Transferring Confidential Information: Best Practices for Safe Data Sharing
It is mind-blowing today to think about how much digital data is transmitted over the internet on a weekly, daily, hourly, and even second-by-second basis. Every time a web page is loaded, or a file is downloaded, a back-and-forth transaction occurs. Likewise, employees and businesses are constantly sharing information at a similar frequency and the ecosystem of trust and whom we share information with has grown exponentially. No longer is this simply restricted to the perimeter of our own businesses, but extends to partners, suppliers, customers, prospects, and influencers around the globe.

Consequently, the challenge now is no longer about whether we have the tools and the technology to share and collaborate, but how we do that securely. Likewise, it is also about understanding what sensitive and confidential information needs to be safeguarded and ensuring that employees are trained and educated around this, and that they have the right policies and technologies in place to secure data. Additionally, the remote or partially remote workforce that emerged from the COVID-19 pandemic looks like it will be here to stay in some capacity for many organizations for some time—which further increases the points at which data can become vulnerable.

Here at HelpSystems we have data security solutions that help ensure your intellectual property and sensitive data is kept safe and secure. Our products run right across the various data protection requirements from classifying data inside your organization at the outset, through to detecting and preventing leaks of sensitive information outside your organization. In this guide we will walk through some best practice approaches, several use cases that highlight how easy it is for sensitive and confidential information to be compromised and how our portfolio of data security solutions can help.
Growing Volumes of Data Are Attractive to Cybercriminals
Data is often an organization’s most valuable asset, and today businesses hold more data than ever, with large volumes being generated, stored, sent, and received. There is more regulation to govern data, requiring organizations to protect it from unauthorized access. There are also more data breaches, resulting in large fines, and the loss of customers and reputation. It’s a challenging environment, especially considering remote work being a permanent reality for many organizations whose employees need to securely collaborate from anywhere.

That said, with so many different collaboration tools, the sharing of information is easier than ever, but it is now more important than ever to keep your confidential information as secure as possible. If your data is vulnerable to cybercriminals or even to human error, be prepared to pay—financially, with personnel resources, and in rebuilding your reputation should a breach occur from within or outside your organization. According to a study by IBM, the average cost of a data breach is now estimated at $3.92 million. Industries that are highly targeted for their valuable personal information like finance, healthcare, and retail can see an even higher toll. No matter your industry, if you store or transfer identifiable, sensitive data, your organization is an attractive target.

Why Do We Need to Secure Sensitive or Valuable Data?
There are many reasons why enterprises need to secure sensitive or valuable information when collaborating inside and outside their organization—this could be because of data regulations, industry compliance, the need to protect confidentiality, or to prevent unauthorized access.

There are many tools that allow organizations to transfer confidential information which makes it easier to collaborate with other people across the globe. However, sometimes it can still feel like a challenge to find a solution that is capable of handling file sharing or the secure sharing of confidential information on a regular basis. Often it can be hard to trace what happens to that information after it has been shared, or to identify whether the information should be shared in the first place.

Best Practices for Sharing Sensitive or Confidential Information
Traditionally, data security focused on controlling the infrastructure—and the networks and devices that operate within it—locking data down and tightly controlling who has access to it. While secure, this makes the sharing of information difficult and can lead to poor productivity as well as hamper competitiveness. Additionally, with COVID-19, we are more likely to see a return to the office that is more hybrid in nature, and this means that employees will still be remote working in the future.

**Protecting the Data**

Appropriate technical and organizational measures must be taken to prevent unauthorized or unlawful access to personal, sensitive, and confidential information, and to prevent accidental loss, or the deletion of any confidential data. This is where UK public sector organizations make it easier for employees to understand what constitutes sensitive information that needs to be protected. For example, the Government’s Protective Marking System—which consists of OFFICIAL, SECRET, TOP SECRET—is designed to ensure that access to information is correctly managed and safeguarded. This has evolved over time and most government departments and public sector organizations around the world will have some form of Protective Marking System in place.

However, private sector organizations don't typically have such policies or systems and often this can leave employees unsure about what constitutes sensitive or confidential information. It is therefore important that organizations look to put in place a culture of security and that employees are educated and trained on how to appropriately classify, handle, transfer, and delete any such data. And of course, that they have the right tools and technology to enable them to do this, efficiently, proactively, and securely.

In deciding the most appropriate way to share confidential information and the level of security required, organizations must always take into consideration the sensitivity of the information and the urgency of the situation, and they should take a risk-based approach in determining appropriate measures. For example, when sharing confidential information, the employee must ensure the recipient of the information understands the purpose for which the information is being shared and any limits i.e., what information may or may not be shared and the circumstances under which it may or may not be shared with others. They also need to ensure that any further handling of the information is secure. This applies whether it is being shared with someone inside or outside the organization.

Additionally, when dealing with external parties, enterprises need to understand what data partners will need access to and why, and ultimately what level of risk this poses. Likewise, they need to understand what controls such parties have in place to safeguard data and protect against incoming and outgoing cyber threats. This needs to be monitored, logged, and regularly reviewed, and a baseline of normal activities between the organization and the external party should be established.
Understanding the Different Use Cases Where Information Can Be Exploited

However, many organizations don’t always recognize that the information they are handling is sensitive or confidential. Below are several scenarios within different departments or sectors whereby data is inadvertently shared or accessed by the wrong individuals. Often this is down to human error versus malicious activity, which is why it is so important to have the training, education, and policies in place.

**Legal Teams or Legal Organizations**
Legal teams within large corporations or legal organizations will have access to sensitive contract, financial, and confidential information. They may, for example, be working on M&A activity. In this scenario, when timescales are critical, neither company involved can risk confidential documentation getting into the wrong hands or even a two-day delay with documentation because it has, for example, been quarantined by a Data Loss Prevention (DLP) tool while it investigates false positives. Equally, any information pertaining to an acquisition, especially if the company is public, must be kept confidential and remain within the confines of the executives directly responsible for the transaction.

Therefore, looking at the scenario where the DLP tool has identified data for quarantine, in order to release that communication, someone in the IT team will have to review documents that they potentially shouldn’t be reading. This could be considered as insider trading if they quarantine it, read it, and subsequently make a trade based on the information they have gained.

**HR and Personally Identifiable Information (PII)**
HR departments are constantly dealing with confidential and PII. For example, there could be a disciplinary where meeting notes and correspondence should be confidential to the individuals involved. Likewise, there will be documents outlining employee salaries and bonuses or health information. Again, if any of these documents do not get the right treatment, information that should be kept highly confidential is susceptible to being shared.
Healthcare

If we think about the volume of data that is circulating right now because of COVID-19, it is easy for that data to get into the wrong hands. Healthcare was immensely disrupted as a result of the pandemic. Routine appointments were converted into telehealth appointments, bringing patient data outside of the hospital’s walls. This means healthcare providers are now accessing patient PII data in remote settings, presenting privacy and security issues.

Likewise, cybercriminals are exploiting these vulnerabilities, which could potentially impact millions of patient records and data, which will likely end up being sold on the dark web. This type of data is critically important to preserve the integrity around sensitive patient/client medical records. Not only that, but with increasing legislation such as US HIPAA compliance, healthcare providers are required to prevent sensitive patient health information from being disclosed without the patient’s consent or knowledge.

Loss of IP

When developing and manufacturing vaccines, research institutions and universities work closely with pharma companies and need to share highly confidential and sensitive data. That said, Astra Zeneca, for example, wouldn’t necessarily want Oxford University sharing certain information with its rivals. But something as simple as a misdirected email could see the wrong recipient receiving critical information about vaccine formulae and suddenly the intellectual property contained in that data is compromised and potentially in the hands of a competitor.

Loss of IP is a huge risk and the consequences outside of loss of IP itself are equally significant. For example, if this did happen, the next time Astra Zeneca embarked on a vaccine project, it might think twice about working with Oxford University if they did not safeguard sensitive data.
The Rapid Move to Cloud and Microsoft 365 Does Leave Security Gaps

Additionally, we saw COVID-19 accelerate digitization and one such digital transformation trend is the move to Microsoft 365. The effectiveness of this collaboration suite is undeniable with many organizations benefiting from its cloud-based capabilities. But in the rush for cost-effective deployments, are organizations missing out on vital security for emails, for example, because the package level they’ve bought into does not provide adequate protection for sensitive data or cyber-attacks?

To avoid the risk of a data breach or confidential information going astray, organizations need to secure their business communication channels. It is all too easy to see an email, especially one that comes from a trusted source, and assume that it is okay to open or reply to this. And while Microsoft 365 is good for dealing with spam and malware and offers various levels of email security, it does not deliver the deep content inspection required to remain truly secure.

Another area of concern, where Microsoft 365 security falls short, is around its ability to detect sensitive information (e.g., PII data) within image files such as screenshots and scanned documents. It is also unable to remove metadata (which might lead to data loss) and malware threats hidden within document and image files. Even with sandboxing to analyze attachments, protection against ransomware is limited. In effect it doesn’t offer a truly comprehensive solution, one that takes a zero-compromise approach to ensure sensitive and critical information protection and control, particularly when dealing with third parties.

To plug the gaps in security, organizations deploy complementary solutions that strengthen the security and enhance the performance of the Microsoft platform.
These are just a few examples of where data can be inadvertently shared through human error or malicious activity. So how do organizations transfer confidential information securely and how do they ensure that only authorized parties receive sensitive data?

Due to its ubiquity, email is a particularly vulnerable channel and one that’s often exploited by cybercriminals posing as a trusted source. Therefore, it is essential that organizations are adequately protected from incoming malware, embedded Advanced Persistent Threats, or any other threat that could pose a risk to the business.

Here at HelpSystems we advocate taking a layered approach to data security that starts with the following steps:

**STEP ONE – Understanding and Classifying Your Data**

The basis of a solid data security strategy begins by identifying and classifying what type of information you need to protect, including critical unstructured data such as intellectual property. By taking this step, you lock down the base control and management parameters needed to help ensure compliance. Whether you need to protect public, financial, personally identifiable information (PII) information, or more, establishing and classifying data to be protected sets the foundation for the additional security layers needed to continue protecting data along its journey.

Data classification tools are critical to ensure that sensitive data is appropriately treated, stored, and disposed of during its lifetime in accordance with its importance to the organization. Through appropriate classification, using visual labeling and metadata application to emails and documents, this protects the organization from the risk of sensitive data being exposed to unauthorized individuals or organizations.

**STEP TWO – Detecting and Preventing Data Leaks**

It’s going to happen. An employee will accidentally send sensitive data to the wrong person, or perhaps transfer an otherwise “safe” document that contains hidden metadata that could compromise your organization. Any number of scenarios can put your organization at risk unless you have a solution in place to detect and sanitize data in real time, before it is sent to the cloud or to third parties, before a breach occurs.

Therefore, organizations need to ensure that documents uploaded and downloaded from the web are thoroughly analyzed, even if they are coming from a trusted source. To do this effectively, they need a solution that can remove risks from email, web, and endpoints, yet still allows the transfer of information to occur. Integrating Data Loss Prevention (DLP) over these channels allows the flow of information to continue while removing threats, protecting critical data, and ensuring compliance. It doesn’t become a barrier to business or impose a heavy management burden. This is important because traditional DLP ‘stop and block’ approaches have often resulted in too many delays to legitimate business communications and high management overheads associated with false positives.

**4.3 Securing and Protecting Your Data**

After you’ve ensured your data is identified and classified, scrubbed of potentially sensitive data, and approved for sending by authorized users, it needs to be sent or transferred securely. This can be achieved by email encryption or, where there are large volumes of data sent on a regular basis, through a Managed File Transfer (MFT) solution. MFT locks down your data at the point it is most vulnerable—while traveling to its destination into unmanaged domains, devices, or applications.
This secure channel provides automated, end-to-end data security over a central platform and offers audit trails, user access controls, and other file transfer protections.

To secure confidential data whenever and wherever it travels, Digital Rights Management software provides organizations with the ability to track, audit, and revoke access at any time. It works by encrypting the data with a unique key that is secured via a cloud platform. Keys are submitted with the data securely, and the platform audits every successful and unsuccessful access request so an organization can track its confidential information at any time.

Layering data security solutions and bolstering the native capabilities in applications such as Microsoft 365 is a proactive approach to protecting your confidential and sensitive information. Data security is only as robust as the various elements that support it. Layering proven solutions to ensure your sensitive data remains secure from start to finish is a proactive approach. HelpSystems’ suite of data security solutions provides the range of data protection needed, including identification and classification, integrated DLP, secure file transfer, and more.

More About HelpSystems Data Security
Our comprehensive data security suite includes:

**Data Classification**
- Identify, label, and control your sensitive or valuable data
- Helps determine data value and build a security-focused culture

**Integrated Data Loss Prevention (DLP)**
- Minimize the risk of a data breach by automatically removing sensitive data from emails and documents as they are sent, received, or transferred to the cloud
- The solution applies an additional layer of sanitization to protect from phishing emails, ransomware, and other Advanced Persistent Threats

**Managed File Transfer (MFT)**
- MFT provides a secure and compliant way to share data outside the organization
- Automate workflows and integrate with third-party applications
- Large file acceleration helps move data quickly and securely

**Digital Rights Management**
- Security that stays with your data wherever it travels
- Track, audit, and revoke access at any time

For more information, visit: [https://www.helpsystems.com/solutions/cybersecurity/data-security](https://www.helpsystems.com/solutions/cybersecurity/data-security)
About HelpSystems

HelpSystems is a people-first software company focused on helping exceptional organizations Build a Better IT™. Our holistic suite of security and automation solutions create a simpler, smarter, and more powerful IT. With customers in over 100 countries and across all industries, organizations everywhere trust HelpSystems to provide peace of mind. Learn more at www.helpsystems.com.