FORTRA

GUIDE

Data Classification: The First Step To Protecting Unstructured Data

Including

- The changing threat landscape
- How tracking and protecting data is increasingly hard
- Shifting the focus to the data
- Where do you start?
- Best practice: user-driven data classification

Indroduction

Today's organisations are attempting to protect their valuable and sensitive information in a volatile threat landscape. Keeping data secure is no longer a matter of building a neat boundary around the company's databases, networks and IT systems so hackers can't get at them. The greatest risk to data security is a threat coming from a new direction: the accidental data loss from within the organisation.

The individuals involved in this threat are not malicious, sophisticated external attackers who can be kept at bay by firewalls and other perimeter defences. They're well-intentioned employees going about their jobs, using standard software and tools to generate and share the content we all use on a daily basis.

Data security breaches and data loss incidents can have a huge impact on brand reputation, shattering customers' trust and loyalty. They hit a company's market value, causing the share price to drop. Loss of intellectual property (IP) can eliminate competitive advantage. In addition, significant fines can be imposed if regulations such as the Data Protection Act, GDPR, CCPA and ITAR regulations for export control are breached, while the post-event clean-up costs can be massive. This is why data protection is higher up the boardroom agenda than it's ever been.

In this whitepaper, we look at how the threat landscape has changed for businesses, the drivers behind the change – both technical and cultural, and the challenges involved in managing, controlling and protecting data. We then introduce a data-centric approach to security which involves users themselves in classifying information, with practical guidance on how to take the first steps in deploying an organisation wide user-driven data classification policy.

The Changing Threat Landscape

The shift in threat is partly down to the evolving nature of work; the collaborative, highly interactive environment in which organisations and their employees now do business, sharing information and ideas through an expanding variety of platforms.

The change in direction of the information security threat from outside to within the organisation has been driven by technology developments that have transformed the way data is accessed, processed and stored. The number of communication channels and devices at our fingertips has proliferated, and their diversity has increased.

Smartphones allow us to be always connected, always 'on'. The availability of collaboration tools like Microsoft SharePoint enables – and encourages – us to share files.

The emergence of Bring Your Own Device (BYOD) and Choose Your Own Device (CYOD) means employees are using the same device for personal and work tasks, and combining the two kinds of data. Employees can sync files across devices for easy access wherever they're working. They can sign up for mobile apps and services that will boost their efficiency and productivity, like Dropbox, without needing to involve IT, and then access them from any browser.

According to IBM, 95% of data security incidents are a result of human error.

We've all been empowered by this new culture of collaboration and flexibility. We're able to communicate, transact, share and work on data with colleagues, partners, suppliers and customers more freely and productively than ever. However, this also leaves the business exposed. The majority of employees' data access, processing, using, sharing and storing is now done independently of IT – and so it's invisible to IT and IT security departments. If an employee owns a device, their employer's ability to control how it's used is limited. When data is stored in the cloud, IT can't control access to it in the same way as data located in on-site physical infrastructure. Combined with the vulnerabilities inherent in some tools and apps not designed for enterprise use, and the ease with which mobile devices can be lost or stolen, this opens the organisation to accidental data loss.

The traditional security perimeter around an organisation has disappeared to be replaced by a dynamic one that needs to be extended all the time to counter new threats around data loss. With patrolling and reinforcing the perimeter no longer enough, businesses must take a balanced approach to their data security strategy – an approach that considers the asymmetrical threat, and guards against accidental mishaps, as much as protects against malicious threats from outside. The challenge every business faces is how to integrate security into the new corporate culture in a way that embraces and fosters, rather than inhibits and restricts, the greater power employees now have to communicate.

Tracking And Protecting Data Is Increasingly Hard

Creating content is easy. As a result, there are huge and ever-increasing volumes of unstructured data inside every organisation: email messages, Word documents, PowerPoint decks, Excel files, images and videos. Data management can simply struggle under the weight; because you don't know what you've got or what's truly valuable you keep everything, and treat it at the highest security level as a default. This leads to higher data protection, storage and retention costs.

When your systems are choked, data governance and compliance with ever-tightening regulations being enforced globally becomes extremely difficult. Again, you don't know what you've got, how sensitive it is, or where to find it. Nor do you know what controls you need to put on it to ensure it's adequately protected.

It's also hard to 'pin down' data. Information is distributed across multiple devices, databases, systems, offices and storage locations – both physical and virtual – in myriad different forms. The employees handling it are mobile, so the data is mobile; it's being taken outside the boundary of the organisation all the time. Data is more shareable and easy to modify than ever, with the click of a key or a button. You may have a data security or classification policy, but how do you enforce it across so many touchpoints, and without supporting processes and rules that are so complex and obstructive that business is slowed down and employees find workarounds?

The only solution is to take a data-centric approach to control and protection.

The True Cost Of An Accidental Data Breach:

TalkTalk

- £60m in business cards
- Loss of over 100,000 customers
- 50% decline in pre-tax profits

Sony

- $416k fine from the ICO
- $272m hit on operating profit
- 9% decline in share price
- $1.25bn estimated lost revenue

Target

- 11% drop in share price
- 46% decline in profits
- $61m in clean up expenses in one quarter alone

BAE Systems

- $78m fine levied for over 2,500 ITAR violations going back to 1995, due to failure to obtain export control approval for equipment on US Munitions List (USML)

Shifting The Focus To The Data

An approach that puts the data itself at the heart of the security strategy – as opposed to the network, application, system, device or the person handling it – focuses as much on appropriately protecting the most critical or sensitive data as on external threats and perimeter defences. The protection has to travel with the data, through its journey. To achieve this, the organisation must break down data silos and treat data as a whole, organic asset. That's the reason Gartner is calling for the availability of data-centric audit and protection (DCAP) solutions that will enable businesses to develop and apply a consolidated data security and governance policy across big data, cloud, databases and files.

One of the core capabilities of DCAP is data classification – and both Gartner and Forrester acknowledge that this is the first foundational step to achieving data-centric security. By applying user-driven data classification at the core of a layered data security approach (which may also include data loss prevention (DLP) or data governance tools, encryption and rights management) organisations can identify the value of their unstructured data and consistently and effectively control the use of it.

Where Do You Start? Before You Can Defend, You Must Discover

Before you know what protection your data requires you need to know what you've got, where it's stored, why you have it and who has access to it.

Once you've got to grips with that, you can identify what is of true value to the organisation – what's business-critical and what's sensitive – and then how to best to treat it. This valuable data might include intellectual property such as product designs and formulas, strategic plans, personal details, contracts and agreements, regulated documents and plans for investment.

Think about what the impact would be if the piece of information was leaked or lost. If it was made public, would it harm the business, or your customers, partners or suppliers? Would it put an individual's security or privacy at risk? Would you lose advantage if a competitor got hold of it? Is it subject to any privacy or data laws, or compliance regulations? Would its loss breach a contract or agreement? Would it incur a cost? Would it damage the brand? Would you lose your job?

Next, decide how to classify the data.

Best Practice: User-Driven Data Classification

Data classification involves the user attaching an appropriate identifier or label to a message, document or file, to give the data a value and let other users know how it should be handled or shared. By classifying data according to its value to the business, organisations can develop more effective data-centric security approaches that safeguard against accidents and reduce risk.

The Maginot Line Principle

The Maginot Line was a line of concrete fortifications, obstacles and weapons installations that France constructed along its borders with Germany in the 1930s. This costly barrier was impervious to most forms of attack.

The French thought they understood the shape of the threat, and could defend against it by building a wall behind which life could go on as normal. The French people were simply not involved in their own defence. The attack, when it came via Belgium, outflanked the line and France fell within six weeks.

The boundary between inside and outside the organisation is increasingly blurred, and your users are the front line. Until you raise their awareness of cyber security and provide them with simple, easy-to-use tools to help them protect themselves, you leave yourself wide open to the next type of attack. If you empower them, you have lots more eyes and ears managing the security risk, without any significant additional investment.

Every company has a choice – keep trying to build a Maginot Line around the organisation or take a smarter route to proactively managing data loss by involving users in data classification.

Using classification tools to implement the approach allows data security controls, rules and policies to be more consistently enforced. These tools apply clear, consistent electronic markings to any type of file and message – for instance 'commercial in confidence', 'internal only', 'public' – and then allow it to be saved or sent only in accordance with the rules that correspond to that marking.

This type of tool plugs into and works seamlessly as part of standard office productivity applications such as Microsoft Office, Outlook and Lotus Notes, to make classifying messages and files as simple and unobtrusive as possible.

IBM estimates that between 0.5 and 2 percent of an organisation's data is critical – i.e. it has a significant financial value to the organisation. This critical data can account for up to 70% of a company's brand or market value.

Metadata: The Magic Ingredient

Most importantly, as well as attaching the label in a visual form, classification tools apply it as metadata, embedding a tag into document or file properties that stays with it wherever it goes. This helps shield the business against accidental data loss – for example, a diligent employee emailing a sensitive document to their home PC to work on at the weekend or someone saving a confidential file in a public folder with the slip of a key.

Attaching the label in two different forms means the value of the data is clearly displayed to the user, while the metadata can be used to direct other security and data management solutions downstream.

Classification that involves metadata labelling drives greater efficiencies across other enterprise security solutions and information management technologies, including DLP, information rights management (IRM), encryption, gateways and event monitoring (SIEM). The marking enables them to apply more accurate security decisions to data by triggering rules so that, for example, any documents or files marked 'Confidential' might be automatically encrypted by an email gateway tool, or blocked from being uploaded to the cloud by a DLP solution.

By avoiding the need for solutions to scan content to work out how confidential a piece of information is, the user-applied classification label reduces false positive errors which can slow systems down, cost a great deal to correct and reduce user trust.

Introducing The Human Element

While it may seem like a 'low maintenance' option, relying on software and tools alone to automatically classify data is a flawed approach. It's easy for an electronic solution to make errors – scanning an email, judging it to be a threat and quarantining it without the user ever knowing, for example.

The most effective approach involves the user in the process. The employee themselves places the identifier on the information at the point of sending or saving it, deciding which classification to apply within a particular context – something a computer just can't do with any real accuracy. For instance, while a document might not be confidential, and the content of an email message might not be confidential, when the two are combined the result could be a message that needs to be treated as sensitive. It's highly unlikely that an automated classification application would pick up on this, as it lacks the vital context that only a human can apply.

For user-driven data classification to work, you need to set a clear policy that enables users to make fast and intuitive decisions about how each document, message or file should be marked. Use clear labels and terminology that will be instantly recognisable and meaningful in the business context, and keep the number of different identifiers to a minimum.

The successful deployment and enforcement of any policy depends on selecting a tool that enables you to consistently apply your classification scheme across the organisation; one that involves your employees, is intuitive to use and adds the all-important metadata. Roll it out to super-users, then gradually across the whole business.

At the same time, consider the improvements that data classification labels can make to other security and data management solutions that you use or may be planning to implement.

> "In today's markets of disappearing perimeters between an organisation and its partners, the need to better manage data and information is critically important.
>
> The basic platform for this has to start with information classification – only through effective classification at the point of creation can the rest of a GRC or information management strategy be put in place Classification allows for better DLP, internal and external document routing, reporting against risk and governance needs, and also happier end users."

Conclusion

Data security is not just a technology issue – it's also a culture issue, which can be enabled by the empowerment of users and application of technology. In this world of shifting security threats, protecting data must become the responsibility of everyone in the organisation who creates, receives, uses, amends, holds, saves and shares data. That's probably everyone.

Used as a core part of a data-centric security approach, a data classification solution which is driven by users will be instrumental in achieving the company-wide culture change required.

It will cut across organisational silos, ensuring that everyone handling data is aware of how to treat it and protect it. It will raise users' awareness of the importance of data security, as well as their own role and responsibilities in it. People will become more mindful of their security decisions, stopping and thinking about the value of what they're creating, sending or saving.

The 5 Steps To Data Classification

1. **Identify** - your sensitive and high value data
2. **Discover** - its location & accessibility
3. **Classify** - data according to its value to the organisation
4. **Secure** - employ security control & protection measures
5. **Monitor** - measure & evolve security practices

By adding an element of automated enforcement, classification tools will simplify the process and make it more efficient, ingraining it into employees' daily processes and workflows and triggering the right behaviour.

At the same time, they will prevent organisations becoming paralysed by over-protective or onerous manual classification processes, allowing them to realise the full benefits of flexible and mobile working, collaboration and a free flow of ideas.

The outcome is an organisation that's security-aware from top to bottom, in which all employees are engaged, committed and empowered to identify, manage and control sensitive data.

Global brands trust us to protect their sensitive data:

pwc

Ministry of Defence

Honeywell

PRUDENTIAL

DEPARTMENT OF DEFENSE UNITED STATES OF AMERICA

AMGEN

SOCIETE GENERALE

Allianz

Raytheon

More Information

For more information about how you can implement a data classification solution as part of your data protection strategy, please **contact us**

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.