

Securing Personal Data!

By *Jennifer Garcia*



A Guide for Business

Better be despised for too anxious apprehensions,
than ruined by too confident security — Edmund Burke

Has it ever crossed your mind that a great part of your daily life is relying directly on computers? Be it the hardware gadget you use, or equipment you use for entertainment, or even the means you use for shopping as well as transportation. A great deal of your personal and private information keeps flowing into and out of your system through a network which is entirely 'PUBLIC'. Yes, we are talking about internet and online data transfer here.

Being the highest success governing factor for any business, data security is extremely important to almost every business. Losing sensitive data stored in your files or on your system or risking it to fall into wrong hands can expose your business to irreversible or highly damaging consequences.

Information like employees' or your personal account and tax details, payroll or personal records of your employees as well as your valued customers, your credit card or other payment cards details can go into wrong hands exposing you to some really horrible business risks that you might not have made a provision of.

In many businesses, the security policies involve the old traditional security methods that mostly fail to secure organization's confidential data and private information from going into wrong hands. These traditional methods include installing of firewalls, antivirus programs and spyware tools. Although, these security tools are designed specially to protect your computer system, but the chances of finding vulnerable holes in this kind of security layer are abundant when so many smart hackers and attackers are lose in the wild-planning and strategizing the most smartest and unstoppable way to break into your system's privacy.

With a more reactive and advanced security monitoring procedure in practice, and a strategic step by step security layer implementation, organizations can avoid many data loss instances, including system misuse, infusion of virus and Trojans, or accidental corruption or data.

A businessman like you would definitely not want to take risks that could lead you to possible fraud or copyright breaches. Therefore, what you need is a solution or a plan that can take away all the pain and distress caused by the threats involving data theft, data loss and data breaches.

Five key principles:

A sound data security plan is built on **five key principles**:

1 Stock piled information: Find out what personal and how confidential information you have stored in your files and on your hard drives.

2. Determine the need: Store the information that is literally needed.

3. Protect it. Protect the information by locking it.

4. Dump it. Properly discard what you no longer require.

5. Make a plan. Create a plan to respond to security incidents.

Stock Piled Information:

To start with, a proper assessment should be carried out to determine what information you have stored already and to find out about all the people authorized to access it. It is important to determine the kind of information you are dealing with and who has or could have an open access to it. Essentially, the most important and confidential information is the one to be given least access to.



Security vulnerabilities arise mostly when the information flowing into and out of the system is kept untraced and unsecured irrespective of their confidentiality and integrity. So, what's best to do in this kind of scenario is to:

- Keep stock of all computers, laptops, disks, home end systems, flash drives and other data storage equipments to find out and verify where exactly does the company store its sensitive data.
- Keep a record of the information by its *Type* and *Location*.

- Trace confidential information that is dealt by your sales department, IT staff, HR office and accounts and finance department or even the external service providers.

Hence, the key areas you have to take care of are:

- ✓ Who sends personal information to your business?
 - Customers
 - Credit Card Companies
 - Banks or financial institutions
 - Credit bureaus
 - Other Business
- ✓ How does this personal information come to you?
 - By email
 - Through a website
 - By mail
 - Through Fax
- ✓ What kind of information is collected online?
- ✓ Do you keep the information you collect in a central database? Or on laptops or other storage mediums?
- ✓ Do you let your employees save company's information in their personal laptops or flash drives or take your data to their homes?
- ✓ Who has access to the information your store and who could gain subsequent access to it?

Determine the need:

In some businesses and organizations, there is a common habit of storing each and every data the company is coming in use with, for, most of the times, no apparent reason but to avoid the hassle of prioritizing, storing and enlisting the information according to its importance and usability.

What most business fail to understand is that storing each and everything in their databases will not only amass their hard drives and other storage equipments with chunks of invaluable and useless data but in case of an unforeseen data breach activity, the information that might appear valueless for the company can become valuable for the person stealing the information from company's database. Such a slipup can expose the business to a number of adverse consequences that the company itself might not have figured out.



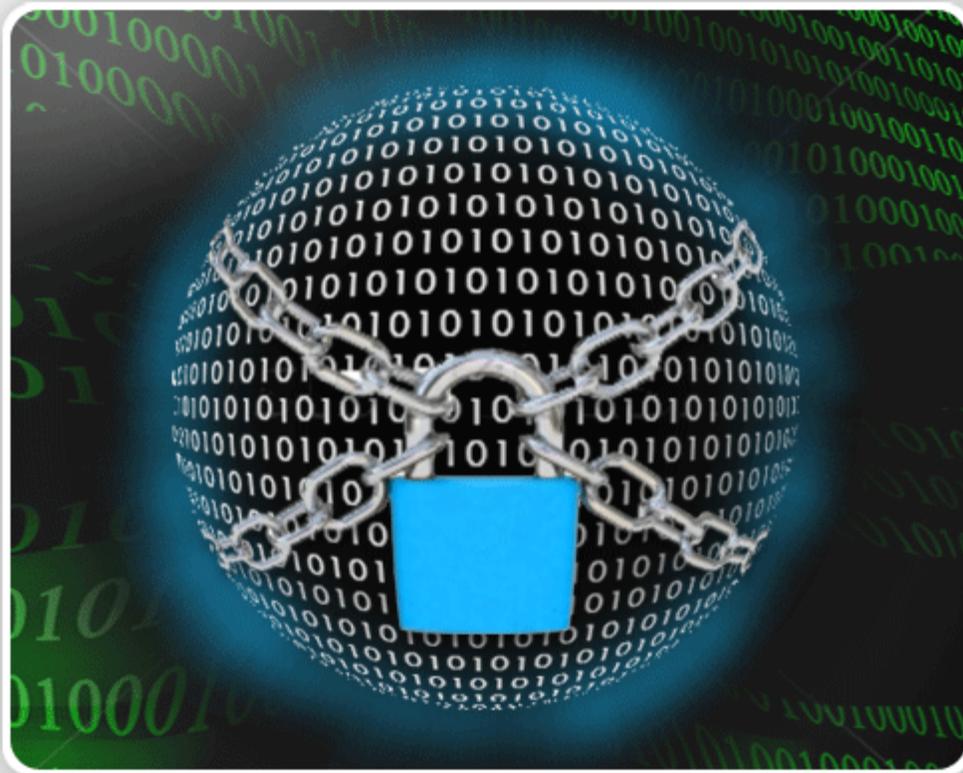
So, if you don't have a reasonable business need for sensitive personally identifying data, avoid keeping it in your storages. Furthermore, keep the collected and stored information for only as long as you are in need of it. As soon as the lawful purpose of storing such information is fulfilled, discard the information properly.

A good example of such information can be Social Security numbers, employee or customer identification number or customer credit card number. The use of social security numbers should be subjected to the lawful business purpose only. Similar rule applies to the use of employee or customer identification numbers as well as the customer credit card credentials. The practice of retaining customer credit card information or personal information of the similar kind longer than necessary may expose the information to become the target of fraud or identity theft.

If you are using a software program that automatically extracts data from electronic forms, make sure that you set it to keep the information for a temporary period of time. However, if your business needs require you to retain customer's personal information longer than usual, you must comply with the law by developing a written record retention policy stating what information is to be kept, how to keep it secure, for how long and how to dispose it off securely.

Protect It:

What makes a data security plan the most effective plan is the deployment of four key security elements in your business setup. These key elements are:



- ✓ Physical Security
- ✓ Electronic Security
- ✓ Employee Training

Let's look at each element step by step:

Physical Security: Although, not many companies and business owners keep their company or business information in the form of paper documents in physical files and folder, but there still exist a class of people to whom paper documentation is the only reliable way to keep information records.



The best defense for such class of people is to keep their files and folder in a real life physical locker or locked drawer. Similarly, CDs, floppy disks, zip drives, tapes and other storage medium should be kept in a locked room or in a locked file drawer. Only employees with a legitimate business need should be given the access to those documents while proper monitoring should be carried out when the information gets accessed.

Identify and control who has the authority to access those rooms or cabinets and make sure that the keys you supplied are the only ones that are being used. The best practice is to install electronic access machines to open the doors so that each time someone accesses the room or locker, the activity can be duly monitored.

More on the lines of physical security of your information is the proper implementation of policy control and rules for employees when they are accessing the information physically.

Few Points to remember:

- Every employee should be instructed to return the files to their secure place once they are done with their work with or on them
- Employees must be reminded not to leave confidential documents openly on their desks when they are away from their seats
- Every employee should be strictly instructed to log off their systems, lock their file cabinets and lockers and lock the office doors when they retire for home.
- Proper access controls should be implemented for the workplace
- Employees must know what to do and who to inform in case of an unusual entry of some strange person in your offices or even the building.
- If your business needs to maintain an offsite storage facility, make sure that limited and listed employees are accessing the storage site
- In case of shipping sensitive information via external contractors, make sure that the information doesn't leave your premises unencrypted and unrecorded.

Electronic Security:

Electronic security of your personal information is a bigger domain and requires many other security practices to be taken into serious consideration. These practices involve the implementation of network security, creating and managing strong and hard to crack passwords, restriction on the unnecessary use of laptops and tabs, limitation on wireless and remote access, and the use of firewalls and antivirus solutions.



Implementation of network security:

This kind of security calls for the identification of all the computers and servers where personal and confidential information is saved as well as all those connections to the computers where that information is stored. These connections may extend to Internet, branch office computer systems, service providers' PCs and wireless devices such as cell phones, tabs and scanners.

Now, once the computers and miscellaneous connections have been identified, the next step is to assess the vulnerability of to all kind of network hacking attacks. These attacks may either be foreseeable network attacks or they can appear without even a speck of prior notice.

Now, when it comes to an appropriate network assessment, you can either run an off-the-shelf security software to detect the open vulnerable ports everywhere on your network or hire a professional security auditor to conduct an all-out security audit.

Few points to remember:

- Never store confidential customer information on any computer with internet connection unless it is the need of your business
- Always encrypt sensitive information before sending it to third parties over internet
- Encrypt the information that you store on your computer network, hard drives, portable devices and other storage devices used by your employees.
- Email transmission should also be encrypted within the course of your business if the emails contain sensitive personal information
- Get help from anti-virus and anti-spyware programs and install them on individual computers as well as on servers within your network
- Stay up to date about new alerts for fresh vulnerabilities and take immediate steps to install vendor-approved patches to the weak area of your software.
- Disable those services that are not required by your business so that potential security problems can be prevented duly
- Use SSL (Secure Sockets Layer) or other secure connection to process the transmission of credit card information or any other sensitive information.
- Always keep a look out for potential vulnerabilities in your web applications and keep on patching them

Creating and managing strong and hard to crack passwords

The next most important step in controlling access to sensitive information is the implementation of strong passwords on your user accounts, your personal account, online bank accounts and all types of accounts that contain your sensitive information. In case of a business information security, every employee should be instructed to use a strong password.

It is recommended that the longer the password, the harder it is for others to guess. Hence, employees should be instructed to select a password that is a mix of characters, letters and numbers. Setting a hard-to-guess password doesn't mean that passwords cannot be copied or stolen in anyway- there are multiple ways to make a around these kind of passwords as well. So the next step in ensuring the security of your passwords is the practice of changing them on a frequent basis.

Few points to Remember:

- Use passwords-activated screen savers to automatically lock computers after a certain period of inactivity
- Designated number of log-in attempts should be limited and the user should be locked out who don't enter correct passwords within that limit
- Warn employees to keep a look out for suspicious unidentified calls or web pages attempting to swindle them into handing over their passwords to them.
- Instruct employees not to reveal their passwords to anyone except to the people from higher authorities.
- Make sure that whenever new software is installed, the vendor supplied default password should be immediately changed to a stronger, personal and secure password.
- Employees should be strongly cautioned to avoid sending sensitive information – passwords, credit card or bank account information, or social security numbers via email unless the data is properly and securely encrypted.

Restriction on the unnecessary use of laptops and tabs:

Laptops, net books and tabs, when at one side, are a great advancement of technology dropping the users at complete ease in processing and storing data even when they are not at their homes or offices, they can pose a great threat to the security of the data they are dealing with.

Organization should, therefore, not encourage the use of personal laptops, tabs and net books to work on the information that belongs to the company. If the employees need laptops to perform their jobs, allow them to work on a company provided gadget only.

If the information employees are working with does not need to be stored on their laptops, even if they are company provided, don't store it. When the employee is done working on that information, wipe such information with a program that overwrites data multiple times to make it unrecognizable.

Few Points to remember:

- Do not always allow laptop users to store sensitive company information on their laptops. Consider allowing them to access the information only.
- For safe access, use thumb print, smart cards or other biometrics or passwords.
- In case of allowing the employee to store the sensitive information on his laptop, encrypt the information and configure the encryption in such a way that the user can't change its security setting without the approval from IT staff.

Limitation on wireless and remote access:

When a major portion of work in any organization is carried out on their networks, the need for network security becomes quite apparent. Network sniffing and eavesdropping is the main security issue associated with the use of networks. Wireless networks and remote server are more prone to network sniffing attacks than any other network. Now, to avoid intruders from peering into your networks and sniff at your sensitive information, a devised plan is required by the organizations to secure their wireless networks.

Few points to remember:

- Find out if your employees are using devices like scanners, cell phones and laptops to connect to your wireless networks.
- Determine if they are transmitting sensitive information within or out of the organization using that unprotected wireless network
- Limit the use of wireless network by securing it with Wired Equivalent Privacy (WEP) or Wireless Protected Access key.
- Use encryption on your networks if you allow remote access to your employees or service providers- companies that troubleshoot or update the software that you use.

Use of firewalls and antivirus solutions:

The increasing growth in the use of networked computers in organizations and business, for emailing or transmitting sensitive information over network, has come with so many security issues as well. Many businesses have been struck with major security breaches followed by some bastion of weak defense that failed to prevent unauthorized intrusion into the networks.

Networks are generally vulnerable to a number of attack avenues like Social engineering attack, Denial-of-service attacks, Protocol-based attacks, Host attacks, War dialing and network eavesdropping techniques. Now, what can supposedly be able to put a strong impenetrable defense wall against these attacks is the use of firewalls and strong anti-spyware solutions. A firewall is a software or hardware designed specifically for the purpose of blocking all hacking attempt coming from outside of your computer network. A firewall makes it miserable for the intruders to trace your computer to sniff onto your data.

Few points to remember:

- Use a firewall in your computer networks to protect your computer from hacking attacks while it is connected to the internet.
- Consider installing a 'border' firewall that separates the network from a public network (e.g. Internet) and blocks the intruder from obtaining access to your computers in such network
- Set proper permissions for employees to view across the firewall. By 'access controls', determine who is allowed to access the network and for what purpose
- Frequently or periodically review access control to maintain their effectiveness
- Use additional firewalls on those computers over your network on which sensitive information is being stored periodically.

Employee Awareness and Training:

Even if your data security plan is a master piece and looks awesome while it's still in the planning phase, it meets no success if you don't aware and train your employees for its implementation. Take out time to carry out security awareness program in your employees, hold proper training sessions to develop an understanding with the non-technical staff, present your security plan to them in a way that is comprehensible by all and make them ready to spot potential vulnerabilities and weak ends in your entire network system.



A properly trained employee force is the best security weapon you can use against data theft and information breaches.

Few points to remember:

- Take out time to elaborate rules to your workforce
- Hold periodic training to emphasize the significance of maintain a proper security defense program
- Before hiring any new employee, always check his or her background to ensure that he will not be a threat to your sensitive information
- Prepare an agreement for all employees to abide by company's integrity, confidentiality and security standards for handling sensitive corporate data
- Send regular reminders to your employees to follow company's policies and legal agreements they signed.
- Provide access to sensitive customer information on a 'need to know' basis
- Update them about the discovery of any new risk or vulnerability
- Instruct your workforce to report suspicious activity and reward those who do that
- Always make sure to terminate password and collect cards and keys from those employees who leave your company or are transferred to other branches or departments.

Dump it:

No business, now a days, runs without the involvement of digital information. Tons of data is produced, processed, transmitted and disposed of, frequently or periodically.



Simple deletion of stored information and trashing the bits and bytes from your computer storages does not get it rid of the electronic information actually.

What happens in reality is slightly different. Your computer stores information inside your hard drive in bits and pieces deeper inside it. You cannot practically dig out all the information from your hard drive and eradicate it ,as deleting stuff at this level is much complicated than you can imagine. Even if you try to delete it by going into command prompt and using a whole lot of commands for this purpose, you will still be at a risk of having some remnants of your sensitive information.

Hence, what appears like a whole dismissed trash to you can be a profitable idea for an identity thief. If you leave sensitive personally identifying information in a dumpster, it can be easily recovered by fraudsters and identity thieves with the help of smart data retrieval software or tools.

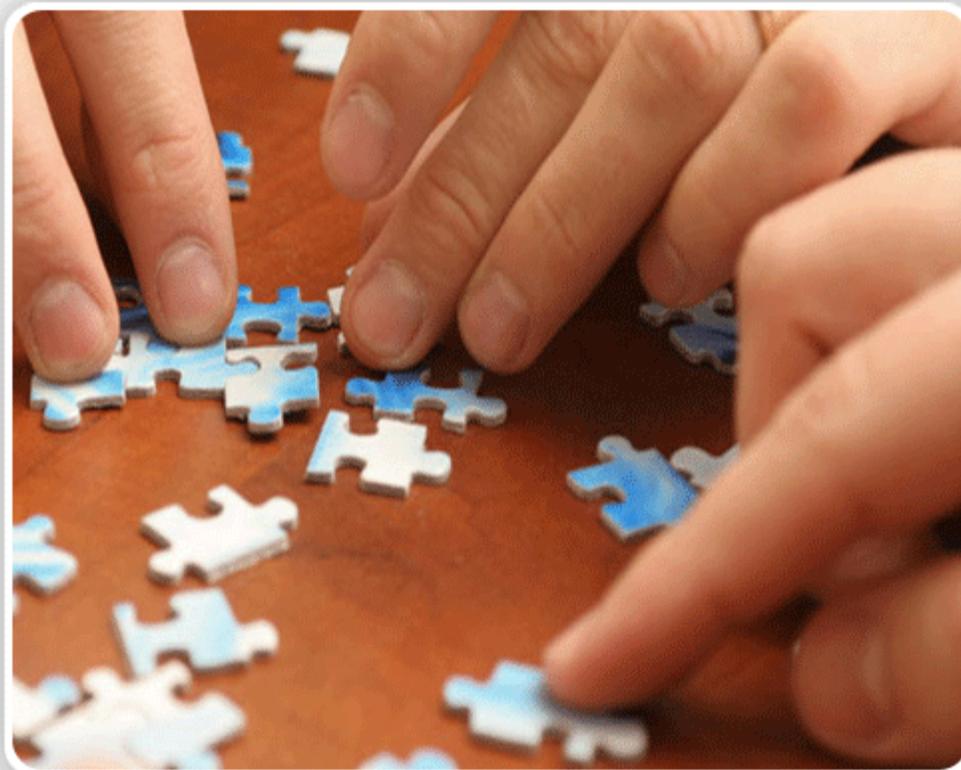
This calls for the implementation of proper company wide data pitching practices. Effective data disposal practice ensures that the information that just got eradicated from your storage cannot be read or reconstructed.

Few points to remember:

- Implement information disposal practices that are effective and appropriate enough to fail the unauthorized use of sensitive trashed information.
- Use effective data and empty space shredding tools to nullify all the attempt of data reconstruction and restoration.
- When you are trashing old computer systems or hard storage drives or devices, use an effective cleaning program to sanitize all the traces of information stored on them.
- For the safe side, consider using a tool that overwrite the empty space of the trashed device or drive multiple times so that not a single spec of information can be recognized by an identity thief.
- Employees who work for you from their homes should also be strongly cautioned to practice the same data disposal activity.

Make a plan:

Although, a sound data security plan is enough to protect the data in your storages and information in your possession, but sometimes data breaches do happen even in the presence of a strong defense system. The impact of such an inevitable breach can, however, be reduced by making a proper plan to respond to events like these. An appropriate response to such an incident is an integral part of the overall security policy and risk mitigation plan.



A senior member of your IT staff should be designated for the sole purpose of coordination and implementation of the response plan. In case of a data breach incident, if some computer is compromised, it should immediately be disconnected from the network. If the network on the whole is invaded, disconnect all systems connected to it. Determine whom to inform in this event both internally and externally. Send a notification to your consumers, law enforcement agencies, customers, credit card service providers, and other service providers or contractors about the data breach that may affect them too.

A successful response plan comprises of:

- Initial assessment process
- Incident reporting to customers and related parties
- Measurement of damages and mitigation of risk
- Identification of the type and seriousness of the breach
- Protection of the evidence.
- Notification to external agencies (e.g. law enforcement agencies)
- Systems recovery
- Compilation and organization of incident report.
- Assessment of incident damage and cost.
- Review of the response and update policies.