Stronger cyber resilience culture needed to combat the digital threat

Tuesday 27 June, 2017

With phishing and social engineering maintaining their position as the top driver of cyber disruptions, there is a need for a stronger cyber resilience culture across organizations, and a focus on the human aspects of the threat.

This is one of the key findings of the Cyber Resilience Report, published today by the Business Continuity Institute, the world's leading Institute for continuity and resilience, in collaboration with Sungard Availability Services ® (Sungard AS), a leading provider of information availability through managed IT, cloud and recovery services.

With the WannaCry ransomware attack still fresh in our minds, it is clear that the cyber threat is very real with this one attack affecting almost a quarter of a million computers across 150 countries. It is also clear that business continuity plays a key role in responding to an incident, and ensuring that the organization is able to manage through any disruption and so prevent it from becoming a crisis.

The Cyber Resilience Report found that nearly two-thirds of respondents (64%) to the global survey had experienced at least one cyber disruption during the previous 12 months, while almost 1 in 6 (15%) had experienced at least 10. Of those who had experienced a cyber disruption, over half (57%) revealed that phishing or social engineering had been one of the causes, demonstrating the need for users to be better educated about the threat and the role they can play in helping to prevent an incident occurring.

The study also found that:

- A third of respondents (33%) suffered disruptions totalling more than €50,000, while more than 1 in 10 (13%) experienced losses in excess of €250,000.
- 1 in 6 respondents (16%) reported a single incident resulting in losses of more than €50,000.
- 1 in 5 respondents working for an SME (18%) reported cumulative losses of more than €50,000. These are significant losses considering 40% of SMEs involved in this study reported an annual turnover of less than €1 million.
- Phishing and social engineering are the top cause of cyber disruption, with over half of those who experienced a disruption (57%) citing this as a cause.
- 87% of respondents reported having business continuity arrangements in place to respond to cyber incidents, indicating that it is now widely accepted as playing a key role in helping to build cyber resilience.
- 67% of respondents stated that their organization takes over one hour to respond to a cyber incident, while 16% stated that it can take over four hours.

The number of respondents reporting top management commitment to implementing the right solutions to the cyber threat increased to 60%, and this is likely due to a number of factors such as the intense media coverage of cyber security incidents, and the impending European Union General Data Protection Regulation, which is due to come into force in less than a year and will have an impact on any organization that holds data on EU citizens.

David Thorp, Executive Director at the BCI, commented: "*Cooperation is key to building cyber and organizational resilience. Different disciplines such as business continuity, information security and risk management need to come together, share intelligence and start speaking the same language if they want to build a safer future for their organizations and communities.*"

Keith Tilley, EVP and Vice Chair at Sungard Availability Services, said: "*Brexit and the pending EU General Data Protection Regulation (GDPR) have thrown up even more questions about data laws and compliance, so data sovereignty is a focus. Companies need to demonstrate a holistic understanding of where their data is hosted, where it's backed up, moved and recovered, as well as who can see it along the way. The fact that data laws are constantly subject to change, with region and country specific regulation, means a headache for large organizations. Establishing how to meet these regulations, as well as global needs will be vital, as will the ability to handle data access, residency, integrity and security.*"

Media:

Business Continuity Institute
BCI CYBER RESILIENCE REPORT
CYBER S
SUNGARD AVAILABILITY SERVICES

Related Sectors:

Business & Finance :: Computing & Telecoms ::

Related Keywords:

Cyber Resilience :: Cyber Security :: Information Security :: Business Continuity ::

Scan Me:

Company Contact:

_

The Business Continuity Institute

T. 0118 9478241
E. andrew.scott@thebci.org
W. https://www.thebci.org

View Online

Additional Assets:
http://www.thebci.org/index.php/bci-cyber-resilience-report-2017

Newsroom: Visit our Newsroom for all the latest stories:
https://www.thebci.pressat.co.uk