FORTRA

WHITE PAPER *(Titus)*

Classification is a Business Imperative

Data Security

The responsibility of securing organizational data needs to be in the hands of anyone who creates it, and not lie solely with the IT department. Unsecured data leaves organizations open to lost intellectual property, significant fines, loss of investor trust, loss of clients, and lawsuits. With the proliferation of data sharing applications, mobile device and remote access, the task of securing data has become too great a responsibility for the IT department to manage effectively on its own.

While technology has the potential to help enforce data security policies, without a pervasive culture of data security users fail to use the technology properly. Either due to a lack of training or the complexity of the security tools, studies continue to show that employees frequently violate information security protocols. And worse, many employees use methods to circumvent security technologies they feel hinder efficient workflow. This combination of data sharing technologies, poor training, and indifference to security policy converts the people inside your organization—those that should be the most trustworthy—into one of the biggest data breach risks.

> ***Data discovery and classification are two essential, yet often overlooked, initiatives that lay the foundation for protecting data.***
>
> **— Heidi Shey & John Kindervag**
> Forrester Research Inc.
> Strategy Deep Dive: Define Your Data.
> April 2013

To secure data, senior executives must set the foundation for a culture of information protection, which includes executive support and involvement, user training and guidance, easy to use technology, and data classification. Classification is foundational to securing your information as it allows users to quickly and easily indicate the value of the data to the organization. The classification is applied as visual markings (to alert end users), and persistent metadata (to inform security technology systems). The process of classifying has the added benefit of acting as a constant reminder to workers that the information they handle has value and its protection is essential. Empowered by the classification, the entire security ecosystem has the knowledge it needs to manage the information according to security policy.

The Data Security Imperative

At the heart of any organization is the data that powers it. From financial data, to employee files, to new ideas and inventions, your organization is filled with information that, if lost or stolen, could seriously impact your business. The proliferation of data sharing tools, such as email, social media, mobile device access, and cloud storage media are making it harder for IT and data security departments to keep your sensitive information from moving outside the central network perimeter. The reality is that the data security perimeter is forever changed as data is accessed and stored in multiple locations.

In 2013, an average of 26.6% of information workers used at least three or more devices (laptops, desktops, tablets, mobile phones) for work.i To make managing information on these various devices easier, workers are using mobile storage media and cloud services to transport your organization's valuable information. With workers uploading data to a wide array of unsecured data sharing solutions, the people you have working inside your organization pose one of the biggest data security threats.

In fact, there is a 60% chance that your organization's data has been seriously compromised without triggering an alert to the security team.ii Even more troubling is the fact that the average time between a data breach and when it is discovered is over 200 days.iii And to add insult to injury, 69% of all breaches are discovered by others outside of your organization, such as your partners and customers.iv It is time to face the fact that your data is slipping through your perimeter like sand through a clenched fist.

It is important to note that the insider threat is not just a malicious user or disgruntled employee, but could also be trustworthy employees who are just trying to work more efficiently. When workers are unfamiliar with correct policy procedures and there are no systems in place to train, inform, and remind them, they engage in risky information handling. Insider breaches, therefore, are not just a technological issue, but a human and cultural problem. You can install technologies to prevent uploading data to a cloud service, but if your users don't understand the value of the data they are using they are likely to see the technology as an impediment to their workflow, and actively seek methods to circumvent security.

From a data protection strategy point of view, the trend to keep all data forever is also having a negative impact on data security. As storage costs dropped, the attention previously shown towards deleting old or unnecessary data has faded. However, unstructured data now makes up 80% of non-tangible assets and data growth is exploding. IT security teams are now tasked with protecting everything forever but there is simply too much to protect effectively—especially when some of it is not worth protecting at all.

Inadvertent misuse of data from insiders tops the list of breach causes in 2013, responsible for 36% of breaches seen in Forrester's data.

— Heidi Shey,
Forrester Research Inc.
Understand the State of Data Security and Privacy: 2013 to 2014. October 2013

The Security Culture Imperative

As organizations struggle to meet the challenge of data security, success will only be achieved through strong leadership. Without executive guidance, security is relegated to IT departments that are already struggling for proper data security funding. IT and data security teams do not have the means to single-handedly foster the culture of security that is necessary to prevent unnecessary insider data risks. In contrast, when senior executive sponsorship is communicated directly to the employees it is less likely that the employees will find excuses to resist the change. A corporate initiative with executive sponsorship has a momentum that can compel workers who might otherwise resist a project sponsored only by their team or department leader.

Given the importance data security plays in the health of an organization, it should be considered as a crucial part of business best practices. Just as there are unique best practices in sales, accounting, and human resources, everyone should consider data security as a general best practice for overall success. The most successful companies will be those that place a high value on protecting their intellectual property, customer information and other sensitive data.

Shifting to a culture of data security will only take place when all employees are continually engaging in corporate security processes. Workers need to be engaged in the security discussion in order for them to be invested in the solution. When the CEO communicates to her employees the importance of security for their job as well as for the organization, employees are much more apt to comply. Once the users are on side in principle, it is important to follow up with tools that are easy to use and provide immediate feedback with corrective suggestions when there is a violation.

The Classification Imperative

Classification is the indispensable foundation to data security as it allows users to identify data, adding structure to the increasing volumes of unstructured information. Classifying data provides it with a voice, announcing to both users and security systems the information's value and how it should be handled. When data is classified, organizations can raise security awareness, prevent data loss, and comply with records management regulations.

Classification is effective because it adds "metadata" to the file. Metadata is information about the data itself, such as author, creation date, or the classification. When a user classifies an email, a document, or a file, persistent metadata identifying the data's value is embedded within the file. By embedding classification metadata, the value of the data is preserved no matter where the information is saved, sent, or shared.

From a worker's perspective, classification forces attention toward the value of the data being used, making employees more aware of the information's sensitivity and how it should be handled. As classifications are applied, they can also be added to the data as protective visual markings. When the classification is visible in the headers and footers of an email or document, consumers of the information cannot deny their awareness of the data's value—even when printed—and their responsibility to protect it.

As information is shared, the classification metadata embedded within the file can be used by data loss prevention (DLP) systems, gateways, and other perimeter security systems to enforce safe distribution and sharing. For example, a DLP system may be configured with a policy that restricts documents classified as "secret" from being transferred via USB to a portable storage device. Similarly, policies which stipulate the necessity to encrypt the most sensitive data can easily be enforced. As workers classify, rights management tools can be invoked based on the classification, applying encryption to outgoing emails or to documents being stored into repositories like SharePoint.

Data classification technologies … that involve the user rather than short-circuit the user are more likely not only to reinforce policies, but also to create a sustainable corporate culture regarding data protection over time.

— Derek E. Brink,
Aberdeen Group
Three Steps to Successful Data Classification.
February 2013.

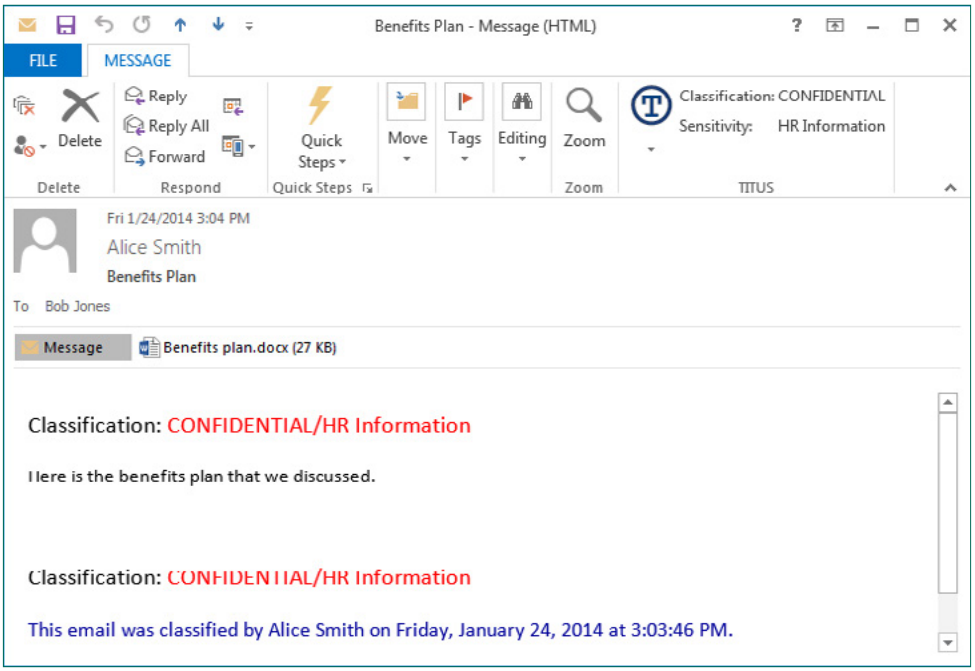

Figure 1 - Classified email showing protective visual markings in the header and footer of the email body.

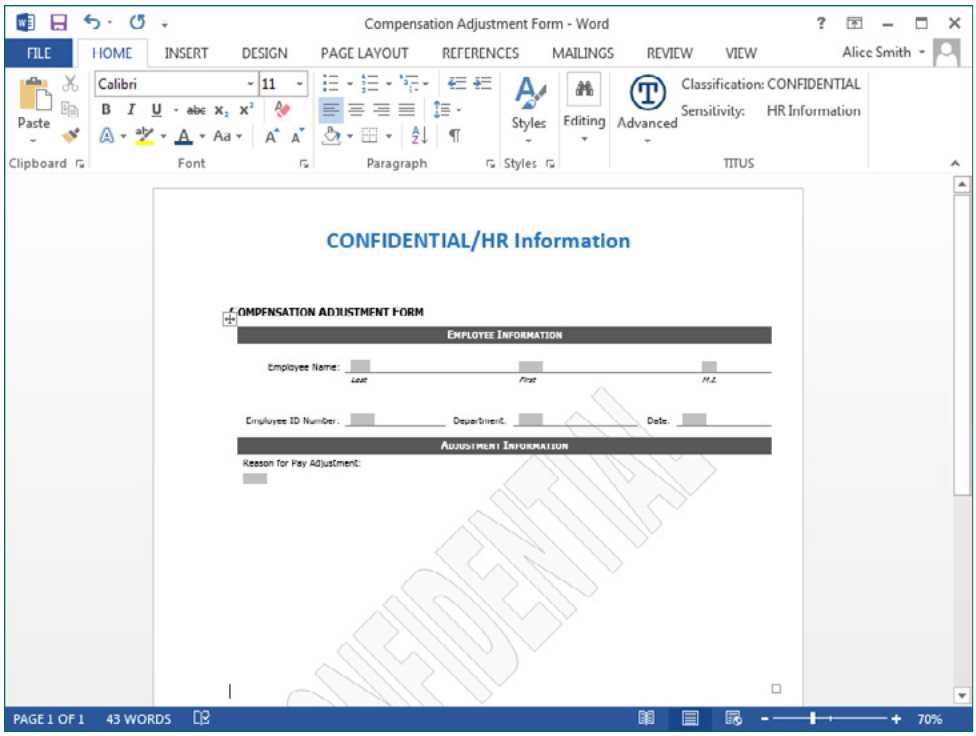

Figure 2 - Document showing protective visual markings in the header and watermark.

Classification can also aid where compliance legislation regulates the protection and retention of company records. By providing structure to otherwise unstructured information, classification empowers organizations to control the distribution of their confidential information in accordance with mandated regulations, such as ITAR, HIPAA, PIPEDA, UK Data Protection Act, SOX, Red Flag Rule, ISO 27001 and many others. As important documents, regulated records may also need to be retrieved quickly for auditing or legal discovery purposes. Classifications can be configured to include additional information indicating into which department and records management category the data belongs. This extra information not only enhances retrieval but can also be matched to retention policies governing how long to keep the data and when it can be safely destroyed.

When classification becomes a part of everyday workflow, security awareness and risk mitigating behavior takes root within the corporate culture. As employees classify, they are reminded to handle data securely. And when data is classified, it contains metadata values the entire security ecosystem can leverage to enforce appropriate information governance and prevent data breaches.

The Titus Advantage

As the leading provider of user-based email and document classification solutions, Titus offers a complete classification management solution for both private and public organizations. Titus products include:

- Message Classification™ for the classification of email in Microsoft Outlook®, Outlook Web App®, Lotus Notes®, and mobile devices.
- Classification™ for Microsoft Office™ for the classification of Microsoft Word®, PowerPoint®, and Excel® documents.

- Classification for Desktop™ for the classification of any file type in Windows Explorer®, including Adobe PDF®, multimedia files, and CAD documents.
- Classification and metadata security solutions for Microsoft SharePoint®

Titus solutions are trusted by over 2 million users within more than 600 organizations in 60 countries around the world. Our customers include: Dell, Nokia, Dow Corning, Pratt and Whitney, United States Air Force, NATO, Canadian Department of National Defence, Australian Department of Defence, and the U.S. Department of Veterans Affairs.

To learn how Titus can help your organization implement its classification policy, please visit: ***www.titus.com***

End Notes

[i] *Understand the State of Data Security and Privacy: 2013 to 2014*. Forrester Research, October 2013. PDF.

[ii] *Maximizing the Business Value of Information: New Principles for Using and Securing Information.* The Corporate Executive Board Company, 2013. PDF.

[iii] *2013 Global Security Report*. Trustwave, 2013. PDF.

[iv] *Verizon 2013 Data Breach investigations Report*. Verizon, 2013. PDF.

FORTRA

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.

