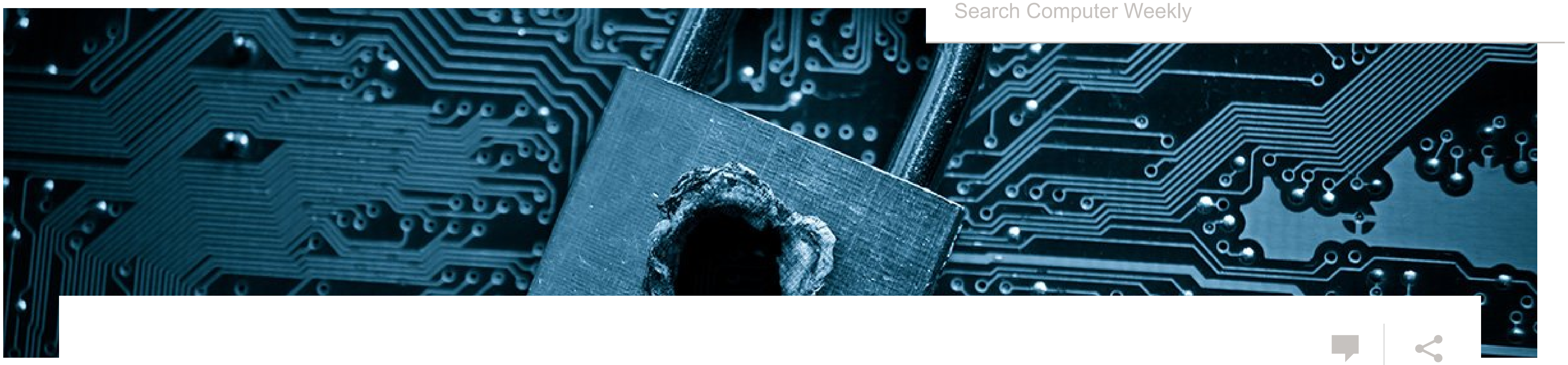

Small businesses hit hardest by cyber crime costs

Small businesses felt the biggest impact of the UK’s cyber crime bill in 2018, research shows

Small businesses in the UK bore the brunt of the £17bn cost of cyber attacks in 2018, according to research from business internet service provider (ISP) Beaming.

Almost two-thirds of UK companies employing between 10 and 49 people – the equivalent of 130,000 businesses nationwide – fell victim to some form of cyber crime last year, the survey found.

The average cost of cyber attacks to small businesses was £65,000 in damaged assets, financial penalties and business downtime.

The puts the total cost of cyber crime across all UK small businesses in 2018 at an estimated £13.6bn. This represents 80% of the financial impact of cyber attacks on all UK business in the past year, with a third reporting that they were hit by cyber crime.

Warwick Ashford
Security Editor
25 Mar 2019 11:25

The survey, conducted by research consultancy Opinium, found that while phishing emails claimed the greatest number of victims (25%), ransomware attacks were the most financially damaging, costing victims £21,000 each on average.

Although the trend for large businesses to fall victim at the highest rate continued, with seven in every 10 companies of more than 250 people being hit, the rate at which small companies succumbed to cyber criminals reached its highest level since Beaming started surveying business leaders in 2016.

Nearly two-thirds (63%) of small businesses reported being a victim of cyber crime in 2018, up from 47% of small businesses in 2017 and 55% in 2016. The proportion of small business victims exceeded that of medium-sized organisations (61%) for the first time in 2018.

Sonia Blizzard, managing director of Beaming, said the research showed that cyber criminals do not care how big a business is. “Everyone is a potential victim, and the cost of an attack can be devastating. Larger businesses fall victim at the greatest rate because they have more people and more potential sources of vulnerability. However, they also tend to have multiple layers of protection in place to limit the spread of an attack and are able to recover more quickly after one,” she said.

Blizzard also noted that small businesses were trusting more data to the cloud and accessing it from lots of locations. “This provides greater flexibility and efficiencies, but also adds to the importance of ensuring data is held and transported securely.”

A specialist ISP can help, said Blizzard, by managing a network with the security of business traffic in mind, assisting with the implementation of additional security measures such as managed firewalls and providing advice to clients to enhance the protection on offer. “When choosing cloud products, businesses should ensure they have the right connectivity to go with it,” she said.

> **“Everyone is a potential victim, and the cost of an attack can be devastating”**
>
> **Sonia Blizzard, Beaming**

More than half of European firms admitted to business disruption and data loss due to cyber attacks in the past 24 months, with UK firms among the most targeted, a recent survey by security firm Kaspersky Labs found.

This disruption was in the form of service disruption (31%), data integrity issues (18%) and data loss (15%), according to the poll of nearly 2,000 European firms.

David Emm, principal security researcher at Kaspersky Lab UK, said the survey findings indicated that the odds of a business falling victim to costly cyber attacks had increased dramatically. “This should act as a stark warning for business owners and IT decision-makers to strengthen their defences,” he said.

Read more about SME security

- Cyber fraud costs SMEs more than £1,000 per case.
- SMEs failing to address cyber threats, despite the risks.
- UK government announces initiatives aimed at boosting SME cyber security, promoting the cyber security profession and supporting cyber security innovation projects.
- SMEs typically face the same threats as bigger organisations, but lack the same level of expertise and other security resources.

Read more on Hackers and cybercrime prevention

ALL | NEWS | IN DEPTH | BLOG POSTS | OPINION | PHOTO STORIES | VIDEOS

Lack of security skills exposing business to attack

Multi-pronged approach to cyber security professional development

Russian cyber espionage groups targeting EU governments

Spike in cyber attacks targeting Cisco Webex

Load More

Start the conversation

[CODE]

Share your comment

☑ Send me notifications when other members comment.

Add My Comment

Latest TechTarget resources

CIO

SECURITY

NETWORKING

DATA CENTER

DATA MANAGEMENT

SearchCIO

JOANN Stores hires new CIO to push customer experience strategy

JOANN Stores' announcement of a new CIO hire is another signal that engaging customers is increasingly part of the CIO portfolio.

Comparing chatbots vs. virtual assistants vs. conversational agents

Is a conversational agent the same as a chatbot or a virtual assistant? Not exactly. IBM Watson VP and CTO Rob High explains the ...

About Us

Meet The Editors

Contact Us

Privacy Policy

Our Use of Cookies

Advertisers

Business Partners

Media Kit

Corporate Site

Contributors

Reprints

Archive

Site Map

Answers

E-Products

Events

In Depth

Guides

Opinions

Quizzes

Photo Stories

Tips

Tutorials

Videos

Computer Weekly Topics