Faster response times needed to combat cyber threat

Wednesday 29 June, 2016

Two thirds of respondents to a global survey by the Business Continuity Institute reported that they had experienced at least one cyber incident during the previous twelve months, and 15% reported they had experienced at least ten incidents during the same period. The frequency of these cyber incidents demonstrates why it is important for organizations to have plans in place to mitigate against them or lessen their impact.

The Cyber Resilience Report, conducted by the BCI and sponsored by Crises Control, found that there was a wide range of response times for cyber incidents. Almost a third of organizations (31%) stated that they responded within one hour. However, one fifth (19%) take a worrying four hours or more in responding to a cyber event, and almost half (44%) take more than two hours to respond. This has clear implications for the time taken to return to business as usual, and the ultimate cost of the incident to the organization.

Even if organizations wish to respond immediately to a cyber attack, the nature of the attack may render them unable to do so. The research found that phishing and social engineering was the top cause of cyber disruption, with over 60% of companies reporting being hit by such an incident over the past 12 months, and 37% hit by spear phishing.

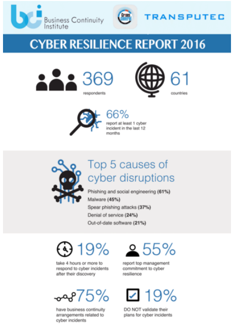
It also found that 45% of companies were hit by a malware attack and 24% by a denial of service. All these forms of attack will, in different ways, render an organization’s own network either contaminated or inoperable. Their website may have been taken down and they may well have to switch off their internet connection until they can secure themselves from further attack.

The research, a study of 369 business continuity and resilience professionals from across the world, also revealed that the costs of these incidents varied greatly, with 73% reporting total costs over the year of less than €50,000, but 6% reporting annual costs of more than €500,000.

David James-Brown FBCI, Chairman of the BCI, commented: “*This piece of research is one of the most timely, insightful and relevant the BCI has ever produced. Cyber attacks tend to target the weakest links of an organisation, and this calls for a greater awareness of ‘cyber crime’. As the cyber threat evolves, it is crucial to stay on top of it, building long-term initiatives and regularly updating recovery plans.*”

Rickie Sehgal, Chairman of Crises Control, said: “*Rapid communication with employees, customers and suppliers is vital for any company in terms of responding effectively to a major business disruption event such as a cyber attack. When your business is at risk, even a one hour delay in responding to an incident can be too long. Taking more than two hours to respond, as almost half of companies do, is just unacceptable.*”

Media:



Related Sectors:

Business & Finance :: Computing & Telecoms ::

Related Keywords:

Cyber Threat :: Cyber Attack ::

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:

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