By Jen Sharp, jensharp.com

Data Privacy and Protection

Shut the front door. And the back door.

Last year, the U.S. experienced six times as many data breaches as any year before, in what has come to be seen as a pandemic, with nine billion records affected over the past five years.

Only a week into 2017, we learned that personal information of every US voter had been leaked and the Social Security numbers of more than a hundred million Americans were stolen. By the end of 2017, we learned that 53 million Uber drivers and customers had personal data breached, and worse yet, hackers working for the Russian government stole U.S. secrets through the antivirus program on one unwitting man's laptop.

But more importantly overall, we learned that we haven't learned. Despite these hard lessons, businesses and even government entities are still severely lacking in protecting private information.

"That's bad news. Is there any good news?"

Yes. Fortunately, it's not that difficult or costly to make huge strides towards improving security, both on a personal level and an institutional one.

"Sure, it's a problem. But are rural water districts and cities really affected?"

Absolutely. Any entity that collects data is already subject to both legal and ethical considerations, and with the growing number of incidents, regulations are increasing in response. For example, the European Union is mandating increased protection for its citizens, regardless of where the data is collected or stored, worldwide. The initiative is called General Data Protection Regulation (GDPR) and will be enforceable this May, with violators subject to fines, even if they are not in Europe or a part of the EU. There is discussion about how other countries might follow suite. If you aren't thinking about data privacy and protection now, you will be forced to soon.

"Okay, so how can my city or district do better?"

By securing your front door, and your back door so to speak, you can not only comply with what is sure to be coming down the pike, but also make a responsible difference for your customers.

The Front Door

Knowing what information is coming into your system is the first step towards taking action. Answer these 10 questions to gain some insight:

1. What information are you collecting?
2. How do you collect this information?
3. Does any of this information personally identify your customer? (e.g. Date of Birth, Mailing Address, Email address, even a photo)
4. Do customers have a username and password to your system?
5. If so, is your site secured with an SSL?
6. Do you store credit card information onsite?
7. If so, is it encrypted at the database level?
8. And are you PCI compliant?
9. If not, does your payment provider encrypt this information.
10. And are they PCI compliant?

Personally identifiable information used to come on everyone's doorstep in the shape of a phone book. However, today, if a would-be hacker obtains just a few key pieces of information, they're able to gain access to the rest of a person's information due to the networking of data. Storing usernames and passwords adds another level of complexity. Even if you do not collect sensitive data, many people use one password for everything, so chances are, you might even have their password to their bank account. If you do store passwords, make sure they are encrypted. Only store information that you need to know in order to do business, nothing extra. Outsource more complicated tasks that require more security expertise, and make sure your vendor places data security on a high priority.

The Back Door

Getting a clear picture of what you do with the information you have is critical for designing a secure process for handling it. Answer these ten questions to gain more insight:

1. Where do you store your data? Is it in hard copy form or digital?
2. Do you backup your data? Do you store that in house or in the cloud?
3. How many people have access to your data? Can the user access their own information and update it?
4. Do you do a background check for employees?
5. Do employees use their own laptops or smart phones for work?
6. Do you have separate user accounts for your software solutions, or do you share one master password with all employees?
7. Do you have a written policy for data security? Does it include guidelines for posting on social media? Does it include best practices for downloading applications from the internet? Does it include a plan for notifying your customers in case of a security breach?
8. Do your computers have good anti-virus and malware software installed?
9. Do you have a wireless connection? Is it secure using at least the level of WPA2 Encryption?
10. How do you deal with your paper data? Do you keep it in locked cabinets? Do you shred documents that are no longer needed or just toss them in the trash?

Some best practices for protecting data from going out the back door are very easy to implement. Many water districts allow their employees to use personal email addresses to represent the district. However, this gives you no control over the data if they ever leave the system. Creating a "forwarding" email with the domain name of your system, such as "office@myruralwaterdistrictnumber.org" means that you can forward all emails to whatever personal addresses you need, but take off the forwarding when that individual leaves the system. It's easy, and if you already own a domain name (cost of about $15 a year), usually the email forwarding service is free.

Another key yet easy practice involves usernames and passwords. When creating a username, make sure you use the name of your organization, not one of your employee's personal name or information. Creating passwords can be a pain, so many people resort to having just one password for everything. While an obvious no-no, there are free utilities that safely allow you to do just that: StickyPassword, Dashlane, 1Password, FastPassare such examples. Passphrases are also better than passwords. And when someone on staff leaves, change the password!

"So, what should I do first?"

You can start by simply taking inventory of the kind of data you take in. Then take a look at how you deal with the data once you have it, and if you even need that data to do your business. Remember, not only are you legally liable for protecting your customers' privacy and data, you are also ethically responsible. Fortunately, implementing a few key practices can go a long way towards shutting both the front door and the back door on data security breaches.

Since 1997, Jen Sharp (JenSharp.com) has served business and government across Kansas and the US and even internationally, specializing in Web development, design & programming including e-Learning, ecommerce, content management systems, and other small business solutions.