GDPR and security awareness top issues for CISOs, notes survey

INDUSTRY VIEW

24 July 2017 | Author: Jay Jay

GDPR, security awareness, and cloud security strategy are the top most concerns of security professionals, says a recent survey of 39 CISOs.

While most CISOs believe breach response is a priority, 63% of them focus more on prevention capabilities rather than response.

A survey of 39 CISOs by ClubCISO has revealed that as many as 78 percent of all CISOs consider the GDPR as the top issue, followed by security awareness (74 percent) and cloud security strategy (61 percent).

GDPR: Building data protection in by design and default

Responding to the survey, 63 percent of CISOs said that breach response was a major responsibility, but this was contradicted by the fact that 78 percent of company boards focussed on prevention capabilities instead of response.

""In the wake of a growing number of cyber-attacks, an increasingly fragmented (and therefore vulnerable) workforce, and a step-up in the complexity and effectiveness of malware, 78% of company boards still place their focus squarely on prevention capabilities, rather than response," said Marc Lueck, chairman at ClubCISO.

"At the same time, these same boards contradict themselves by prioritizing breach response very highly. In fact, 63% cite it as a major responsibility of the CISO. In other words, boards want CISOs to clean up the mess after a breach, but they're not necessarily taking a balanced approach to investing in solutions that enable them to do this quickly and effectively," he added.

Cloud adoption booming in the UK despite cyber-security concerns

In short, a majority of companies are focussing on tackling visible and perceived security risks as and when they come instead of fixing root causes and security processes. Raef Meeuwisse, author of *Cybersecurity Exposed: The Cyber House Rules*, said to *Infosecurity* that breach response is much more expensive for organisations compared to if security is embedded in systems by design.

RECOMMENDED

FEATURES / NEWS / OPINION / THREATS

Crypto currency hacks: Hacking the unhackable

IOT / NEWS / THREATS

IoT soldiers' communications intercepted and disrupted in mock cyber attack

INFORMATION SECURITY / NEWS / THREATS

Hackers targeting Scottish Parliamentarians' email accounts with weak passwords

CURRENT AFFAIRS / FEATURES / LEGISLATION/GDPR / NEWS / OPINION

What can we expect from the new Data Protection Bill?

CURRENT AFFAIRS / NEWS

Indicted cybersecurity expert Marcus Hutchins thanks people's 'amazing support'

MOST POPULAR

INFORMATION SECURITY / LEGISLATION/GDPR / NEWS

Why the new Data Protection Bill isn't the GDPR

NEWS / THREATS

Existing ransomware myths impacting cybersecurity of UK businesses

CURRENT AFFAIRS / LEGISLATION/GDPR / MANAGEMENT / OPINION

GDPR Compliance in Six Steps

CURRENT AFFAIRS / NEWS / THREATS

Hutchins' conviction could land a big blow to the ethical hacking community

He compared the response of company boards with 'bailing water out of a boat that is riddled with holes'. Companies should fix security holes and vulnerabilities first instead of applying fixes, and this will ensure that symptoms will be permanently addressed.

"The organizations that are coming through the major cyber-attacks unscathed are not doing anything super-clever, but they are applying all the basic and sensible security basics, such as timely patch management, restricted installation (administration) rights, regular back-ups and AI anti-malware," he added.

Businesses must make biometrics part of their cyber security DNA

A separate survey of CISOs also revealed that as many as 80 percent of organisations in the UK are in favour of cloud adoption despite concerns on long-term security risks associated with the cloud. As many as 37 percent of such organisations have recently launched Cloud computing projects for the first time.

"Quite simply, CIOs cannot blindly trust that public cloud services will work flawlessly and be delivered perfectly at all times. The more responsibility CIOs hand over to providers, without ensuring that established ITSM principles are applied, the more they open themselves up to blame if one of those services fails," noted Paul Cash, managing partner at Fruition Partners who conducted the survey.

"CIOs should still be managing cloud services internally, rather than abdicating responsibility to the provider. Otherwise they risk losing control, and increasing both cost and risk to themselves and the business," he added.

Source: Infosecurity Magazine

INFORMATION SECURITY / NEWS / THREATS

Hackers release more HBO episodes after HBO declines to cooperate

INFORMATION SECURITY / NEWS / THREATS

SonicSpy spyware using Android apps to steal device information

ANALYSIS / INFORMATION SECURITY / MANAGEMENT / NEWS

13 things SMEs need to do to keep lucky

INDUSTRY VIEW / INFORMATION SECURITY / NEWS

China's new cybersecurity law forbids citizens' personal data to be stored outside China

INFORMATION SECURITY / LEGISLATION/GDPR / MANAGEMENT / NEWS

9 surprising things that are illegal under data protection rules