Bloor

White Paper

White Paper by Bloor
Author **Fran Howarth**
Publish date **January 2016**

For the EU's new data protection regulation, encryption should be the default

...and should be seen as a strategic part of the entire security system

To protect sensitive data, organisations need to take a holistic view of security, implementing integrated controls to ensure that they have a viable security management platform in place. Encryption has a strategic part to play and should be part of the security posture of any organisation.

Author **Fran Howarth**

Executive summary

Data breaches have become an everyday occurrence and numerous well-known organisations have been named and shamed, denting their reputations and wreaking financial damage. But any organisation, whatever its size or line of business, can be a target. Every organisation has some form of sensitive data such as financial records, customer details and employee information that is highly prized by criminals and the vast majority of organisations rely on technology to run their business. Technology, especially the use of disruptive technologies such as big data and cloud-based services, provides for greater productivity, flexibility and improved information access. But it also increases the chances that sensitive information can be inappropriately accessed, lost or stolen.

As well as this, there are many regulations and industry standards that require that stringent safeguards are applied to personal and sensitive data. Of these, the EU data protection rules affect many organisations. Now, with agreement on the new general data protection regulation of the EU having been reached, they are set to get tougher, with higher sanctions available for non-compliance and affecting a wider range of organisations than previously. The new regulation will come into force in 2018 and will require organisations to reassess the security controls that they have in place. Along with this new agreement, provisional agreement has been reached on a new network and information security directive, which will likely come into effect in the same timeframe. This will require that providers of essential services notify the relevant authorities of any security incidents experienced. The time to prepare is now.

This document discusses the changes being made to the European data protection landscape and suggests that encryption should be the default choice for protecting data. However, this should just be part of the overall data security strategy, which must be comprehensive and consistent.

Fast facts

Given today's need to protect sensitive information, encryption should be the tool of choice for any organisation. Encryption should be applied to all data, whether at rest, in motion or, when practical, even in use.

However, because decrypting data leaves it in the clear, encryption access controls are required to track all those interacting with such data, and what they are doing with the data.

Security intelligence, achieved through integration with security information and event management (SIEM) systems, will allow organisations to ward off even the latest threats.

Audit and reporting capabilities should go hand in hand with encryption controls.

The bottom line

To protect sensitive data, organisations need to take a holistic view of security, implementing integrated controls to ensure that they have a viable security management platform in place. Encryption has a strategic part to play and should be part of the security posture of any organisation. With this and complementary controls in place, organisations will be better able to ward of the advanced threats that they face, as well as achieve compliance with the data protection regulations that they face.

“Given today's need to protect sensitive information, encryption should be the tool of choice for any organisation.”

Data protection a pressing concern

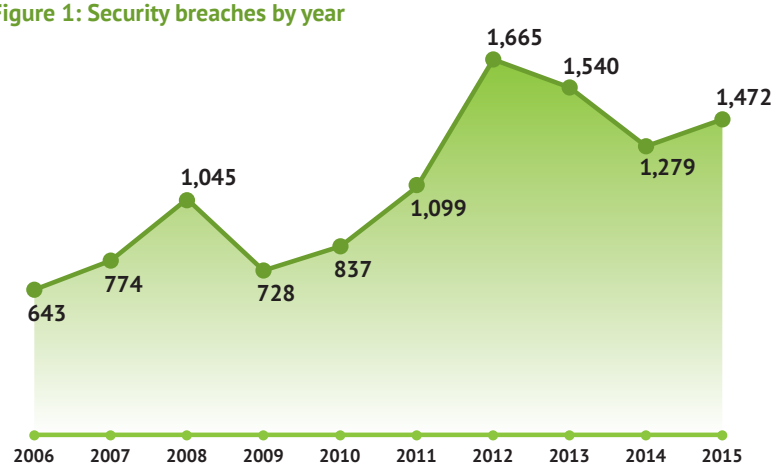
> **Per organisation, the Ponemon Institute estimates the cost of a breach to be US$3.8 million in 2015.**

Sensitive data is at greater risk than ever before. Data breaches are everyday news – as can be seen from statistics from the *Open Security Foundation,* which show that there had been 1,472 breaches reported in 2015. The fallout can be huge, with personal identities stolen, firms going out of business, and brand and reputational damage that has seen a fair few heads roll at large organisations.

In terms of the financial burden of breaches, a recent report from *Grant Thornton* estimates the worldwide cost to business to be US$315 billion. Per organisation, the *Ponemon Institute* estimates the cost of a breach to be US$3.8 million in 2015. Organisations of all sizes can be impacted. According to *PwC*, 90% of large organisations experienced a breach in 2015, as did 74% of small organisations. Whilst much focus is placed on external attacks, insider threats also weigh heavy. Not only do they have access to sensitive data and can make mistakes, but they are often targeted by attackers looking to steal valuable information. According to Vormetric, 89% of respondents feel that they are becoming more vulnerable to insider risks, and 34% state that they feel very or extremely vulnerable.

Regulation and the need to abide by industry standards and best practice guidelines, many of which require stringent controls be applied to sensitive data, are a further concern. Every organisation needs to abide by data protection laws – and the burden is set to grow.

Figure 1: Security breaches by year



Source: Open Security Foundation

Data protection regulation in the EU needs to be upgraded

Data protection regulations in the EU were introduced 20 years ago in the form of the data protection directive, which all member states ratified into their own laws. Some member states already had some form of data protection legislation, such as France. Introduced in 1978, its legislation is said to have been the inspiration for the EU data protection directive. Upon inception, the directive was said to be the most stringent piece of data protection legislation worldwide.

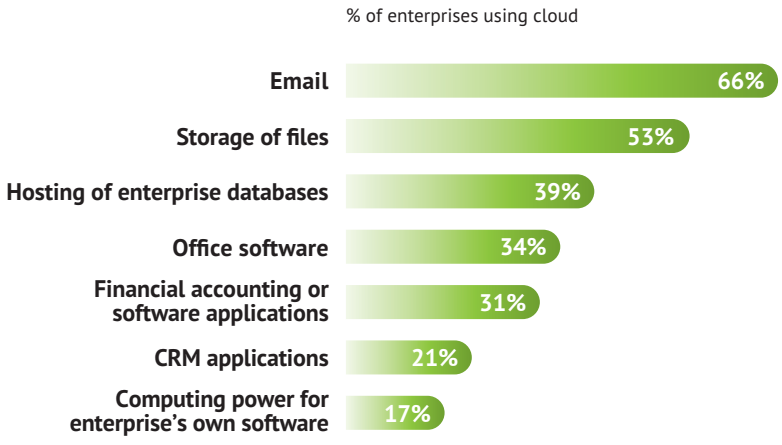
The 1995 directive was intended to unify legislation across Europe and provide a level playing field for organisations operating across borders. But much has changed in the past 20 years. In 1995, the internet was in its infancy. According to ***Internet Live Statistics***, less than 1% of the world's population was connected to the internet in 1995; today that figure is around 40%. According to ***Eurostat***, 73% of organisations operating in the EU maintain a website, rising to 94% in Finland and with a low of 42% in Romania. On average, 30% of organisations make use of social media, although this varies widely by country. Cloud computing is also one the rise. According to the ***Cloud Industry Forum***, 84% of enterprises in the UK are using cloud services and the vast majority intend to increase their use.

When data protection laws were introduced across the EU, developments such as these could not be envisaged. When information is locked away in a filing cabinet, it is relatively easy to secure. As more and more data is transferred in electronic form and posted to the internet or cloud services, security becomes more of an issue. And data has also become more valuable – it is no longer just of interest to private individuals or organisations, and their competitors, but to a much wider range of actors from organised crime to nation states, for whom such information is of enormous value.

Another factor that has changed the technology landscape since 1995 is the consumerisation of IT. Employees are increasingly demanding that they have their say in the choice of devices that they use, not just for leisure, but also for work. Not only do they wish to use their own devices, but also the cloud-based applications of their choice. According to Eurostat, across Europe, 21% of individuals use cloud services to store files – but young people are three times likelier to use cloud services than those aged 55 and above. ***Workshare*** found recently that employees are regularly using cloud-based file share applications, yet only 28% had authorisation from the organisation to do so. According to ***Symantec***, through the use of unsanctioned file sharing services, 83% of large enterprises and 70% of SMEs have had sensitive information placed in the cloud without organisational oversight.

According to Eurostat, across Europe, 21% of individuals use cloud services to store files – but young people are three times likelier to use cloud services than those aged 55 and above.

Figure 2: How cloud services are being used



Source: Eurostat

Member states began revising their own laws

The spiralling number of data breaches over the past 20 years led to the introduction of mandatory data breach notification legislation, starting with California in 2003. Now the majority of US states have some form of notification requirements in place.

Until now, there has been no such legislation in place at a European level. To provide greater protection for sensitive data within their borders, many EU member states went their own way and rewrote their laws to be more far-reaching than the EU directive. Many have made provision for the use of sanctions in the event of a data breach. An example is Spain, which is considered to be the strictest, with fines of up to 600,000 euros imposed per breach incident.

This resulted in there being a patchwork of data protection laws across the EU, muddying the water for any organisation active in more than one jurisdiction.

Another factor that has upped the ante on data protection is the revelations made regarding surveillance by government agencies, ostensibly for the purposes of national security. There have been various instruments put in place at an EU level to safeguard the transfer of data from EU member states to those jurisdictions not considered to have comparable levels of security. The use of these instruments has been interpreted differently by member states and one of the key instruments, the use of the Safe Harbour agreement, has recently been declared invalid.

The new EU data protection regulation

All of these factors contributed to the realisation that data protection legislation in the EU needed to be updated. New legislation that builds on the data protection directive of 1995, rather than completely rewriting it, was agreed upon in December 2015 in the form of the general data protection regulation of the EU. It is expected to be formally adopted by the European Parliament and Council in the first half of 2016 and should come into force in early 2018. As a regulation, rather than a directive, member states are immediately required to adhere to its requirements, without the need to pass their own national legislation.

The intention is not only to create a level playing field across the EU, but to increase the dragnet of those organisations that must comply with data protection obligations. When the regulation comes into effect, any organisation that collects, stores, processes or shares the data of EU residents, whether or not they have operations in the EU, must comply with its requirements.

The definition of personal data has always been broad in terms of data protection legislation in the EU, without even the definition of sensitive personal data being included. The new data protection regulation looks to expand the definition even further. In the new regulation, online identifiers such as IP addresses that could be used to create profiles of individuals and to identify them are included. Therefore, personal data should be considered to be any information relating to an individual.

One benefit to organisations with cross-border operations will be that they no longer need to deal with the data protection agency in each separate member state. Rather, they will be able to deal with just the authority where they are primarily based, with the exception of data on employees. It is estimated that this measure will save organisations 2.3 billion euros per year.

The regulation will, however, place a burden on organisations in terms of the need to appoint a data protection officer for those organisations that have more than 250 employees or that process information on more than 5,000 individuals within a twelve-month period. The difference between a data protection and a compliance officer is that a data protection officer will be more directly responsible for data security and processes for handling data security.

For high-risk situations regarding the rights and freedom of individuals, organisations will have to conduct data protection impact assessments. Among activities identified by the European Commission as high risk are processing activities that include information about health or race, large-scale public video surveillance, or information involving children, or genetic or biometric data.

“One benefit to organisations with cross-border operations will be that they no longer need to deal with the data protection agency in each separate member state.”

One of the most major changes regards mandatory breach notification, which many organisations will find particularly onerous as they are expected to notify the authorities within 72 hours of discovery of the breach. Where the breach is likely to impact the rights and freedoms of the individuals concerned, those individuals should be notified without undue delay.

Sanctions are also to be set at high levels for non-compliance, especially for repeat violations. Warnings may be issued for first-time offences or for non-intentional non-compliance. But where an organisation is deemed to be culpable, organisations could be fined 4% of global turnover or 20 million euros, whichever is higher, for serious offences, or 2% of global turnover or 10 million euros, whichever is higher, for more minor offences.

Impact of the general data protection regulation at a glance

Expanded scope: *any organisation the processes data of EU citizens must comply, no matter where they are located or data is stored.*

Personal data: *the definition of sensitive personal data has been expanded to include genetic and biometric data, as well as online identifiers such as IP addresses or cookie identifiers, as well as other identifiers such as RFID tags.*

Breach notification: *data protection authorities must be notified of a breach within 72 hours of its discovery unless the breach is unlikely to result in a risk for the rights and freedoms of individuals. Records must be kept of all breaches that the authorities are not notified about. Where the breach is likely to impact the rights and freedoms of individuals, data subjects must be notified without undue delay.*

Sanctions: *Data protection authorities can impose fines for non-compliance of up to 4% of an organisation's global revenue or 20 million euros, whichever is higher. A 2% fine or 10 million euros, whichever is higher, is applicable for more minor breaches.*

Data protection officer: *a data protection officer must be appointed by organisations with more than 250 employees or that holds 5,000 records or more. SMEs for which data processing is not a core activity are exempt from this requirement.*

Data protection impact assessments: *where processing is deemed to be high risk for the rights of individuals, organisations must conduct a data protection assessment prior to processing. The assessment must detail the safeguards, security measures and mechanisms put in place to address risk and ensure compliance with the regulation.*

"A recent survey by Vanson Bourne of 300 organisations in France, Germany and the UK found that 69% of respondents acknowledge that the data protection regulation will affect their business."

The network and information security directive

At the same time as agreement was provisionally reached on the general data protection regulation, the first ever EU-wide cybersecurity rules, which have been advocated by the European Parliament for some time, in the form of the network and information security directive were provisionally agreed upon. The rules will apply to providers of essential services such as electricity, water, healthcare, banking and transport services, as well as digital services such as search engines, online marketplaces and cloud computing.

Whilst not much detail is yet available about what the directive will constitute, the implementation period is expected to be in two years time. Details have not yet been released of what form of liability will be imposed on organisations that do not take reasonable measures to ensure the security of their networks, although the obligation to declare breaches and security incidents is included. Security incidents can include those caused by technical failures, unintentional mistakes, natural disasters or malicious attacks.

A recent survey by Vanson Bourne of 300 organisations in France, Germany and the UK found that 69% of respondents acknowledge that the data protection regulation will affect their business.

Now is the time to prepare

A recent survey by ***Vanson Bourne*** of 300 organisations in France, Germany and the UK found that 69% of respondents acknowledge that the data protection regulation will affect their business, although 18% claim to have no idea of the impact, despite the fact that they store and process data. In total, 90% of respondents state that they store and process personal data, and 40% share it externally using means such as email, portable storage and the postal system. Slightly more than two-thirds are worried about the burdens that compliance will place on them.

The new general data protection regulation specifies that organisations must take appropriate technological and organisational measures to protect data, including putting in place strong privacy controls. It states that organisations should adopt internal policies and implement measures that meet the principles of data protection by design and data protection by default. This means that data protection and privacy should be considered right from the beginning of the security planning process. Among measures to be taken are minimising the amount of data collected, restrictions on data sharing and the implementation of and adherence to retention policies.

Appropriate safeguards for securing data include encryption and pseudonymisation. The use of encryption avoids the need for breach notification, as long as it has been competently implemented, since this makes the data unintelligible to anyone without authorisation to access it. The regulation also introduces the concept of pseudonymisation. Pseudonymisation means the processing of data in such a way that it can no longer be attributed to a specific individual without the use of additional information. Therefore, pseudonymised data must be kept separately from any additional information to ensure non-attribution to an identified or identifiable persons.

Encryption and pseudonymisation enable one of the principles of data protection by design which is that privacy protections must follow the data, wherever it resides and throughout its entire lifecycle. Another strong safeguard is the use of adequate access controls and strong authentication.

To ensure ongoing security of data, all systems should be regularly, if not continuously, monitored and a process should be put in place for regularly testing, assessing and evaluating the effectiveness of the technical and organisational measures for ensuring security. When assessing security, organisations should take into account the risks associated with data processing and storage, including accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

As well as taking measures such as these, adherence to industry standards and best practices will help organisations to achieve compliance with the general data protection regulation. These include PCI DSS, the ***SANS Top 20 Critical Security Controls***, and ISO 27001 or ISO 27002 information security standards. ISO 27001 will help to ensure that the principle enshrined in the regulation that appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. It is designed for organisations that wish to achieve accreditation for their information security management systems. ISO 27002 provides a code of practice with regard to information security management systems but does not provide accreditation. In the event of a breach, the courts will likely take into account compliance with either ISO 27001 or ISO 27002 as a sign that an organisation has the necessary safeguards in place when assessing issues of negligence.

The use of encryption will lessen the impact

According to the Vanson Bourne survey, 69% of respondents state that they will need to make investments in technology to reduce the impact of the new general data protection regulation, with just 16% stating that there would be no need. As shown in **Figure 3**, the top two investments likely to be made are in encryption, and analytic and reporting technologies.

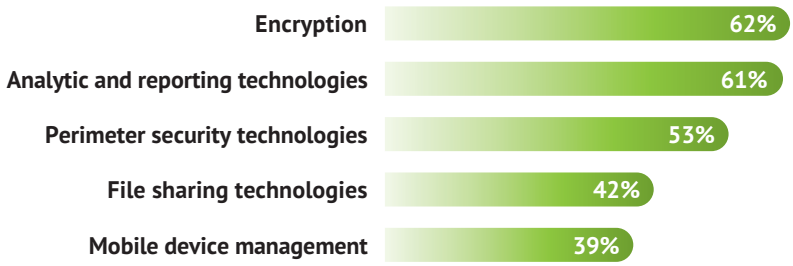
Given that many breaches are looking to uncover sensitive information, encrypting all such data makes good business sense. This requires that an organisation takes an inventory of the information that it produces, stores and communicates so that it knows not only what it has, but where and how it is stored, and which information is shared with third parties such as suppliers. When considering what data is sensitive, a good rule of thumb is everything that is meant to be internal to the organisation and anything that could compromise an individual.

Data to be encrypted should include both structured and unstructured information stored in databases or included in spreadsheets, word documents, presentations and archives.

As well as this, data should be encrypted as it moves out of the organisation, placed in the cloud, or stored and accessed on mobile devices. For this, it is vital that cryptographic keys remain with the organisation, never being stored in the cloud. Ideally, keys should be stored in a hardened appliance, through which centralised encryption policies can be enforced. This will prevent any unauthorised access by employees of the cloud provider and will also scupper attempts by governments to demand access to data, with associated gagging orders to prevent the service provider from informing customers that they have complied with the order. Eric Schmidt, the chairman of Google, has openly said that "the solution to government surveillance is to encrypt everything." The same truism holds for protecting from hacker surveillance.

When considering what data is sensitive, a good rule of thumb is everything that is meant to be internal to the organisation and anything that could compromise an individual.

Figure 3: Technology investments for achieving data protection regulation compliance



Source: Vanson Bourne

When choosing an encryption solution, there are different types of encryption that are suited to different purposes. Data at rest on servers or any type of storage system is best protected with file-level encryption, which ensures that data is inaccessible to system administrators, is protected from advanced targeted threats, and access by users can be logged and controlled. To protect data in databases from administrators, additional cryptography should be employed in the form of tokenisation, which preserves the format of the information, but which masks sensitive data such as credit card, identification card and bank account information, as well as customer names. This will greatly aid in ensuring PCI compliance, as well as regulations that demand that sensitive data is adequately protected. For endpoints that are easily lost or stolen, full-disk encryption is taking over from file- and folder-level encryption. It removes the decision by a user as to whether they need to encrypt data or not and has no impact on the performance of the device, making it transparent to the user.

Whatever encryption type is used, it should be easy to deploy, with no changes required to applications, and should provide the ability to discover and encrypt data that has been left unencrypted.

“Whatever encryption type is used, it should be easy to deploy, with no changes required to applications, and should provide the ability to discover and encrypt data that has been left unencrypted.”

Table 1: Comparing encryption types

Risk	Booted full-disk encryption	File-level encryption	Application encryption or tokenisation
Data unrecoverable when drive lost or stolen	Yes	Yes	Yes
Data made inaccessible to root and system administrators	No	Yes	Yes
Data made inaccessible to database administrators	No	No	Yes
Data protected from advanced threats using root credentials for data exfiltration	No	Yes	Yes
Control and log users and processes that can access stored data	No	Yes	Yes
Assure backups and snapshots are encrypted	No	Yes	Yes

Source: Vormetric

Encryption by itself is not sufficient

Encryption is an extremely useful technology for protecting data and should be seen as a strategic part of the entire security system deployed by any organisation. It will certainly lessen the impact of any security incident that threatens sensitive data, whether the threat comes from internal or external sources, but it is not in itself enough. Rather, it needs to be backed up with access controls that audit and report on authorisations granted, and to be integrated with controls that provide visibility over sensitive data and that guard against the latest threats seen.

Encryption access controls are necessary for ensuring that only authorised users can access data and for controlling what they can do with it. Even after a user is granted access to an encryption key, access is continuously controlled, enforcing controls on user entitlements to access information, as well as other factors such as time of day. They can even stop an authorised user from providing access to another person. In order to effectively control access, integration with Active Directory, or any other LDAP directories used by the organisation, is a must.

Integration with security information and event management (SIEM) systems provides greater visibility over who is accessing what and what they are doing with data, combined with other forensic information contained in the SIEM system. Visibility is key to ensuring both security and for achieving and proving compliance with regulations, which will be especially important given the sanctions that will be available with the new data protection regulations. SIEM systems can also provide further security by identifying emerging issues in real time. They also aid in strong auditing and reporting of access controls by correlating and analysing all related log data.

“In order to effectively control access, integration with Active Directory, or any other LDAP directories used by the organisation, is a must.”

Summary

New disruptive technologies are changing the way we do business and the way that data flows around networks, both internal and external, such as cloud-based services. They allow easier access to data – both for business users and for attackers. The new general data protection regulation of the EU that was agreed in December 2015 aims to increase the protection of sensitive data, taking into account new technology developments and increasing the sanctions that can be imposed for non-compliance. It is due to come into force in early 2018. In the same timeframe, the network and information security directive will come into effect, requiring all providers of essential services to notify the relevant authorities of any security incidents they suffer. All organisations should start preparing now and should ensure that the technology that they have in place is up to the task. Encryption technologies are ideal for safeguarding sensitive data and should be the default option. But, by itself, encryption is not enough. It needs to be a strategic part of the organisation's data security system, working alongside complementary technologies that include access controls and security intelligence systems. This will give organisations the peace of mind that their sensitive data is adequately controlled, with centralised management to provide a comprehensive, consistent data security strategy.

All organisations should start preparing now for the impact of the EU data protection regulation and should ensure that the technology that they have in place is up to the task.

FURTHER INFORMATION
Further information is available from
www.BloorResearch.com/update/2268

About the author

FRAN HOWARTH
Senior Analyst, Security

Fran Howarth specialises in the field of security, primarily information security, but with a keen interest in physical security and how the two are converging. Fran's other main areas of interest are new delivery models, such as cloud computing, information governance, web, network and application security, identity and access management, and encryption.

Fran focuses on the business needs for security technologies, looking at the benefits they gain from their use and how organisations can defend themselves against the threats that they face in an ever-changing landscape.

For more than 20 years, Fran has worked in an advisory capacity as an analyst, consultant and writer. She writes regularly for a number of publications, including Silicon, Computer Weekly, Computer Reseller News, IT-Analysis and Computing Magazine. Fran is also a regular contributor to Security Management Practices of the Faulkner Information Services division of InfoToday.

Bloor overview

Bloor Research is one of Europe's leading IT research, analysis and consultancy organisations, and in 2014 celebrated its 25th anniversary. We explain how to bring greater Agility to corporate IT systems through the effective governance, management and leverage of Information. We have built a reputation for 'telling the right story' with independent, intelligent, well-articulated communications content and publications on all aspects of the ICT industry. We believe the objective of telling the right story is to:

- Describe the technology in context to its business value and the other systems and processes it interacts with.
- Understand how new and innovative technologies fit in with existing ICT investments.
- Look at the whole market and explain all the solutions available and how they can be more effectively evaluated.
- Filter 'noise' and make it easier to find the additional information or news that supports both investment and implementation.
- Ensure all our content is available through the most appropriate channels.

Founded in 1989, we have spent 25 years distributing research and analysis to IT user and vendor organisations throughout the world via online subscriptions, tailored research services, events and consultancy projects. We are committed to turning our knowledge into business value for you.

Copyright and disclaimer

2nd Floor
145–157 St John Street
LONDON EC1V 4PY
United Kingdom

Tel: **+44 (0)207 043 9750**
Web: **www.BloorResearch.com**
email: **info@BloorResearch.com**