# A SAFE HARBOUR

**Colin Tankard** *explains how encryption has become the building block for data security*

**Encryption, whereby information is converted from a readable format into one that obscures its meaning from those without the authorisation or ability to decipher it, has long been used to protect sensitive information from prying eyes. Ever since the end of the Second World War, as the use of computers has become widespread, algorithms for encrypting data have become increasingly common, enabling vast swathes of information to be encrypted both quickly and efficiently.**

Encryption is invaluable for ensuring that sensitive information that falls into the wrong hands, if it is lost or stolen, is prevented from being of use to anyone without the ability to decrypt that information. It satisfies requirements for data confidentiality and integrity by ensuring that information has not been tampered with.

In recent years, ensuring the security, confidentiality and integrity of data has become an ever more pressing concern. Information and data produced and collected by organisations, including intellectual property and personally identifiable information related to customers, employees and business partners, is valuable not just to the organisation concerned, but also to criminals who can use it for financial gain.

**65 percent of large firms reported having suffered a data breach in the past year**

According to recent research by Thales, 91 percent of IT executives state that they feel vulnerable to data security threats. A recent government survey found that while 65 percent of large firms reported having suffered a data breach in the past year, more than half of medium-sized firms and one third of small organisations had been breached, showing that no one is immune.

In the Breach Level Index 2019, almost five billion data records had been lost or stolen since 2013, but only 4 percent of those records were encrypted. Any data breach can cost the organisation involved dearly, both in terms of lost revenues and damage to its brand and reputation.

According to IT Governance, in their data breaches and cyber attacks report, in February 2020, 623 million records were breached, but this doesn't tell the full story, as there were a whopping 105 incidents, making February 2020 the second leakiest month it had ever recorded.

Encryption has a vital role to play in keeping sensitive and confidential information safe from prying eyes. The use of encryption is the best strategy for any organisation for maintaining security of data when it is in storage or is being transmitted, such as over the internet. Initially considered to be a complex technology to deploy and manage, it has now moved on and can easily be used by anyone.

## SAFEGUARDING DATA

But it is not just a good strategy to choose to encrypt sensitive data; it may also be required. Organisations face a wide range of regulations and industry standards that they must adhere to. In the US, the majority of states have laws regarding data breach notification and those doing business in Europe have similar pressures from the General Data Protection Regulation (GDPR), which specifically 'calls out' encryption and pseudonymisation as suitable, appropriate safeguards for protecting data.

What many of these regulations and industry standards, such as PCI-DSS for protecting payment card information, have in common, is that they provide a safe harbour when encryption has been implemented. For example, the majority of laws that mandate data breach notification contain clauses whereby notification is not required when data that has been lost or stolen has been encrypted, since the data cannot be compromised, unless the encryption code or method is also compromised.

When it comes to ensuring that data is properly secure, there are four critical questions that need to be asked: Who has access? It is not a lot of use locking up the family silver if everybody in town has a key to the strong room! The absolute minimum number of people must have the keys to the encryption and they must never pass them on without clear, documented permission.

When has the data been accessed? For the reassurance of the business and its prospective clients, as well as to ensure corrections can be made if data does leak, all access to encrypted material must be effectively logged. Not difficult to do, but crucial.

Is the data secure in the first place? If there is a flaw in your systems already, then your encryption processes may be worthless. You can only build on secure foundations and essential secondary controls will establish if those foundations are compromised.

When does complacency set in? A few years ago operators bought off-the-shelf firewall software for their PCs and considered themselves to be safe for all time. As we know, they were wrong. Basic computer security has had to be improved and updated on an almost daily basis. The people who are trying to get past your security are continually improving their attacking systems; your encryption needs to be dynamic and proactive. Beware a false sense of security!

Encryption by itself is not the only technology that organisations should have in place to protect sensitive data, but should be a strategic part of the entire security system, alongside complementary technologies such as access controls, monitoring systems, auditing and reporting capabilities.

**ALL SENSITIVE DATA SHOULD BE ENCRYPTED BEFORE IT IS UPLOADED TO CLOUD SERVICES**

The tight control of the actions of privileged users is of particular importance, in terms of what they can access and what they do with the information. This is necessary owing to the need to counter insider threats, which are estimated to account for 43 percent of all breaches, many of which are attributed to actions by privileged users. Not all insider threats are caused by malicious intentions, as accidents can occur, such as inadvertently sending information to a recipient other than was intended, but insider threats can be the most damaging, since internal users can have access to the most sensitive and valuable information that an organisation possesses. These controls should be tightly integrated so that there are no security gaps that could be exploited, so that organisations are better able to both ward off advanced threats while meeting their compliance objectives.

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 Box, file sharing services account for 39 percent of all company data that is uploaded to cloud services and 34 percent 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 while 82 percent encrypt data in transit, just 9 percent encrypt data at rest in the cloud. Meanwhile, just 1 percent of providers offer encryption services where the customer retains control of the encryption keys, which could lead to data being inappropriately accessed.


www.intersec.co.uk

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.

While 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 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 relating to people is 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 more selectively than encrypting, such as for 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.

Another core capability to add is cryptographic key management. This is the mechanism which stores and changes encryption keys as required, which should be centralised to ensure that policies can be consistently applied across all data, both when in transit and when at rest. Efficient key management can be achieved through use of a physical or virtual appliance or, increasingly can be provided as a service, especially for cloud applications.

In 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 its use. There are some challenges, especially where Data Leakage Protection (DLP) is deployed on endpoints or servers, as DLPs can't read encrypted data and will block it. This may lead to some organisations allowing encrypted data to pass through a firewall, which obviously defeats the objective, as users exfiltrating data from the organisation will encrypt it first.

An encryption solution, once deployed, works with both the existing infrastructure, as well as future growth or strategies. It is an important part of any organisation's data security landscape and should always be the starting point for new data deployments and be considered a core part of any data security strategy that organisations develop. For both data security needs and for achieving regulatory compliance, encryption should be considered to be the baseline ●

**Colin Tankard** is Managing Director of cyber security and data management company Digital Pathways, specialist in the design, implementation and management of systems that ensure the security of all data whether at rest within the network, mobile device, in storage or data in transit across public or private networks.

**Pseudonymisation techniques substitute data with random codes or tokens**