



Securing your data—an affordable necessity

Written by Ceron Moffatt, Mail & More, Inc. Research & Development Manager

How secure are your data? What data should you be securing? Questions like these are faced by any business where data are considered a primary asset which must be protected. Although most small to mid-size businesses know the importance of storing data securely, many don't understand the need of having a detailed, formal plan for handling this security. And, there is also concern about the cost! Be assured that putting the right technologies, protocol and policies in place can be done and it can be affordable.

The bottom line is, you cannot afford not to have security in place for your data. The consequences of security compromises or privacy violations could: (1) jeopardize a company's ability to provide service; (2) reduce revenue flow through fraud or destruction of proprietary or confidential data; (3) violate business contracts, trade secrets and customer privacy; and (4) reduce the confidence held by customers, suppliers and employees in your company.

It is important to define the objective of the security policy you are establishing. This statement ensures that data are protected in all of their forms as they exist in all processing environments during all phases of their life cycle from unauthorized or

inappropriate access, use, modification, disclosure or destruction. This should serve as a guideline for the steps you take in developing your security plan. It is also important to be mindful of any federal regulations, such as HIPPA, that affect how to plan this security policy.

A good way to start is to determine what data need to be secured. List how each category of data are generated or collected, used, stored and shared. Examples of data that should be secured include:

- Customer data: Customers want assurances they can trust you with their data.
- Product information: Unique intellectual property is the lifeblood of a company.
- Employee information: All details of personal information need to be protected.
- Company information: Unauthorized use harms a company's reputation and stability.

Then identify the potential threats to these sensitive data. Keep in mind that security threats come in all shapes and sizes, and originate externally or internally from within an organization. These could include employee theft, hacking, fire, water, or even physically removing the system from the facility.

Next, review available options and processes to secure this sensitive data at each level of access, including collection, use, storing and sharing. Be mindful that workstations also need securing and these solutions often include software and hardware solutions. Mandatory password rotation, cameras, security badges, and ID cards can all be used to screen and monitor data access at workstations. Windows Vista *Ultimate* and the Mac OSX are examples of reliable solutions that offer a secure

level of encryption for your system if falls into the wrong hands. BitLocker in Vista *Ultimate* and FileVault for the Mac both have requirements that need to be reviewed and addressed before using. TrueCrypt is a free open source tool that will encrypt your data on the fly and supports Windows Vista/XP, Linux and the Mac OS X. However, a determined hacker can bypass the password logon and obtain the password to get into a system by booting into Linux from a USB stick. Unfortunately if this occurs, then having an encrypted hard drive will do you no good. TrueCrypt uses what is called Plausible Deniability to hide a data area of volume ([Hidden Volume](#)), or a spot on the hard drive. There is another level of Plausible Deniability that hides the operating system ([Hidden Operating System](#)) that works along the same lines. Hidden volumes can prevent hackers from successfully getting into a system. For more information regarding TrueCrypt, access their website through www.truecrypt.org. Workstations need securing also, and these solutions typically combine hardware and software solutions.

Portable devices such as, USB sticks, iPods, or even phones with Bluetooth capabilities enable employees to work out of the office, whether it involves remotely accessing company data or downloading to work with it afterhours or during work-related travel. Customer demands for prompt communications greatly increases sensitive data security threats. Mobile work forces, using mobile devices accessing company data either remotely or from a portable device, are needed to respond to customer inquiries. Companies must write policies that govern the handling of sensitive data; develop written procedures that instruct employees how to correctly access this

data; and utilize software applications and hardware to block, manage, and monitor the access to sensitive data needed by employees for their work.

Data security also involves planning for disruptions to accessibility. Your business continuity plan should include your data threats, list your methods to mitigate these threats, and present your plan to recover and resume operations should these threats become a reality. This plan should include how to identify the security breach and how to communicate a security breach to identified critical staff members. This plan should also include the steps followed in the case of an incident. Regular review of your business continuity plan is important to assess its current relevance to your operations, as well as familiarize appropriate staff with the procedures in place.

The on-going costs of data security can be managed by continuously reviewing policies procedures. Due to the size and nature of the data stored, some businesses will spend thousands of dollars keeping their data secure, while other companies will be able to manage their sensitive data by using much more reasonably priced options. Ultimately, these costs can be passed along to consumers and in the competitive marketplace, the businesses that practice prevention and planning are the businesses that survive.