Press release

71% of UK C-suite willing to cover up a data breach if they could escape fines finds nCipher survey

Survey of UK IT leaders reveals impact of regulatory challenges, emerging technologies and employee engagement on security priorities

Cambridge, UK – May 29, 2019 – nCipher Security, the provider of trust, integrity and control for business critical information and applications, reveals UK IT leaders are alarmingly willing to cover up a data breach, with more than 3 in 5 (61%) saying they would do so if it meant they could escape fines.

It is now over a year since the implementation of the EU General Data Protection Regulation (GDPR), which obligates organisations to disclose breaches of personal data within 72 hours of becoming aware, when feasible. However, senior business leaders are more willing than managers or directors to cover up their organisation falling victim to a data breach, with 71% at C-level saying they would do so, compared to 57% of the latter category.

Ahead of the 2019 InfoSecurity Europe conference, nCipher Security surveyed 250 IT decision makers with responsibility over security purchases, revealing attitudes towards data breaches, regulation, security training and emerging technologies.

Investment in security training met by lack of employee engagement

While investment in technology is the biggest driver of security spending over the next 12 months, employee training and education is not far behind, taking up 29% of the average budget. However, despite 83% of businesses providing cyber training to staff at all levels, several factors are highlighted as major challenges to employee engagement.

For example, 66% said that they were hampered by a lack of skilled resource in-house to conduct the training, while the same percentage of respondents were challenged by an unwillingness to change process and behaviours.

In addition, 55% of IT leaders pinpointed a lack of support from the board and wider C-suite as a challenge, as well as a lack of best practice guidelines to work towards and implement (63%). Interestingly, all of these challenges were found to be much more acute within mid-sized companies (250-999 employees).

Emerging technology – a double edged sword for security

Cloud and Internet of Things (IoT) were revealed to be the emerging technologies most widely seen as a threat to organisations, at 63% and 62% respectively. At the same time, 80% confirmed that they are using these kinds of emerging technologies to "better identify threats to their business".

This demonstrates that businesses are continuing to push ahead with the adoption of innovative but experimental technology to gain an advantage and maintain relevance in their markets even though they might not have the right skills in place. However, this is tempered by a risk factor and scepticism towards these same technologies that is felt most keenly by those at C-Level within the business, creating an interesting paradox that organisations seem to be struggling to navigate.

ePR and GDPR causing confusion

This sense of risk is exacerbated by a compliance and regulation landscape that is becoming ever more complicated, and indeed costly – 30% of the average cyber security budget is spent on meeting compliance needs. GDPR isn't the only data regulation for businesses to concern themselves with; later this year it will be complemented by the ePrivacy Regulation (ePR), also enacted by the European Union. While 92% of respondents are aware of the latter, just 32% completely understand how it builds on GDPR and 37% are unaware of how it will affect their organisation.

Clearly there is much more for IT leaders to do to educate themselves and prepare their business for the impact. If the correct steps towards GDPR compliance have already been taken, businesses will be well on track, however there needs to be a greater awareness of regulatory nuance and how this will impact the way they collect and use customer data.

Peter Galvin, chief strategy and marketing officer, nCipher Security says:
"Organisations are under a greater obligation than ever to disclose data breaches, particularly when personal information is at risk, but evidently many IT leaders – particularly at C-Level - still feel they can avoid being subject to fines and other punitive measures from regulatory bodies.

"By implementing the right security measures to protect their business critical information and applications up front by using tools such as encryption, investing in training and talent as well as understanding the regulatory landscape, businesses can take steps to avoid a damaging breach in the first place."

Other key findings include:

- Just a quarter (28%) of organisations provide security training when employees join, and this lack of immediate training leaves them at risk
- Only 63% of businesses update training and repeat annually, meaning the majority of employees are unaware of the latest threats and how to protect themselves
- Over 8 in 10 (83%) have a plan in place if they were to become a victim of a data breach. This figure falls to 73% in businesses employing 1-249 people
- C-level respondents are concerned about emerging or future technologies as a threat to their business, much more so than their counterparts at manager and director level. The biggest discrepancy is regarding blockchain, with 71% of the former category seeing it as a threat as opposed to 51% of the latter
- 77% of organisations have plans in place to revisit or update their business approach to cyber security, based on emerging or future technologies.

nCipher Security will be exhibiting at Infosecurity Europe 2019 on stand F105. Visit us to learn how our cryptographic solutions guard against today's threats and attacks, enable compliance and protect your business applications.

Follow us on LinkedIn, Twitter, Facebook, YouTube and Instagram – search nCipherSecurity.

About nCipher Security

Today's fast moving digital environment enhances customer satisfaction, gives competitive advantage and improves operational efficiency. It also multiplies the security risks.

nCipher Security, a leader in the general purpose hardware security module (HSM) market, empowers world-leading organizations by delivering trust, integrity and control to their business critical information and applications.

Our cryptographic solutions secure emerging technologies – cloud, IoT, blockchain, digital payments – and help meet new compliance mandates, using the same proven technology that global organizations depend on today to protect against threats to their sensitive data, network communications and enterprise infrastructure. We deliver trust for your business critical applications, ensuring the integrity of your data and putting you in complete control – today, tomorrow, at all times. www.ncipher.com

###

For more information please contact:

nCipher Security
Megan Nemeh megan.nemeh@ncipher.com +1 408 887 5064
Liz Harris liz.harris@ncipher.com +44 7973 973648

UK Media
Hotwire PR nCipher@hotwireglobal.com