GOVERNOR ERIC J. HOLCOMB'S
INDIANA EXECUTIVE COUNCIL ON CYBERSECURITY
302 West Washington Street, IGC-South, Room E208
Indianapolis, IN 46204

Watson, Jon

"Small business guide to data protection"

Comparitech.com

URL: https://www.comparitech.com/blog/vpn-privacy/small-business-data-protection/

Accessed: 15 October 2019

Synopsis: It's virtually impossible to run any sort of business today without generating or collecting data. Some of that data is critical data that is needed to sustain the life of the business, and some of it will undoubtedly be personal customer data.

To ensure the health of any business, both points need to be addressed. Business data has to be available and plentiful enough to support the activities of the business, but organizations also have an obligation to keep customer data private and secure.

If a business were to lose its own data, it may find itself **unable to carry out operations efficiently** or at all. That is bad enough, but mostly only affects the business itself.

By contrast, if a business were to lose its customers' data, that could **lead to legal action** including government investigations and fines, as well as civil cases and large damaging judgements. Even a company's stock price can be adversely affected after a public data breach. This article deals with both aspects.

Small Business Guide to Data Protection (Updated for 2019)

Jon Watson@lahmstache March 13, 2019

Businesses are liable for securing their own data as well as that of customers. We explain how to protect information from various threats.

It's virtually impossible to run any sort of business today without generating or collecting data. Some of that data is critical data that is needed to sustain the life of the business, and some of it will undoubtedly be personal customer data.

To ensure the health of any business, both points need to be addressed. Business data has to be available and plentiful enough to support the activities of the business, but organizations also have an obligation to keep customer data private and secure.

If a business were to lose its own data, it may find itself **unable to carry out operations efficiently** or at all. That is bad enough, but mostly only affects the business itself.

By contrast, if a business were to lose its customers' data, that could **lead to legal**

action including government investigations and fines, as well as civil cases and large damaging judgements. Even a company's stock price can be adversely affected after a public data breach. This article deals with both aspects.

Principles of protecting data

Data doesn't just appear; it travels. Data is collected somewhere, it is transferred from the collection point to a storage point, it is processed in some way, and it travels to access points as needed by the business. That process can be very complicated or it can be very simple. A simple example is taking an order on an ecommerce website:

1. **Collected**: The website collects personal delivery information and payment information on the checkout page.
2. **Transferred**: That data is transferred to the web server and probably stored in a database on that server.
3. **Processed**: That data may be processed to support ancillary functions such as decrementing the inventory of the items sold, or to generate packing slips.
4. **Accessed**: Order fillers need to view some of that data in order to fulfil the order and prepare it for delivery.

In each step of that process, there are opportunities for unauthorized access or data loss. Continuing with the website ecommerce store as an example, here are some steps to take which can help protect that data.

Protecting data in transit

This type of order data "transits" many times. The first transit is from the customer's' web browser to the ecommerce web server. Contrary to common belief, we do not "visit" a website, rather the website comes to us. Webpages are downloaded to our computers where we interact with them and send data back to the web server.

In this case, in the final step of filling out the shopping cart data, the customer has entered their credit card info **on their own computer** and then it is **transmitted to the web server**. That sensitive credit card information is sent over the internet which is a very unfriendly and dangerous place.

Data in itself is useless; it will usually be transferred many times in its lifetime. Employees in order fulfillment need to know what was ordered, shipping companies need to know the customer's name and address, credit card companies need to know how much to charge the account.

It's unlikely all of this happens in one spot which means this information is sent to a number of places, and in some cases, perhaps to third-party organizations outside of the organization that collected the data in the first place. Each of those transfers needs to be done via a secured method.

Solutions

The most effective way to protect data on this leg of transit is to ensure your website

uses an SSL certificate and that **your site uses the HTTPS protocol**, at least on pages that collect sensitive data.

This step ensures that data in transit between your web server and your customer's browser is encrypted as it crosses the internet. If your customer's sensitive data was intercepted by a bad guy, he would not be able to do much with it because it would be an encrypted blob of gibberish.

If it's not possible to use SSL encryption for some reason, you can **add encryption to almost any data transfer** by using a Virtual Private Network (VPN). There are a number of things to take into account when selecting a small business VPN so it pays to do your research.

Perimeter 81 is SaferVPN's offering dedicated to businesses.

There are other ways to transfer data securely, for example, by **encrypting files before sending**. Encrypted files can safely be sent via email as an attachment, although sensitive data should never be sent in the body of an email or via unencrypted attachments.

Older, offline methods such as faxes should not be discounted. Fax machines hooked up to the Plain Old Telephone Systems (POTS) don't transit the internet in an easily trackable way and provide more security than email. It's important to be sure that a true fax machine is being used on both ends; modern day "email to fax" services or "cloud-based" fax services can be hard to distinguish from proper POTS fax

connections. The disadvantage of the former is that those services use the internet to transfer data which eliminates their privacy advantage.

Securing stored information

Once data has been stored somewhere, it is considered "at rest." Data at rest is stored on some form of disk drive in a database, in individual files such as PDF documents, or in a wide variety of other formats. When considering how to protect your data at rest, the format of the data may be important.

There are two main ways in which data at rest can be maliciously accessed. A bad guy can use legitimate means to access the data such as **stealing a working password** from an employee through phishing.

Or the machine storing the data itself can be attacked and the disk contents copied elsewhere for examination later. It can be hard to pry usernames and passwords out of people; sometimes it is much easier to just steal the entire computer from the front desk while it is unattended.

If data is stored online such as in an ecommerce store, it may be easier to attack another site on the server to gain access to the file system and **copy the database** than try to guess a Magento admin's password.

Sometimes the data breach is a crime of opportunity – there are cases of discarded computers that still contain sensitive data on their hard drives.

Solutions

Data that is not in use should be encrypted until it's needed. This works well for data that doesn't need to be accessed often. It can be harder to manage for data that is accessed by a wide variety of people or systems very frequently.

To protect against access via login credentials, legitimate people accessing the data should **use strong passwords and individual accounts**. Multiple people using the same username and password make it all but impossible to determine how or when the breach occurred. Password managers make it extremely easy to create and retrieve strong passwords, so there's little reason to share passwords anymore.

Sticky Password is just one of the great free password managers available.

Protecting against someone stealing a physical machine or a virtual copy of data involves physical security and access control.

1. **Physical security**: Never leave laptops unattended. Many employees feel that a corporate laptop isn't as important as their own because a corporate laptop will simply be replaced if lost. However, the data on a company laptop may be priceless and, once lost, could put the company's future in jeopardy. Desktop computers should be physically locked to something big. There is a wide variety of computer locks (such as Kensington locks) available for just this purpose. All computer disks, on laptops or other devices, should be encrypted to make it as hard as possible for a bad guy to recover data from it.
2. **Access control**: Where possible, computers that process sensitive data and storage devices should be kept in a restricted area. There should be no non-IT staff with physical access to the file storage servers, for example, so that server should be placed in a locked room. If the general public is on the premise as part of normal business activities, then all unnecessary computers and storage devices should be removed from public view. Thieves can steal entire bank machines by crashing through walls with a front-end loader. How secure is your reception area?

Protecting data from unauthorized access

Unauthorized access refers to an unauthorized person accessing data. This could mean a bad guy that has managed to infiltrate the network, or it could mean a legitimate employee accessing data that they're not entitled to. There are two concepts at work here: authentication and authorization.

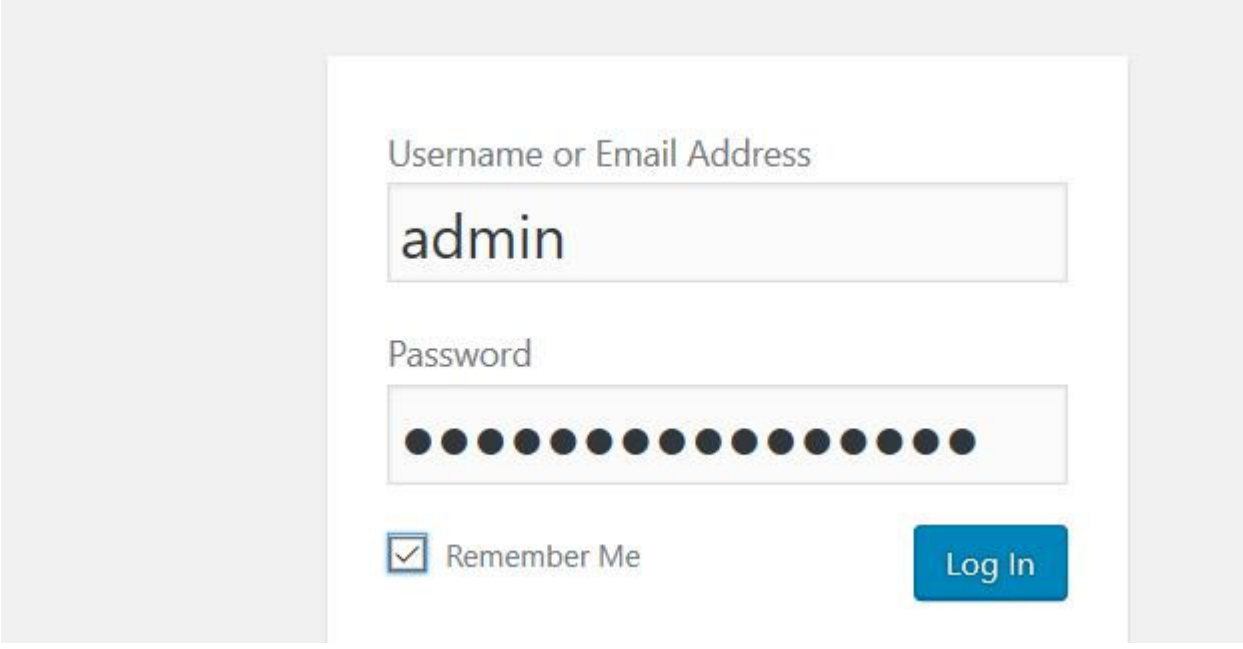
1. **Authentication:** Authentication involves determining the identify of a user, but has nothing to do with what that person is allowed to do. In most cases, a username and password combination is provided to log to a system. The holder of that username and password is a legitimate employee and the system should duly record that the person has logged in.
2. **Authorization:** Authorization takes place after authentication. Authorization determines if an authenticated person is allowed to access a resource. Before determining whether a user can access a resource, the person has to be authenticated to confirm their identify.

Here's an example to illustrate: Nancy logs in to her workstation and is now an authenticated user. She then sends a document to a network printer and it prints because she is authorized to use that printer. Nancy then tries to access the company personnel files and is denied access because she is not authorized to view those files.

Solutions

To ensure authentication and authorization processes are efficient, **every computer system should create audit logs**. Audit logs provide a trail to allow investigators to go back in time and see who logged in to various systems, and what they attempted to do while logged in.

It's also important that no one shares usernames and passwords, as discussed above. If usernames and passwords are shared among employees, there is no way to prevent unauthorized access or find out who accessed what. If everyone uses the same username, everyone is authenticated, and that username has to be authorized to do everything.



Ideally no one should use the username "admin" as it's so easy to guess.

It's inevitable that conversations about access control focus on keeping the bad guys out. However, it is **equally important that the good guys don't get locked out**. If you end up in a situation where systems administrators or other critical

people are locked out, that situation can rapidly deteriorate into everyone being locked out and the business being unable to carry on.

Every critical system should have at least two administrators or one administrator and at least one other person who is competent to perform administrator-level activities if given the correct credentials.

Mitigating the risks of data loss

The impact of data loss can range from "didn't even notice" all the way up to "I've been called to a Congressional hearing to testify." The **loss of critical business data can cripple a business** and cause it irreparable operational harm. In addition, data loss can cause embarrassment, result in damage to a company's reputation, and even drastically affect stock prices for years.

The term "loss" is used in this sense to mean data that has been destroyed, not data that has been breached and disclosed elsewhere. Computers store data in very rudimentary ways using magnetics, semiconductor chips, or laser 'pits,' for the most part. Each of those methods has its bad days and data can be simply become garbled and unrecoverable.

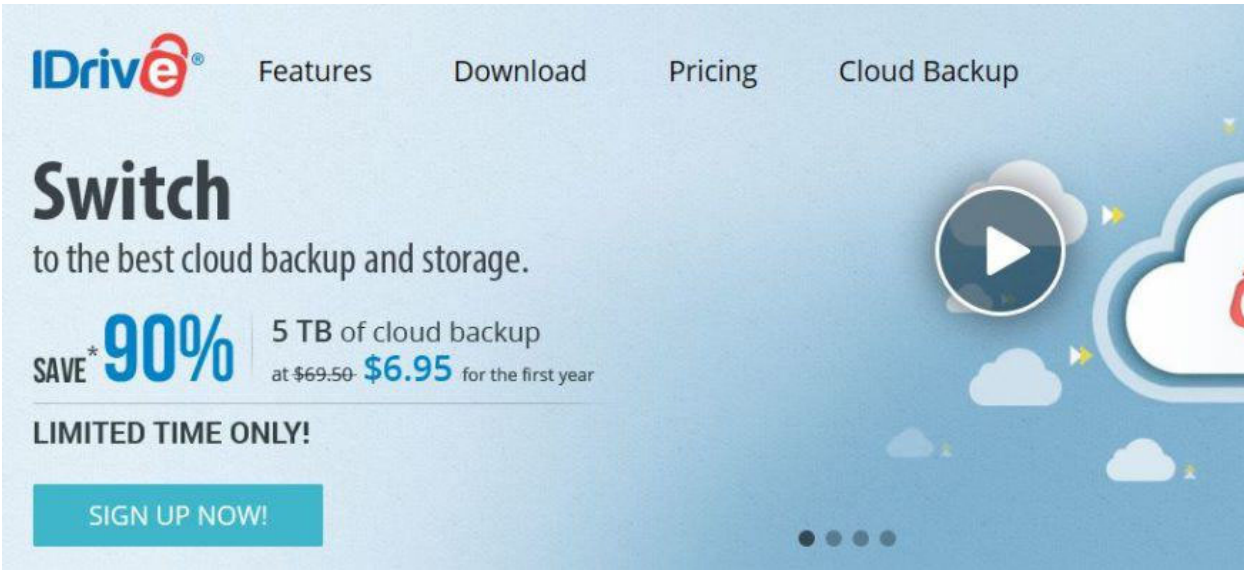
Human error, such as overwriting important files, or accidentally formatting a hard drive can also destroy data forever. Computers are also **not immune from physical disasters** and data has been lost due to fire sprinkler systems flooding offices or electrical surges damaging the drives beyond repair.

In the age of small computing, people lose USB sticks and drop their phones into toilets daily. In a moment of inattention, a single employee can click a malicious link in an email and kick off a world-wide ransomware attack that irreversibly encrypts every single file.

Sometimes nothing at all happens and the disk drive just reaches its end of life and fails. There's literally an unending list of ways data can be destroyed.

Solutions

Accepting that data loss is an inevitable risk, it makes sense to ensure critical data is backed up. Creating a reliable backup plan used to be an arcane art that only experienced systems administrators could pull off. In extreme cases, that may still be true, but these days almost **anyone can purchase offsite backups for a few dollars** per month. There are a few questions you'll want to ask prospective backup companies, and you'll also want to be very sure that your backups will be encrypted.



iDrive is just one of many options for cloud backup and storage,

If your information is particularly sensitive, or your industry regulations don't allow for cloud backups, there are other alternatives.

Backups that are kept on site can be useful for human-error types of situations that require a quick fix, such as restoring a single file. However, onsite backups won't do much for you if the office is flooded, there's a fire, or the backups are stolen.

As such, offsite backups are a critical part of any backup plan and while cloud backup services are the easiest way to achieve this, there's no reason why trusted employees can't take encrypted backups home periodically. Keep in mind that once the data leaves the premises, it still needs to be protected, so **strong encryption is crucial**.

Your industry may also have data retention laws which means you might have to keep old data you no longer use in order to be compliant. The longer data is kept, the more opportunities there are for it to be destroyed. Therefore, long-term retention data is an ideal candidate for offsite storage.

Protecting employee-owned devices

An overarching concern which complicates all aspects of data protection is the proliferation of remote workers, or workers with Bring Your Own Device (BYOD) devices. There can be an advantage to allowing remote work as it opens up the talent pool so the best workers can be hired. It also increases the number of places where company data can be lost or compromised.

BYOD, and remote devices in general, carry a risk of data loss and data leakage. Phones and tablets are small and go with us everywhere, and they are frequently lost or damaged.

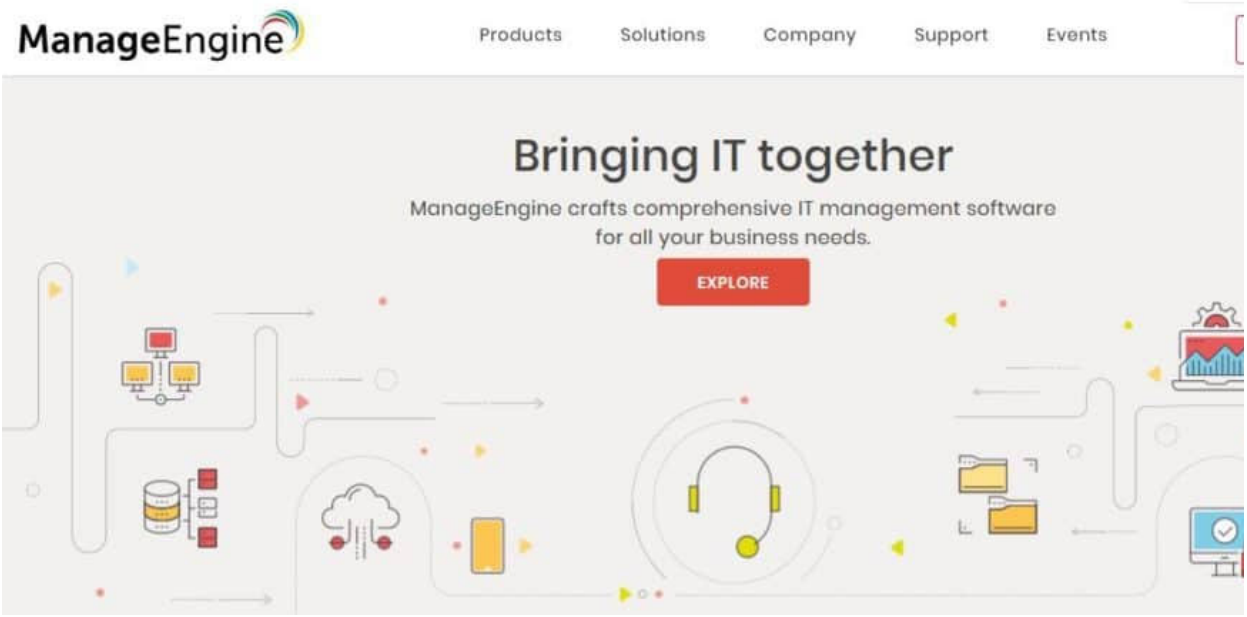
Solutions

Ideally, remote workers will use Virtual Network Computing (VNC) to access their desktops in the office. Even if the remote worker will never attend the office, allowing

access only through **VNC provides for greater control** over what that remote worker can do.

VNC servers can be configured to disallow file transfers, and since VNC does not create an actual network connection like a VPN does, the remote worker's computer is never connected to the work network. This can help prevent the spread of malware into the office network if the remote worker's computer has become infected. Allowing access through a VPN connection will provide easier access to more office resources, but also has the higher risk of infection and data theft, since the remote computer will actually share the office network to some degree.

If you're allowing BYOD, it's a good idea to implement a mobile device management (MDM) system which can do things like **remotely wipe all the data from the phone** and locate the phone if it has gone missing.



ManageEngine Mobile Device Manager Plus is one example of MDM software.

It's also desirable to use an MDM solution that provides for data segregation. Sharing work and personal contacts in the same address book, for example, creates a high risk of data leakage because it is easy to incorrectly select a personal contact as a recipient and accidently send sensitive company information.

Planning for unavailability of data

During the course of business, there may be times when the office is unavailable. Small events such as a fire in the office building may make your office inaccessible for a few days. Large events, such as Hurricane Sandy in 2012, can take underground areas of a building out for years.

The exercise of planning for events like this falls under the concept of Business Continuity Planning (BCP). BCP planning tries to answer the following question: "How would we carry on business if our office/servers/store was unavailable for an

extended period of time?"

Solution

Offsite backups can play a big role in BCP planning. If current offsite backups exist, then it may be possible for employees to work from home or other remote locations using that data to keep things going. Other considerations may include failover phone numbers which can forward to employee cellphones to keep the phones open.

Knowing how to access your data

This may seem like a silly question. Sadly, we can attest from experience that it is not. Many small businesses have relied on a mish-mash of third parties to look after their data over the years and in some cases have no idea where any of it is actually stored. Part of any proper data loss prevention plan is knowing where your data is to begin with.

Consider our simple ecommerce website again. At a bare minimum, it has the following:

1. **Registrar account**: A domain registrar is a company that sells domain names. Your domain's nameservers are controlled by your domain registrar. Name servers are a critical control element of your website so you should know who that is and have the account credentials.
2. **Hosting account**: Your website files physically reside on a web server somewhere in the world. The company that provides that service to you is your web host. Ensure you know who your web host is and that you have the account credentials.
3. **Email account**: Your web host may not also be your email host. Many companies use third-party email providers such as Google. Ensure you know where your email is and that you have the account credentials.
4. **Backups**: If you already have backups setup, where do they go? If you don't have access to them and know how to restore files, those backups aren't doing you much good.

The same types of questions should be asked about all of your data systems until you have a fairly good understanding of where all your data is. Trying to find this information in an emergency is the worst time.

Aside from the practical need to know these things, your industry may also regulate the geographical regions where you are allowed to store data.

Customer data considerations by country

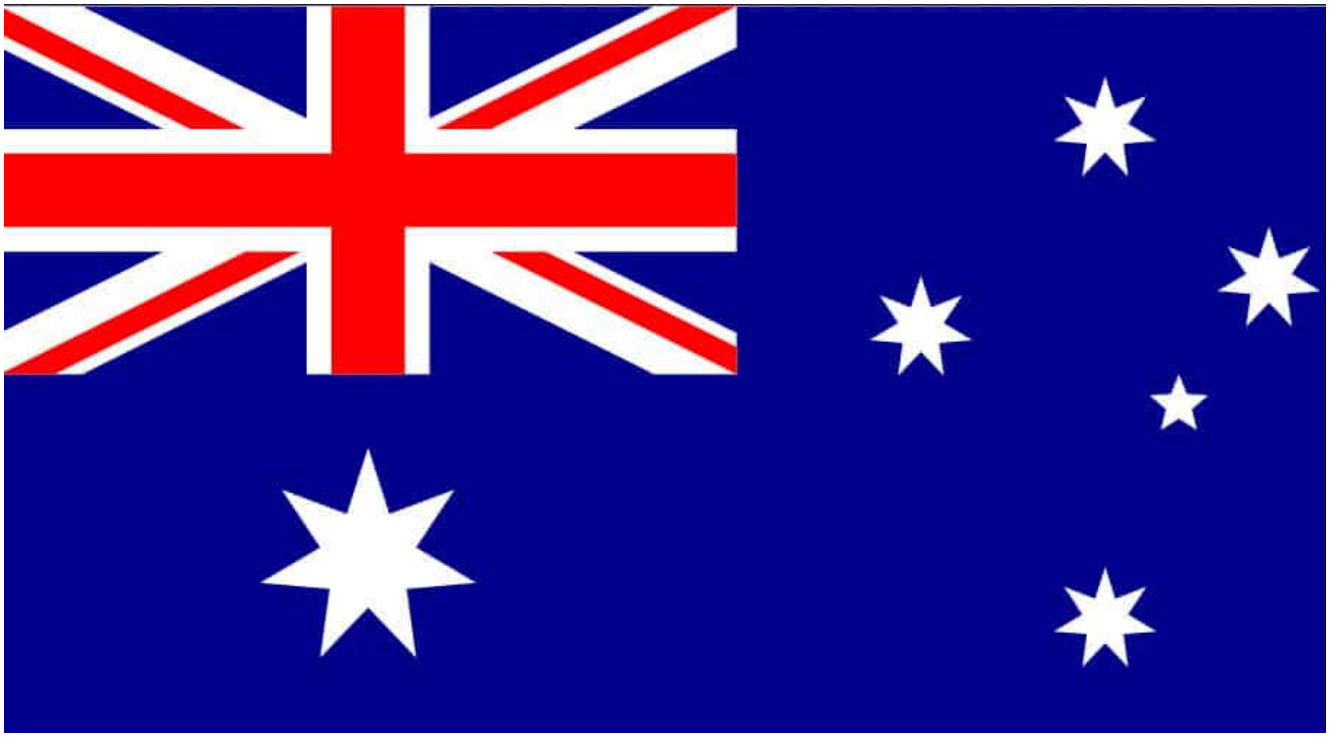
Customer data usually needs special consideration. It's one thing to lose your internal spreadsheets. Legally, it's quite a different thing for your customer data to be stolen or used inappropriately. Over 80 countries have some sort of privacy legislation that applies to businesses that collect customer data. The fundamental

obligations of most of these acts boil down to these points:

1. Obtain permission to collect customer data before doing so.
2. Collect as little information as possible.
3. Use data in the way you have permission for.
4. Safeguard information against unauthorized access.
5. Make data available to your customers.

Here is a very quick overview of the general state of privacy legislation in the US, UK, Canada, and Australia. It gives some clues as to what type of protection organizations are expected to provide for customer data, as well as a sense of the penalties for violations.

Australia



Much like Canada and the UK, Australia has a federal privacy act aptly named the *Privacy Act*. It was first passed in 1988 and has been amended and expanded since then. The act is based on the concept of 13 Australian Privacy Principles.

Legislation

The *Privacy Act* initially only covered the handling of private information by government agencies and government contractors. It has since been extended to also cover private sector businesses.

All Australian businesses with total sales of over 3,000,000 AUD have obligations under the privacy act. A small list of businesses such as health-related and financial businesses are also subject to the act regardless of total sales.

Giving customers their information

Principle 12 of the *Privacy Act* deals with "Access to, and correction of, personal information." With few exceptions, a person's request for their personal information must be provided, but there is no stated deadline in which to do so. Agency requests must be handled within 30 days, but if the requestor is a person then the only requirement is to "give access to the information in the manner requested by the individual, if it is reasonable and practicable to do so."

Penalties

There are different penalties for violating the *Privacy Act*, depending on how grievous the breach is. Monetary values for breaches are not stated in the Privacy Act. Rather, violations are assigned a number of penalty units based on the severity of the offence. Serious violations are assigned 2,000 penalty units whereas less severe offences are assigned as few as 120 penalty units.

Section 4AA of the Australian *Crimes Act* dictates the value of a penalty unit in Australian dollars and is updated from time to time. Currently, a single penalty unit is 210 AUD (subject to indexing) which means severe offences can be in the 420,000 AUD range. In reality, the courts in Australia sometimes only require an apology.

Canada

Legislation

Canada's Federal data protection rules for businesses are contained in the Personal Information Protection and Electronic Documents Act (PIPEDA). Some provinces such as Alberta, British Columbia and Quebec have their own provincial data protection acts which are similar enough that PIPEDA does not apply to businesses in those provinces. Therefore, depending on what province you're doing business in, you will need to be familiar with PIPEDA or one of the following provincial legislative

acts:

- Alberta: *Personal Information Protection Act*
- British Columbia: *Personal Information Protection Act*
- Quebec: *An Act Respecting the Protection of Personal Information in the Private Sector*

In addition, Canada has a separate *Privacy Act* which controls how the Federal Government is to handle personal information within government agencies.

PIPEDA requires organizations to gain consent before collecting personal information. However, it is interesting to note that PIPEDA does not apply to individuals who collect personal data for personal use, or organizations that collect personal information for journalistic use.

The Office of the Privacy Commissioner in Canada maintains an overview of the various Canadian federal and provincial privacy acts.

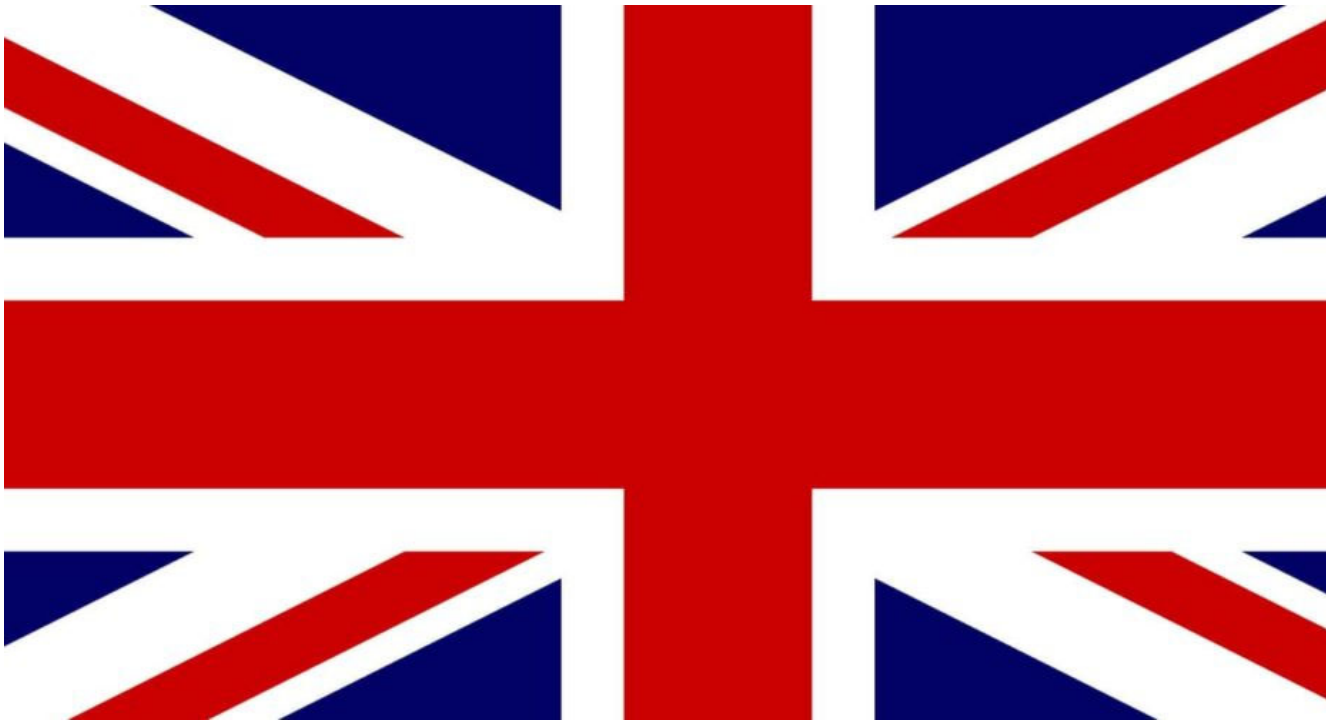
Giving customers their information

Information held by federal agencies can be requested by filling out an information request form. To request personal information held by another type of organization, contact that organization. The provincial or territorial ombudsman office can help.

Penalties

PIPEDA violators can face fines up to $100,000 *per violation* for knowingly violating the act.

United Kingdom



Legislation

The United Kingdom's Federal protection act is the aptly named *Data Protection Act*. Unlike Canada, the UK Data Protection Act applies across the board to business and government alike.

Giving customers their information

UK citizens have the right to find out what information an organization has about them. Not all information has to be released though. Data that does not have to be released includes information about:

- information about criminal investigations
- military records
- tax matters, or
- judicial and ministerial appointments

Organizations can also charge money to provide this information to people. The UK Information Commissioner's Office website can provide advice and guidance, as well as investigate data handling complaints.

Penalties

The UK Data Protection Act provides for fines up to GBP 500,000 and even prosecution for violations.

United States

The United States is somewhat unique in that it has less federal-level privacy legislation than most other countries. Instead, most privacy acts in the US are industry or state-based. It can therefore be hard to discover the laws that may apply to any specific business. A good place to start is the US Federal Trade Commission's Privacy and Security page.

Legislation

The United States' *Privacy Act of 1974* controls how information can be collected, used, and disclosed by Federal agencies. In part, it states:

> No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains.

The act then lists several exceptions to this directive. Some of them, such as the exemption for "routine use" may seem a little broad in the 21st century.

The bulk of US privacy laws are related to industries or generated at the state level. Therefore, it's important for an organization to assess which states it will be considered operating within, and also if there are any industry-specific privacy regulations which apply at any government level.

Some big Federal US privacy acts are:

- Health Insurance Portability and Accountability Act (HIPPA): this act pertains to the administration of health care in the US.
- Children's Online Privacy Protection Act (COPPA): this act deals with online collection of data on children under 13 in the US.
- Fair and Accurate Credit Transactions (FACTA): this act deals with the obligation of credit bureaus to provide credit information and fraud-prevention tools to US citizens.

Giving customers their information

The US Privacy Act dictates that individuals have the right to obtain the information that federal organizations have about them. To make a request, people would contact the applicable agency. For private businesses, the requirement for an organization to provide records to individuals would rely on the existence of legislation applicable to that industry or state. Again, the best place to start is probably going to be the United States Federal Trade Commission website.

Penalties

The federal Privacy Act contains penalties, but since the Privacy Act is only applicable to the US federal government that is not the case for other organizations. The penalties for privacy violations in the US will depend on which act was violated and what penalties are contained therein.

The rate at which data losses and breaches have occurred over the past few years is

alarming. Most of those breaches are possible because organizations are simply not expecting it. Ransomware attacks on a global scale succeed because employees *still* click malicious links in emails. Businesses lose their online ordering capability for days, instead of hours, because they don't know who to contact when their website goes down. All of this can be very neatly mitigated with encryption, backups, and some system knowledge.

Image credit: "Internet Cyber" by Gerd Altmann licensed under CC BY 2.0

PRIVACY ALERT: Websites you visit can find out who you are

The following information is available to any site you visit:

Your IP Address: **108.59.55.247**

Your Location: **Indianapolis, IN**

Your Internet Provider: **Indiana Office of Technology**

This information can be used to target ads and monitor your internet usage.

Using a VPN will hide these details and protect your privacy.

We recommend using ExpressVPN - #1 of 84 VPNs in our tests. It offers outstanding privacy features and is currently available with three months extra free.

Visit Express VPN