BRIDGET McCREA | Contributor

With Cyberattacks on the Rise, Companies May Spend More on Cybersecurity

With damage from cyberattacks on track to total $10.5 trillion annually by 2025—a 300% increase over 2015—companies of all sizes are spending more on security solutions to protect their networks and data.

A top concern for organizations across most industry sectors, cyberattacks can include everything from data theft and malware to ransomware and very basic phishing attacks, among other threats. As technology has advanced and as more data is being shared online, the number of threats and attacks has increased exponentially.

In its most recent *Cyber Readiness Report*, insurance provider Hiscox reveals that 48% of global companies reported a cyberattack in the past 12 months, up from 43% in 2021. In response, organizations and governments have upped their cybersecurity budgets by about 60% to a current $5.3 million. That represents a 250% increase over the amount spent on cybersecurity in 2019, according to Hiscox, which pegs the median cost of a cyberattack to just under $17,000 (a 29% increase over 2019's cost).

"One of the most telling findings in this year's report is that the cyber threat is now seen as the dominant risk to business in seven out of eight countries – ahead of the pandemic, economic downturn, skills shortages and other issues," Hiscox's CEO points out in the report. "If awareness of danger is the first step in dealing with it, that is surely an encouraging sign. On the downside, the number of firms reporting attacks has gone up, as has the severity of the attacks themselves. There can be no doubting the scale of the challenge."

Cyberattacks Proliferate

If it continues on its current trajectory, damage from cyberattacks will total about $10.5 trillion annually by 2025—a 300% increase from 2015's levels, according to Cybercrime Magazine's *2022 Cybersecurity Almanac*.

Measured as a country, cybercrime—which was predicted to inflict damages totaling $6 trillion globally in 2021—would be the world's third-largest economy after the U.S. and China. On their own, ransomware attacks cost organizations $20 billion in 2021—up from $5 billion in 2017 and $325 million in 2015, according to Cybersecurity Ventures.

These and other realities are pushing more organizations, governments and individuals to reassess their cybersecurity strategies and solutions. "As the digital economy grows, digital crime grows with it," McKinsey & Co., points out in a new report. "Soaring numbers of online and mobile interactions are creating millions of attack oppor¬tunities. Many lead to data breaches that threaten both people and businesses."

In surveying 4,000 midsized companies, McKinsey uncovered some of the key trends that are pushing organizations to rethink their cybersecurity approaches and invest in solutions that help them stay out in front of the "bad actors" that are trying to infiltrate their systems, steal their data or interrupt their operations. Some of the drivers include:

- **Attackers are targeting smaller organizations.** "From a demand perspective, fast-growing smaller organizations are exposed to proliferating digital touchpoints and ecosystem relationships," it says. "In addition, malware such as ransomware can pose an existential threat to small and midsize businesses (SMBs) and midmarket companies in a way it often doesn't to large enterprises."
- **More cybersecurity regulations are being introduced.** McKinsey says that at least 45 states and Puerto Rico introduced (or considered) more than 250 bills or resolutions that deal significantly with cybersecurity, including the U.S. National Defense Authorization Act and Executive Order 14028.
- **Chief information security officers want better visibility into cyberthreats.** Over the past three years, companies have improved their log volume (activity taking place in the cloud) visibility from about 30% to about 50% on average. McKinsey says they're now pushing toward 65-80% over the next three years.
- **Finding talent is more difficult than ever.** The global cyber-talent shortage is in full swing right as cyberattacks are ramping up. Because they can't just "throw more people" at the problem, organizations are looking for solutions that can help them identify, thwart and/or manage the threats.

Large Addressable Market

As the global economy continues to digitize, McKinsey predicts that the number of cyberattacks will grow and regulatory pressures will force companies to better protect their data and information. Amid the talent deficit, the race to implement more advanced solutions to combat cybercrime is sure to continue. In fact, the research firm says the addressable market for security solutions providers, which totaled about $150 billion in 2021, is likely more in the $1.5-$2 trillion range.