Data Security – *Made Simpler*

FAQs

Q1: Given all the things I need to juggle to run my business, why should I make Data Security a priority?

A1: One word – ***"Trust."*** As hard as you've worked to earn your customers' trust in you and your business, it can take just one trigger to break that trust. *Your ability to keep your customers' sensitive data secure is one of those make-it-or-break-it triggers.* Customers expect that every business – large or small – that collects their sensitive personal information will protect it. Beyond customer expectations, there's the law. Depending on your type of business and the states in which your customers reside, you may be legally required to protect the personal information you collect.

Q2: This feels overwhelming. How do I even start this process?

A2: It will be less overwhelming if you approach this piece by piece. First – determine what makes sense for your type of business. This will be based on the type of data that you collect and store, and the kind of resources you have managing that data.

If your small business keeps information about customers in several formats (e.g., on paper, on computers, and online), you should sit down with a team of your employees and discuss these issues together to make sure you consider all viewpoints.

1) Inventory all your data and its various types and forms.

2) Inventory all the different sites where you store data.

3) Inventory potential sources for data leaks.

4) Evaluate the costs versus benefits of different security methods.

5) Write this all down, and you'll have just created the foundation of your written security policy!

Refer to Chapter 1 of "Data Security – *Made Simpler"* for some useful checklists that will make this process easier for you and your team.

Q3: What are four (4) minimum things a small business should be doing for data security?

A3:

1) *Minimize what you save and store.* If you don't need it, don't collect it...and don't store it. If you have it and don't need it any more, destroy it – responsibly.
2) *Restrict and limit access – by everyone – to sensitive data.* Use locks on doors and file cabinets and virtual locks (mail security and network access control) on your computer systems, emails and files. Limit employee access to data to those that need it to do their jobs. Take precautions when mailing records. Encrypt sensitive electronic information in <u>every</u> site it is stored – on computers; On laptops On PDAs, iPhones and iPods; On USB drives (sometimes called "thumb" drives"). Transmit data over the internet using secure connections (SSL technology), and make sure to use network access control technology for remote access by employees and consultants.
3) *Use effective passwords...and issue a unique password to every employee.* Never use the default password that comes from another product or service provider. Never use obvious passwords, such as your name, business name, family member's name, "12345," "ABCDE," "password," or your user name. Change passwords every 45-60 days.

4) *Block potential intruders...knowing that antivirus is NOT enough.* Stay informed and protect your IT systems from viruses and spyware by using complete endpoint (desktop, laptop and server) protection – not just antivirus protection and firewalls. Make sure these protections are up-to-date and incorporate antispyware, intrusion prevention, and behavior-based protection, which does much more than the simple antivirus and firewall technologies of yesterday.

Refer to Chapter 1 of "**Data Security – *Made Simpler***" for more information on these four guidelines and potential resources to help.

Q4: What are the five (5) things small businesses should do to secure their online banking credentials (e.g., PINs, passwords, tokens, et)?

A4: *1) Initiate payments under dual control.* Ensure that all payments are initiated from your bank accounts only after the authorization of two employees.

2) Update virus protection and security software. Ensure that all anti-spyware, anti-malware, and security software and mechanisms for all computer workstations and laptops that are used for online banking and payments are robust, up-to-date, and that there is a process for periodically checking that they remain up-to-date.

3) Have dedicated workstations. If possible, restrict the use of certain workstations and laptops to be utilized solely for online banking and payments.

4) Reconcile accounts daily. Monitor and reconcile accounts daily against expected credits and withdrawals. If unexpected activity is seen on your account, notify your financial institution immediately.

5) Use robust authentication methods. Set up methods to access your accounts via multi-channel authentication.

Refer to Chapter 2 of "**Data Security – *Made Simpler***" for more information on these five guidelines and potential resources to help.

Q5: What's the best way to destroy paper documents?

A5: Shred them yourself, or hire a reputable shredding company to do it for you. *Never just toss paper documents containing sensitive information in the trash or dumpster.*

Q6: What are some of the best ways to destroy electronic documents?

A6: Use data wiping software, as it permanently removes information by writing new, meaningless information on top of old information. CDs and DVDs can be shredded. Computer hard drives can be "magnetically degaussed," which uses extremely strong magnets to remove the magnetic encoding that stores data – which is a very affordable way to responsibly destroy old hard drives.

Refer to Chapter 4 of "**Data Security – *Made Simpler***" for more information about these methods and potential resources to help.

Q7: What are some common myths about destroying data that I should be aware of?

A7: Here are three examples:

1) *Breaking or smashing an old computer DOES NOT necessarily destroy the information it houses.* Just because you break the machine does not mean you're breaking the media where the data is stored (on the hard drive).

2) *Microwaving CDs and DVDs DOES NOT destroy the information on them, and can release toxic fumes into your microwave or cause a fire.*

3) *Placing data into the "Recycle Bin" on your desktop DOES NOT destroy the information. Neither does clicking "Delete."* It still exists and can be recovered.

Refer to Chapter 4 of "**Data Security – *Made Simpler***" for more information.

Q8: What are the key things I should tell my customers in my Data Security Policy?

A8: Here are some ideas to get started.

1) *If you are encrypting sensitive information in every site it is stored* – both stationary and portable – tell them that.

2) *If you restrict access to sensitive data*, outline the key ways you're doing this (i.e., locking cabinets and closets, limited access to solely employees that need the information to do their job, etc.) – tell them that, too.

3) *Consider obtaining a third-party seal* that verifies your small business uses an appropriate level of security to protect your web site (e.g., BBB *OnLine* seal or *Hacker-Safe* seal). Display your SSL certificate (e.g., *Verisign)* if your web site accepts electronic payments, which communicates customer data is secure during the transfer process.

Refer to Chapter 1 of "**Data Security – *Made Simpler***" for other ideas of specific data security precautions you may be taking that are appropriate to communicate to your customers. But whatever you say you are doing, make sure you're doing it! And if you change the way you secure data, make sure you update your policy and your customer communications to reflect that change. You can also refer to Chapter 5 of "**Data Security – *Made Simpler***" for potential resources of companies that validate safety of web sites or provide online data security seals of approval.

Q9: Is there anything I should <u>not</u> communicate in my Data Security Policy?

A9: Yes.

1) *DO NOT SHARE detailed information about your security systems so that criminals might use that information to evade them.*

2) *DO NOT tell customers there is no risk of ID theft, or that their information is "100% safe." No matter how hard you try to protect customer information, there is always a chance that someone may obtain it and misuse it.*

3) *DO NOT guarantee or promise that a customers' information can never be lost or stolen unless you tell customers what you will do if that promise if broken.*

Refer to Chapter 5 of "**Data Security – *Made Simpler***" for more detailed guidance.

Q10: What type of "red flags" might signal suspicious behavior and an attempt at fraud?

A10: Here are just a few examples:

1) *A "customer" opens a new account that contains suspicious elements...such as a P.O. Box for a home address or an email address that seems to have someone else's name.*

2) *A customer presents you with suspicious documents, such as an ID card that appears altered, different addresses on different forms of ID, or a P.O. Box as a home address.*

3) *Your (or one of your employees) notice unusual activity relating to a customer's account.*

Refer to Chapter 6 of "**Data Security – *Made Simpler***" for more detailed guidance.