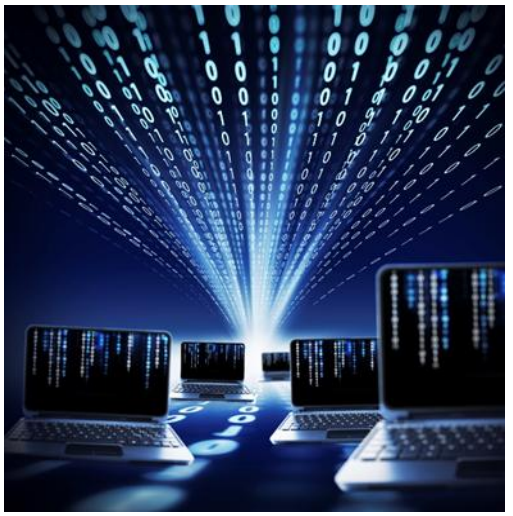
GALAXYCONSULTING
Information Management Solutions

Issue 3 March 2016

Data Security

How to Prevent Risk



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

In This Issue: Data Security

Data Security

By Eleonora Babayants

Data security should be a priority in your organization.

For hackers, large-scale data breaches such as Home Depot, Neiman Marcus, and Staples are gold mines. For businesses, keeping valuable customer data out of the hands of cyber-thieves is a constant battle. Companies need to safeguard against every possible vulnerability across their entire infrastructure.

In 2014, the total number of reported data breaches in the United States hit a record high of 783, averaging about 15 per week, based on information compiled by the Identity Theft Resource Center (ITRC).

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.

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.

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.

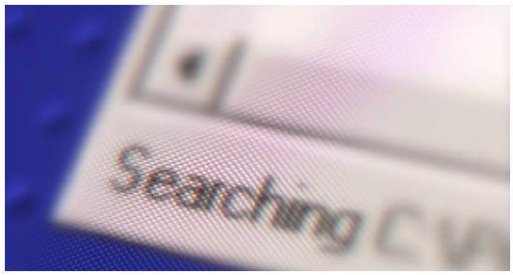
This prompted Forrester to conclude that most enterprises will not be able to respond to a data breach without undermining their customers' trust or dragging their own corporate reputations through the mud.

Companies need 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 reduce the cost of breaches significantly and goes a long way toward reassuring customers who might have been thrown into a panic.

Data security 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.

Data security is 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.

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



Data Security

Data security should be a priority in your organization.

How to Prevent Risk

The key is to make sure that you are not leaving the front door open for hackers to get in.

Industry News

- New SaaS Discovery Platform from Content Analyst
- Knowledge Gamification from RightAnswers
- Content Analyst and BA Insight Partner
- Search Technologies Unveils Aspire for Elasticsearch

How to Prevent Risk

by Eleonora Babayants

The first step toward data security is having a high-level company executive who is responsible for data security. The key to addressing information security is first understanding what customer information is stored in company databases. Create a data inventory and determine what data is sensitive. Then segment out the sensitive and non-sensitive data.

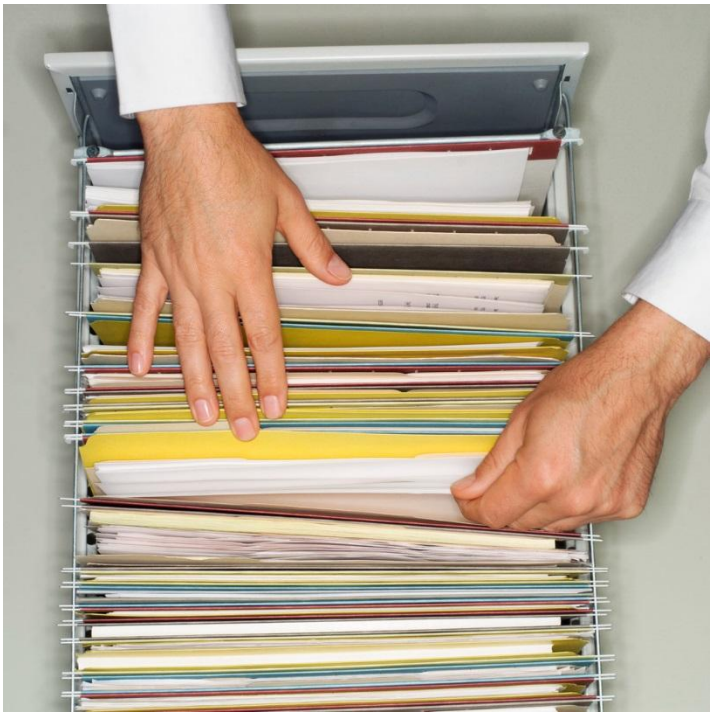
Systematically purge the data that your organization no longer needs.

Take an inventory of all of their 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.

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.

Contact centers are vulnerable to hackers. They use interactive voice response (IVR) systems for surveillance and data-gathering as a precursor to phishing schemes with agents, who are unwittingly coaxed into giving out sensitive information to unauthorized callers. In most cases, the call center agents is tricked by skilled fraudsters who use a variety of social engineering techniques to get them to break normal security procedures. The only real defense is proper training and protocols.

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.

Even worse than careless employees or outside hackers, though, are the contact center agents who knowingly engage in illegal activities, using their jobs to gain access to information that they can sell or use on their own.

To help contact centers deal with this threat, call center technology can completely prevent skimming by agents. At the point in the transaction where the agent needs to collect the credit card information, systems can automatically pause recordings. With other solutions, the call can be transferred to an IVR system. Agent-assisted solutions can allow agents to collect credit card information without ever seeing or hearing it. The agent remains on the phone and customers enter their credit card information directly into the system using their phones' keypads. The standard dual-tone multi-frequency tones are converted to monotones so the agent cannot recognize them and they cannot be recorded.

In this environment, contact center managers and other employees need to be trained to spot at-risk employee behaviors. Training alone, though, is not enough. Employees need to know that there will be serious repercussions for violations of company practices and security protocols. Companies need to have a clearly defined formal policy so that employees know if they violate it, there are consequences that they will have to face.

Companies need to foster a security-aware culture in which protecting data is a normal and natural part of everyone's job. 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.

Companies need to foster security aware culture in which protecting data is a natural part of daily work

Industry News

New SaaS Discovery Platform from Content Analyst

Content Analyst has released Cerebrant, which the company describes as an SaaS-based discovery platform designed to enable subject matter experts in any industry to gain rapid insight into the ever-increasing amount of unstructured content they must analyze.

Further, it says, Cerebrant enables users to quickly and effectively find the most relevant internal and external content and discover important, non-obvious relationships buried within massive collections of unstructured information.

Knowledge Gamification from RightAnswers

RightAnswers has introduced gamification to enhance enterprise knowledge and improve customer service by driving the right behaviors. The company says RightAnswers gamification encourages customer service agents to contribute to the knowledge and improve its quality, resulting in an up-to-date knowledgebase that can better resolve customer issues.

The company explains that companies using gamification can assign points to behaviors they want to promote, such as creating or updating a knowledge article, sharing knowledge with peers, etc.

Content Analyst and BA Insight Partner

BA Insight and Content Analyst Company have formed a strategic alliance to safely access large internal collections of high-value, unstructured content for insight and discovery within several key vertical industries.

The companies say Content Analyst's Cerebrant SaaS-based discovery platform, combined with BA Insight's Content Connectivity software, enables users in health information, energy, financial and other key verticals to securely connect to the repositories of unstructured content residing in enterprise portals, databases, mailbox and archiving systems, CRM applications, content and collaboration platforms, etc.

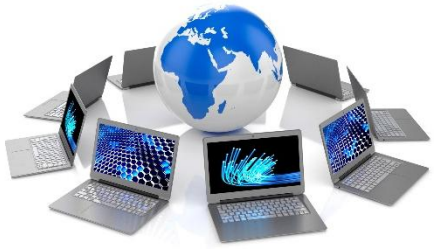
Search Technologies Unveils Aspire for Elasticsearch

Search Technologies has launched Aspire for Elasticsearch, which is designed for customers that need to ingest unstructured data from multiple content repositories, process that content and index it in Elasticsearch.

Aspire for Elasticsearch, which is part of Search Technologies' Aspire family, is a robust content processing framework developed primarily for handling unstructured data for customers to clean, enrich and normalize content ingested by Elasticsearch. It includes connectors for file systems, RDBs and Web content.

Additional Aspire connectors for many other popular content repositories can be licensed to support the ingestion of content and metadata, including document security ACLs, if present, enabling full document-level security to be implemented within search and analytics applications.

About Galaxy Consulting



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

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.