



Reporter, The -
Camden, Miller,
Morgan
Camdenton, MO
Circ. 2000
From Page:
6
4/21/2010
14415



service experience including working for newsmen, linguists, and other...
Socket says businesses face increased risk of identity theft

LAKE OF THE OZARKS -
Identity theft is a serious issue, and businesses have far more to lose than individuals.

The responsibility that comes with the use and storage of customer information also brings the risk of legal and financial consequences if that data is lost or stolen.

Putting security measures in place is vital to limiting the liability companies face.

Many businesses collect personal information such as names, addresses, bank account information, income and credit histories, and Social Security numbers.

Possessing such sensitive data makes companies a target for cyber criminals and identity thieves.

According to the Aberdeen Group, a technology-focused research organization, businesses lose \$221 billion worldwide every year due to identity theft.

"Modern computer criminals are intelligent, highly motivated and well organized," said Dave Sill, IT

Manager for Socket, a Missouri-based telephone and Internet provider. "Businesses need to secure their data in order to protect their customers and themselves."

Taking steps to protect customers' information can save companies a lot of money and hassle.

Companies need to address three main areas to prevent customer information from being stolen or misused:

- * Physical security;
- * Network and data security; and
- * The selection and training of employees.

Physical security is often overlooked when a business seeks to protect customer information. Thieves can retrieve customer infor-

mation via a stolen laptop or a document retrieved from a nearby dumpster.

Labeling company equipment, investing in a document shredder or shredding service and installing

security cameras are a few options to improve physical security and, in turn, customer data.

Most companies also have significant gaps in their digital networks and IT systems, making it easy for data thieves to gain entry.

Sill suggests using anti-virus software and a firewall to prevent attacks, as well as updating Web servers periodically to fix security bugs.

Companies should also be careful and selective when hiring new

employees who will have access to sensitive customer data.

Employers should do background checks on new hires and train them on how to access and handle customers' personal information.

"Oftentimes a criminal will pose as someone else to obtain access to customer information," said Sill. "Even well-meaning employees can cause significant damage if not properly trained on how to handle these situations."

Do not fall victim to a scam claiming customer data has already been compromised.

If identity theft is suspected, companies have the right to ensure they are handing over information to the actual authorities by insisting on a

written formal request.

If an attack has occurred, the Federal Trade Commission recommends contacting other entities who may be affected as well, such as credit card companies.

Be careful when notifying customers whose personal information has been compromised. The FTC provides comprehensive guidelines to handling identity theft at www.ftc.gov.

Identity theft is a harsh reality facing businesses and consumers. While putting preventative meas-

County:
Camden

14415-04-21_6001





ures in place may seem costly, they may be a small price to pay.

Do you have a technology-related question you'd like to see featured in Socket Tech Talk?

Let us know by visiting www.socket.net/techtalkfeedback or by calling

1-800-762-5383.

Socket Tech Talk is provided as a service to distribute general information concerning technology-related topics.

Reporter, The -
Camden, Miller,
Morgan
Camdenton, MO
Circ. 2000
From Page:
6
4/21/2010
14415