Best Practice

Security and privacy — Legislative burden or commercial opportunity?

Beth Rogers

Beth Rogers is a member of the South East Regional Board of the Chartered Institute of Marketing, a regular speaker at Cranfield School of Management and Group Business Development Manager for an international IT services company. She also serves on the Ethical Committee of Standard Life. She is the author of a number of books, reports and articles.

Keywords: privacy, information security, permission seeking, customer touchpoint, legislation, e-commerce

Beth Rogers
Logical Group
110 Buckingham Avenue
Slough
Berkshire SL1 4PF
UK
Tel: +44 (0)1753 797106
Fax: +44 (0)1753 819284
E-mail: beth.rogers@logical.com

Beth Rogers

Received (in revised form): 14 May 2003

Abstract

Developing an online sales channel that is easy and convenient for customers comes with the legislative responsibility of providing unprecedented high levels of security and privacy. Consumer perceptions of electronic media are exceptionally sensitive, and legislation has followed their concern. By managing this burden proactively, suppliers may turn it into an opportunity.

Introduction

Technology enables speedy collection and consolidation of customer data so that suppliers can offer immediate and personalised service. Being able to use those data relies on customer trust, so information systems security to protect the data from cybercriminals and privacy procedures to protect them from internal misuse are vital.[1] Customers have to weigh up the convenience and usability of online services against the risks associated with sending confidential information electronically. The risks are real.

Pranksters and malicious fraudsters are the true 'baddies' in the e-marketplace. Laws exist to deal with them, but few public resources are devoted to detecting and prosecuting cybercrime. The UK Government does not collect statistics on internet crime, but in the USA there has been an annual computer crime and security survey since 1995, conducted by the FBI and the Computer Security Institute. In 2002, 90 per cent of 503 security practitioners surveyed said that they had detected security breaches in the last 12 months. Only 34 per cent of incidents were reported to law enforcement; 80 per cent of respondents reported financial losses as a result of security failures, but only 44 per cent were willing or able to quantify them.[2]

Unlike in the physical world, where notices such as 'cars and contents are left at the owner's risk' and 'beware, pickpockets operate in this area' can exonerate companies from any responsibility for crime, suppliers bear an onerous responsibility to prevent cybercrime affecting their customers, which has driven investment in sophisticated security systems. In addition, recent legislation is driving new privacy processes, increasing the complexity of the supplier's role in protecting online customers.

Customer concerns drive legislation

IT industry analysts Gartner suggest that the potential for a high-profile privacy-abuse scandal is increasing, and by 2005 at least one major company will have suffered a high-profile customer backlash over mismanagement of customer information.[3] Outcry has followed recent examples of suppliers taking customer consent for granted. In March 2002, Yahoo! made changes to some marketing activity and reset user preferences to 'opt in'. Intense media interest cast an unfavourable light on Yahoo! for doing so. Advertiser DoubleClick faced class-action lawsuits for using cookies to monitor web surfing activity.[4] Electronic sales channels are still relatively new, and media hype has fuelled consumers' heightened perceptions of risk.

Legislation reflects customer concern

Legislation is already reflecting these customer concerns. Canada was early to legislate with the Personal Information Protection and Electronic Documents Act of 1 January 2001. Each state has an information and privacy commissioner. Ontario's commissioner is Ann Cavoukian, who sees her role as taking companies beyond the compliance mindset to realise that there are competitive advantages in adopting privacy-sensitive practices.[5] Privacy laws exist in some Asian countries, such as Japan and Hong Kong. In the USA internet privacy regulation is piecemeal, affecting just financial services and healthcare, although general legislation has been proposed.[6] The UK Government is required to enact the provisions of the EU directive on privacy and electronic communications by July 2003.[7]

Consent requirements

The proposed UK legislation requires suppliers to take steps to safeguard the security of their services, and take measures to prevent unauthorised access to communications and protect confidentiality. In addition the customer must be protected from marketing practices that they might perceive as intrusive. Customer consent is required for use of cookies that provide identification when they sign on to a supplier site. Consent must be obtained for the processing of personal data in order to provide value-added services. Consent is also required to send direct marketing messages by automatic call forwarding, fax, e-mail or SMS. Customers must be informed about public directory use and given an opt-out. Existing customers as well as new prospects have the right to opt out.

The legislation aims to 'give control back to the customer'. Ironically, tracking software, such as cookies, is intended to make control easy for customers by saving them time and offering them easy access to personalised services. What would Amazon be like without recommendations to browse? Marketers need to present the privacy versus access trade-off with some care so that customers can make informed decisions.

Adopting best practice presents an opportunity to impress customers and refine segmentation. Customers who do opt in to share their information are potentially more likely to be retained and to be profitable. The legislative burden may be a commercial opportunity.

What is best practice?

Best practice encompasses both securing the customer's data from external attack, and preventing internal use that the customer has not authorised. It also involves consulting and understanding customers, in order to produce confidence-winning policy and procedures.

Network infrastructure security

Oracle's chief privacy officer and chief security officer say that security and privacy will always be closely related. Security is necessary for privacy, as without it personally identifiable information could be stolen or misused.[8] One of the fastest-moving areas of technology of the past few years has been security hardware and software. Network security is an unrelenting arms war. Financial losses caused by nuisance computer viruses have ensured that companies have invested in each new protection device.

Security is an arms war

The market for information systems security devices was led by investment in firewalls, the first line of defence of the network which monitors connections to the internet and limits exposure of the internal system to the internet. This soon proved to be insufficient to stop hackers, and intrusion detection systems, which monitor unusual traffic that may indicate an attack, are now considered essential. A state-of-the-art network also utilises vulnerability assessment tools to seek out weak links in the network so that restorative action can be taken, and gateway anti-virus products to protect the company and customers from viruses. Identity and access management tools that establish the true identity of customers are needed, and are evolving from passwords and PINs to biotechnology such as fingerprints and iris recognition. Encryption systems are available to provide protection from eavesdropping, and forensic software creates transaction logs to trace problems.

But as each security loophole is closed, another opens. The increased use of mobile and wireless devices has presented considerable challenges to network managers, as they require new protocols and new investment.

Designing security into applications

Besides securing the network, it is imperative to build security features into individual applications, or functions within applications. This might include monitoring all publicly accessible content from branches, websites, interactive voice response systems and call centre communications that could put the company at risk, and monitoring usage patterns and locations to search for suspicious activity, for example the same person in different countries at the same time. Tracking attempts to use the application that fail at the identification or verification steps, and initiating proactive processes to check the sources of failure, can provide useful feedback.[9]

Balance security with accessability

Of course, customers also want to be able to access applications, so it is desirable to give them some options when it comes to levels of security. Suppliers need to keep the length of time it takes to be authorised to see information on a website to a minimum. Customers lose interest if the connection and display period for a website takes too long. It is possible

to tailor the verification processes based on the risk of the transaction requested.[10]

As a general principle, suppliers should analyse continuously updated information on customer behaviour to build the usability of the touchpoint, and continuously updated information about criminal behaviour to build the security functionality. Greater benefits will come through the use of proactive security systems, which will become more intelligent in identifying the patterns of fraud. These systems will give customers greater confidence and trust in the supplier's ability to manage their transactions.

Nevertheless, the technical arms race against criminals will continue. New technologies to circumvent security and exploit vulnerabilities in technology continue to arise daily. New customer touchpoints also bring new challenges, such as 3G mobile handsets.

Permission seeking

Publicise privacy policy

Permission seeking is a legislative requirement which can be used as a tactical opportunity to communicate the company's privacy and security policy to prospects and customers. After all, reputable suppliers building customer relationship management databases are not the primary source of internet users' fear. Customers need to know that the suppliers they use are doing as much as possible to protect them from cybercriminals, as well as from overenthusiastic marketing practices. If convinced, satisfied and loyal customers may volunteer more information about their preferences. The communication may also reduce waste by identifying prospects and customers who are not interested in repeat business.

Customer consultation

Permission seeking creates an opportunity for broader consultation. It is generally asserted that consumers who buy over the internet regularly have sophisticated expectations. They expect the supplier to have a single, accurate view of their custom and to use it to offer segmented and personalised services. Yes, they expect to be able to opt in or opt out of particular communications and they expect a robust security and privacy policy, but they also expect easy-to-use, convenient services.[11]

Primarily the role of marketing, customer consultation is critical to achieving best practice in balancing security and privacy concerns with the need for accessibility. Some simple activities can keep a company in touch with customer perceptions.

'Voice of the customer' reviews

A 'voice of the customer' review of each customer touchpoint can uncover issues and irritants that affect customers on a regular basis. This activity can identify issues with the working of the general touchpoint functionality, as well as how security affects it. Reviewing identification and verification processes can highlight reasons for poor service take-up and also identify alternative technologies or methods that maintain effective security but are easier on the customer.[12]

Overall policy

From the customer's point of view, transparent company policy is important. To ensure that a security and privacy policy is best practice, it should incorporate the following elements, observing the detail that the new EU legislation will require.[13] The supplier should state its policy and procedures to secure its network and customer-facing applications. Customers also value explanations about information collection, usage and sharing. Customers must have choice, ie the right to opt in or opt out of providing certain personal information. In addition, if suppliers want to send them information, they should seek permission per category of information. Customers should have the right to view, modify and delete information kept about them. Suppliers should facilitate customer enquiries and complaints about access, usability and privacy issues. They should also make their security and privacy policy easily available.

Winning customer confidence

Once companies have a command of customer expectations and deliver best practice, customer confidence will become a true asset.

Summary

Internet shopping has reached the 'early majority'. It has also attracted criminal activity. The nature of the medium ensures that the impact of fraud damages both the customer and the supplier. So suppliers are protecting customers and themselves from the threat. This is a considerable management challenge. Not only do organisations have to deal with the balance between ensuring customers can enjoy accessibility, usability and functionality with security, but they also have a new legislative duty to manage the distinct privacy perspectives of their customers and balance these with their own need to communicate.

Suppliers have to accept that customers and legislators seem to have much higher expectations of security and privacy for trade conducted electronically, and this has a knock-on effect at all customer touchpoints which are technology-enabled. Companies have no choice but to keep upgrading their capabilities. Nevertheless, the companies which use permission seeking to explain their investment in managing the delicate balance of security/privacy with accessibility, and to seek feedback to enable better segmentation and targeting, may gain a tactical advantage. Marketers then have to keep upgrading their capability to leverage that investment in security and privacy to consolidate customer satisfaction and preference.

Continuously upgrade

References

1. Rountree, D. (2002) 'Surveying the online banking channel', banktechnews.com.
2. Sieberg, D. (2002) 'FBI: Cybercrime rising', CNN.com.
3. Janowski, W. (2003) 'US enterprises must prioritize privacy management', Gartner Research, April.
4. Janowski, W. (2002) 'Worst practices in customer privacy management', Gartner Research, June.
5. Jayson, S. (2003) 'Cavoukian communicates the business benefits of privacy', www.1to1.com.
6. Singh, M. and Cowles, R. (2002) 'Internet privacy issues: How should they be resolved?', Gartner Research, June.

7. Directive 2002/58/EC of the European Parliament and of the Council, 12 July 2002.
8. Reisman, A. (2003) 'Tackling privacy and security at Oracle: Two heads are better than one', www.1to1.com.
9. Costelloe, D. (2002) Internal research conducted for Logical Advisory Services.
10. *Ibid.*
11. De Lotto, R. (2002) 'BCP: Financial services privacy and security concerns', Gartner Research, February.
12. Costelloe, ref. 9 above.
13. Directive 2002/58/EC, ref. 7 above; 'Creating a business privacy policy', US Postal Services, www.usps.com/privacyoffice.

Background reading

De Lotto, R. (2002) 'Concerns and responses: Customer ID programs', Gartner Research, September.

De Lotto, R. and Collins, K. (2003) 'Managing customers' privacy and preferences is not easy', Gartner Research, March.

Janowski, W. and Marcus, C. (2002) 'Managing conflicts of customer insight and privacy in CRM', Gartner Research, June.

Jayson, S. (2003) 'New safeguards rule helps keep personal data secure', www.1to1.com.

Wheatman, V. (2002) 'Security and privacy in 2003: Complex and uncertain', Gartner Research, December.