RESEARCH REPORT

Data protection priorities in 2016: **CIO research report**

Egress Software Technologies

egress®

Introduction: Data security on the agenda

Understanding of cyber security has never been greater. High-profile data breaches seem to hit the headlines every week, the Snowden Effect continues to make waves and encryption is now being incorporated as standard into consumer applications used in everyday life. The net result: businesses, their partners and their customers are now much more aware of potential data breaches and the need for effective security measures to protect sensitive information.

The penny seems to have dropped at an organisational board level as well. Cyber security now sits high on the agenda of most executive priorities across the enterprise – with the added pressure of the need to comply with new stringent EU data protection laws.

Despite this, the very fact the data breaches continue to rise prompts the following questions:

1. Are organisations able to effectively deploy encryption across their businesses to protect sensitive data throughout its lifecycle?

2. How are businesses prioritising their information security investment and is it in the right areas?

This report takes the findings of a recent survey[1] into CIO and board-level data protection priorities, adding weight to these concerns by demonstrating an alarming lack of confidence in information security systems. In fact, of the CIOs surveyed, 87% admitted to being worried that their current policies and procedures are not only putting their company at risk, but will also leave them exposed under the new EU General Data Protection Regulation (GDPR).

87%

of CIOs are concerned that their organisation will be exposed under the new EU GDPR regulations

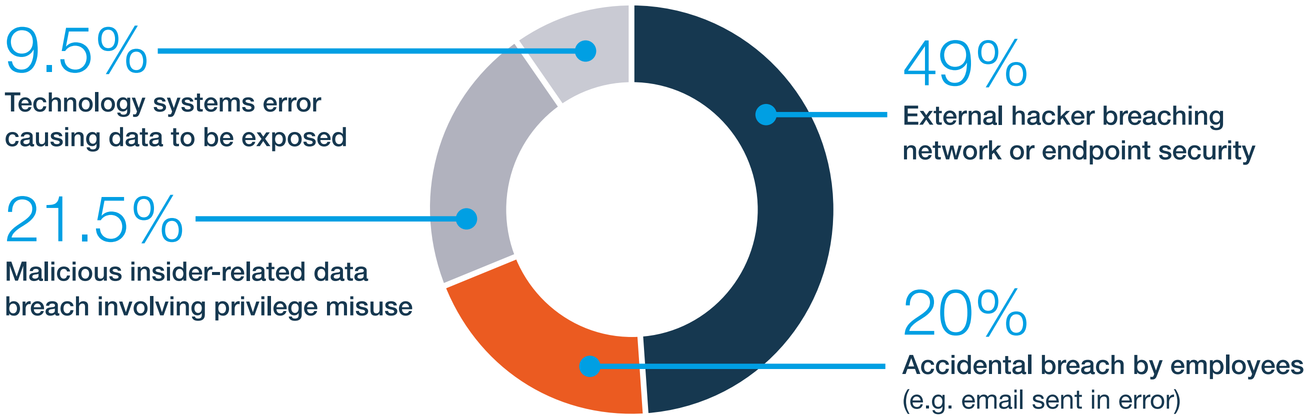
[1] The study sampled 200 CIOs from companies of 1,000+ employees.

Data security priorities are out of step with reality

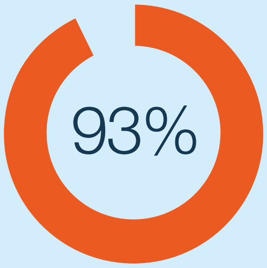
Throughout 2015 high-profile organisations were repeatedly the focus of media attention following cyber-attacks on their customer data, helping to educate much of the market about the importance of protecting customer data. Inevitably, this has led to a prioritisation of information security at a board level, when arguably even 18 months ago this wasn't the case.

Consequently, it comes as little surprise that 49% of CIOs report external hackers breaching network or endpoint security as the biggest information security priority for their boards. Only 20%, meanwhile, considered an accidental breach by employees (e.g. email sent in error) as their board's top priority.

What is the biggest **information security priority** for your board when protecting your customer data?



However, this shows a concerning disconnect with reality. For example, one aspect that has the potential to be overlooked is information shared in error with unauthorised users. These days, it seems that everyone has sent an email to the wrong address.



In fact, a recent Freedom of Information (FOI) request to the Information Commissioner's Office (ICO) demonstrated that **93% of data security breaches occur as a result of human error** – that is, people making mistakes when sharing sensitive information, organisations having poor processes and systems in place, and an overall lack of care when handling data.

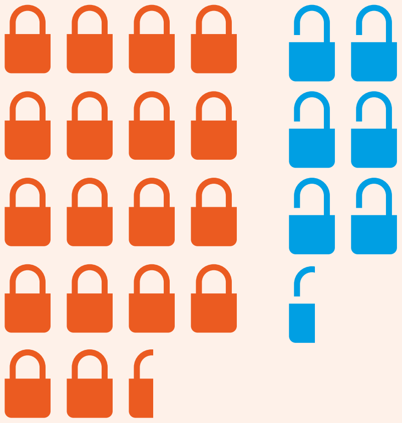
The emphasis being placed on cyber-attacks therefore has the potential to become a distraction for many organisations. There is little point securing the business from external attack when an internal error or lack of clear process could lead to an accidental breach and expose the organisation to financial penalties and loss of customer confidence any way.

Additionally, the number of reported breaches caused by human error is only set to rise with the enforcement of the EU GDPR now firmly on the horizon for 2018. The new legislation will bring with it a mandatory notification processes of **72 hours for data breach incidents and fines of up to 4% global turnover for organisations that have put sensitive customer data at risk**. It is little wonder therefore that 87% of CIOs are concerned their organisation might be exposed under the upcoming regulation.

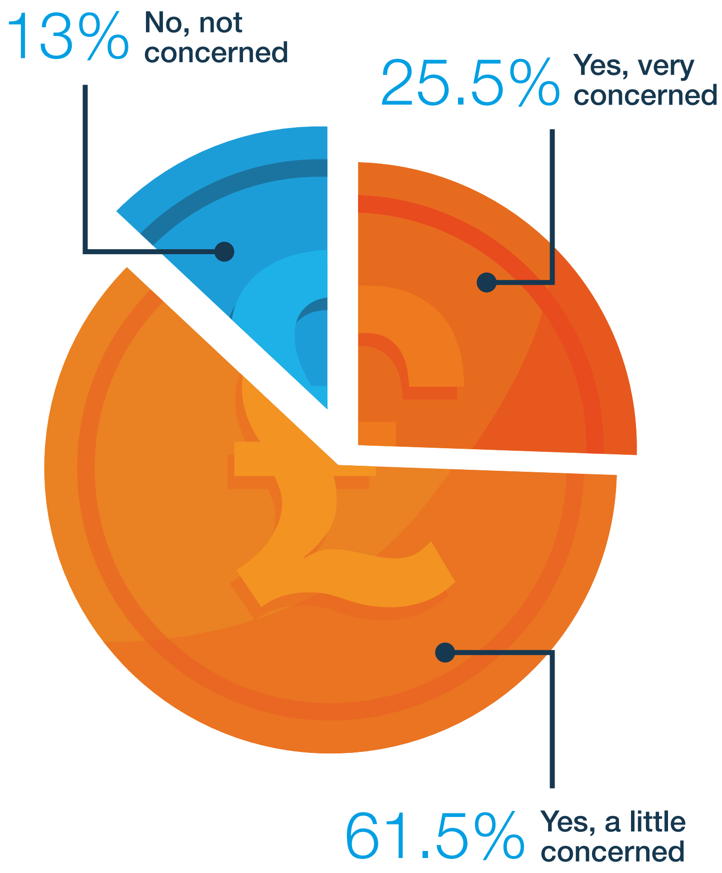
Do you intend to tighten up data sharing processes within your organisation and provide your employees with encryption?

YES: 73.5%

NO: 26.5%



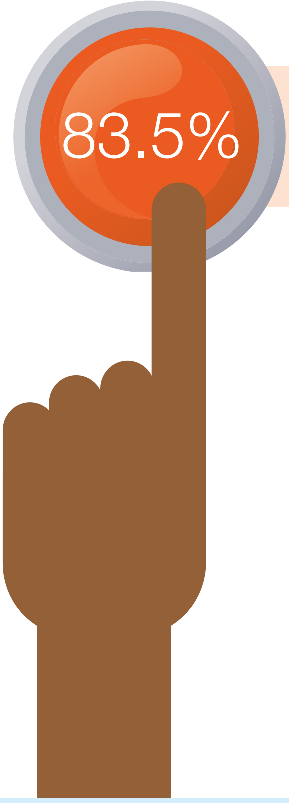
Are you concerned your organisation might be exposed under the new regulations?



These perceived vulnerabilities are consequently driving changes across industry, as shown by the 73.5% of respondents who are committed to tightening up data sharing processes within their organisation and providing their employees with encryption technology over the coming two years. This also raises concerns regarding the organisations that have identified the risk, but as yet are failing to invest in new technology or processes to resolve it. However, there is clearly a discord between this number and the 87% who feel their organisation will be exposed under stringent new rules from the EU. Of equal concern is that more than one-quarter (26.5%) don't plan to make any changes ahead of enforcement of EU GDPR. While their current systems and processes may be suitable under today's legislation, it is likely there could be a few shocks in store once the EU GDPR comes into force.

It's time to face up to the real issue

With legislative changes imminent and the threat of reputational damage caused by data breaches ever-present, investment in technology designed to protect information has risen dramatically in the last few years. However, the question remains: **Is this money being spent in the right areas?** The validity of this approach is called into question by 83.5% of respondents noting they would prioritise technologies based on perceived ease of deployment rather than their ability to secure data.

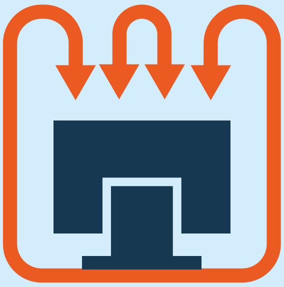


83.5% of CIOs prioritise security products based on perceived ease of deployment

However, by responding directly to the needs of customers, information security vendors are able to offer solutions that, for example, make email encryption as easy to use as standard email by deploying it centrally across the enterprise and seamlessly integrating via ADFS, SAML2 or other protocols. The focus is now very much on delivering information security, but not at the expense of staff efficiency – be it email encryption, secure collaboration or any other technology designed to securely exchange data electronically.

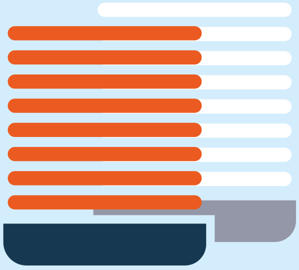
Employees are crying out for solutions and processes that support them to do their jobs and securely share sensitive data on a daily basis – be that via encrypted email or secure collaboration. Yet if IT teams are more concerned about potential pressures on IT helpdesks (44%), potential disruption to work processes (31.5%) and complex integrations (23%), there is little appetite to tackle the issue head on and businesses remain at risk.

Top three concerns when deploying encryption-based secure communication solutions...



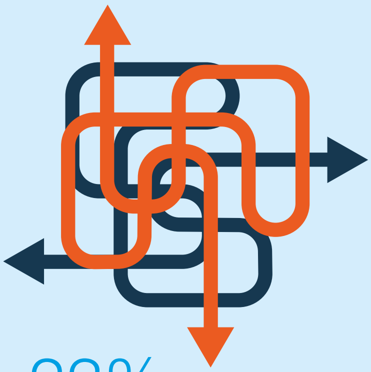
44.5%

High pressure on IT helpdesks



31.5%

Disruption to productivity

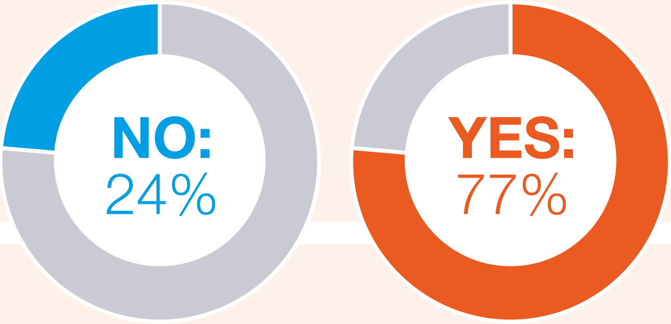


23%

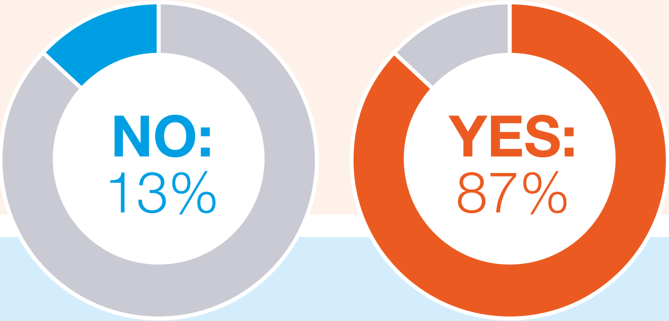
Issues integrating with existing systems

It is also apparent that even when technology is implemented, concerns remain for CIOs. 76.5% of respondents were frustrated that users choose not to use the tools made available to them, with 87% of these acknowledging this made their company more vulnerable.

Are you frustrated that users are avoiding using the tools provided to share information securely?



Are you concerned that this could be puting your organisation at greater risk of a data breach?



Reflecting on the findings, Egress Software Technologies CEO Tony Pepper:

> “This research is definitely a wake-up call for businesses’ priorities. Now it’s time for organisations to respond by investing in the right areas and, in doing so, tackle the heart of the problem. By procuring easily deployable technology that is simple for staff to use, not only will they gain end-user buy-in but will also protect the sensitive customer data they share. At the end of the day, this will not only help customer confidence but, by defending organisations from data breaches, will protect them from the reputational damage and large financial penalties that invariably follow a breach!”

Conclusion: A time for action

Organisations must also appreciate that, despite best efforts to the contrary, human error continues to play a major part in data breaches – and avoidance to acknowledge this now will only throw them in the path of the EU GDPR later. Mitigating this risk will require a balance of technology and process that puts protecting customer data at the centre but doesn't impact on productivity.

Firstly, organisations should be monitoring the data flowing in and out of their network, understanding what sensitive information individuals and departments are sharing, how they're sharing it and who they're sharing it with. Armed with this information, decision-makers can implement necessary and informed data protection measures, meaning everyone who needs to access encryption technology can do so. In addition, the ability to enforce policy scanning and encryption at the network boundary means that technology can catch mistakes that humans inevitably miss.

> "Decision-makers must also recognise that 'one-size-fits-all' does not apply for information security measures..."

Decision-makers must also recognise that 'one-size-fits-all' does not apply for information security measures, so solutions need to offer the necessary levels of flexibility to reflect this. Email, for example, will not always be the most suitable solution for sharing information. Employees may need to send confidential information by large file transfer or collaborate with individuals in other organisations on sensitive project materials. Uptake of encryption technology can be achieved by simply offering employees the correct tools. This can be further increased by providing a seamless and unified end-user experience, for example using single sign-on technology and selecting complementary solutions within an individual portfolio.

All this must be underpinned by employee awareness, helping staff to understand the causes of errors and developing procedures to reduce this risk. When employees understand and appreciate the impact that a breach of customer data can have – from damaged reputation to financial penalties and legal proceedings, they will be incentivised to use the encryption technology available to them.

Ultimately, organisations need to strike a balance between internal and external cyber security threats to ensure all-round defence of sensitive customer data. As this report shows, in the current information security landscape, particular care must be taken to not prioritise the fear of hackers breaching the network over the reality that employees carrying out their day-to-day jobs pose a bigger risk to confidential data. The sooner organisations wake up to this reality, the better – not simply in relation to the upcoming EU GDPR but by increasing consumers' and service users' trust by protecting their sensitive information.

Egress Software Technologies Ltd

Egress Software Technologies is the leading provider of hosted and on-premise encryption services designed to secure all forms of electronic information and delivered to customers in both the Public and Private Sectors via a single platform: Egress Switch.

The award-winning Switch portfolio of products includes Secure Email, Secure File Transfer, Secure Web Form and the latest online collaboration offering, Secure Workspace.

www.egress.com

✉ info@egress.com
☎ 0844 800 0172
@EgressSwitch