

Data Leak Risks:

A Problem Mid-Size Organizations Can't Ignore

Code Green Networks
3975 Freedom Circle
Suite 900
Santa Clara, CA 95054
(408) 213-2300
info@codegreennetworks.com
www.codegreennetworks.com

Executive Summary

More than 220 million private records have been breached in the last three years. With the average cost of a data-leak incident reaching \$6.3 million in 2007, organizations of all sizes must act to protect sensitive data.

Status-quo security technologies, such as firewalls and anti-virus scanners, are designed to keep out attackers – not to protect sensitive information from leaving the organization.

New policies must be created and technologies deployed to protect sensitive data from either inadvertently or intentionally leaking outside the corporate walls.

This applies to large enterprises, as well as small- and mid-sized organizations that face the same data-leak challenges and regulatory requirements, with fewer IT resources and smaller budgets.

The High Cost of Data Leaks

While small- and mid-sized organizations have invested heavily in security technologies like firewalls, anti-virus scanners and spyware protection, they've overlooked a subtler but more common risk: data leaks.

Previous generations of security technology focused on keeping the bad guys out. That strategy made sense in a time when digital assets weren't business-critical resources, and there weren't as many points of entry into and out of the network like WebMail, instant messaging, laptops and mobile devices.

Today, digital assets are the lifeblood of information-rich organizations, and losses undermine competitiveness. High-profile data leaks, such as those experienced by TJX, Home Depot, or Pfizer, end up costing organizations millions. TJX, for instance, agreed to pay nearly \$41 million to those whose credit card information was affected by the breach – and that doesn't take into account the damage done through lost business and bad press.

According to the Ponemon Institute, the price tag of the average data-breach incident is \$6.3 million. What, though, does that number mean? It means that companies experiencing data breaches lose customers, suffer bad press, are fined by industry regulators and spend exorbitant amounts of money investigating the breach and correcting the root problems that led to the breach.

Additional costs include actions needed to lure back customers and re-establish brand trust. New advertising campaigns, product giveaways and free services like credit monitoring are all common after a breach.

Overcoming the Myth: "It Only Happens to the Big Guys"

Many high-profile data leaks, such as the one suffered by TJX, get all the press but can be misleading to the average business owner – painting an inaccurate picture about the nature of data leaks and luring lesser-known companies into a false sense of security. The TJX database was breached by hackers, yes. The typical data breach, on the other hand, comes from within the organization. Even in the TJX case, internal policies were partly to blame, with poor security practices opening the door for hackers.

Malicious insiders, overworked IT staffers, poorly trained knowledge workers, and opportunistic contract workers all constitute a much greater risk than external threats. Yet, in the typical mid-sized organization, security focuses almost entirely on outsiders. Once a person gets access to the corporate network, that person is considered trustworthy. This is a big mistake.

Lest we paint too grim a picture, it's important to note that inside threats aren't always intentional. Simple human error can be just as problematic. A recent survey by Deloitte found that human error is the number one cause of security failures for 75% of the companies questioned. Human errors were often responsible for network outages and system breakdowns.

Losing a laptop, misconfiguring a server or firewall, sending out emails that contain confidential customer data, and even sending out clear-text emails over public networks are all common behaviors that put your organization at risk.

Data Leaks by the Numbers

- Data leaks involving customer data cost companies \$197 per record in 2007
- The average cost per incident was approximately \$6.3 million
- 65% of the cost of a breach is due to lost business
- Over 220 million records have been breached since January 2005

Sources: the Ponemon Institute and the Privacy Rights Clearinghouse

What Are the Sources of Data Leaks?

Thirty-five states now have laws in place that require notification when an individual's confidential information has been compromised. Mishandled medical records, social security numbers, credit card numbers and the like trigger mandatory notification. As a result, these types of breaches – those associated with identity theft – get all the attention.

A less publicized but just as costly class of leaks involves proprietary data assets. Lost intellectual property, stolen sales records and compromised brands don't trigger consumer notification laws, but they pose serious financial and competitive risks. This type of breach results in just as many soft costs as hard costs.

Risks from Within

- Intellectual property theft costs U.S. business about \$250 billion each year.
- The U.S. economy loses an estimated 750,000 jobs due to intellectual property theft.
- Insider attacks have become the number one security threat for U.S. businesses, topping traditional threats like worms and viruses.
- Financial fraud is the single most costly type of attack, while the loss of customer and proprietary data comes in at number two.
- Sources: The U.S. Commerce Department and the 2007 CSI Computer Crime and Security Survey

The most common sources of proprietary data loss and intellectual property theft are:

Malicious insiders

Disgruntled workers are like in-house hackers. The most dangerous time for any company is during an organizational change. Mergers and downsizing erode employee loyalty, which often leads to stolen or compromised data. Even during times of relative calm, employees come and go, and when they go, they often attempt to take confidential information – be it sales information, intellectual property or marketing strategies – with them.

Email and careless employees

The most common avenue for data loss is email. One careless email sent to the wrong recipient or one accidental "reply-all" message containing confidential information can pose big problems. Worse, an employee falling for a targeted phishing attack could put an array of data assets at risk.

New technologies

Web 2.0 is considered a boon to business, but it also poses challenges. While advocate blogs by your marketing and engineering teams provide a cost-effective way to get your message out, they can also inadvertently reveal confidential information. Similarly, online collaboration tools must be monitored to ensure that they don't expose proprietary information.

Partners and contractors

One of the horror stories of outsourcing is the overseas factory that delivers your product and then makes its own pirated run of that same product to sell locally. Partners and contractors pose smaller, but still significant risks. They have access to sensitive data but are far less loyal than on-staff employees.

Competitors and corporate espionage

Mid-sized organizations often believe that corporate espionage is something only Fortune 500 companies face. Unfortunately, this isn't the case. Mid-sized organizations can be seen as having less stringent defenses, and thus are considered easier targets. Nefarious competitors will seek to steal intellectual property, valued employees, and customer information.

Unique Challenges Faced by Mid-Sized Organizations

To cope with data leaks, most large enterprises have deployed dedicated security solutions, such as email encryption and data-loss prevention solutions. Large enterprises also have security teams as part of their larger IT staffs, targeted teams that constantly research and procure products to strengthen their company's security posture.

The mid-sized enterprise doesn't have these luxuries. Like most new technologies, first-generation email security and data-loss prevention (DLP) solutions targeted the large enterprise. Simply put, they were too expensive and too complex for mid-tier organizations with smaller budgets and fewer IT resources.

What options do mid-sized organizations have, then? Until recently, the best course of action was to create policies, educate employees, and wait for technology to mature. After all, technology evolves and becomes more affordable and usable over time.

Fortunately, that time is now. Market forces, including acquisitions in the technology space and increasing consumer awareness, have accelerated the evolution of DLP and email encryption solutions. Costs are coming down and next-generation solutions are taking ease-of-use into account.

Top Pressures Driving Companies to Deploy DLP Solutions

1. Compliance with internal security policies
2. Compliance with external regulations
3. Demand from customers
4. Ability to collaborate safely with those outside the organization
5. Demand from business partners

Source: Aberdeen Group, May 2007

Data Leak Strategies for Mid-Sized Organizations

Let's take a step back from technology for a moment. Technology is necessary to combat data loss, but it isn't the only solution – nor is technology deployment the first step your organization should take.

1. The first step is to assess your digital assets. What is your most sensitive data? What will cause you the most problems if compromised? Where do these assets reside and who has access to them? How and when are these assets audited?
2. Next, treat valuable data as such. This is important from a security policy perspective, and it's also critical if you ever go to court. If your employees leave confidential customer lists lying around in public areas or you store proprietary information in poorly protected databases or readily accessible servers, you are in essence saying, "This information has little value." Courts take these factors into account when deciding cases and awarding damages.
3. Third, understand your risks. What regulations must you adhere to? What are the penalties for non-compliance? How sensitive is your intellectual property; if competitors access it, are they simply accessing common industry knowledge or do you lose a competitive advantage?
4. Fourth, create data-usage policies and a way of enforcing them. Determining risks will help you tailor policies to protect your data, but you must then train users on those policies and hold them accountable.
5. Finally, assess your technology options and deploy solutions that protect your most sensitive digital assets.

What to Look for in a DLP Solution – Effectiveness, Ease of Use and TCO

The three most critical factors for a mid-sized organization are effectiveness, ease of use, and total cost of ownership. On the surface, effectiveness goes without saying. If the solution can't stop data leaks, it's not really a solution, right?

Effectiveness is tricky to measure, however. Content inspection and email filtering are table stakes. In the typical work environment, though, webmail filtering and email encryption are equally important. In addition, effectiveness isn't just about the technology itself. It also involves users and administrators.

It's important to think deeply about ease of use. First, are the policies generated by your DLP solution easy for your knowledge workers to adhere to? If you enforce data-use policies that undermine productivity or slow communication flows, you'll have a knowledge-worker mutiny on your hands.

Next, is the solution easy for IT to manage and maintain? Too often, ease of use is a shortcut phrase for "easy to deploy." That may be enough for a large organization, but for the mid-sized entity, ease of use must go well beyond the deployment phase. A solution requiring labor-intensive administration and policy configuration isn't appropriate for organizations with few IT resources.

A solution appropriate for mid-sized enterprises should have templates and wizards that simplify policy creation, should automatically enforce those policies, and should generate alarms and reports when incidents occur.

The final consideration is cost. Total cost of ownership involves not only the sticker price of the solution but your own daily maintenance and administration costs.

DLP Evaluation Checklist

1. Is it effective at inspecting content?
2. Does it address both email and webmail?
3. Does it encrypt outbound email traffic?
4. Does it include templates and wizards for easy policy creation?
5. Does it automatically enforce policies?
6. Does it automatically trigger alarms and generate incident reports?
7. Does it tie in well with enterprise content management systems?
8. Is it easy to maintain and administer?
9. Does the vendor have experience in the mid-market?
10. Does it have a low total cost of ownership?



www.altaware.com
sales@altaware.com
(866) 833-4070

Your Code Green Networks Reseller



About Code Green Networks

Code Green Networks delivers data loss prevention solutions that protect private employee and customer information and safeguard intellectual property across all electronic communications channels. The company's easy-to-deploy, easy-to-manage content inspection appliances rapidly detect and prevent potential data leaks, helping organizations automate compliance and mitigate risks from internal breaches that can result in loss of revenue, financial penalties and irreparable damage to a corporation's image, brand and customer loyalty.

For more information about Code Green Networks, visit <http://www.codegreennetworks.com>