INDUSTRY WHITEPAPER

Is data security in **Financial Services** simply a box-ticking exercise?

A four step guide to protecting your organization's reputation and your customers' data

egress®

In their day-to-day role, banks, insurance providers, brokers and credit unions have to process and exchange enormous amounts of data, most of which contains private and confidential information.

This therefore requires security in order to protect it. As more and more of this information goes digital and needs to be communicated electronically, it is critical that financial services providers maintain the levels of privacy and security their customers and partners have come to expect. A primary aspect of this is ensuring compliance with the Gramm-Leach-Bliley Act (GLBA).

GLBA compliance – the recognised benefits

As anyone working in financial services knows, the GLBA requires organizations to explain their information sharing practices to their customers and to safeguard sensitive data. Under the specific details of the Safeguards Rule, institutions must develop a written security plan that describes how the company is prepared for, and plans to continue to protect clients' personal information. By embracing GLBA compliance, many organizations have not only avoided expensive fines and the reputational damage of a high profile data breach, but also see tangible improvements in the service they deliver. To ensure compliance, financial services providers have been forced to invest in the necessary technology, processes and training to protect sensitive information. What's more, in turn this investment also improves connectivity and communication between staff, customers and external partners.

Is there a disconnect between compliance and data breach prevention?

If we look at the steps taken to achieve data security compliance alone, it might seem as if the financial services industry is doing everything it can to prevent data breaches and unauthorised access to customer data.

Current research, however, suggests otherwise. The 2015 Breach Level Index report shows that since 2013, the number of data breaches in US financial services has increased by nearly 50%.

At the same time, the scale and publicity surrounding breaches has increased dramatically. Examples include:

> "...25% of all breaches in 2015 were as a direct result of accidental loss or human error"

- The US Federal Deposit Insurance Corporation (the Federal Government's bank insurance agency) admitted to having lost **160,000** personal banking records as a result of the inadvertent actions of seven departing employees
- JP Morgan Chase reported the sensitive and personal information of **76 million** households and **seven million** small businesses had been compromised. Lost data included usernames, addresses, phone numbers and email addresses
- Global Payments Inc. reported **1.5 million** card accounts had been compromised in a data breach. The cost of the breach was estimated at **more than $90m**
- Citibank stated a data breach affected **360,000** credit card holders and was estimated to have cost the bank over **$19.4m**

The BLI report also indicates that 25% of all breaches in 2015 were as a direct result of accidental loss or human error.

How can financial services providers protect themselves and their customers?

The majority of organizations will be able to demonstrate that they have the necessary processes and systems in place to meet GLBA compliance requirements. However, with breaches and their associated costs on the increase, and many businesses suffering the reputational consequences of a headline-grabbing incident, a fresh approach to data security is required.

In most cases, financial services providers need to consider a four step approach:

1. Planning

In many cases, organizations are under such pressure to act that planning is overlooked in favour of investment in new systems and processes intended to mitigate the risks of a data breach. As a result, organizations end up with badly implemented processes, and systems sitting in silo that are hard to use and sit outside an end user's day-to-day work practices.

Instead, organizations need to first consider their people and processes, and then the best-fit technology solution (if appropriate). In most cases, by limiting the changes to current processes, and implementing technology that is easy to use and integrates into an existing set of infrastructure, organizations have the best chance of successfully managing the transition to new working practises.

2. People

For any change in process or technology to be successful, an organization needs its people to understand and embrace the importance of data security.

Education therefore plays a key role in any organization's move towards maintaining GLBA compliance. In most cases, staff will immediately recognize the importance of security when sharing sensitive data, but will often be unsure of how to identify information that needs to be secure versus data that doesn't, and the associated process for securing it.

By putting in place simple processes, easy-to-use technology and the underlying training, an organization can ensure its people are its first line of defence rather than its biggest vulnerability.

At the same time, providers should consider data security solutions that take decision-making away from the end-user. For example, email and file classification can be implemented as part of a Data Loss Prevention (DLP) solution to integrate with email and file encryption. Consequently, an organization can put in place policy that decides whether an email or a document should be secured (encrypted) at the gateway, rather than relying on a member of staff to remember to encrypt before sending from their desktop.

3. Technology

One very obvious way to help protect your organization against a data breach and work towards GLBA compliance is to implement data security technology.

The Federal Trade Commission (FTC), the agency charged with policing and protecting consumer affairs, themselves state that the use of encryption should be a mandatory requirement when protecting sensitive data.

"if data security solutions are difficult to use... users will typically revert back to older, less secure methods for sharing data"

As part of any investment in technology, the following should be considered:

a. **Ease of use** – if data security solutions are difficult to use or require considerable investment in training, users will typically revert back to older, less secure methods for sharing data – often via clear text email.

b. **Integration** – the more data security technology can integrate into existing infrastructure, the greater the usage levels. This is particularly important given the shift towards the Cloud and mobile working practises. For example, an organization moving to Microsoft Office 365 needs to know that their choice of email encryption solution or secure large file transfer mechanism will seamlessly integrate into a hosted Exchange environment. Similarly, when staff are constantly on the road, secure and easy access to encrypted data via mobile devices is equally important.

c. **Protect data throughout its lifecycle** – no longer can secure information sharing be treated in silo. From the point of creation, to sharing it internally with colleagues or externally with customers and partners, sensitive data needs the appropriate levels of protection and care applied to it. As a result, organizations need to consider how they combine / integrate secure data exchange mechanisms – such as email encryption, large file transfer and secure online collaboration – with classification, DLP, auditing and reporting. Only by treating data security with this holistic approach will financial services providers be able to mitigate the risk of a breach and demonstrate the necessary levels of GLBA compliance.

4. Auditing and reporting

GLBA compliance and investigations caused by a data breach are not new concepts to the market, but they do require organizations to have a strong grip on reporting and tracking. Typically, as part of any breach investigation, organizations will be required to report:

- Where sensitive data is being transmitted
- How it is being transmitted (email, large file or collaborative environment)
- Who had access to the data
- Where the data is stored at rest and in transit

> "Reliance on multiple reporting tools that are separate from one another limits both the effectiveness of any auditing and speed of response."

In order to achieve this level of reporting, an organization is going to need sophisticated auditing technology in place that tracks data sharing at all times and can provide detailed and accurate reports within a short timeframe. Reliance on multiple reporting tools that are separate from one another limits both the effectiveness of any auditing and speed of response.

Not only is this technology instrumental in ticking the GLBA compliance box, but financial services provides can also benefit more generally by starting to reduce the number of breaches affecting the industry. As a result, they can better protect their organization and in turn their customers.

www.egress.com

info@egress.com
1-888-505-8318
@EgressSwitch