Item	Yes	No	Not Applicable/Comments
Employee Training			
1. Before hiring employees, are reference checks and/or background checks run on those who will have access to sensitive data?	□	□	
2. Do new employees sign an agreement to follow the company's confidentiality and security standards for handling sensitive data?	□	□	
3. Are employees regularly reminded of company policy—and any legal requirement—to keep customer information secure and confidential?	□	□	
4. Is access to consumers' sensitive personally identifying information limited to employees with a "need to know"?	□	□	
5. Is there a procedure in place for ensuring workers who leave or transfer to another part of the company no longer have access to sensitive information?	□	□	
a. Are passwords terminated, keys and identification cards collected as part of the check-out routine?	□	□	
6. Is ongoing employee training conducted?	□	□	
a. Does the training include:			
• Employees at satellite offices, temporary help and seasonal workers?	□	□	
• Recognizing security threats?	□	□	
• Company policies regarding keeping information secure and confidential?	□	□	
• The dangers of spear phishing—emails containing information that makes the emails look legitimate?	□	□	
• Phone phishing?	□	□	
• Notification of potential security breaches, such as a lost or stolen laptop?	□	□	
• Dangers of transmitting sensitive personally identifying data—Social Security numbers, passwords, account information—via email.	□	□	
Security Practices of Contractors and Service Providers			
1. Have contractors and security providers' data security practices been evaluated?	□	□	
2. Do contracts address security issues for the type of data the service providers handle?	□	□	
3. Are service providers required to notify the company of any security incidents they experience, even if the incidents may not have led to an actual compromise of data?	□	□	
4. When using a service provider for storage (email or files), does the contract outline an offloading process for data if the contract is not renewed?	□	□	
5. Is there a plan in place to address operations if the service provider is unavailable due to a service outage or data breach?	□	□	

Item	Yes	No	Not Applicable/Comments
Pitch It			
1. Have information disposal practices to prevent unauthorized access to—or use of—personally identifying information been implemented?	□	□	
2. Are paper records disposed of by shredding, burning or pulverizing them before discarding?	□	□	
3. Is data on old computers and portable storage devices securely erased before disposal?	□	□	
4. Are employees who work from home (or remotely) following the same procedures for disposing sensitive documents and old computers and portable storage devices?	□	□	
Plan Ahead			
1. Is there a plan in place to respond to security incidents?	□	□	
2. Is there a senior staff member designated to coordinate and implement the response plan?	□	□	
3. Does the plan address the following:			
a. Disconnecting any compromised computer immediately from the network?	□	□	
b. Investigating security incidents immediately to take steps to close off existing vulnerabilities or threats to personal information?	□	□	
c. Whom to notify in the event of an incident, both inside and outside the organization?	□	□	
d. Does the plan in place include verification of the quality of backed up data and testing of the data restoration?	□	□	

Consumers, law enforcement, customers, credit bureaus and other businesses that may be affected by the breach may need to be notified. In addition, many states and the federal bank regulatory agencies have laws or guidelines addressing data breaches[1]. It is strongly recommended that an attorney be consulted.

[1] FEDERAL TRADE COMMISSION - 600 Pennsylvania Avenue, NW, Washington, DC 20580 business.ftc.gov/privacy-and-security

[2] Ibid.

Additional Resources

These websites and publications have more information on securing sensitive data:
National Institute of Standards and Technology (NIST); Computer Security Resource Center; www.csrc.nist.gov
SANS (SysAdmin, Audit, Network, Security) Institute; The Top Cyber Security Risks; www.sans.org/top-cyber-security-risks
United States Computer Emergency Readiness Team (US-CERT): www.us-cert.gov
OnGuard Online; www.OnGuardOnline.gov (Computer security tips, tutorials and quizzes)
Copier Data Security: A Guide for Businesses at www.ftc.gov/tips-advice/business-center/guidance/copier-data-security-guide-businesses