Top 10 cybercrime facts you need to know in 2018

Cybercrime is now the number one threat facing U.S. businesses of all sizes, including SMBs.

Last year's high-profile ransomware attacks have shown business owners that cyber-criminals don't discriminate when it comes to their targets. With experts agreeing that 2018 will be an even bigger year for cybercrime, no business can afford to be complacent.

If you're not convinced, check out these 10 alarming cybercrime facts that reveal the scale of the problem that's costing small firms big money.

01

$7.35 million is the average cost of a data breach in the United States, according to the Ponemon Institute – a 5% increase from 2016. The average cost for SMBs is $690,000.

02

61% of SMBs experienced a cyber-attack in the last 12 months, up from 55% the previous year. 54% of firms had data breaches involving the theft of customer and employee information.

03

Every 39 seconds a hacker attacks an internet-connected computer in the United States. The Clark School at the University of Maryland also found that 1 in 3 Americans has already been the victim of a cyber-attack.

04

More Americans pay ransoms than businesses in any other country. Symantec's 2017 Internet Security Threat Report found that 64% of U.S. businesses admit giving in to ransomware demands, compared to the 34% global average. There's no guarantee that paying a ransom will release hijacked data, and doing so encourages cybercrime to continue.

05

1 in 5 businesses faced downtime of 25 hours or more following ransomware attacks last year, according to Osterman Research. Many had to shut down their systems for longer than 100 hours. U.S. businesses have more downtime than the global average.

06

Most threats are caused by employees. 54% of data breaches are the fault of negligent workers or contractors clicking on suspicious emails and websites, up from 48% last year according to the Ponemon Institute's 2017 State of Cybersecurity in Small & Medium-sized Businesses.

07

U.S. businesses are less confident in their ability to prevent ransomware attacks than most countries. Only 7% of organizations told Osterman Research they felt "very confident" about data security compared to the 10% global average.

08

Cybersecurity vacancies will triple to hit 3.5 million job openings worldwide by 2021. Cybersecurity Ventures predicts that the U.S. alone will have more than half a million unfilled positions as the demand for security experts outpaces the supply.

09

$5 billion was the worldwide toll of ransomware attacks in 2017, according to Cybersecurity Ventures estimates – more than 15 times the cost just two years earlier ($325 million). Ransom demands themselves are only a fraction of this cost. More money is lost to downtime, productivity losses and fines.

10

$6 trillion will be the global cost of cybercrime by 2021. The projected rise of organized crime and state-sponsored hacking will make cybercrime more profitable than the global drugs trade, involving the greatest transfer of economic wealth in history.

Are you ready for the next WannaCry?
Talk to your IT partner to find out how to better protect your business.

Sources

https://www.prnewswire.com/news-releases/ibm–ponemon-institute-cost-of-a-data-breach-dropped-10-percent-globally-in-2017-study-300476378.html

https://keepersecurity.com/2017-State-Cybersecurity-Small-Medium-Businesses-SMB.html

https://www.securitymagazine.com/articles/87787-hackers-attack-every-39-seconds

https://www.symantec.com/security-center/threat-report

https://www.malwarebytes.com/pdf/white-papers/SecondAnnualStateofRansomwareReport-USA.pdf

https://keepersecurity.com/2017-State-Cybersecurity-Small-Medium-Businesses-SMB.html

https://www.malwarebytes.com/pdf/white-papers/SecondAnnualStateofRansomwareReport-USA.pdf

https://cybersecurityventures.com/jobs/

https://cybersecurityventures.com/ransomware-damage-report-2017-5-billion/

https://www.gartner.com/newsroom/id/3784965