Taking Control Of Sensitive Data

By: Colin Tankard - Digital Pathways Ltd

Taking control of sensitive data

Executive summary

Data protection is becoming an ever more pressing concern. The threat landscape is complex and adversaries are increasingly sophisticated. Sensitive data that falls into the wrong hands can cause widespread damage, both to the individuals concerned and organisations, which can suffer financial and reputational damage.

This is something that is not being lost on regulators. Data protection compliance requirements are increasing and becoming more stringent. A particular case in point is the General Data Protection Regulation (GDPR) of the EU, which has particularly onerous requirements for protecting personal data and which has widespread implications, reaching way beyond the shores of Europe to govern the protection of data regarding any EU citizen, no matter where the data processor or controller is based, and where the data is stored.

There are a number of technologies that can help with data protection efforts. Of these, the use of encryption and pseudonymisation techniques—the only technologies specifically called out in GDPR—are considered to be best practice. In recent years, these have become much easier to implement and manage and are well suited to protecting data no matter where it resides or how it is being transmitted. For best results, these technologies should be used as part of an enterprise-wide information governance programme that includes data classification capabilities and robust access controls.

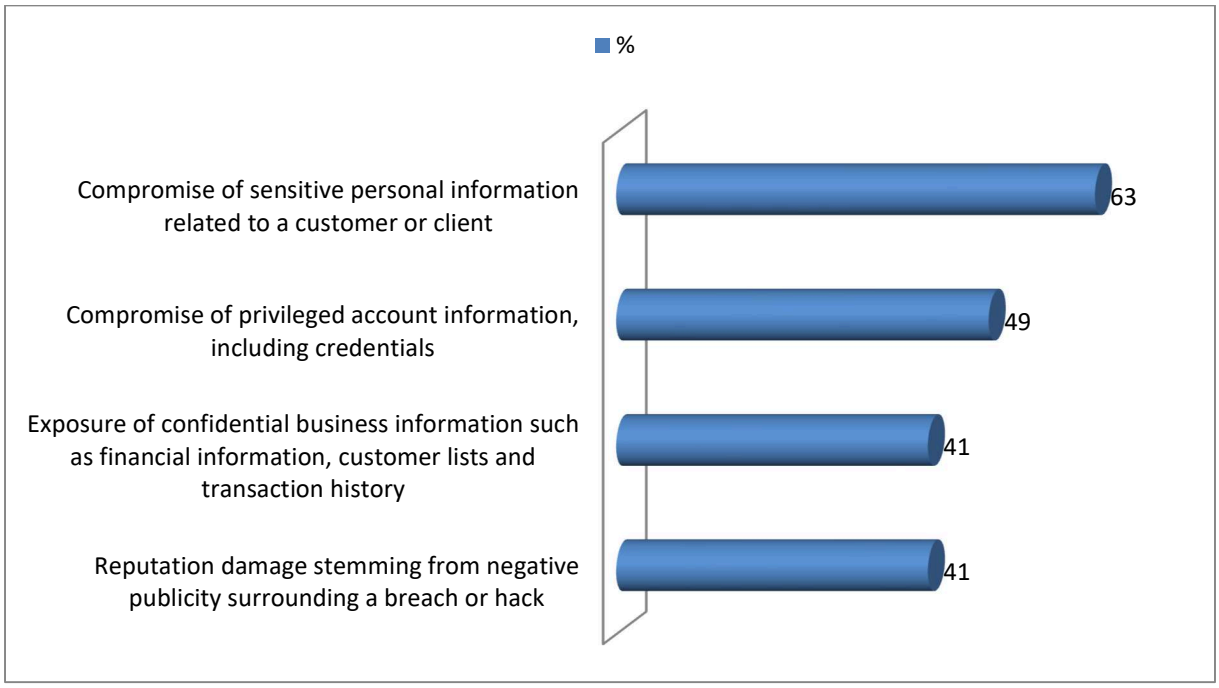
Data protection increasingly onerous

Once seen as the responsibility of the IT department, data protection has become a topic that affects everyone, both in their business and their private lives. Sensitive information can be highly valuable. Examples include, anything related to an individual that can be used for financial fraud or other nefarious activities and intellectual property that is essential for the livelihood of a business.

Information theft has been an issue for many years, but has become decidedly easier in the digital economy. Every organisation faces a barrage of threats that make it essential that adequate safeguards are in place to protect sensitive data. Those threats can originate from within an organisation, can be caused by an external attacker, or can be a combination of both, such as an adversary who gains control of a legitimate user's credentials and uses them to access sensitive data.

According to a recent survey by the SANS Institute, external actors are seen as causing the most damaging threats by just 23% of respondents, whilst threats from insiders, whether unintentional or malicious, were cited as having the most potential to cause damage by 76%. People internal to an organisation often have access to the most critical information, thus giving them the potential to cause greater harm. The types of information that could be compromised by insiders are shown in Figure 1.

Figure 1: Top concerns with regard to insider threats



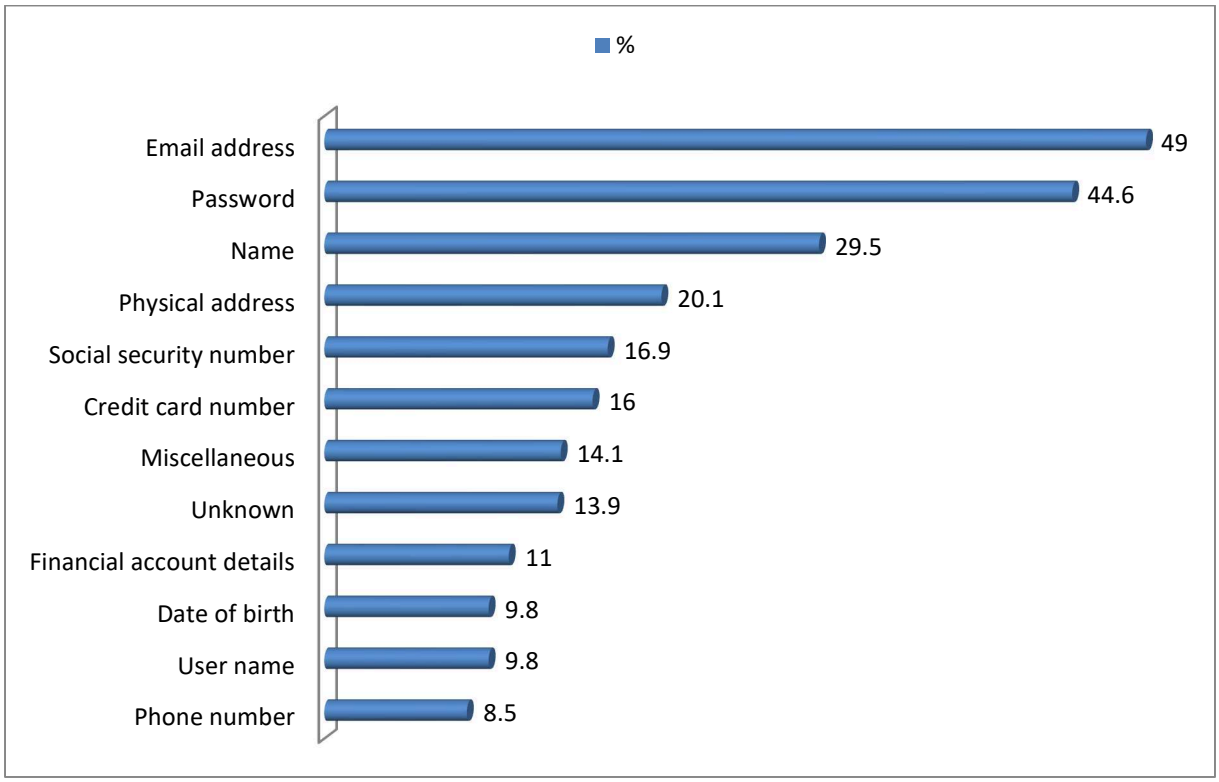
Source: SANS Institute

Data breaches and compromises are of great concern to any organisation owing to the financial and reputational damage that can ensue. But they can also have significant legal consequences since regulations and industry standards, such as PCI DSS, which demands high levels of security for payment card information, are placing a greater emphasis on data security—and are increasingly imposing sanctions for the loss of information that can put people at risk.

General Data Protection Regulation (GDPR) is now being enforced. Whilst it is an instrument developed by the EU, every organisation that processes personal data related to EU citizens, no matter where they are based or the data is stored, must comply with its requirements or face weighty fines and sanctions that are significantly higher

than for any other regulatory device. And, the definition of personal data is extremely broad within GDPR, encompassing virtually any information that could be used to identify a person. Figure 2 shows the types of information that organisations report as having been exposed during security incidents, all of which fall into the EU's definition of personal data.

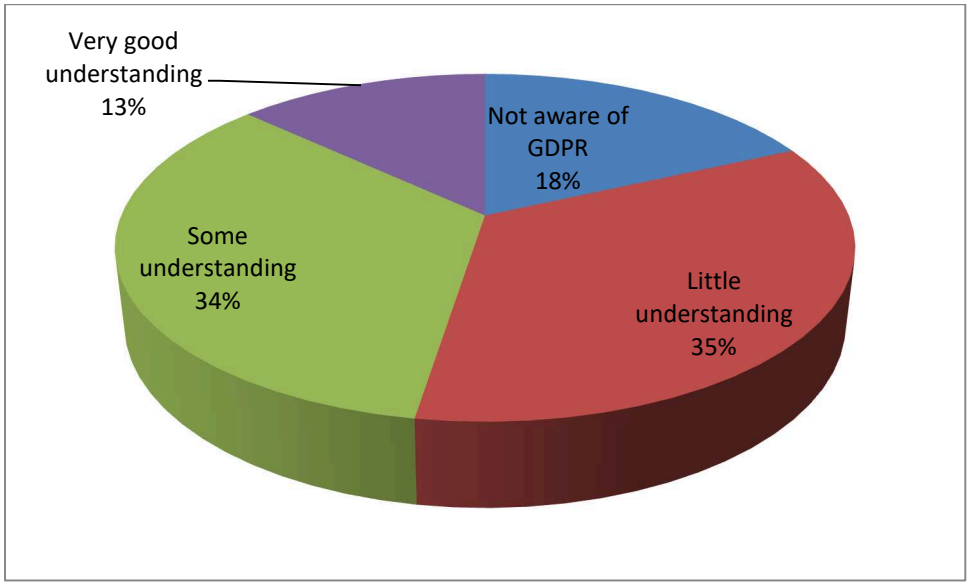
Figure 2: Incidents by type of data exposed



Source: Risk Based Security

However, many organisations are not prepared to meet the demands of GDPR. As Figure 3 shows, many businesses in the UK claim to have little understanding of what GDPR means for them. Even where an organisation has taken steps to review their privacy statements and document how they would respond to, for example a Subject Access Request (SAR), they do not know how they will find all the data within their network, especially data held in backups, emails or in the cloud. Given recent reports in the Press that companies are receiving 50-60% more requests for information under a SAR, the workload to comply without technology to search and discover all the data required, is immense.

Figure 3: Awareness of GDPR



Source: Federation of Small Businesses

According to research from Erwin, Inc., the vast majority of organisations in the US are similarly unprepared for meeting the demands of GDPR, with just 6% stating that they are prepared. Almost two-thirds are either unaware of whether or not they have the budget for data governance, or do not have a budget in place. Even so, 98% of survey respondents state that they view data governance as crucial from a business perspective.

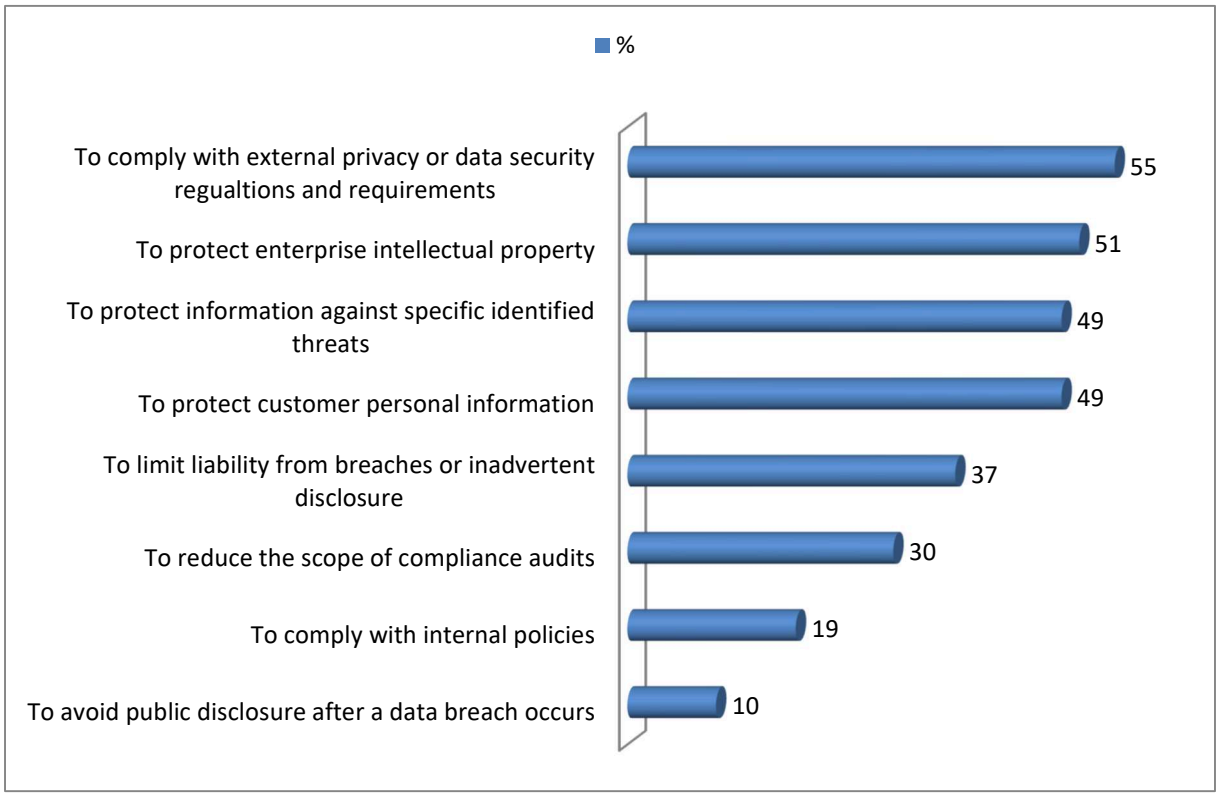
Achieving greater data control

GDPR, as with most government regulations, is not overly specific regarding the controls that organisations must implement in order to adequately protect personal data from loss. It introduces the principle of data protection by design and default, stating many times in the text of the regulation that organisations must take appropriate technical and organisational measures to ensure that personal data cannot be lost, destroyed or damaged in any way.

However, GDPR does specifically mention two technologies that businesses should implement in order to improve their data protection capabilities—encryption and pseudonymisation. The use of such technologies will not only help with compliance with regulations that include GDPR, but will also help with breaches of information

such as intellectual property, which are outside the scope of regulations, but can be extremely damaging to the enterprise concerned. Figure 4 shows the drivers that organisations are reporting for their use of encryption.

Figure 4: Top drivers for encryption

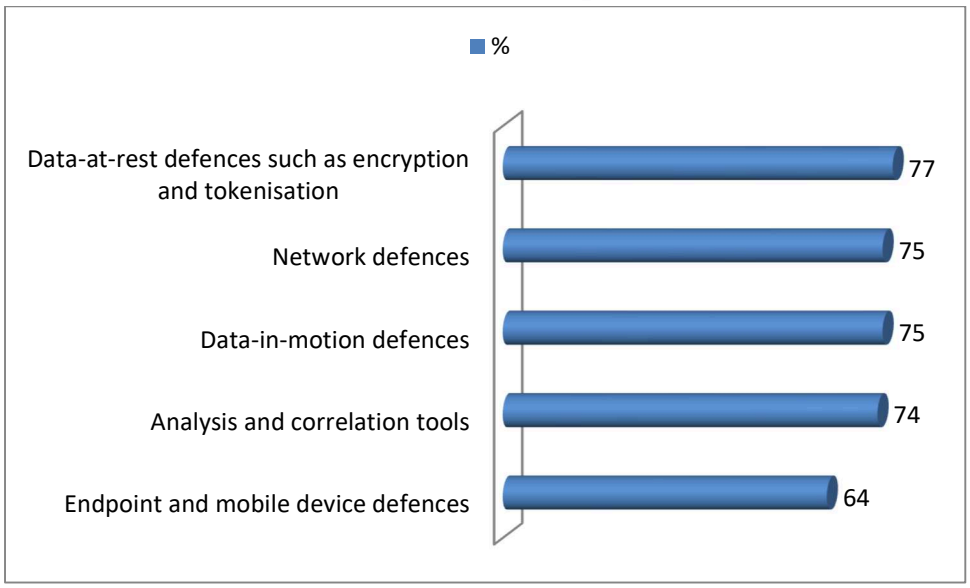


Source: Ponemon Institute

> *"In recent years there have been numerous incidents where personal data has been stolen, lost or subject to unauthorised access. In many of these cases, these were caused by data being inadequately protected or the devices that the data was stored on being left in inappropriate places—and in some cases both. The Information Commissioner has formed the view that in the future, where such losses occur and where encryption software has not been used to protect the data, regulatory action may be pursued."*
>
> *Information Commissioner's Office*

Encryption is essential for protecting information that is in storage, such as on a device, in a database or in a cloud service, as well as when it is being transmitted generally, referred to as data at rest and data in motion. It ensures that data is safeguarded against loss or unauthorised access. For regulations such as GDPR that mandate notification of authorities and data subjects in the case of a personal data breach, notification can be avoided if the data has been protected in such a way that it cannot be accessed by those without authorisation to do so. In the case of encryption, a person would need access to the cryptographic key used to encrypt and decrypt the data. As Figure 5 shows, encryption is seen as one of the most effective measures for protecting data.

Figure 5: Most effective defences for protecting data



Source: Thales

Data from Thales shows that 41% of organisations have a baseline encryption strategy in place and 64% use encryption for satisfying local privacy and data sovereignty laws.

Another factor that is increasing the need for data control and protection is that most of the data used within an organisation is not stored on devices or services over which it has complete control.

Smartphones are almost ubiquitous today and are increasingly being used in a business setting, even those that are personally owned by employees rather than being issued by the organisation. Such phones and other mobile devices, including portable storage devices, are capable of storing large volumes of information, much of which is considered to be sensitive. For better data control, information stored on mobile devices should be encrypted, either at a disk level for total protection or at a file level for just protecting sensitive data.

Some devices offer containerisation capabilities, enabling sensitive corporate information to be stored on a separate container to the user's own personal information, such as their photographs. The container in which corporate data is stored is completely separated from the other and can be protected by encryption to safeguard the data contained there.

In order to ensure that employees and other users have sufficient data protection controls on their devices, technologies such as enterprise mobility management tools can enforce factors such as the use of encryption before a device is allowed to connect to network resources. This will help to ensure that only sanctioned devices are able to store sensitive corporate information. Many also provide the capability to remotely wipe data from a device should it be lost or stolen.

The increasing use of cloud-based services is another complication for effective data protection. Some cloud services support the use of encryption and other methods of data protection, but many people use cloud-based file sharing services, many of which were originally developed for consumer use and for which security controls are variable. According to Skyhigh Networks, file sharing services account for 39% of all company data that is uploaded to cloud services and 34% of users admit that they have uploaded sensitive and confidential information to file sharing services. The same survey looked at the encryption practices of cloud service providers, finding that whilst 82% encrypt data in transit, just 9% encrypt data at rest in the cloud. Further, just 1% of providers offer encryption services where the customer retains control of the encryption keys, which could lead to data being inappropriately accessed.

Because of factors such as these, organisations should ensure that all sensitive data is encrypted before it is uploaded to cloud services and that it remains encrypted when in storage. They should use a service that guarantees the retention of control of all encryption keys, which should then be stored securely and with tightly controlled access.

Whilst encryption is seen as a best practice for data control and protection, it cannot be used in all circumstances, such as when data is in use for processing purposes. This is where the use of technologies such as tokenisation and data masking—referred to as pseudonymisation in GDPR—come into play. The difference between encryption and pseudonymisation is primarily in the way that data is handled. Encryption uses an algorithm to scramble data so that it is unreadable, whereas pseudonymisation techniques substitute data with random codes or tokens.

With tokenisation, applications can still operate using tokens so that sensitive data is hidden, reducing any risk of exposure. An example of where it would be used is for medical research purposes where large sets of data related to people are analysed, but sensitive data that could be used to identify a person is replaced with tokens.

As with encryption, data masking scrambles information, but it is often done much more selectively than encrypting, such as whole databases. An example of where it is particularly useful is in redacting sensitive data in documents such as emails and office productivity documents so that they can be sent largely in plain text, but with sensitive information such as credit card numbers hidden, or masked.

Both data masking and encryption are suitable technologies for protecting communications, especially via email, which remains the most prevalent mechanism in use. The entire contents of emails and their attachments can be encrypted so that nothing can be read by those without the appropriate authorisation. However, this can be considered to be overkill if used across the board, since many communications are fairly general in nature and encrypting every message adds to the burdens of users and increases time lags. Data masking provides an alternative by redacting sensitive information—similarly to how paper documents containing sensitive information have critical details redacted by hand.

Developing an information governance plan

No technology should be seen as a silver bullet. Whilst encryption and pseudonymisation are considered to be best practice for data control and protection and are specifically called out in GDPR, they will not magically deal with all GDPR issues. In order to embrace the concept of data protection by design and default, the use of these technologies should be part of an overall information governance programme that should be enterprise-wide in scope.

Developing an information governance plan

- *Having a fully documented information governance plan is critical because there is a central figure or group in charge of the programme to monitor compliance.*
- *Maintain a fully documented training programme to prove everyone that handles data has been fully trained on how to comply with regulatory requirements.*
- *Understand where all personal information is stored within your organisation's systems. This is similar to data maps prepared for e-discovery requests.*
- *Ensure all personal data is securely stored and fully removed from all systems when no longer needed. This means complete data access logs, end-to-end encryption and documented expungement procedures and logs.*
- *In the advent of a breach, have a documented procedure that notifies everyone affected in the prescribed time frame.*

Source: Iron Mountain

In order to protect all of the sensitive data in an enterprise, the organisation must ensure that it knows where all personal and sensitive data is stored so that there will be no gaps in protection. Ownership of all data should be defined and an executive put in charge of overseeing the information governance programme to ensure it gets the attention it requires. In order to get all employees involved, a data protection training and awareness programme should be established.

Once all data has been discovered and mapped, it is necessary to establish the level of sensitivity and criticality to the organisation of all information. This is essential so that information can be categorised in order that appropriate levels of protection can be applied. Protective marking can then be activated to all data according to its classification, such as if information is confidential or whether it is considered to be

general with little sensitivity. Those markings will be reflected in the appropriate levels of protection applied to prevent information being communicated in an inappropriate manner, such as being sent via email in unencrypted form.

Access controls should then be applied to all data according to its defined sensitivity, paying particular attention to the role of privileged users. Generally, organisations should look to assign the least level of access privileges required to persons according to their role and their need to process and communicate personal and sensitive information. Yet, this is not a one-off exercise. People regularly change roles, leave or are hired by another organisation requiring that access entitlements are regularly reviewed to ensure that they are appropriate as situations change and so that no one has more access privileges than their current role requires.

Data classification elements

Access: enable design, development and enforcement of user roles and permissions for each information/data category.

Actions: establish appropriate control activities for each category, including both administrative policies and procedures, as well as technical security controls such as encryption to achieve business objectives and mitigate risk.

Audit: be able to generate accurate reports about activities related to information and data to demonstrate compliance, proactively identify anomalous events and rapidly respond to incidents.

Source: SANS Institute

With any data protection mechanisms, it is essential that they are not too great a burden on users, who will attempt to get around the controls if they feel that their productivity is being drained. This requires that the controls put in place are applied automatically. For example, when a user attempts to send an email, they should be prompted to ensure that the appropriate classification has been selected so that protections can be applied according to policy. Should a user attempt to send an email without the required level of protection applied, they can be provided with a prompt that includes reasons as to why that particular communication needs to be protected. Those who consistently flout the rules that have been set should be provided with further training regarding data protection requirements.

Recommendations

Data security tools must be adapted to the expanded environments that are a reality today, including cloud-based services and mobile devices. The most suitable tools are those that offer services-based deployments and that provide automated platforms to reduce usage and deployment complexity, as well as staffing requirements.

The use of encryption is considered to be best practice and should be for all environments, services and devices in use. Encryption will help considerably for meeting compliance objectives and for warding off advanced threats. Ensure that any solution chosen enables cryptographic keys to be handled by the organisation itself, and never allow the data storage/service provider to handle the encryption as well as the data, as this could lead to data being inappropriately accessed. Ensure that encryption can be applied automatically according to the sensitivity of data, as defined during the data classification process and outlined in the security policy.

Conclusion

Encryption as a technology is versatile, robust and easy to deploy. The myth of it having performance issues when used, has long gone and where needed, can be totally transparent to the user or application. It requires no modifications to applications, or additional training of staff in how to use the encryption. There are some challenges, especially where Data Leakage Protection (DLP) is deployed on endpoints or servers, as DLP can't read encrypted data and will block it. This may lead to some organisations allowing encrypted data to pass through their DLP system, which obviously defeats the objective, as users exfiltrating data from the organisation will encrypt it first.

At Digital Pathways, our experience and knowledge in encryption technologies enables us to work around situations, such as DLP, in order to ensure that the encryption solution deployed works with both the existing infrastructure, as well as future growth or strategies. Encryption is an important part of any organisation's data security landscape and it should always be the starting point for new data deployments, especially when considering cloud-based services.