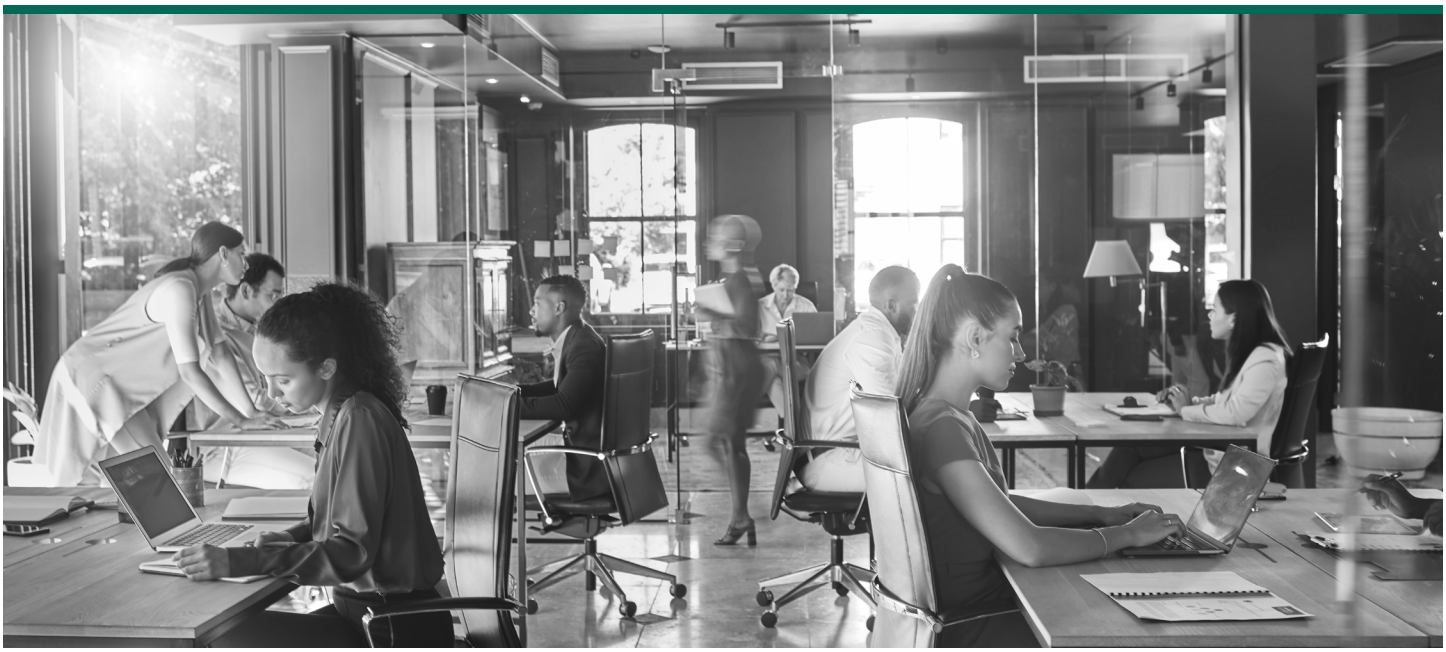
FORTRA

GUIDE (Cybersecurity)

Preventing unwanted sensitive data acquisition on the corporate network

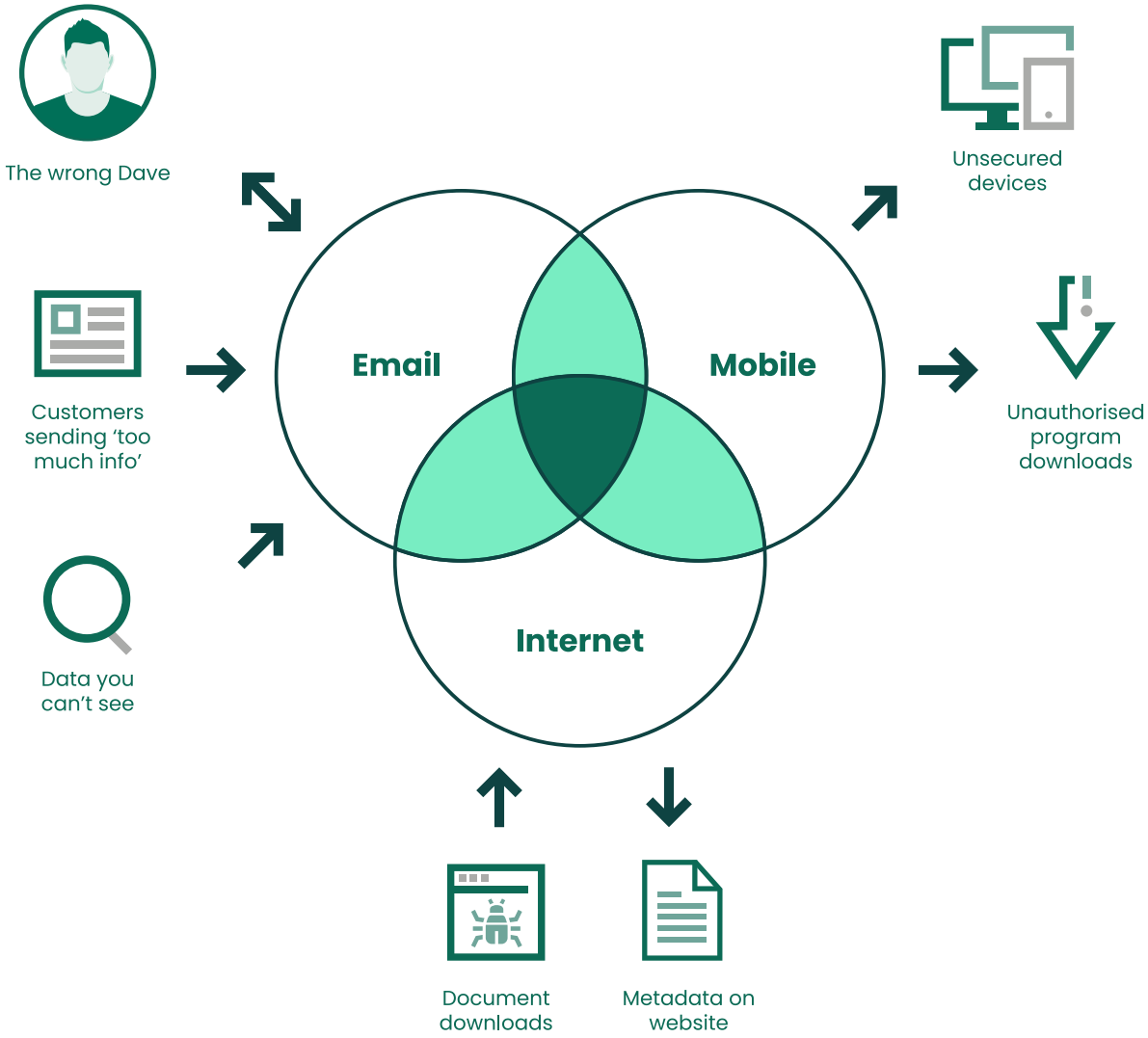
What are the implications for organizations unintentionally receiving and storing sensitive data and how can organizations mitigate against the risks?



As an organization, you will be aware of the 'insider threat' – malicious or inadvertent sensitive data leaks (from within) and the risks they cause to business. But, have you ever considered the risk from acquiring unwanted sensitive information through your digital business collaboration channels and the additional risks this poses to your organization?

Unwanted Sensitive Data Acquisition

What are the risks and where do they come from?



How to mitigate the risks in five easy steps

1.
Educate employees - understand the resks and make them aware

2.
Create and implement data protection policies and processes

3.
Deploy technology to secure email and web collaboration

4.
Regulate removable devices and secure data tranfers

5.
Understand legislation to ensure compliance

The threat of unwanted sensitive data acquisition, the act of unintentionally receiving and storing critical information, is a ticking time bomb for data breaches in the future. In a world of digital collaboration and increasing legislation, the adage 'ignorance is bliss' won't help, especially when it comes to data protection. This paper explores the risks of sensitive data acquisition through the three most widely used digital business collaboration channels:

- **Email** – receiving emails with sensitive information by mistake
- **Mobile** – inadvertent sensitive data transfers onto the corporate network via mobile devices
- **Internet** – acquiring unwanted sensitive data via website downloads.

In a post-GDPR world, organizations are more aware than ever of the need to properly secure sensitive data and the consequences that breaches can cause. An important factor within this is understanding that receiving unwanted sensitive data onto the corporate network, if not appropriately secured, could lead to a €20 million fine.

No matter what vertical or region you operate in, the risks, if left unchecked, have the potential to cause serious issues for non-compliance and should be addressed. Gaining a clear understanding of the issues enables the right measures to be put in place and closes the gaps in your information security infrastructure.

The threat of unwanted sensitive data acquisition through email

Return to sender

In today's technology-driven ecosphere, email is undoubtedly the main tool for business communication, and it's estimated that the average employee receives 121 emails per day. It's therefore no surprise that this business communication channel poses the highest threat to organizations in terms of unauthorized exposure of sensitive information because of the volume of sensitive data constantly being sent and received.

GDPR compliance means that unauthorized access to personal data must be reported to a data protection regulator as it could have a detrimental impact for the individuals concerned. Therefore, if employees receive emails that contain sensitive information unauthorized and ignore the email, neither deleting nor reporting the incident, the company is held liable for irresponsible data handling.

There are a variety of ways that emails can be the cause of unwanted data acquisition and become a compliance issue. A few examples have been outlined below.

'The Wrong Dave' scenario

The most common way an employee can acquire unwanted sensitive data is by receiving it in an email. Consider the situation where an employee needs to send an email with sensitive information either included in the message, or in an attachment. Since Outlook 'stores' the history of email addresses that a person has sent emails to previously, there will often be more than one person with the same first name in an email address – for example, David ('Dave'). In a hurry, an email containing sensitive information could be sent to the wrong Dave. Only after it is sent – sometimes just a split second later – does the sender realize the mistake they have made. But it's already too late; 'the wrong Dave' has now been sent sensitive information he should not have access to. While this can be embarrassing if it's an internal email, if it has been sent outside the organization, then action needs to be taken as the company Dave works for is now responsible for protecting that sensitive data. If the recipient simply deletes the contents without notifying the appropriate department – who can properly 'cleanse' the email and archive systems – the sensitive information remains stored on the corporate network in an unstructured manner. The receiving organization is then vulnerable to additional (often costly) work or even compliance fines should the matter surface later through an audit check, a 'right to be forgotten' (RTBF) request or should a data breach occur.

Customer service/support

Customers often email their service or supplier organizations, or employees of those organizations directly, with a query or request. In many cases, the customer includes sensitive information that the employee should not have access to. For example, an account number would suffice to find and action a request, but the customer may also include their full name, telephone number and email address within the details too. Where a payment needs to be made, they may even include their personal credit card details in the email and these emails remain sitting in the company or employee inbox.

While employees may not think twice about receiving this kind of information, it presents the company with a major compliance issue. The email holds personal details that only certain employees should have authorized access to. This data is classed as 'unstructured data' as it isn't presented in the form of a database. Customer data like this should be processed and appropriately protected in compliance with GDPR.and programs stop at what assets the organization maintains.

'Invisible' (hidden) sensitive data

As well as receiving sensitive data in the body of emails, there might also be hidden information contained in attachments that the employee is unaware of. This could include documents or spreadsheets with hidden columns containing sensitive information which should have been removed. Or hidden sensitive metadata such as an author name, email addresses, or other sensitive data included in a Word file. This unwanted sensitive data acquisition makes it a challenge for organizations to track, protect and/or delete the sensitive data to comply with RTBF requests and GDPR in general.

Technology tips to mitigate unwanted data acquisition risks through email

Organizations should take risk mitigation steps to both improve employee mindset around handling sensitive data, as well as enforcing rules to ensure unwanted sensitive data acquisition is reduced. Technology should be implemented to prevent any mistakes, acting as a 'safety net' for businesses rather than a silver bullet. Clearswift's Adaptive Redaction solution, built into all of its core email security products, detects and removes sensitive information from email messages and attachments before they enter the network.

Rather than a 'stop and block' approach, Clearswift's solution detects and redacts only the sensitive information (for example, PII and PCI data) rather than the stopping the entire email from being delivered. This safeguards employees from unwanted sensitive data acquisition without preventing collaboration and impacting operational efficiency. Further to this, Clearswift's sanitization technology automatically detects and removes 'hidden' sensitive information (such as author names, revision history and more) contained within inbound documents and files via email.

Sensitive data acquisition via mobile devices on the corporate network

Mobiles devices are now part of our everyday lives. From mobile phones and laptops, to iPads, portable hard drives and a variety of other remote devices; each one presents a potential security challenge. Every mobile device connected to the corporate network creates another potential entry point or point of origin for security threats and to prevent this from happening, organizations need to secure their endpoints to ensure the corporate network remains protected.

Unsecured work devices

While malicious attackers can use remote devices as a way to hack into the corporate network, the more common reason for organizations to consider security measures for the endpoint is to prevent the unauthorized transfer of sensitive information. If employees acquire sensitive company data on their work device that is not secured in line with industry regulations – such as GDPR or PCI DSS – the entire company can be penalized. Yet, less than half of organizations have technology deployed to enforce data encryption policies on mobile/remote devices.

Unregulated device connection to the corporate network

More and more often, employees connect their personal devices for work purposes. This means that when they access the corporate network or server with their personal device, they have the potential to:

1. transfer and store sensitive data on their device which is then taken outside of the secured corporate network and cannot be 'discovered' by the company when it does a sensitive data audit, or
2. accidentally transfer sensitive data from their personal device onto the corporate network (for example, family contact details or other sensitive personal information), which the company is then liable to protect.

Unauthorized program downloads

With the use of SaaS programs now prolific, employees will often download tools on their company equipment that are not vetted by the IT team. This use of 'shadow IT' can lead to sensitive data being stored in unknown programs, making it even harder for Information Security teams to locate and secure data and resulting in non-compliance.

Technology tips for mitigating unwanted sensitive data acquisition via mobile devices

Today, it is vital to secure every device and endpoint against both data loss and unwanted sensitive data acquisition and there are several steps an organization can take to secure the corporate network.

The first is to ensure employees are aware of the risk they pose in handling sensitive data on mobile devices. Educating employees on the ways in which their work and personal devices can cause a security issue will ensure they pick up on things such as unwanted data acquisition, malicious threats and data loss risks.

In addition to this, organizations must have processes in place that ensure employees follow correct protocol when it comes to working remotely and transferring critical data onto their devices. For example, allowing employees to only access sensitive information on company-approved devices will limit the risk of unwanted data acquisition going unnoticed, or having a protocol to follow should an employee receive sensitive data that they shouldn't have, or if they've accidentally transferred sensitive information from their device onto the corporate network.

Technology should also be implemented to protect employees and ultimately the business. The first step is to take control of what devices can connect to the network. Clearswift's Endpoint DLP offers a three-fold protection for organizations:

1. Complete device control – Clearswift's Endpoint DLP solution provides a fine level of granular control over removable media devices, including hard drives, USB sticks, CDs, DVDs and a variety of other modern device types, to restrict use to specific device manufacturers, or to individual devices to ensure only that authorized devices can connect to the network.
2. Automated discovery and protection –Using Clearswift's Deep Content Inspection Engine, Endpoint DLP scans the network and 'discovers' critical information wherever it is stored, whether on desktops, notebooks, servers, network or cloud shares. The solution ensures all remote devices are secured with the same protection level as office devices, preventing the copy or transfer of unauthorized information. The transfer of critical information can also be logged, blocked or encrypted to ensure any unwanted data acquisition does not compromise the business if undiscovered.
3. Regulation readiness – The solution also detects and secures critical information based on content or regulation, including cloud and file server storage. The built in and customizable lexical expressions category discovers a variety of critical information types (such as PII, PCI medical records, passports numbers etc.) based on company policy and industry regulations.

How to avoid unwanted data acquisition via documents downloaded from the Internet

Download for a data breach

Downloading documents from websites and cloud collaboration applications is now common practice for many organizations. The finance department downloads an invoice, the HR department a CV, and the sales team a request for proposal form. As we go about our daily business, many of us forget or are simply not aware there is active content and hidden metadata embedded in everyday documents that have the potential to cause major data breaches.

When a document is created, it automatically has sensitive information attached to it – no matter what application it's created in. This could be the author's name, revision history, application software name, document version numbers, file location maps and track changes. So, even metadata can be compromising if shared – not just for those sharing the document, but those receiving it too.

When employees download a document from the internet, the organization is at risk of unwanted data acquisition – the act of unintentionally receiving and storing critical information. Whether the critical information is obvious or not, the end result presents a variety of security issues. Therefore, it is important that employees understand the security risks involved with downloading documents and the precautions they should take before doing so.

Non-compliance with data protection regulations

The first security risk to consider is the role of regulation in protecting sensitive data. With the threat of crippling fines looming over organizations, good information governance within the network is critical.

For example, take company A and company B working together as third party suppliers and sharing customer invoices via a web portal. If a customer of company A submits an RTBF request, having unwanted data on this customer hosted on company B's network puts both organizations at risk of being non-compliant. If company B isn't even aware it's received this customer's data, it makes it even more challenging for company A to complete the RTBF request. Under GDPR, the entire supply chain is responsible for proper data handling and so both organizations are at risk of receiving a fine

Cybercriminals

Unwanted data acquisition also provides an opportunity for cyber criminals. A company does not want to receive sensitive data hidden in documents as this puts them at risk of non-compliance, but they also need to be aware that documents they have on their own website could be used for malicious intent.

Metadata that seems of no importance can be invaluable to cyber criminals. For example, a document on corporate network might contain metadata about what software it has been created in, enabling a cyber criminal to attack the known vulnerabilities in that software on the network. In addition, the hidden document author name metadata makes it easy for cyber criminals to find an employee's email address – by Googling or on LinkedIn for example – allowing them to launch a phishing campaign against the company with the intention of stealing critical information or infecting the corporate network with malware.

Competitor advantage

It is worth thinking about hidden sensitive data in terms of giving away information that your competitors could use to their advantage. For example, competing organizations might look for hidden metadata in documents on websites to gain an advantage. Mistakes can happen; someone might inadvertently embed sensitive financial information into a spreadsheet and then mistakenly upload/share it for all to view or download.

It's also not unheard of for some competitive companies to deliberately share documents containing unwanted sensitive data and use this to cause compliance issues for the receiving company.

Under GDPR, any critical data must be stored properly, but if an organization is unaware of the critical data lying within the document, they cannot delete or secure the information. When it comes to auditing or even a RTBF request under GDPR, the business is liable for a huge fine that damages both revenue and reputation.

Technology tips for detecting and preventing unwanted sensitive data acquisition through websites

While ensuring employees are aware of the threat of unwanted data acquisition via website downloads is a vital step in mitigating this risk, having technology in place to automatically ensure documents are sanitized is key to reducing unwanted data acquisition.

Clearswift's **Secure Web Gateway** inspects all content being downloaded from, and uploaded to, the Internet. Using lexical analysis capability and Clearswift's redaction and sanitization technology, hidden sensitive information and metadata is automatically detected and removed from documents during the upload (and download). Either by searching file uploads for key watermarks within the documents that indicate sensitive data or by understanding the content, the data leak can be identified, stopped and proper repercussive actions taken, so a sanitized and safe document is uploaded and published.

For organizations who already have a web solution in place, but don't have advanced redaction and sanitization capabilities, Clearswift's **Secure ICAP Gateway** integrates seamlessly with existing web infrastructure to bolt-on these advanced features.

Depending on the content within the document, Clearswift's web solutions can mobilize **Data Redaction** which, if required, automatically detects and redacts unwanted sensitive information before it is brought into ('acquired by') the corporate network, or uploaded to websites and collaboration applications. The **Document Sanitization** feature within Clearswift's unique **Adaptive Redaction** technology ensures details such as revision changes, author information and software versions are automatically removed from documents to ensure organizations always adhere to information security regulations and are protected against unwanted data acquisition.

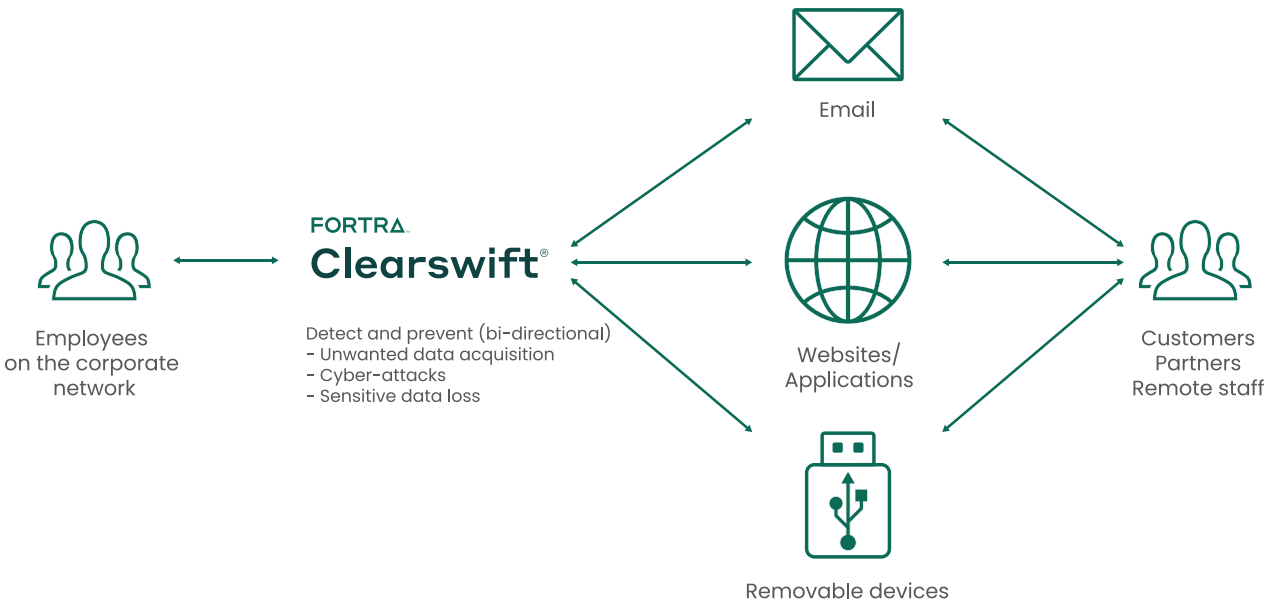
Preventing unwanted data acquisition into the corporate network

People, processes and technology are central to a good information security strategy. From a technology perspective, organizations can deploy solutions to control which employees can access and share sensitive data and files stored on the network. Best practice is to implement data loss prevention (DLP) solutions that enable deep content inspection on:

- all email content and attachments (internal sharing and in/out of the network)
- corporate documents and collateral being uploaded or downloaded from websites and cloud applications
- information being transferred to/from removable devices.

Inspecting all content flowing in and out of the network ensures that the information being transferred and shared is compliant. If there is an issue with data leaks or unwanted data acquisition, the sources can be identified, and the appropriate measures taken to mitigate the threat.

Content inspection flow in/out of the corporate network



1. Educate employees

The first step is around awareness; make sure employees understand the risks and consequences around acquiring unwanted sensitive data. This helps create a culture of awareness and ensures that employees take care when handling sensitive data on a dayto-day basis.

2. Create and implement data protection policies and processes

To ensure employees handle and process sensitive data securely, official data sharing processes and policies should be implemented and regularly reinforced so that employees don't become complacent after the initial training. Making sure policies and procedures are updated as new compliance regulations come into effect will also help mitigate the risk.

3. Deploy Data Loss Prevention technology to secure email and web collaboration

Technology should be implemented to prevent any mistakes, acting as a 'safety net' for organizations rather than a silver bullet. Clearswift's Adaptive Redaction technology is built into its core email and web security products, allowing the automatic detection and redaction of sensitive information from email messages and attachments, and downloaded files before they enter the corporate network.

Rather than a 'stop and block' approach, Clearswift's solution detects and redacts only the sensitive information (for example, PII and PCI data) rather than the stopping the entire email from being delivered. This safeguards employees from unwanted sensitive data acquisition without preventing collaboration and impacting operational efficiency. Further to this, Clearswift's sanitization technology can automatically detect and remove 'hidden' sensitive information (such as author names and revision history) contained within inbound documents and files shared via email or uploaded/downloaded via the internet.

The same Clearswift technology that prevents unauthorized inbound data acquisition can also be used to prevent outbound data loss, without compromising continuous collaboration.

4. Removable device regulation and secure data transfer control

Take control and gain visibility of what devices can connect to your corporate network by deploying an endpoint solution. Clearswift Endpoint DLP automates the security of all devices and regulates what information can be transferred to/from the corporate network.

5. Fully understand the legislation your business needs to comply with

Vital to the success of deploying information security solutions is understanding the different regulations organizations must comply to. Everything from GDPR, PCI DSS, GLBA, SOX/J-SOX and NCUA need to be considered when determining how to best deploy security solutions, including those designed to prevent unauthorized data acquisition, data loss and cyber-attacks. Defining and creating the policies (set of rules) to encompass all the requirements can be time consuming, however the use of pre-defined tokens and templates within the technology that will enforce them can simplify matters. These tokens and templates also make it easier to update the policies when required.

While the initial set up may take some time, technology can be rolled out in phases as part of a prioritized information security strategy to mitigate the risk of employees making mistakes, secure company critical information flowing in and out of the network, and to comply with both company and regulatory data protection requirements.

For more information, visit www.clearswift.com.

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.