Top security tips to safeguard privacy

—How to avoid being headline news for the wrong reasons!

The 'Perfect Storm'

Recently, privacy breaches have been very much in the news. Although breach notification laws in many jurisdictions are prompting companies to disclose breaches more promptly than in the past, there are also many more incidents occurring.

Several factors have combined to create this 'perfect storm'. Criminals have discovered it is highly profitable to harvest and use personal information to commit financial fraud and identity theft, so the number and sophistication of attacks is on the increase.

Many enterprises have gone beyond having just an online brochure and now have a web presence which involves interaction with customers. Web applications are too often deployed without adequate safeguards, thus exposing their systems to web attacks.

Motive and opportunity thus combine to create the conditions for data breaches which can result in fraud or identity theft for individuals, and in fines, lawsuits, reputational damage and loss of customer trust for businesses.

Puddle phishing

But perhaps you think that because you're smaller, criminals won't bother with you. Bad news! In a phenomenon quaintly known as 'puddle phishing', criminals are increasingly focusing their attention on smaller companies because they are a 'softer target' than the big banks and retailers. According to Visa, since 2005 small businesses represent less than 5% of exposed accounts but have been the source of 80% of identified data security compromises.

Through the minefield

The Data Protection Act requires that customer data be "safeguarded against unauthorised or unlawful processing and accidental loss or destruction or damage."

Recent high-profile breaches at HMRC and other organisations have provided the Information Commissioner with a receptive audience for his proposals to get much tougher on companies which are careless with their customer's information. Jail terms for directors have been suggested!

What can responsible businesses do to comply with the law and protect their customers' privacy? Following are some practical suggestions to help you through the minefield.

Why collect it?

Don't collect data you don't really need for business or store it for any longer than necessary. Challenge the business rationale for all customer or prospect information collected.

For example, holding credit card details on your website for the 'convenience' of customers exposes sensitive financial data to criminals. Why should they bother with dumpster diving when they can just hack into your database?

Practice safe surfing

Ensure you have up to date internet security software on all PCs and laptops and automated processes for keeping it up to date. Even web surfing on what appear to be innocuous or recognised sites can expose users to malware, which may also be hidden in Word and Excel documents, Adobe PDFs, pictures or zipped files.

As operating systems tighten up their security, criminals increasingly are targeting vulnerabilities in browsers, in office software, in media players and in other desktop applications. To help prevent users computers being compromised via malicious web pages or other client-targeting attacks, don't allow users administrative privileges to install software.

Lock up your data

Encrypt laptops which contain sensitive data. Don't forget PDAs, smart phones and USB memory sticks need encryption and anti-malware protection too. A survey of taxi drivers found that Londoners left 3,000 laptops, 5,000 pocket PCs, nearly 1,000 USB sticks and 55,000 mobile phones in the back of licensed cabs during a six month period in 2006.

Most breach disclosure laws allow laptop losses to go unreported if they are fully encrypted. At the other extreme, Nationwide was hit with a fine of almost £1m by the FSA following the theft of a laptop containing details of nearly 11 million customers. "Nationwide's customers were entitled to rely upon it to take reasonable steps to make sure their personal information was secure," said the director of enforcement at the FSA.

Top security tips to safeguard privacy—Page 2

—How to avoid being headline news for the wrong reasons!

Gone but not forgotten!

Review disposal practices for electronic media. Ensure hard drives are securely wiped, not just files deleted or formatted. In fact, considering how little value a used hard drive has, it would be better to physically destroy them.

A few years ago, two Bank of Montreal branch computers filled with sensitive customer information were offered on eBay for six hours before the buyer realised they contained hundreds of customer files; these files included account balances and information on lines of credit, credit cards, personal pensions and insurance. The result was a public relations nightmare for the Bank of Montreal.

Untrusted websites

If your website is interactive (e.g. contains user forums, user-generated content, collects customer data via forms, sells products or services and takes credit card data) have your web-based applications and the back-end databases tested for security. You have a duty of care to your customers since they can't test these applications themselves. This is especially important if the apps are bespoke or heavily customised packages.

The SANS Institute, a respected international security organisation, reports that "web application vulnerabilities in open-source and custom-built applications accounted for almost half the total number of vulnerabilities discovered in the past year, and they are being exploited widely to convert trusted web sites into malicious servers serving client-side exploits and phishing scams."

Third party problems

Review policy and practices for transfer of customer data to third parties, especially overseas, for example when outsourcing. Outsourcing does not absolve you of responsibility for protecting customers' personal information. You must ensure that suppliers are contractually tied to specific conditions that stipulate how data can be transmitted, accessed, used, stored, shared, and safeguarded.

This should include prohibitions against the subcontracting of work without notification and agreement, lest your data be held to ransom by a transcriber in Pakistan, as happened to University of California Medical Center.

High-tech brings risks as well as opportunities

New technologies such as Wi-fi and VOIP bring with them both opportunities and risks. Ignorance is not a defense, so if you don't have the skills in house to adequately assess the privacy impact and risks of new technology systems, get some outside help to do so BEFORE you deploy them.

Assess the risks you are taking

Commission an independent risk assessment and implement the recommendations. Alternatively, use publicly available risk assessment tools to do it yourself.

There is no such thing as perfect security, so being able to demonstrate that you have fairly balanced risks and cost considerations will stand you in good stead if you ever do experience a breach.

You are the weakest link

People are the weakest link in the security chain, but they can be a big asset to your security programme. Of course you already carefully vet new hires and require them to read and sign your policy document covering information security and acceptable use of computers.

Take the next step and subscribe to security awareness newsletters which provide tools such as quizzes, screen savers, posters and a continuous source of ideas. Ensure your staff are trained to recognise social engineering techniques.

Be proactive

This issue isn't going away. As a responsible business, you must be vigilant in safeguarding your customers' information.

Being proactive about privacy management will bring many benefits, including protecting your firm's reputation; avoiding fines, lawsuits and other financial and non-financial penalties; and helping you gain an edge over competitors who fail to embrace privacy best practices that consumers are increasingly looking for when deciding where to buy.

Susan Johnson, CA, CISSP (certified information systems security professional), is the Managing Director of Horizons Global Consulting, a professional consulting and advisory firm based in London that helps clients with all aspects of privacy and security management, from technology to the boardroom. Contact Susan at 07963 998972 or visit the website at www.SusanJohnson.ca for more information.