Making InfoSec Part of the Culture

Carolyn Harrison, Marketing Director , BeCyberSure

BeCyberSure

"The GDPR takes effect in May 2018. If you haven't done so already, you need to start preparing for it now, not this time next year."

Ken Macdonald
Head of ICO Regions

ico.
Information Commissioner's Office

But why does this affect me?

Excuses - including your supply chain

- I'm too small to need to do anything or be of interest
  - Usually easier target
- Nothing worth stealing
  - stepping stone
- My type of business is not a target
  - Every organisation is of interest to the criminal – they do not discriminate
- I don't handle money
- I outsource - IT, payments, HR etc
  - You are still responsible the accountability is not outsourced
- Someone else will pay or be responsible, they always do (eg., banks, Insurance)
  - Not any more!

Simple actions?

- That you are able to map and identify all personal data and its flow (as defined under the GDPR) collected, held or processed by your company, including work conducted on behalf of clients and any of your proprietary data which is processed by third parties on your behalf.
- That you are aligned with Article 32 of The GDPR – 'The Security of Processing' and in particular the pseudonymisation and encryption of personal data.
- That your collection, retention and processing of personal data has been subject to a Privacy Impact Assessment (PIA) and is in line with other requirements of the law in respect of limitation, minimisation, accuracy, retention and data subjects' rights.
- That your consent mechanisms (or other legal reasons for holding personal data) are compliant.
- Data Subject rights considerations (review, correction, destruction, transfer, etc).

Simple actions?

- Your purge and destruction processes.
- Transfer policies (including cross-border transfer).
- Subject Access Requests and related matters (ie. correction and transfer policies, etc).
- Breach notification and other event management plans, ensuring that your ISMS not only satisfies your recent ISO27001 accreditation but equally the additional aspects of GDPR
- Determine whether you need to appoint a Data Protection Officer (DPO).
- That all contracts (existing and new) entered into by your business reflect the requirements of the GDPR.
- Staff training and awareness (this is an area where the regulator is planning to place significant emphasis).
- Potential conflict with other legal compliance regimes (eg., MiFID II, PSD2, Solvency2, NYCRR500, et al).

Who is accountable?

Who should lead the evolutionary journey to being compliant?

The opportunity

Who has the most to gain?

PEOPLE
not devices

Education and training

- Are your employees aware of their obligations and liabilities with respect to the GDPR.
- Do you have an evidenced training programme in place
- Do you validate it and check
- How realistic and effective is your BCP and crisis management plan and regular training
- What is your organisations policy on paying ransomware?

- Who is likely to (inadvertently) keep you vulnerable?

Some interesting facts….

- 12,500 hand held devices , including USB drives get left behind in taxi cabs in London and New York every six months
- Half have no pin code, data is freely available
- UK dry cleaners find over 22,000 USB drives every year
- Globally, more than 20 million unprotected USB drives are lost a year!
- One fifth of people finding a USB drive will use them…
- More than a third of workers (35%) store more than 20 files on their USB flash drives, meaning that the loss of a single USB flash drive can expose a high volume of sensitive corporate information

"Don't view getting data protection right as something you're being forced to do; view it as something that you really want to do because it helps you build better, stronger relationships with your customers."

Garreth Cameron
Group Manager (Business and Industry)

ico.
Information Commissioner's Office

"Cyber security is not an IT issue, it is a boardroom issue. Companies must be diligent and vigilant. They must do this not only because they have a duty under law, but because they have a duty to their customers."

Elizabeth Denham
Information Commissioner

ico.
Information Commissioner's Office

PEOPLE
PROCESS
GOVERNANCE
TECHNOLOGY

95% of data losses involve insiders*

(user error or malicious act)

*IBM

Continuous cycle:

Awareness

Education

Training

The Human Firewall

80% of Data Breaches at larger companies have their genesis in the supply chain*

*Verizon

"Accepting broad accountability for data protection encourages an upfront investment in privacy fundamentals, but it offers a payoff down the line, not just in better legal compliance, but a competitive edge."

Elizabeth Denham
Information Commissioner

ico.
Information Commissioner's Office

About BeCyberSure

- Global Specialist covering the full spectrum of the 'Information Security' threat, including physical security, cyber security, governance, GDPR readiness, education and training and business continuity issues
- Some of the best names in the industry with a wealth of knowledge and years of experience that spans international borders and industry sectors – including from police, military and intelligence services backgrounds
- Our team incorporates professionals who understand the threats to business and specialists who are able to continually evaluate and pro-actively protect your organisaton