

Information Hot Spots

Do You Know Your Organization’s Information “Hot Spots?”

Addressing data vulnerabilities is about more than a good firewall—understanding the flow of information within your organization helps protect against a data breach

Too often, businesses large and small think of data security as strictly an IT department concern. Companies get lulled into a sense of complacency that they have eliminated risks because they have invested heavily in virus software and other protections from cyber intrusions.

ID theft expert Brian Lapidus, chief operating officer of Kroll’s Fraud Solutions, has unique frontline experience helping today’s businesses safeguard against and respond to data breaches. Below he outlines some of the steps that companies should take when evaluating their sensitive data hot spots.

The truth is that the loss, theft or misuse of sensitive personal information can happen anywhere within the organization. It is up to management to provide an enterprise-wide solution that identifies, monitors, and protects these data “hot spots.” This is not as easy as it seems—trying to figure out just what are your company’s information hot spots may feel like the proverbial needle-and-haystack search, but it is well worth it.

Identify the data

What types of personal identifying information does your company collect and keep names, dates of birth, Social Security numbers, credit card numbers, or other types of identifiers? Once you have determined this, you need to categorize for each population you serve—customers, vendors, employees.

Inventory the data

Now that you understand what types of personal identifiers you collect, it is essential to know where these elements reside. This may seem easy, but it is far more difficult than most companies realize. Total enterprise security means understanding just how employees use data and where they might keep it—from the database right down to the files housed at an employee’s desk. As the business changes over time, it is important to properly “overhaul” this inventory and keep it up to date.

Audit data points of entry, access, or exit

Now that you know what your data consists of and where it is located, you must focus on how it is collected, accessed, archived, and destroyed. Safeguards must be in place at all entry and access points. Access will also involve determining who within the organization needs the data and making it available to them only. For disposal, it is important to first define a timeline—how long should certain data be kept? Providing employees with reliable means to destroy records, such as cross cut shredders, help ensure compliance.

Provide employee training

Training your employees to understand the value of sensitive data and to follow security protocols is vital to having a plan that works. Without it, employees may not recognize the important part they play when handling such data.

Implement an incident response plan

Even with a superior plan and vigilance on the part of employees, breaches will still happen. Too many companies make the mistake of thinking a good data security plan makes the office an impenetrable fortress. Auto insurance can't stop an accident. It is important to develop an incident response plan that will enable key personnel to act quickly and accurately when a breach does occur.

Developing a Plan to Identify "Hot Spots"

These steps are a good general starting point for developing a plan to identify the various types of sensitive information, the organizational hot spots, and a protocol for handling this data. While no office can totally prevent the loss, theft or misuse of data, determining information hot spots will go a long way towards increased awareness and more informed data handling practices.

Kroll's Fraud Solutions
866 419 2052
www.krollfraudsolutions.com
www.kroll.com

