New McAfee Report Estimates Global Cybercrime Losses to Exceed $1 Trillion

December 7, 2020

Latest Report from McAfee and CSIS Uncovers the Hidden Costs of Cybercrime Beyond Economic Impact

News Highlights:

- Global losses from cybercrime now total over $1 trillion, a more than 50 percent increase from 2018
- Two-thirds of surveyed companies reported some kind of cyber incident in 2019
- Average interruption to operations at 18 hours; the average cost was more than half a million dollars per incident
- IP theft and financial crime account for at least 75 percent of cyber losses and pose the greatest threat to companies
- Damage to companies also includes downtime, brand reputation and reduced efficiency
- 56 percent of surveyed organizations said they do not have a plan to both prevent and respond to a cyber incident

SAN JOSE, Calif.--(BUSINESS WIRE)--Dec. 7, 2020-- **McAfee Corp. (Nasdaq: MCFE) –** McAfee today released a new global report titled "The Hidden Costs of Cybercrime," which focuses on the significant financial and unseen impacts that cybercrime has worldwide. The report, conducted in partnership with the Center for Strategic and International Studies (CSIS), concludes that cybercrime costs the world economy more than $1 trillion, or just more than one percent of global GDP, which is up more than 50 percent from a 2018 study that put global losses at close to $600 billion. Beyond the global figure, the report also explored the damage reported beyond financial losses, finding 92 percent of companies felt effects beyond monetary losses.

"The severity and frequency of cyberattacks on businesses continues to rise as techniques evolve, new technologies broaden the threat surface, and the nature of work expands into home and remote environments," said Steve Grobman, SVP and CTO at McAfee. "While industry and government are aware of the financial and national security implications of cyberattacks, unplanned downtime, the cost of investigating breaches and disruption to productivity represent less appreciated high impact costs. We need a greater understanding of the comprehensive impact of cyber risk and effective plans in place to respond and prevent cyber incidents given the hundreds of billions of dollars of global financial impact."

The Hidden Costs of Cybercrime

The theft of intellectual property and monetary assets is damaging, but some of the most overlooked costs of cybercrime come from the damage to company performance. The survey revealed 92 percent of businesses felt there were other negative effects on their business beyond financial costs and lost work hours after a cyber incident. The report further explored the hidden costs and the lasting impact and damage cybercrime can have on an organization, including:

- **System Downtime**– Downtime is a common experience for around two thirds of respondents' organizations. The average cost to organizations from their *longest* amount of downtime in 2019 was $762,231. Thirty-three percent of survey respondents stated IT security incidents resulting in system downtime cost them between $100,000 and $500,000.
- **Reduced Efficiency**– As a result of system downtime, organizations lost, on average, nine working hours a week leading to reduced efficiency. The average interruption to operations was 18 hours.
- **Incidence Response Costs**– According to the report, it took an average of 19 hours for most organizations to move from the discovery of an incident to remediation. Many security incidents can be managed in-house, but major incidents can often require outside consults with high rates that form a significant portion of the cost of a large-scale incident.
- **Brand and Reputation Damage**– The cost of rehabilitating the external image of the brand, working with outside consultancies to mitigate brand damage, or hiring new employees to prevent against future incidents is part of the cost of cybercrime. 26 percent of the respondents identified damage to brand from the downtime experienced because of a cyberattack.

Companies Unprepared for Cyber Incidents

Through the research and analysis, the report found a lack of organization-wide understanding of cyber risk. This makes companies and agencies vulnerable to sophisticated social engineering tactics and, once a user is hacked, not recognizing the problem in time to stop the spread. According to the report, 56 percent of surveyed organizations said they do not have a plan to both prevent and respond to a cyber incident. Out of the 951 organizations that actually had a response plan, only 32 percent said the plan was effective.

The report concludes with key ways for businesses to deal with cybercrime. These include uniform implementation of basic security measures, increased transparency by organizations and governments, standardization and coordination of cybersecurity requirements, providing cybersecurity awareness training for employees, and developing prevention and response plans.

Download a full copy of the Hidden Costs of Cybercrime report for a complete analysis of the research as well as visual representations of the data.

Methodology

McAfee commissioned independent technology market research specialist Vanson Bourne to undertake the research that this report is based on.

Between April and June 2020, the quantitative study was carried out, interviewing 1,500 IT and line of business decision makers. Respondents came

from the US (300), Canada (200), the UK (200), France (200), Germany (200), Australia (200) and Japan (200). Respondents' organizations have 1,000 or more employees and were from all sectors except construction and property. However, only IT decision makers were interviewed in the Government sector.

Interviews were conducted online using a rigorous multi-level screening process to ensure that only suitable candidates were given the opportunity to participate.

Additionally, CSIS utilized a survey of open source material on losses accompanied by interviews with Government officials, and an estimate adjusted by national income levels using International Monetary Fund (IMF) income data to determine the cost of cybercrime.

About McAfee

McAfee Corp. (Nasdaq: MCFE) is the device-to-cloud cybersecurity company. Inspired by the power of working together, McAfee creates consumer and business solutions that make our world a safer place. www.mcafee.com

View source version on businesswire.com: https://www.businesswire.com/news/home/20201206005011/en/

McAfee Media Contact
Craig Sirois
media@mcafee.com

Source: McAfee