Tips to Prevent Data Breaches in Your Business

Author: eFraudPrevention

BankUnited

Protect your business against potential data breaches with these quick tips.

Keep Only What You Need

Reduce the volume of information you collect and retain only what is necessary. Minimize the places you store personal data. Know what you keep and where you keep it.

Destroy Before Disposal

Cross-cut shred paper files before disposing of private information. Also destroy CDs, DVDs and other portable media. Deleting files or reformatting hard drives does not erase data. Instead, use software designed to permanently wipe the drive, or physically destroy it.

Safeguard Data

Lock physical records in a secure location. Restrict access to employees who need to retrieve private data. Conduct employee background checks and never give access to temporary employees or vendors.

Safeguard Data Privacy

Employees must understand that your privacy policy is a pledge to your customers that you will protect their information. Data should only be used in ways that will keep customer identity and the confidentiality of information secure. Of course, your employees and organizations must conform to all applicable laws and regulations.

Continually Update Procedures

Do not use Social Security numbers as employee ID or client account numbers. If you do so, develop another ID system now.

Establish Password Management

A password policy should be established for all employees or temporary workers who will access corporate resources. In general, password complexity should be established according to the job functions and data security requirements. Passwords should never be shared.

Secure All Computers

Implement password protection and require re-logon after a period of inactivity. Train employees to never leave laptops or PDAs unattended. Restrict tele-working to company-owned computers and require use of robust passwords that are changed regularly.

Control Use of Computers

Restrict employee use of computers to business. Don’t permit use of file sharing peer-to-peer websites. Block access to inappropriate websites and prohibit use of unapproved software.

Keep Security Software Updated

Keep security patches for your computers up to date. Use firewalls, anti-virus and spyware software; update virus and spyware definitions daily.

Encrypt Data Transmission

Mandate encryption of all data transmissions. Avoid using public Wi-Fi networks; they may permit interception of data.

Manage Use of Portable Media

Portable media, such as DVDs, CDs and USB "flash drives," are more susceptible to loss or theft. Allow only encrypted data to be downloaded to portable storage devices.

Establish an Approval Process for Employee-Owned Mobile Devices

With the increased capabilities of consumer devices, such as smart phones and tablets, it has become easy to interconnect these devices to company applications and infrastructure. Use of these devices to interconnect to company email, calendaring and other services can blur the lines between company controls and consumer controls. Employees who request and are approved to have access to company information via their personal devices should understand and accept the limitations and controls imposed.

Govern Internet Usage

Most people use the internet without a thought to the harm that can ensue. Employee misuse of the internet can place your company in an awkward, or even illegal, position. Establishing limits on employee internet usage in the workplace may help avoid these situations. Every organization should decide how employees can and should access the web. You want employees to be productive, and this may be the main concern for limiting internet usage, but security concerns should also dictate how internet guidelines are formulated.

Manage Email Usage

Many data breaches are a result of employee misuse of email that can result in the loss or theft of data and the accidental downloading of viruses or other malware. Clear standards should be established regarding use of emails, message content, encryption and file retention.

Govern Use of Social Media

All users of social media need to be aware of the risks associated with social media networking. A strong social media policy is crucial for any business that seeks to use social networking to promote its activities and communicate with its customers. Active governance can help ensure employees speak within the parameters set by their company and follow data privacy best practices.

Oversee Software Copyright and Licensing

There are many good reasons for employees to comply with software copyright and licensing agreements. Organizations are obliged to adhere to the terms of software usage agreements and employees should be made aware of any usage restrictions. Also, employees should not download and use software that has not been reviewed and approved by the company.

Report Security Incidents

A procedure should be in place for employees or contractors to report malicious malware in the event it is inadvertently imported. All employees should know how to report incidents of malware and what steps to take to help mitigate damage.

All content is for informational purposes only and does not constitute legal, tax, or accounting advice. You should consult your legal and tax or accounting advisors before making any financial decisions.