GALAXYCONSULTING
Information Management Solutions

Data Security

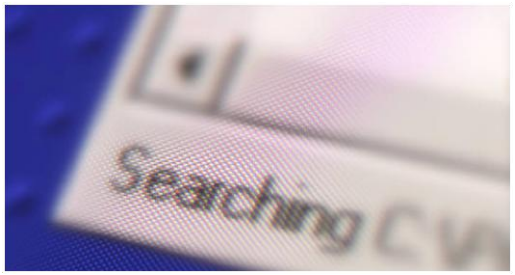
White Paper
By Galaxy Consulting

April

A

At Your Service…Today…Tomorrow
We Appreciate The Privilege Of Serving You!

May 2016



Abstract

Data security should be a priority in your organization. Data breaches are expensive. The top 13 breaches of last year alone cost the affected companies more than $32 billion. After the initial incident, the exposed information can take on new lives. Once the data is out there, it is completely exposed and the backlash of a breach can seem never ending and be costly well beyond the initial event.

This white paper is about data security. It describes the importance of it and solutions to prevent data loss.

Why Data Security?

Reducing the number of data hacks is becoming an important item on the enterprise agenda. For hackers, large-scale data breaches such as Home Depot, Neiman Marcus, and Staples are gold mines. For businesses, keeping valuable data out of the hands of cyber-thieves is a constant battle.

Companies, on average, can expect to encounter 17 malicious codes, 12 sustained probes, and 10 unauthorized access incidents each month, according to research from the Ponemon Institute, a provider of independent research on privacy, data protection, and information security policy.

Forrester Research noted that outside of banking and national defense, many industries are "woefully immature" when it comes to making the necessary investments in data breach protection, detection, and response. This prompted Forrester to conclude that most enterprises will not be able to respond to a data breach without undermining their customers' trust or dragging their own corporate reputations through the mud.

Despite the growing number of attacks, many companies are still not doing nearly enough to secure their customers' personal and financial information. For many companies, the wake-up call only comes after they have fallen victim to a large-scale, high-profile breach.

As many as 35% of data breaches have started with basic human error, such as sending an email with personal information to the wrong person or storing company files on laptops or tablets that were lost or stolen.

Companies need to safeguard against all possible vulnerabilities across their entire infrastructure and to prevent data breaches from happening. They need to have an incident response and crisis management plan in place. Efficient response to the breach and containment of the damage has been shown to significantly reduce the cost of breaches and goes a long way toward reassuring customers who might have been thrown into a panic.

The only real way to save money and keep security costs low is to take preventive steps to avoid common vulnerabilities and to minimize their impact. A good enterprise security solution will keep your information secure, will allow you to maintain your business' reputation, and will cost significantly less than a data breach.

The damage of a breach goes well beyond fines and fees. Fines and fees are certainly an issue, but data breaches impact consumer confidence and companies share prices. Unfortunately, for many organizations, security improvements and overhauls seem overwhelming, and few initiatives get off the ground unless there is a significant problem. At that point, the damage has already been done.

First Steps

Enterprise security is the cross-departmental problem that affects many different stakeholders. Everyone from executives to operations, development, and security needs to be on the same page before any action takes place. This means your organization's security requirements need to be carefully outlined and agreed upon while aligning with each department's strategic goals.

It is important to have a high-level company executive who is responsible for data security. The key to addressing information security is first to understand what information is stored in company databases.

General Governance Controls

It is important to establish general governance controls such as:

- Understand your data topology – holistically across the enterprise: how much, where, who owns it, and what value does it provide.
- Employ real-time indexing of content – to keep track of its changes.
- Store the intelligence about your content (metadata).
- Create an information intelligence service center and include data analysis, governance analysis.
- Employ change management to stay current of new forms of content and new business requirements.
- Become proactive in deploying policies for securing data, storing data, sharing data and enforcing compliance.
- Remove obsolete or unnecessary content.

- Define content life cycle and retention policies.
- Tier your access to enable relevant data to be closer to users and devices that are local.
- Educate the organization on the value of good governance; it is less about control and more about raising the intelligence and health of information.
- Categorize your information and determine its value and rank.
- Use content approval function in your CMS.
- Efficiently store records in compliance with retention of records management policies. Create retention schedule, content controls, consistent disposition of content in accordance with records management policies for content preservation, remediation, and retention.
- Keep track of what info is created, stored, and accessed.
- Use auto-classification and semantic tools within the search engines.
- Move relevant documents from desktops and shared drives to your central documents repository.
- Create efficient document versioning and check-in/check-out management for information consistency.
- Create robust administration of users to ensure that each as access rights for only documents that they are authorized to have access to.

Digital Preservation and Governance

Create a data inventory and determine what data is sensitive. Then segment out the sensitive and non-sensitive data. Systematically purge the data that your organization no longer needs.

Digital records that have a long-term retention schedule are at risk when hardware devices, software applications and file formats become obsolete. Obsolete software file format is also a concern. Many first generation business and personal productivity tools are retired, and the inability to retrieve or view older digital records is becoming a reality.

Migration, conversion and adoption of open standards are accepted approaches to solve the problem of accessibility over time. Those approaches, however, are not widely adopted at this time.

Decisions to retire older enterprise applications raise content preservation concerns. As organizations begin infrastructure renewal projects, particularly as new SaaS and cloud-based applications become viable alternatives, IT and records professionals must assess the risk of losing information in those older systems. Decisions to maintain older systems in read-only mode, to migrate data into newer systems or to dispose of older systems all together must be made in accordance with business, legal and compliance needs.

Take an inventory of all IT assets and business processes and analyze them for vulnerabilities that could expose sensitive data, for example, cardholder data. The next step would be to fix those vulnerabilities. This assessment should be performed at least once a year. Make sure that the company's data security program meets industry best practices, government regulations, and the company's business objectives.

Make sure your web site uses encryption for processing customer's data. Once your company no longer needs customer data, such as payment cards or any other personal information, it should be securely deleted. It is crucial for companies to segment data so that a breach in one file does not open other data repositories.

Companies should use Internet firewalls at all times, keep their operating systems and other business software up to date, and install and maintain antivirus and anti-spyware programs. Because many companies allow employees to use their own mobile devices, including smartphones, tablets, and laptops for business, these devices should be protected in the same way. Limit some company applications and data so that employees can't access them from unsecured mobile devices.

Role-based access control (RBAC) is another key component in preventing data breaches. Clearly defined roles and access policies for users and applications can ensure that all exposure to data is appropriate and based on a well-defined set of policies. A well-defined policy will scale with your organization and allow you easily to maintain privileged access management in the future. By identifying all the elements in your environment and assigning them roles via your policy, you easily will be able to audit who has access to what and when.

It is extremely important that companies limit data access to those employees who need it setting up appropriate security permissions in your data systems. You can put data logging in place, with alarms for when something happens out of the ordinary. This way you will know when someone is doing something with the data that does not coincide with their job description. The increased transparency is especially important in highly regulated industries, in which compliance is extremely important.

Data security, therefore, has to be a business-wide endeavor. IT professionals, company executives, and employees at every level must work together to protect critical data assets from internal and external threats. Companies need to foster a security-aware culture in which protecting data is a normal and natural part of everyone's job.

Data security is also a constant game of what-ifs. The only certainty is that cyber-criminals will never stop learning and sharing information that will help them to get into high-profile targets. They will never stop trying to break into corporate databases. The information is just too valuable on the black market. The key is to make sure that you are not leaving the front door open for hackers to get in.

Social Media Security

Organizations, including small and midsize businesses, non-profits, corporate enterprises, even governments, are no doubt being inundated with automatic cyber-attacks, hacks, spam, phishing scams, DDoS (distributed denial of service) attacks and other forms of electronic malware. Much of this malware also no doubt comes from social media use. Interestingly though, many organizations are not prepared or putting effort into scanning this content for malware stemming from social media use.

Short links distributed through tweets, wall posts and other forms of communication are generated by bots that are designed to appear human online, though they are not. The information gathered through deploying these bots can be devastating for an organization. Imagine that employee clicks on one of these links and critical business information becomes vulnerable to automated information harvesting.

This information can be used in a variety of ways including business or government espionage, theft of important customer or internal financial information, theft or distribution of important trade secrets like research or prototypes and illegal or compromising use of other critical data.

There are tools that can scan this content and monitor user behavior to ensure secure communications. One of the tools that can manage social media is HootSuite.

Privacy Compliance

Recently, high-profile cases involving breaches of privacy revealed the ongoing need to ensure that personal information is properly protected. The issue is multidimensional, involving regulations, corporate policies, reputation concerns, and technology development.

Organizations often have an uneasy truce with privacy regulations, viewing them as an obstacle to the free use of information that might help the organization in some way.

But like many compliance and governance issues, managing privacy will offer benefits, protecting organizations from breaches that violate laws and damage an organization's reputation. Sometimes the biggest risks in privacy compliance arise from the failure to take some basic steps. A holistic view is beneficial.

Privacy Compliance Components

Rather than being in conflict with the business objectives, privacy should be fully integrated with it. Privacy management should be part of content management program.

An effective privacy management program has three major components: establish clear policies and procedures, follow procedures to make sure that organization's operation is in compliance with those policies, and provide an oversight to ensure accountability. Example of questions to consider: is data being shared with third parties, why the information is being collected, and what is being done with it.

Expertise about privacy compliance varies widely across industries, corresponding to some degree with the size of an organization. Although large companies are far from immune to privacy violations, they might at least be aware and knowledgeable about the issue.

The biggest mistake that organizations make in handling privacy is to collect data without a clear purpose. You should know not just how you are protecting personal information but also why you are collecting it. It is important for organizations to identify and properly classify all their data.

International Considerations

Increasingly, organizations must consider the different regulations that apply in countries throughout the world, as well as the fact that the regulations are changing. For example, on March 12, 2014, the Australian Privacy Principles (APPs) replaced the existing National Privacy Principles and Information Privacy Principles.

The new principle is applicable to all organizations, whether public or private, and contains a variety of requirements including open and transparent management of personal information. Of particular relevance to global companies are principles on the use and disclosure of personal information for direct marketing, and cross-border disclosure of personal information.

It is important to consider international regulations in those countries where an organization has operations.

Technology Role

The market for privacy management software products is still relatively small. The market for this software is expected to grow rapidly over the coming years. The current reform process for data protection has created a need for privacy managing technology.

Products from companies such as Compliance 360 automate the process of testing the risk for data breaches, which is required for the audits mandated by the Economic Stimulus Act of 2009. This act expanded the Health Insurance Portability and Accountability Act (HIPAA) of 1996 requirements through its Health Information Technology for Economic and Clinical Health (HITECH) provisions.

These provisions include increased requirements for patient confidentiality and new levels of enforcement and penalties. In the absence of suitable software products, organizations must carry out the required internal audits and other processes manually, which is time consuming and subject to errors.

Enterprise content management (ECM), business process management (BPM) and business intelligence (BI) technology have important role in privacy compliance because content, processes, and reporting are critical aspects of managing sensitive information.

As generic platforms, they can be customized, which has both advantages and disadvantages. They have a broad reach throughout the enterprise, and can be used for many applications beyond privacy compliance. However, they are generally higher priced and require development to allow them to perform that function.

Privacy in the Cloud

Cloud applications and data storage have raised concerns about security in general and personally identifiable information (PII) in particular. Although many customers of cloud services have concluded that cloud security is as good as or better than the security they provide in-house, the idea that personally identifiable information could be "out there" is unsettling.

PerspecSys offers a solution for handling sensitive data used in cloud-based applications that allows storage in the cloud while filtering out personal information and replacing it with an indecipherable token or encrypted value.

The sensitive data is replaced by a token or encrypted value that takes its place in the cloud-based application. The "real" data is retrieved from local storage when the token or encrypted value is retrieved from the cloud.

Thus, even though the application is in the cloud, the sensitive information is neither stored in the cloud nor viewable there. It physically resides behind the firewall and can only be seen from there.

This feature is especially useful in an international context where data residency and sovereignty requirements often specify that data needs to stay within a specific geographic area.

Challenges for Small Organizations

Small to medium-sized organizations generally do not have a dedicated compliance or privacy officer, and may be at a loss as to where to start.

Information Shield provides a set of best practices including a policy library with prewritten policies, detailed information on U.S. and international privacy laws, checklists and templates, as well as a discussion of the Organization for Economic Co-operation and Development (OECD) Fair Information Principles. Those resources are aimed at companies that may not have privacy policies in place but need to do so to provide services to larger healthcare or financial services organizations.

Among the resources is a list of core privacy principles based on OECD principles. Each principle has a question, brief discussion and suggested policy. For example, the purpose specification principle states, "The purposes for which personal information is collected should be specified no later than the time of data collection, and the subsequent use should be limited to fulfilling those purposes or such others that are specified to the individuals at the time of the change of purpose." The discussion includes comments on international laws and a citation of several related rulings.

Plans for Future

Business users and consumers alike have become accustomed to the efficiency and speed of digital data. However, more strict regulations are inevitable. Organizations should become more aware of having to prevent data breaches, and to make sure they have the systems in place to do this. Companies should also be concerned about reputation damage, which can severely affect business.

Along with reliable technology, the best way forward is to follow best practices with respect to data privacy. Technology is essential, but it also has to be supported by people and processes. Once aligned, in order to determine whether you are succeeding, create a series of success metrics which will help to align your team as well as demonstrate if you are improving along the way.

Final Recommendations

Your organization will not master data security with its first effort. It is important to realize that securing your data is an iterative process that needs to be closely monitored and improved upon. Leveraging tools like dashboards and reporting can provide a quick snapshot of your key metrics and enable you to communicate your progress effectively across stakeholders. Setting up regularly scheduled meetings to review the execution of your data security initiative and how it aligns with your overall business and security goals is vital. Re-assess the set of metrics and processes periodically if you find data security initiative is stalling.

Data breach prevention is possible. By starting with these best practices, you can help keep your infrastructure secure and mitigate the costs associated with a hack.

Galaxy Consulting has 16 years' experience protecting organizations' data. We have done it for many companies. We can do the same for you! Contact us today for a free consultation!

About Galaxy Consulting

Galaxy Consulting provides services in business analysis and usability, content and knowledge management, records management, information architecture, enterprise search, taxonomy development and management, document control, and information governance.

Galaxy Consulting was founded with the mission and vision of helping organizations to manage their valuable information assets. Many of our clients, both large and small, have dramatically improved efficiency and reduced unnecessary labor hours through efficient methods, processes, and solutions we created.

Galaxy Consulting believes in partnerships with our clients. We are committed to working with you and to helping you transform your business. We will increase efficiency and productivity, maintain regulatory and legal compliance, improve collaboration, enhance innovation, and reduce costs through effective information management!

Call us TODAY to schedule a free, no obligation consultation!

Contact Us

Office: 650-474-0955
Mobile: 650-716-3609
Info@galaxyconsulting.net
www.galaxyconsulting.net