
Keeping your
data safe
AVG Business

Data is the key

Data fuels the modern world, informs and reflects our economies, and shapes our lives. Data is also the lifeblood of small business, of large corporates, of governments and of individuals too. When data flows quickly and easily from place to place, person to person, business to business, things get done. When it doesn't, the ship begins to creak. When that flow stops completely, the ship begins to sink.
That's why protecting it is a top priority.

Introduction

From tax returns to passwords, from credit card details to customer email addresses, businesses all over the world use data to conduct their affairs and get things done. That is precisely why it is vital to ensure that high security measures are in place in your business.

Joanna Brace is Vice President of Marketing & Product Marketing, AVG Business. Her track record spans brand-building, product development and marketing strategy. She joined AVG from Skype.

Creating, storing and managing data isn't new; it's been around for thousands of years. Ever since we've had the ability to mark a notch on a piece of wood, data has existed. What has changed is the volume and type of data we capture, what we use it for, and how we collect, store and share it. This has major implications for security and privacy which is why it is an aspect of data that, in my role, I take a great personal interest in.

Another difference to business life now compared to just twenty years ago is that some businesses only exist because of the data. Finding original ways to harness data to the needs and desires of specific audiences is the prime means to get a low cost-based business up and running in the internet age. Smart businesses further on in their development know how important data is for marketing, CRM and financial reporting as they continue to grow. Quite simply, data is driving the commercial world we live in.

As business becomes ever more dependent on data, it's inevitable that protecting it must be a critical priority, from the moment it's collected to the moment it's securely erased. It's the data that holds the key to understanding your business's past, present and its future growth. We underestimate its importance at our peril.

Collect, protect

Contemporary businesses rely on a wide variety of data types. How these businesses manage the collection and protection of that data is crucial to ensuring customer satisfaction.

Your business gathers and uses data which relates to its core activities: production, marketing, sales, fulfilment and invoicing. Knowing which data types play the biggest role in the operation and success of your business is vital. Knowing how to adequately protect those data types is even more so.

For example, when you want to create a new product, you'll need a specification so you can produce it. When you want to call a potential customer or send them an email alerting them to your new product, you'll need a name, telephone number, or email address so you can market what you've produced. When you want to take an order, you'll need to collect payment card details to process the transaction and an address to send out an invoice for it. Finally, when you want to deliver the goods, you'll need times, dates, a courier, as well as an address to fulfil the order.

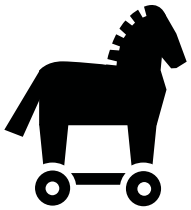
Here there are already multiple forms of data coming into play. Integrating protective measures is essential from the outset, reinforcing the data management process and adding ballast at the point of data release. For example, you can protect the accuracy of your data as it's being collected through your website contact form. Ask the user filling out the form to read a blurry image of words or numbers (also known as a CAPTCHA code) and add those characters into the form i.e. something only a human could do and not a spambot.

Following that with the deployment of a secure database, encryption and password protected access, ensures multiple layers of protection.

Without that data, your business can't do business!

Danger areas

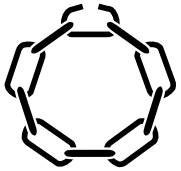
Knowing what the particular danger areas are regarding your data, and at what point during the management process your data is most at risk, will enable you to understand how it can be compromised and how to protect it. Here are some of the more common threats.



Malware
These programs can disrupt operations, gather data or access private systems. It can be installed by downloading email attachments or when running new software that has been downloaded so be wary of less reputable sites.

Social Engineering
Where hackers tactics to infiltrate or gain the confidence of your employees and then mine them for passwords or data. It is a form of confidence trick and can be used to fool a business into disclosing sensitive customer data.

Device Theft
Whether caused by a disgruntled employee, an employee leaving their device in a public place or a break in, device theft is still an easily preventable breach.



Weak Networks
Insecure networks - those with weak passwords, out of date antivirus software, or lacking a firewall - are much more easily hacked.

The Insider Threat/Frenemy
A threat from people within your business - this could come from current or former employees who have information concerning security practices, data and computer systems.

Hacking
Any website or intranet can be hacked by people on the inside and outside (the largest threat). Depending on their specific goal and motives, hackers may want to corrupt, misuse or sell the data they steal.

What it's worth

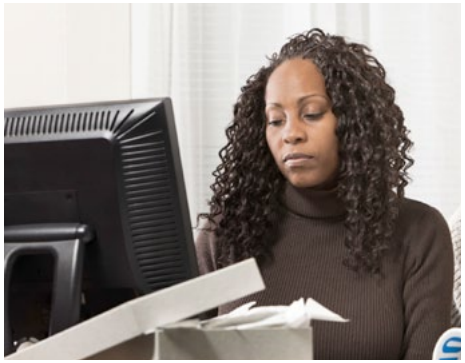
You won't be able to send out an order if your customer database crashes, contains inaccurate information, is hacked or stolen. And how costly could that be for your business?

The simple loss of one order can resonate through your business. Consider the various consequences: The extra resource required to complete the missing order; the investigative resource required to right the wrong and ensure the problem does not repeat; then there's the more chilling loss of customer confidence to bear in mind.

By the time you have factored in those things, the cost can easily multiply way beyond the value of one order. That's why protecting your business data isn't just about protecting one device or one database, it's about protecting the ability to deliver a service or product to your customer. What value would you place on that?

There are other important reasons to protect your data too. In the US businesses have to comply with a variety of State and Federal laws and regulations; in the UK, companies have to comply with the Data Protection Act.

Economic regions also have their own requirements that member and non-member states need to be aware of such as the EU's Data Protection Directive. Failure to manage your customers' data in accordance with these laws can result in fines, litigation, and even criminal convictions; failure to comply might also affect the ability to deliver a service or product to your customer.

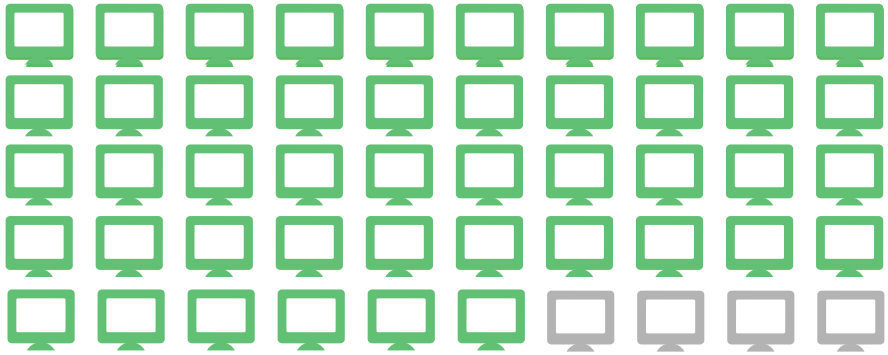


There are legal, as well as operational, reasons to protect your data.

To help your business protect its data, it can follow the guidelines set out in ISO / IEC 27002, the international standard for information security. Alternatively, it could even achieve formal compliance.

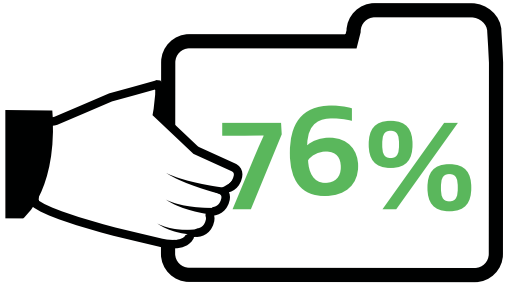
Data studies

The story of data breaches in numbers*



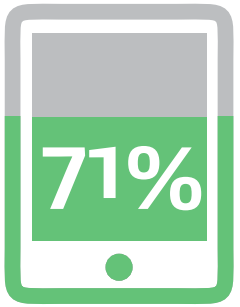
92% of breaches were perpetrated by outsiders

of breaches resulted from privilege misuse and abuse



of network intrusions exploited weak or stolen credentials

of breaches are considered to be opportunistic attacks



of breaches targeted user devices

*http://www.verizonenterprise.com/DBIR/2013

What if?

Ostriches don't make good business leaders. Burying your head in the ground is not the way to fully appreciate risks and potential outcomes. Understanding how your business might be affected if the worst were to happen can help you decide what data to protect, where it needs protecting and how to do so.

How secure is your business? Click on the image above to use our SMB health check (see back page for full URL).

If your data becomes lost, corrupted, misused or point-blank stolen, the impact will likely be felt in at least one of three areas of your business:

- **Your finances**
- **Your operations**
- **Your reputation**

Financial loss is always harmful whether as a result of having to pay out to repair a compromised system, compensate customers, or to pay fines to the relevant authorities if you are found to be in breach of legislation. It will have a detrimental and unforeseen effect on your revenue and cash flow.

Any loss in operational capacity could be significant because not having the right data at the right time in the right format may prevent orders being taken or fulfilled. Paralysis or inactivity is no good for the heartbeat of any small business.

Any loss in customer trust could also hamper your future success and the reputation of your brand or business. Your customers may reasonably think that, if you were hacked once, why couldn't it happen again? Confidence in your brand or business can drain faster than the battery of your smartphone when you are in emergency mode. Social media and the many ways to share information can exacerbate the problem.

In reality the likelihood of suffering a breach is determined by how desirable your data is and how weak your means of security are. Have you really fully considered the true extent of damage to your customer relationships and business status that a data breach or data loss might invoke?

Strategy

So what can you do? How can you protect your data without it costing your business the earth? Putting a cost-effective strategy in place can save you in many ways further down the line.

The first step in creating a strategy is to truly understand what is meant by data protection. Think of it in terms of the CIA acronym: Confidentiality, Integrity and Availability.

This means your data needs to be kept confidential; it should only be available to the people with the relevant privileges. Your data should maintain its integrity and be in the format the user requires it to be (and not to have been materially altered by the system capturing, storing or transmitting it). Finally, your data should be available whenever the person with those relevant privileges is requesting it.

The second step is to undertake a strategic review. Ask yourself: Where is your data coming from? Where is it going? How is it being transported there? Then ask yourself: What security measures have you got in place to protect the data at each stage of its journey?

The answers to those questions will define the landscape in which your data operates and will therefore clarify the nature of the threats and risks it will face. Once mapped, you can allocate the relevant security measures against the specific risks and threats you have identified. This may include a mixture of technical expertise or tools purchase, redesigning your security protocols or a wholesale change in your business's attitude towards data security.

Where is your data coming from, where is it going and how is it being transported there?

Data security must be discussed and supported at every level within your business. The importance of every staff member with regard to data security should be consistently underlined.

Protective steps

There are plenty of good security measures all businesses can apply today that will help prevent or reduce the chances of data loss, breach or theft. These tools and solutions come in many shapes and sizes.

Putting the basics in place

- Use strong passwords
- Install firewalls
- Install antivirus
- Install encryption software

Staff awareness

- Impress the importance of staff caution
- Educate staff on the dangers of using public areas to access data
- Highlight the responsibility of every staff member

Starters and leavers process

- Identify the specific data, devices and access privileges new starters need
- Adopt a controlled exit policy for leavers
- Review returned devices, wipe or securely destroy data where necessary

Maintenance, upgrades and planning

- Back up your data
- Scan network and devices frequently for necessary upgrades
- Change passwords regularly
- Create an Emergency Response Plan in case of theft, breach or loss

After the event

If your business's data is compromised, you'll need to act swiftly, understand what's happened, repair the damage, and prevent the problem from happening again.

Having a pre-prepared plan will help you act quickly, effectively and with confidence in the case of a breach, theft or loss. It may sound dramatic but being prepared for the worst case scenario, and thinking through those consequences, will put you in a great position should a breach, theft or loss occur.

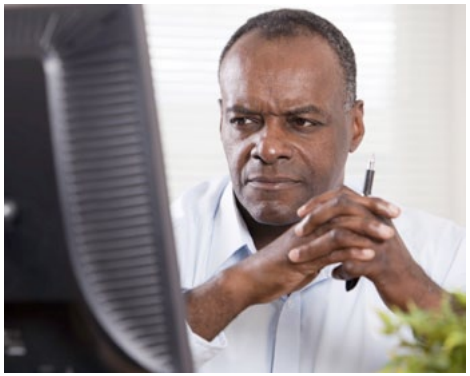
Depending on the gravity of the incident, it may be better to call in the police and let the experts investigate and resolve it. In the case of theft this is obviously the appropriate response.

However, it is far more common for businesses to react and cope with the consequences of breaches and losses themselves. So, what steps can businesses take directly?

If the incident concerns data held on a mobile device you may need to consider whether or not you can (or should) wipe or disable the device remotely. A step such as this might provoke staff disapproval - especially if the device is the property of an employee - so a Bring Your Own Device policy is always recommended.

Remember to always plan in advance. Back up your data. If remote wiping or disabling isn't possible, you risk wiping personal and company data or you simply cannot access the data any more, your backed up data can be restored to a certain point.

And while a simple back-up might not be the ideal solution, because it will inevitably involve some gaps, it will go some way to putting you back in the position you were in prior to the breach or theft. Don't underestimate its importance.



Remember to always plan in advance. Back up your data.

*Tips on implementing a Bring Your Own Device policy: http://blogs.avg.com/business/coping-byod/

Safety first

It’s not difficult to see why your business data is so valuable. Without it you can’t do business. That’s why you need to protect it. Even simple measures can help; a strong password being the most relevant, quickest and easiest to apply and completely free too!

Take security issues seriously and get protected...now!

Learn more about internet security at www.avg.com/business-security
*** Small Business IT Security Health Check**
www.avg.com/small-business-it-security-healthcheck