Ten Steps to Protecting Your Sensitive Data

Data loss prevention has become a major focus for companies of all sizes. One reason is that our increasingly mobile employees carry an increasingly large collection of sensitive data. Companies now purchase more laptops than desktops—and those laptops are loaded with sensitive information: everything from patient, customer and employee records to intellectual property, financial data, and passwords.

With more data traveling outside the network perimeter more often, it presents a very attractive target to cybercrooks. And security incidents are on the rise. According to McAfee's Unsecured Economies report, the research team saw almost as much new malware in the first half of 2009 (1.2 million unique examples) as it did in all of 2008 (1.5 million).

The mitigation costs from a single data loss can quickly exceed the costs of protecting the data in the first place. In fact, in the last year, one in five midsize organizations had a security incident that directly caused their organization to lose $41,000 in revenue on average[1].

Key Points

Organizations need to protect their data, as the damages from even a single loss can be staggering:

- Lost revenues
- Possible heavy fines
- Damage to company reputation
- Loss of customer confidence

Following these 10 best practices can help protect your sensitive data:

- Take inventory of the regulations your business is subject to
- Identify known content risks
- Talk to stakeholders
- Know where your data is
- Set formal rules for creating and changing policies
- Put alerting and enforcement mechanisms in place
- Delegate controls and responsibilities
- Maximize existing IT investments
- Go with a platform approach
- Build your solution as needed

Step 1: Assess the regulations your business is subject to

There's no shortage of laws, regulations, and industry mandates facing companies. While companies in highly regulated industries like healthcare, finance, and government were once the only ones concerned with compliance, today almost no business is immune. Whether public or private; big or small; in the U.S., Europe, or Asia; every company should have a well-thought-out data protection plan.

Begin by understanding that you are likely subject to the laws and regulations of each geographic region that you conduct business in. Then realize that most of these regulations share two common facets: First, they are typically focused on protecting data that can uniquely identify a person, patient, customer, or employee. Second, many regulations are satisfied if this critical data is protected using encryption. Obviously you need to research the specifics as they apply to your company. But at the end of the day, data protection simply makes good sense.

Step 2: Identify known content risks

Whether storing Social Security numbers, credit card information, or medical records, it's crucial to have the right tools to scan your network for known risks. These tools should be capable of scanning file shares, databases, content management stores, and all your other various data repositories. Often, organizations will know where a portion of this data resides, like a server used by the finance or human resources department, but discovery mechanisms are required to find all instances of sensitive data. These might include legacy servers, desktops, or other places long since forgotten by the IT team. Furthermore, the discovery engine needs to have automation mechanisms for running over time, as new content is created or added to the network.

1. Bloor Research, *The Security Paradox Survey*. December 2009

Recent examples of sensitive data loss incidents:

- *February 2010*—Hard drives containing health information for 500,000 customers were stolen from BlueCross BlueShield. Data included names, addresses, diagnoses, Social Security numbers, and dates of birth.
- *January 2009*—A laptop containing names, addresses, Social Security numbers, and fingerprints was stolen from a locked Continental Airlines office in Newark, NJ.
- *August 2009*—A laptop was stolen from an Army National Guard contractor. The laptop contained personal information on 131,000 soldiers, including names, Social Security numbers, and bonus payments.

Step 3: Talk to stakeholders

Effective data protection begins with a high-level understanding of the data that's important to each stakeholder. Get them involved early by asking what kinds of data their department generates and consumes. Who handles what data? What do they do with it? How do they collaborate? Where do they store and archive their data? From an operational perspective, who in their department will act as the authorized contact to remediate any issues that come up?

Each department knows their data, so this isn't a difficult task. But it is important. It wouldn't be appropriate or practical to expect IT to determine if a given type of data were sensitive or not.

Step 4: Know where your data is

Understanding where your data is stored may not be as obvious as it sounds. Of course, it's on file servers, in databases, and on individual computers. But what about the backup drives, thumb drives, smartphones, and other personal devices that employees bring into the office? And what about the systems they use at home? Think beyond the equipment that the company has formally issued to employees. It's important to understand who has access to all these personal systems and devices.

Step 5: Set formal rules for creating and changing policies

You will undoubtedly have a number of people contributing to the policies that you put in place to protect your organizational data. You'll want to think about how policy additions and changes will be proposed, communicated, and deployed to avoid any disruptions to normal business processes.

Step 6: Put alerting and enforcement mechanisms in place

No security strategy is complete without mechanisms to alert on and take real-time action against threats. Notifications sent to IT administrators as well as HR, legal, and compliance officers are important. But end-user alerts can be invaluable for educating and modifying employee behavior to ensure proper handling of sensitive records.

Enforcement actions can range from simple email notifications of privacy breaches to more proactive mechanisms that force emails containing sensitive data through encryption servers before they leave the company. Along these lines, enforcement activities can also include denying access to webmail, such as Gmail and Yahoo! Mail, and public instant messaging services, like Windows Live Messenger and Yahoo! Messenger—which are known conduits for security breaches.

Step 7: Delegate controls and responsibilities

So far, we've covered the importance of identifying content risks and putting policies and mechanisms in place to protect sensitive data. You will also need to delegate control over policies and responsibilities should a breach occur.

Clearly, different owners will need different levels of access to your data and the policies that secure that data. You will likely need one or more people to identify sensitive records, define policies, and then circle back to ensure that the information is being appropriately protected.

More importantly, however, delegation is critical to the remediation steps that will be necessary if there is a security breach. Should a department data owner address the incident or a compliance officer? What if a reconfiguration issue is required on an end user's desktop and IT staff intervention is required? What if user training is a requirement? And how are you going to manage the remediation processes and track them to completion? You need to put workflow procedures in place to handle such incidents. What's more, your organization needs to ensure that the sensitive data that triggered the incident is now safeguarded and only accessible by a privileged few users and managers.

Step 8: Maximize existing IT investments

Over the last 15 to 20 years, organizations have invested heavily in various Internet technologies. They've built out their networks. They've deployed applications on these networks. And they've worked hard to secure everything in the process. Whatever you put in place to protect your sensitive data should make the most of these technologies—both in terms of functionality and people skills.

For example, an ideal policy enforcement solution should plug into existing infrastructure elements like email gateways, network switches, web proxies, and encryption solutions. Similarly, the privacy solution should leverage intrusion detection systems, firewalls, and vulnerability assessment solutions that may already exist in the environment. This will give you better visibility into low-level network activity and boost the accuracy and overall effectiveness of the privacy solution.

Step 9: Go with a platform approach

Ensure that whatever solution you consider deploying can provide you with centralized management and the kind of deployment, enforcement, and reporting tools that your business needs. A traditional, best-in-class approach can quickly leave you with a number of siloed solutions from different vendors, all requiring separate care and maintenance and resulting in compromised security. The costs for such a siloed approach quickly mount. Your personnel have to be trained on multiple systems. You don't have the benefit of organization-wide reporting. End-user training requirements are high. And, of course, each vendor points at the other when there's an issue.

Customers agree and studies support that a platform approach is the only way to go. A unified platform allows you to start with one solution and add others as needed—without having to replicate infrastructure or undergo considerable new training. The platform approach also ensures that deployment is trouble free, and that third-party solutions can tie into it through known interfaces.

Step 10: Build your solution as needed

Many customers find value in first tackling a project that addresses a pressing need. Start with laptop protection, file encryption, removable media encryption, or even data loss prevention—based on your specific need.

The McAfee approach to data protection allows you to begin with the solution that makes sense for you. Additional solutions can be added later as needed. Going with the McAfee approach, you can solve an immediate tactical problem and still be positioned for strategic success.

Choose McAfee Data Protection Solutions

Only McAfee offers a portfolio of data protection solutions with the breadth and depth to truly provide comprehensive coverage of your company's most precious asset—your data. Whether you're looking to leverage the power of McAfee® Data Loss Prevention (DLP) solutions, or see how one of the McAfee encryption solutions can help you meet your data security goals, McAfee can help you quickly and easily encrypt data on laptops and USB drives, gain full visibility over the data leaving your endpoints, and enforce endpoint controls. And it takes a lot less time to deploy and manage than you might think.

Stop data loss before it happens, manage compliance with industry and government regulations, and do it all without interrupting legitimate business activities. It's easier than you might think if you follow these 10 steps using McAfee DLP solutions.

McAfee, Inc.
3965 Freedom Circle
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

9156brf_dtp_10-steps_0310_ETMG