Small Business Security Guides

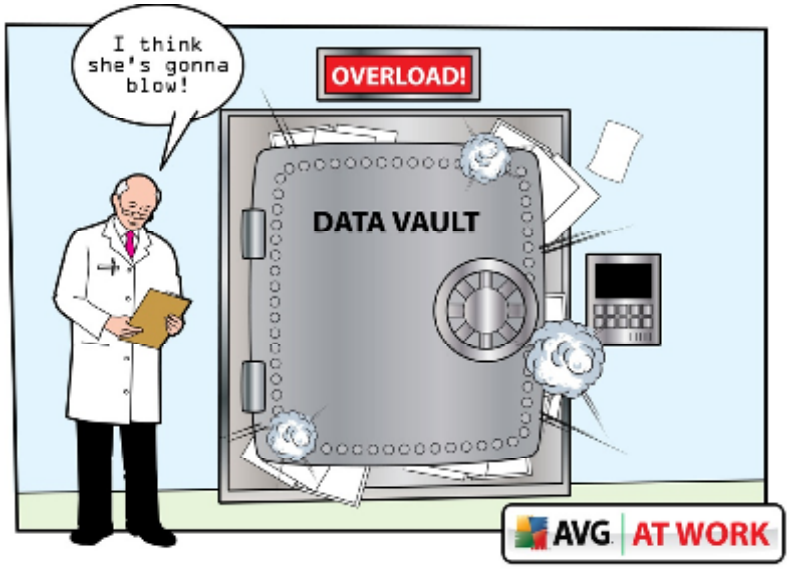
Customers, employees & businesses: who suffers as a result of a data breach?

AVG | AT WORK

Customers, employees & businesses: who suffers as a result of a data breach?

Protecting data on your own computer is relatively straightforward but what about information that connects to your business, which is out of your IT department's control?

Did You Know:
- Companies can be fined up to £500,000 for failing to safeguard customer data
- Only 28 percent of companies in a recent survey had formal policies on Internet security in place
- 330 million records containing sensitive personal information have been involved in data security breaches since 2005



Updating anti-virus protection, keeping up with security patches and assuming that any online link that looks questionable is bad news are just some of the ways that average PC users should take to keep themselves secure. But what risks exist to the data that is out of our central control? A whole range of public and private sector companies hold confidential information on various elements of our business, which we trust them to keep safe. Unfortunately sometimes that trust is misplaced.

Incidents when data is lost or stolen from a company are known as data breaches and they are on the increase. A recent study from the United States National Cyber Security Alliance revealed that 65 percent of small businesses surveyed hold customer data, while 33 percent admitted to storing credit card information. Despite admitting that the Internet was critical to their operations, only 28 percent of the companies surveyed said they had formal policies on Internet security in place. More concerning, only 35 percent said they provided any kind of training on Internet safety and security to their staff and only 14 percent said they had anyone solely focused on IT security within the company.

The size and shape of the typical company most likely to be hit by a data breach is easy to define in some ways i.e. it is all businesses. From sole traders and two-man partnerships to government departments and big corporations, the hackers who perpetrate the intrusions that lead to a data breach are not fussy. They don't discriminate among their targets and here's why. A small business may have a good deal of valuable corporate data that cyber-criminals will want to "scrape", yet only have a relatively weak and porous data security layer in place protecting it.

The UK's Revenue and Customs Department (HMRC) was subject to one of the most infamous data breach incidents in recent history when records relating to around 25 million individuals were exposed after two CDs went missing. The subsequent fall-out resulted in a legal inquiry into data practices at HMRC and across the government sector and in a positive result for consumers: more powers for the UK's Information Commissioner and the Data Protection Act which he regulates and enforces.

The Information Commissioner's Office (ICO) was recently granted the power to fine companies up to £500,000 if they were found to have been negligent when it comes to looking after data. "Getting data protection right has never been more important than it is today," says Information Commissioner, Christopher Graham. "As citizens, increasingly we are asked to complete transactions online, with the state, banks and other organisations using huge databases to store our personal details. When things go wrong, a security breach can cause real harm and great distress to thousands of people."

The ICO advises that UK businesses and consumers should directly approach any company that they feel has lax data controls or worse, has suffered a data breach. If that initial approach fails to result in action, the ICO can then intervene on the business or consumer's behalf. "If necessary, we will look into the complaint. If we think the law has been broken, we can give the organisation advice and ask it to solve the problem. In the most serious cases we can order it to do so," the ICO explains. However the organisation has no powers to award any kind of compensation directly.

The United States is similarly tightening up legislation to regulate companies that are careless with information. Lawmakers recently introduced two new bills designed to compel companies to be upfront about data breaches - the Personal Data Privacy and Security Act of 2009 (S.1490) and the Data Breach Notification Act (S.139). An enforcement body has also been set up which is known as the Office of Federal Identity Protection part of the Federal Trade Commission. The lawmakers were motivated to tighten up data protection efforts given that some experts estimate that 330 million records containing sensitive personal information have been involved in data security breaches since 2005.

The US Cyber Security Alliance's StaySafeOnline campaign has a stern warning for companies that don't take security of their customer's information seriously. "Your customers are your business. You would never knowingly put them at risk, but lax computer security practices can do just that" the organisation states. "As we've seen in recent high-profile data breaches, customers don't take kindly to having their information lost, stolen or compromised. Protecting your customers' sensitive data is both good policy and good business."

The message here is that corporate data is as much a part of a company's assets as is its intellectual property, its staff and skills base and its fixed cost assets from the carpets to the

photocopier – and it must be treated as such. Failure to realise the gravity of this core tenet of modern business is tantamount to flagrantly posting the entirety of the corporate database on the company's homepage. Businesses have a commercial responsibility to close to the door to the data centre, keep it locked and ensure that policies exist to govern who the key holders are.

StaySafeOnline advises companies to make sure they have policies in place when it comes to protecting customer data but also advocates a range of measures similar to those that home users should follow when it comes to securing their own information. "Keeping your customers safe requires that your own computer systems are fully protected," the organisation advises. "The best policies in the world won't protect your customers if your network and resources are at risk of attack or preventable failures."

While it's good to stay abreast of what government is doing to make sure companies look after your data, one of the more obvious questions is how do you know if a business which holds information on your company has been breached? According to the US Computer Emergency Readiness Team (CERT) there are some tell-tale signs to look out for:

- unusual or unexplainable charges on bills
- phone calls or bills for accounts, products, or services that you do not have
- failure to receive regular bills or mail
- new, strange accounts appearing on invoices
- unexpected denial of corporate credit cards

Based on those clues, if US businesses suspect that their details might have been exposed by a security attack on the company they should, as in the UK example, contact the company in question initially by phone and letter if necessary. Contacting the main credit reporting companies - Equifax, Experian and TransUnion- is also a smart move, as is filing a report with the local police so there is an official record of the incident.

It's also important to consider if a breach in one organisation could have an impact on other confidential information. CERT advises that if for example, a thief has access to an employee's Social Security number, then the company should contact the Social Security Administration. The personnel department or the employee themselves should also contact the Department of Motor Vehicles if any driver's license or car registrations have been stolen.

There are many organisations and agencies that can help if you think your employee's data or your own corporate data has not been properly safeguarded but, as with many things, prevention is often more effective than a cure. So when it comes to many channels via which data breaches can target both you and your customers, the best approach is to only share information when you have to and only with companies you trust. If you can standardise this within your company's core operational procedures and ensure that this ethos is carried downwards into the entire staff base, then you will be taking the safest possible corporate steps on the road ahead.

So to finish, let's return to our first question - customers, employees & stakeholders: who suffers as a result of a data breach? The answer should be clear at this stage. Quite simply everybody suffers from hacks that lead to data leakages. Operationally, the business suffers directly from a potential loss of trading profits, so corporate and individual stakeholders are worse off. Employees are compromised and customers lose faith in the company's ability to function at a level even vaguely resembling best practice. It's a vicious circle and a downward spiral, but the shame of it is that it is all so preventable. We urge you to lock your data down now.


AVG SMB group at:
bit.ly/avglinkedin


Become an AVG Fan at:
facebook.com/avgfree


Read our blogs at:
blogs.avg.com


Follow us at:
twitter.com/
officialAVGnews


Become an AVG
affiliate at:
avg.com/affiliate

Watch our Channel at:
youtube.com/officialAVG

AVG Technologies CZ, s.r.o.
Lidická 31, 602 00 Brno
Czech Republic
www.avg.cz

AVG Technologies USA, Inc.
1 Executive Drive, 3rd Floor
Chelmsford, MA 01824
USA
www.avg.com

AVG Technologies UK, Ltd.
Glenholm Park, Brunel Drive
Newark, Nottinghamshire,
NG24 2EG
United Kingdom
www.avg.co.uk

AVG Technologies GER GmbH
Bernhard-Wicki-Str. 7
80636 München
Deutschland
www.avg.de

AVG Technologies CY Ltd.
Arch. Makariou III.
2-4 Capital Centre
1505, Nicosia, Cyprus
Fax: +357 224 100 33
www.avg.com