TECHNICAL WHITE PAPER

Knowledge is power: How understanding your data can prepare you for the **EU GDPR** and prevent **data breaches**

egress®

Faced with an ever-changing threat landscape and the need to comply with assorted data security regulations, it can be difficult for organisations to keep on top of information security trends.

Nonetheless, there are some pressing issues that require prompt action, and IT decision-makers should be aware of two things:

1. Data breaches are becoming increasingly prevalent.
2. The upcoming EU General Data Protection Regulation (GDPR) is set to transform the way organisations store, secure and retrieve sensitive data. This includes not just personally identifiable information (PII) about customers, but sensitive commercial data as well.

Accordingly, many organisations are taking action to solve these issues simultaneously. They want to implement data security solutions that prevent data breaches and also help them meet the new, more stringent and punitive compliance requirements of the GDPR. In this white paper, we're going to be taking a look at the best ways for organisations to do this, the key idea being that having a deeper understanding of the types of data your organisation holds and shares is crucial for both GDPR compliance and the prevention of data breaches.

Why is this important?

Well, as the UK's Information Commissioner Elizabeth Denham stated at the 2017 Data Protection Practitioners' Conference, the GDPR is "a framework that should be used to build a culture of privacy that pervades an entire organisation."

This organisation-wide culture of privacy is exactly what an understanding of data promotes, and is exactly what works in the prevention of data breaches. Since every person in every organisation accesses and shares some amount of data, securing / protecting it needs to involve everyone. With every user accessing some quantity of data, it is not enough to invest in security solutions for a subset of the organisation, such as providing email encryption functionality for one team.

> "The GDPR is a framework that should be used to build a culture of privacy that pervades an entire organisation."

Also, people usually unintentionally have access to much more sensitive data than they should. The lack of visibility that IT administrators have over how their users are accessing and sharing sensitive commercial content and PII leaves their organisation at risk of a data breach, whether through human error or internal and external maliciousness.

Yet, how are organisations supposed to adequately protect sensitive data when they don't know what is sensitive, who has access to it or how it is being used?

Risks and consequences

Data breaches increasingly make the news. Companies who have been negligent with the storage and sharing of customer data often find their reputations damaged and finances affected. After Yahoo! suffered multiple massive data breaches, the deal for their acquisition by Verizon was reduced by $350m. Further, fines imposed by regulators can add increased pressure to organisations struggling in the wake of a breach. TalkTalk, for example, received a £400,000 fine from the ICO for failing to adequately protect customers' data and suffering a data breach due to a cyber-attack. Yet despite being a record-breaker, many were quick to point out that this fine is actually very low in comparison with TalkTalk's commercial value and have suggested that a fine under the GDPR would have affected the company much more significantly.

The EU GDPR aims to give users more control over their data, as well as simplify the regulatory landscape within the EU, affecting any country that stores the personal data of EU citizens. One of the major aspects of the regulation is the sanctions imposed if organisations fail to comply and suffer a data breach. This could be a fine of €20m or up to 4% of the annual worldwide turnover, whichever is larger. So the severity of fines imposed is going to increase, and this can only lead to greater reputational damage and financial penalties.

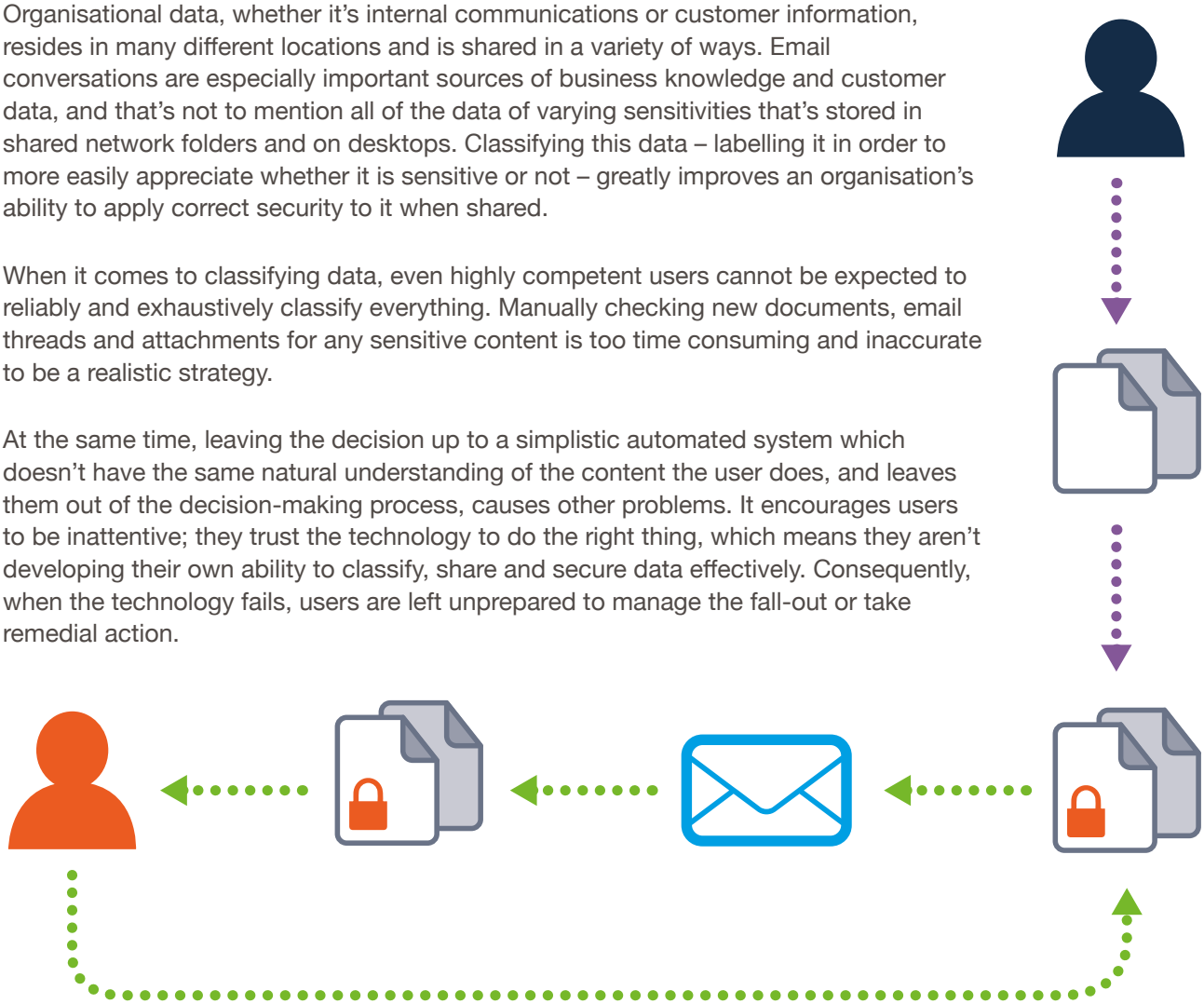
How can you gain a greater understanding of the data you have?

With the GDPR coming into force in May 2018, and many data breaches already gaining worldwide exposure, now is the time to act. The first step is to begin by understanding what data users are creating, sharing and storing.

Organisational data, whether it's internal communications or customer information, resides in many different locations and is shared in a variety of ways. Email conversations are especially important sources of business knowledge and customer data, and that's not to mention all of the data of varying sensitivities that's stored in shared network folders and on desktops. Classifying this data – labelling it in order to more easily appreciate whether it is sensitive or not – greatly improves an organisation's ability to apply correct security to it when shared.

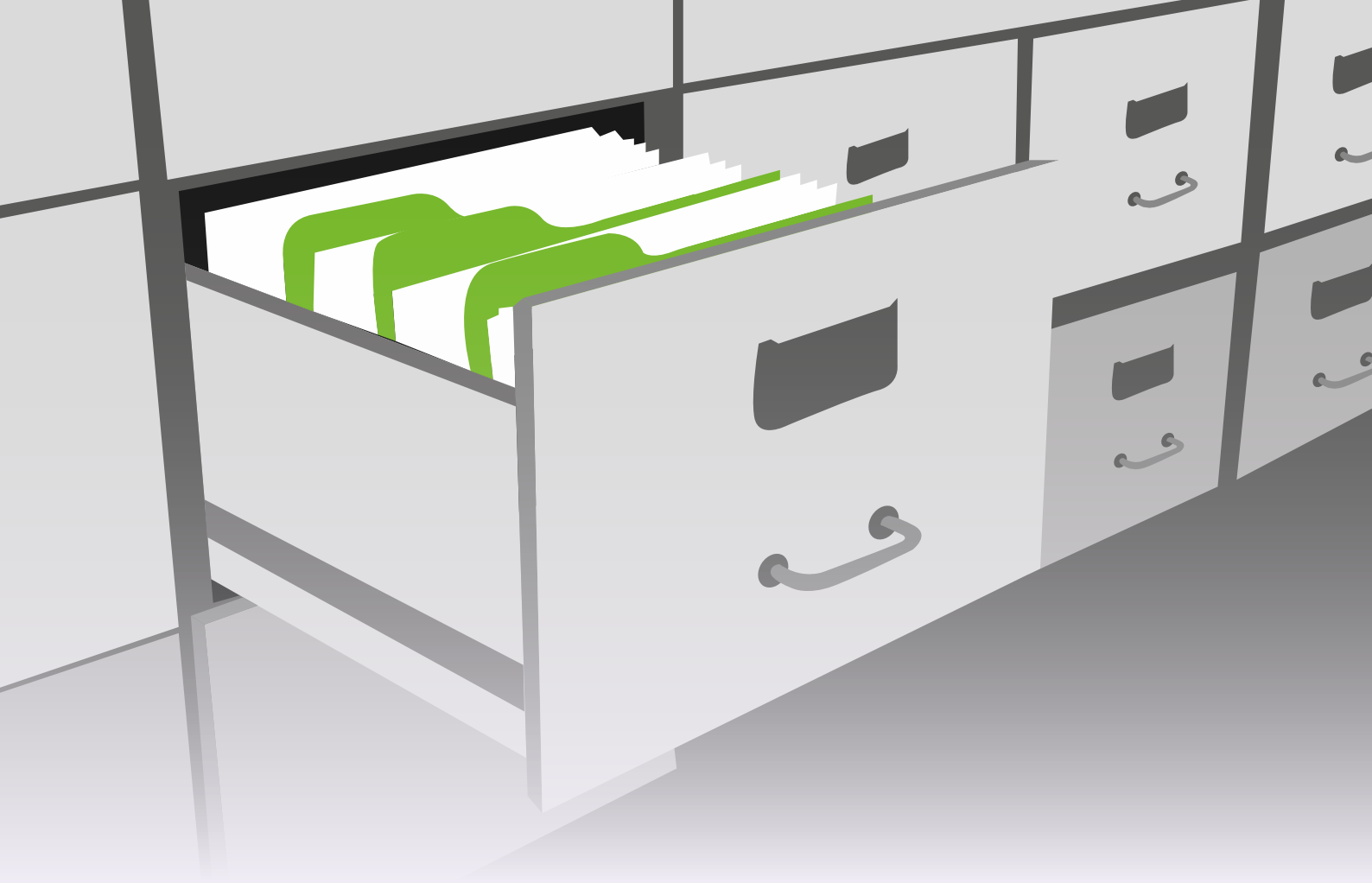
When it comes to classifying data, even highly competent users cannot be expected to reliably and exhaustively classify everything. Manually checking new documents, email threads and attachments for any sensitive content is too time consuming and inaccurate to be a realistic strategy.

At the same time, leaving the decision up to a simplistic automated system which doesn't have the same natural understanding of the content the user does, and leaves them out of the decision-making process, causes other problems. It encourages users to be inattentive; they trust the technology to do the right thing, which means they aren't developing their own ability to classify, share and secure data effectively. Consequently, when the technology fails, users are left unprepared to manage the fall-out or take remedial action.



Instead, using advanced classification technology that works alongside the user provides the best of both worlds. A user's understanding and judgment can be augmented by intelligent software that recognises data and offers advice on appropriate security measures, presenting this information in an unobtrusive, user-friendly way. As such, users improve their understanding of good data security practice but have the benefit of a safety net.

So, the underlying technology should be integrated and cooperative, working alongside rather instead of the user, but how does classification work in practice, and what other features are important?

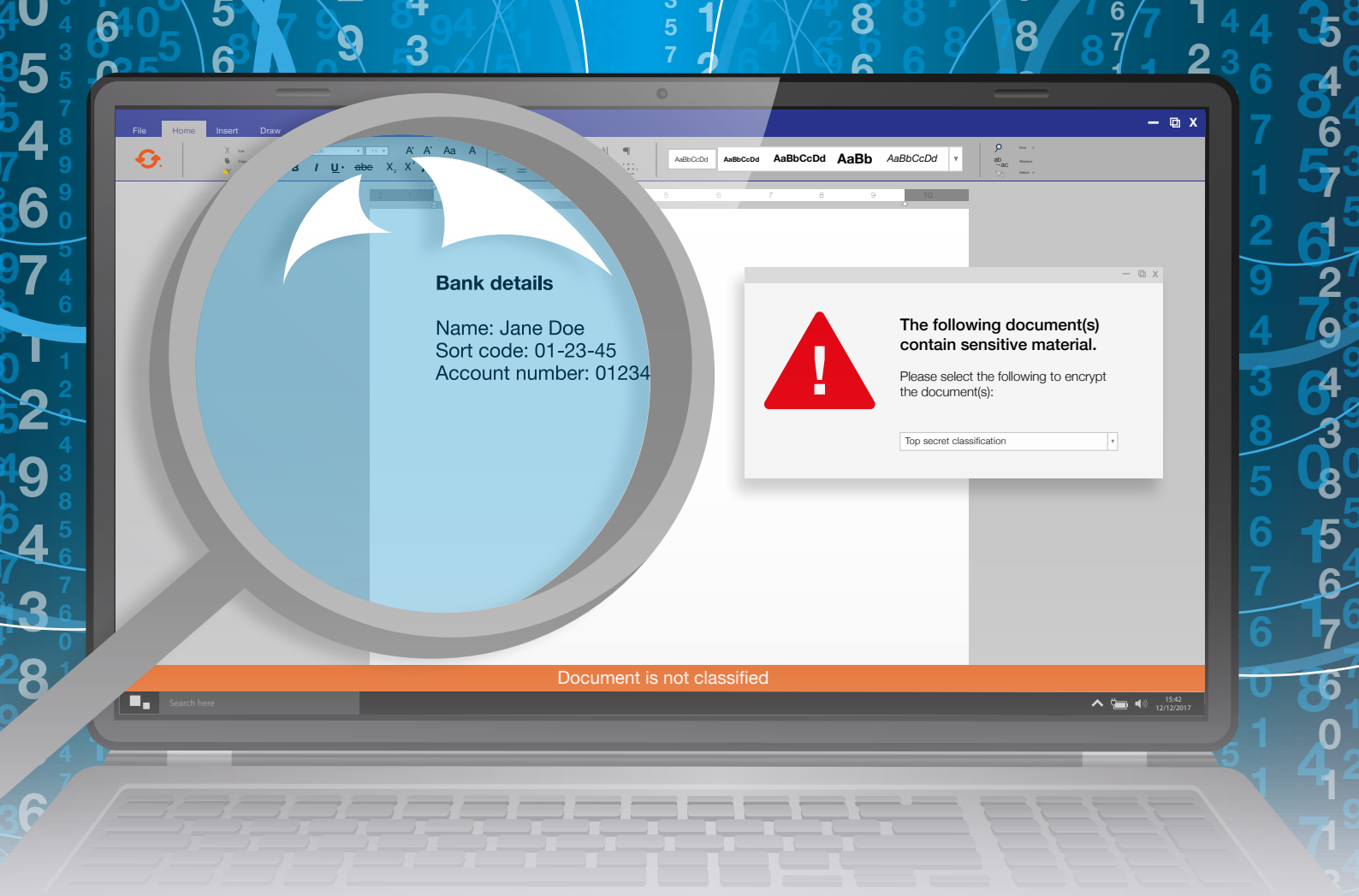


Classification at the point of creation

Classifying information at the point of creation is the crucial first step towards GDPR compliance and data breach risk mitigation.

What does classification entail? Put simply, it's a way of marking a document in a certain way. In practice, classification is most effective when done in two ways. Firstly, visually identifiable information – such as headers, footers and watermarks – are added to the document. This helps users understand the sensitivity of the document they are accessing and sharing, supporting their individual approach to data security and raising the level of data protection in an organisation as a whole. User-centric, visual classification is crucial for reducing incidences of human error and data breaches caused by accidentally sending sensitive data to the wrong recipient.

Secondly, adding meta data to a document when classifying it means it's easy for data security technology to handle the document in a certain manner. This document fingerprinting enables the tracking and auditing of a document's journey, even if it is edited or renamed at a later date. Proof of transmission is hugely beneficial for compliance reasons, demonstrating the veracity of sent documents and specific recipients.



These two classification modes, then, combine to help prevent data breaches and meet regulatory standards. Technology should implement these modes effectively, working with the user to improve their understanding but also ensure mistakes are rectified.

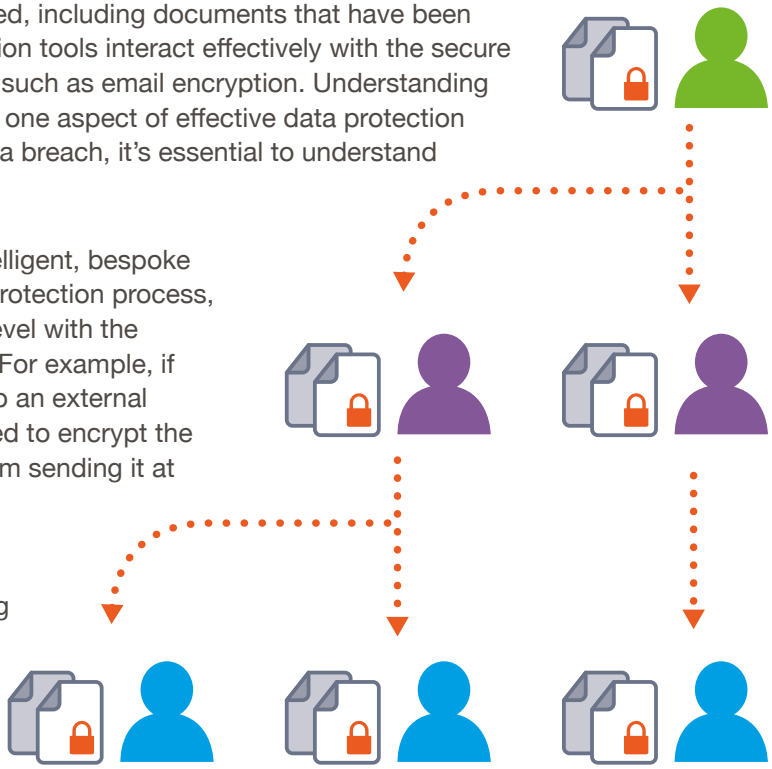
When a user saves a document they've been working on, a classification tool that features integrated data loss prevention (DLP) should detect PII such as bank details or medical records, alerting the user to the potential security risk and prompting them to take action. Do they want to continue and save it without classifying, or they do they want to save the document at a recommended level of classification, such as OFFICIAL-SENSITIVE or SECRET?

Of course, every organisation is different and creates different types of data, hence they have different needs and preferences when it comes to classifying this data. While the underlying technology is the same, organisations should be able to customise the system, using policy-based control to adapt how the classification system interacts with the user. For example, some organisations may require a certain level of classification for specific PII types, and so enforce this, but others may still provide users with an option.

However, classification is only the first step. Its major benefit is that it lets you continually manage, understand and control classified data as it is edited, shared and stored throughout its lifecycle.

What happens to the data next?

Whether intentionally or not, data gets shared, including documents that have been classified. Hence, it's crucial that classification tools interact effectively with the secure sharing setup that organisations might use, such as email encryption. Understanding the types of data sitting in a network is only one aspect of effective data protection strategy. When it comes to preventing a data breach, it's essential to understand and manage how sensitive data is shared.



Email encryption that integrates with an intelligent, bespoke classification system streamlines the data protection process, synchronising a document's classification level with the security applied when it is sent in an email. For example, if a user tries to send a classified document to an external domain, they can be recommended or forced to encrypt the email before sending, or even prevented from sending it at all, depending on the organisation's email security policies.

By encrypting emails and attachments using a suitable method, benefits also include being able to manage recipient access in real-time, revoking access or removing recipients when required.

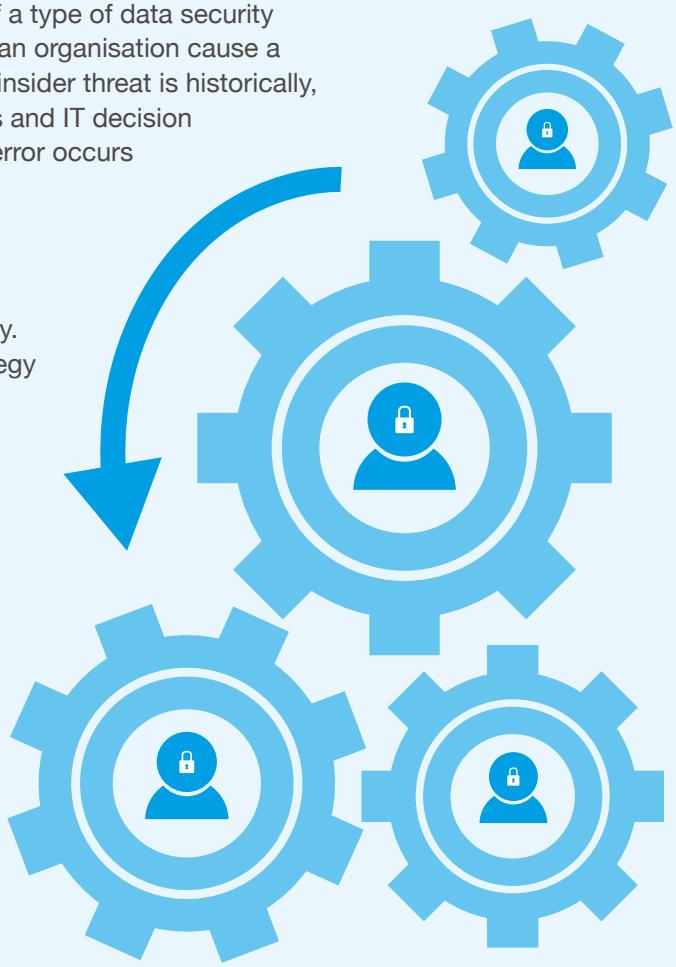
Meta data added to content upon classification can be used for auditing and reporting. If effective auditing is in place, classified documents can be tracked as they are shared, even when edits are made and file names are changed. Many legal and regulatory obligations require proof of both a document's origin and transmission. Comprehensive audit data improves IT administrator and CIO understanding of how their users are classifying and securing data, if at all. This then allows them to make valuable changes to their information security strategy and pinpoint more exactly where improvements are needed in order to maintain compliance. These improvements are usually about targeted user education and training.

Data security is about tackling the insider threat

The effectiveness of user education in preventing data breaches and adhering to compliance obligations should not be underestimated. To return to a point made earlier, data security needs to involve everyone. Everyone shares data, and breaches or regulatory lapses can occur at any level of an organisation, so everyone needs to know what data they hold and how they should treat it.

Human error, due to a lack of user training or a misunderstanding of what sensitive data entails, is a leading cause of breaches. It's part of a type of data security risk known as the insider threat, whereby users inside an organisation cause a data breach – either inadvertently or intentionally. The insider threat is historically, dangerously, misunderstood and deprioritised by CIOs and IT decision makers. This partly due to its abstract nature: human error occurs unexpectedly and erratically.

If the goal is to reduce risk of a data breach and demonstrate compliance to regulations, especially the GDPR, the insider threat needs to be tackled effectively. Reducing the chance for human error is a crucial strategy here, and use of classification is an essential tactic. The right classification solution is one that works with the user in an intelligent, user-friendly way, helping organisations understand how to treat their data securely and compliantly.



Egress Software Technologies Ltd

www.egress.com

info@egress.com
0844 800 0172
@EgressSwitch

Egress Software Technologies is the leading provider of security services that protect shared information throughout its lifecycle, delivered using a single platform: Egress Switch.

The award-winning Switch Platform includes email and document classification, email and file encryption, secure managed file transfer, secure online collaboration, and secure email and file archiving.

egress