C-SUITE LIBRARY

SPONSORED BY:
Secureworks

BOARDROOM CYBERSECURITY 2022 REPORT

CYBERCRIME FACTS, FIGURES, PREDICTIONS AND STATISTICS

CYBERSECURITY VENTURES

STEVEN C. MORGAN, FOUNDER OF CYBERSECURITY VENTURES

BOARDROOM CYBERSECURITY REPORT

INTRODUCTION

Boardroom and C-suite executives tell us reports on cybercrime and cybersecurity are too technical, and use terms they don't understand.

Steve Morgan, founder of Cybersecurity Ventures

Our goal with this report is to provide a board of directors and the CEO with cyber economic facts, figures, predictions and statistics which convey the magnitude of the cyber threat they are up against, and market data to help understand what can be done about it.

– Steve Morgan, founder of Cybersecurity Ventures and Editor-in-Chief at Cybercrime Magazine

BOARDROOM CYBERSECURITY REPORT

TABLE OF CONTENTS

BOARDROOM CYBERSECURITY REPORT

JUST THE STATS

BOARDROOM AND C-SUITE EXECUTIVES are cringing over cybercrime damages, which are predicted to cost the world $7 trillion USD in 2022, according to Cybersecurity Ventures.

CYBERCRIME. Cybersecurity Ventures expects global cybercrime costs to grow by 15 percent per year over the next four years, reaching $10.5 trillion USD annually by 2025, up from $3 trillion USD in 2015.

RANSOMWARE. Ransomware will cost its victims around $265 billion (USD) annually by 2031, Cybersecurity Ventures predicts, with a new attack (on consumers and organizations) every 2 seconds. This is up from $20 billion in damages and an attack every 11 seconds in 2021.

CYBERSECURITY. Cybercrime will propel global spending on cybersecurity products and services to $1.75 trillion (cumulatively) for the five-year period from 2021 to 2025, according to Cybersecurity

JUST THE STATS

Ventures. We predict expenditures for cybersecurity products and services globally will grow to nearly $459 billion (annually) in 2025.

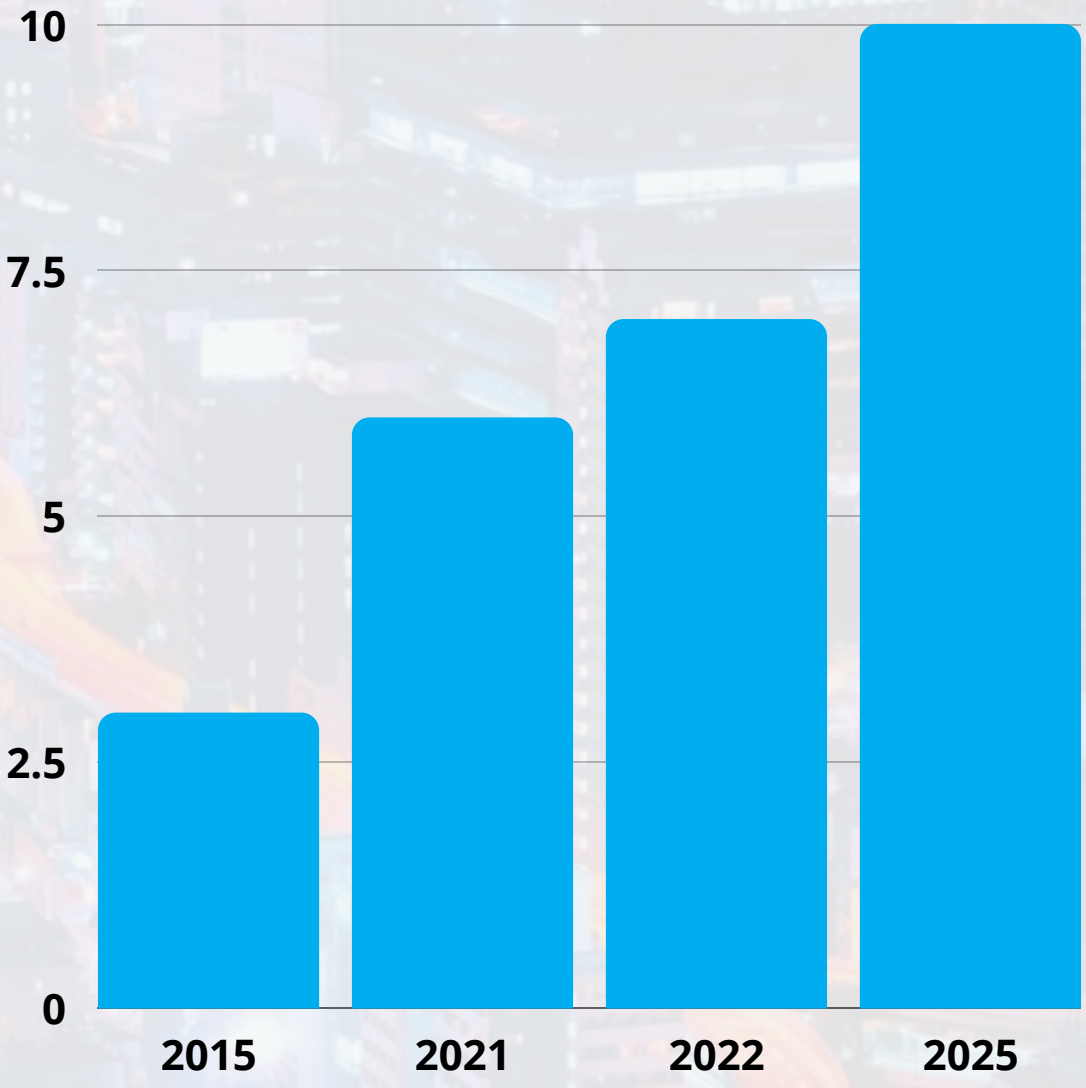
CYBERINSURANCE. Cybersecurity Ventures predicts the cyberinsurance market will grow from approximately $8.5 billion in 2021 to $14.8 billion in 2025, and exceed $34 billion by 2031, based on a CAGR (compound annual growth rate) of 15 percent over an 11-year period (2020 to 2031) calculated.

WORKFORCE. The number of unfilled cybersecurity jobs worldwide grew 350 percent between 2013 and 2021, from 1 million to 3.5 million, according to Cybersecurity Ventures. We predict that in five years from now, the same number of jobs will remain open.

BOARDROOM. Cybersecurity Ventures predicts that by 2025, 35 percent of Fortune 500 companies will have board members with cybersecurity experience, and by 2031 that will climb to more than 50 percent. This is up from an estimate of 17 percent in 2021.

GLOBAL CYBERCRIME COSTS

Cybercrime damage costs are predicted to grow from $3 trillion USD in 2015 to $10.5 trillion in 2025.



BACK TO THE FUTURE

The chief information security officer (CISO) role dates back to 1994, when financial services giant Citigroup (then Citicorp, ranked 17th on the Fortune 500 at the time) set up a specialized cybersecurity office after suffering a series of cyberattacks from Russian hackers.

Steve Katz was anointed CISO.

“I was running information security at JPMorgan at the time, and the rumor on Wall Street was that Citicorp had been hacked,” recalled Katz, in an interview with Cybersecurity Ventures.

“You know we had the hack so you have a blank check to set up anything you want,” Katz was told by his new bosses, who were tapped by the CEO and board at Citicorp to shore up their digital defenses. “We want to make sure it doesn’t happen again. We want you to build the best information security department anywhere on the globe.”

BACK TO THE FUTURE

Katz traveled the globe as Citi's ambassador, regaining trust from the bank's most important clients. He also built an exceptional team the board had asked for.

Fast-forward 28 years and today's boards and CEOs aren't nearly as involved with cybersecurity as Citi was when the world's first CISO was hired.

All too often it's not until an organization suffers a cyberattack that the board gets involved. And by that time, money isn't going to solve the problem.

"The reality is that business executives can't outspend the (cybersecurity) issue and they must be prepared," says Theresa Payton, former CIO at The White House and a top global cybersecurity expert who routinely advises boardroom and C-suite executives.

"Cybersecurity no longer exists in a vacuum," adds Payton, "and it must be elevated to the conversations

BACK TO THE FUTURE

held in the boardroom and with senior leadership as entire divisions, departments, and organizations. Cybersecurity is a team sport. We're all responsible."

It's time for boardroom and C-suite executives to go back to the future around cybersecurity, and take charge of defending their businesses.

The statistical data in this report is intended to spark conversation and motivate action around cybersecurity at the highest levels of organizations globally. We encourage CIOs and CISOs to borrow generously from our report when entering the boardroom.

CYBERCRIME

Boardroom and C-suite executives are cringing over cybercrime damages, which are predicted to cost the world $7 trillion USD in 2022, according to Cybersecurity Ventures.

If it were measured as a country, then cybercrime would be the world's third largest economy after the U.S. and China.

Cybercrime costs include damage and destruction of data, stolen money, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, post-attack disruption to the normal course of business, forensic investigation, restoration and deletion of hacked data and systems, and reputational harm.

Cybersecurity Ventures expects global cybercrime costs to grow by 15 percent per year over the next four years, reaching $10.5 trillion USD annually by 2025, up from $3 trillion USD in 2015. This represents the greatest transfer of economic wealth

CYBERCRIME

in history, risks the incentives for innovation and investment, is exponentially larger than the damage inflicted from natural disasters in a year, and will be more profitable than the global trade of all major illegal drugs combined.

The damage cost estimation is based on historical cybercrime figures including recent year-over-year growth, a dramatic increase in hostile nation-state sponsored and organized crime gang hacking activities, and a cyberattack surface which will be an order of magnitude greater in 2025 than it is today.

To mitigate the threat, cybersecurity should be a discussion topic in the boardroom of every company.

The SEC recently proposed new rules that would require U.S. public company boardroom disclosure of corporate directors with cybersecurity expertise.

In 2021, 17 percent of the 449 Fortune 500 companies that appointed new board members

CYBERCRIME

selected people with cybersecurity experience, according to the latest Heidrick & Struggles Board Monitor Report. That's up from 8 percent in 2020.

The FTC says board members need to talk the talk and walk the walk. They should demonstrate a sophisticated grasp of the data security challenges their company faces and act in a way that sets the tone for the entire organization.

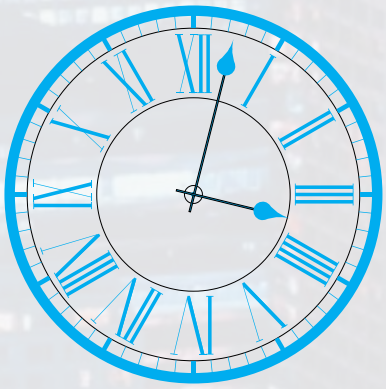
Jamie Hoxie, Assistant U.S. Attorney for Cybercrime in New Jersey, said the DOJ wants cybersecurity to be "a CEO-level priority both in the level of security on their network" and in "baking in security in the way tech is built — rather than today, when it often occurs by bolting it on or making it the responsibility of the user to configure technology."

Cybersecurity Ventures predicts by 2025, 35 percent of Fortune 500 companies will have board members with cybersecurity experience, and by 2031 that will climb to 50 percent. What about your board?

CYBERCRIME TO THE SECOND

A breakdown of global cybercrime damage costs predicted by Cybersecurity Ventures in 2022:

- $7 trillion USD a Year.
- $583 billion a Month.
- $135 billion a Week.
- $19.2 billion a Day.
- $799 million an Hour.
- $13.3 million a Minute.
- $222,000 a Second.



How much is cybercrime costing your organization annually?

Building cyber resiliency in an organization requires proper oversight from the boardroom based on a clear plan built on economic analysis, according to the World Economic Forum.

RANSOMWARE

A 2017 report from Cybersecurity Ventures predicted ransomware damages would cost the world $5 billion (USD) in 2017, up from $325 million in 2015 — a 15X increase in just two years. The damages for 2018 were predicted to reach $8 billion, for 2019 the figure was $11.5 billion, and in 2021 it was $20 billion — 57X more than it was in 2015.

Ransomware will cost its victims around $265 billion (USD) annually by 2031, Cybersecurity Ventures predicts, with a new attack (on consumers and organizations) every 2 seconds as ransomware perpetrators progressively refine their malware payloads and related extortion activities. The dollar figure is based on 30 percent year-over-year growth in damage costs over the next 10 years.

At the Cyber 2021 Conference at Chatham House, the UK's National Cyber Security Centre Chief Executive Officer Lindy Cameron said that ransomware attacks are the "most immediate threat" to all nations, with attacks linked to the Covid-19

RANSOMWARE

pandemic likely to persist for many years to come. Cameron warned that businesses and boards need to do more to protect themselves. The board will also be more demanding of CISOs and will require them to improve their communication skills, according to the Corporate Governance Institute.

“Two years ago boardroom execs were calling me in a time of crisis,” says Barry Hensley, Chief Threat Intel Officer and SVP at Secureworks©. “Now they’re planning ahead, looking into what their cyberinsurance covers, and they’re investing into the right places in order to mitigate risk.”

There’s not a week that goes by when Hensley isn’t talking to a boardroom executive about ransomware. “Leaders want to understand where they play a role in any security risk. They realize a breach may go public. Ransomware is the most damaging (cybercrime) from a business perspective.”

“In my view it (ransomware) is now the most

RANSOMWARE

immediate cybersecurity threat to UK businesses and one that I think should be higher on the boardroom agenda," said Cameron.

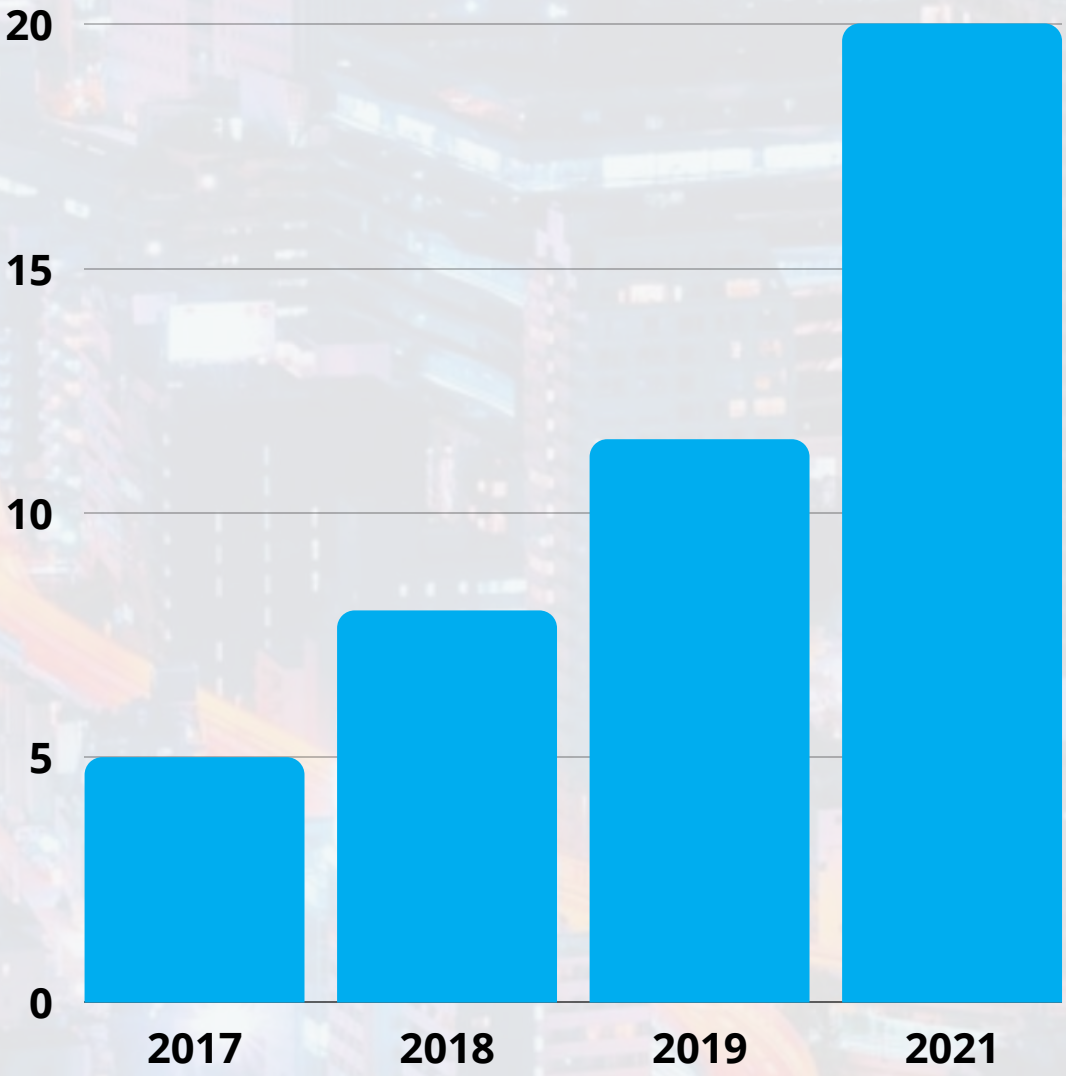
According to the World Economic Forum's annual report, The Global Cybersecurity Outlook 2022, 80 percent of cyber leaders now consider ransomware a "danger" and "threat" to public safety and there is a large perception gap between business executives who think their companies are secure and security leaders who disagree.

Some 92 percent of business executives surveyed agree cyber resilience is integrated into enterprise risk-management strategies; only 55 percent of cyber leaders surveyed agree. This gap between leaders can leave firms vulnerable to attacks as a direct result of incongruous security priorities and policies.

Ransomware is clearly a discussion topic for the boardroom. But is it being raised before or after your organization is struck?

GLOBAL RANSOMWARE COSTS

Ransomware damage costs are predicted to grow from $325 million in 2015 to $265 billion in 2031.



CRYPTOCRIME

Rapid growth in the use of decentralized finance (DeFi) services is creating a new soft spot for global financial systems, fostering new methods of cryptocrime for criminals whose “rug pulls” and other attacks will, Cybersecurity Ventures predicts, cost the world $30 billion in 2025 alone.

That’s nearly twice the $17.5 billion lost in 2021 — and expected to grow by 15 percent annually.

Cybercriminals’ attention to crypto is manifesting in a range of ways, including direct exchange hacks — such as the $30 million theft from Crypto.com in January — and scams designed to trick people into handing over their cryptocurrency holdings for any number of false purposes.

Scammers took $7.7 billion from victims thanks to crypto scams last year alone, reports CryptoSlate — an 81 percent increase compared to 2020 — and the Federal Trade Commission last year noted that losses had increased 10X over the previous 12 months.

CRYPTOCRIME

Blockchains have a bridge problem, and cybercriminals know it. Recent hacks on crypto bridges, including Horizon, Nomad, and Ronin, have collectively totaled hundreds of millions of dollars in monetary losses and related damages.

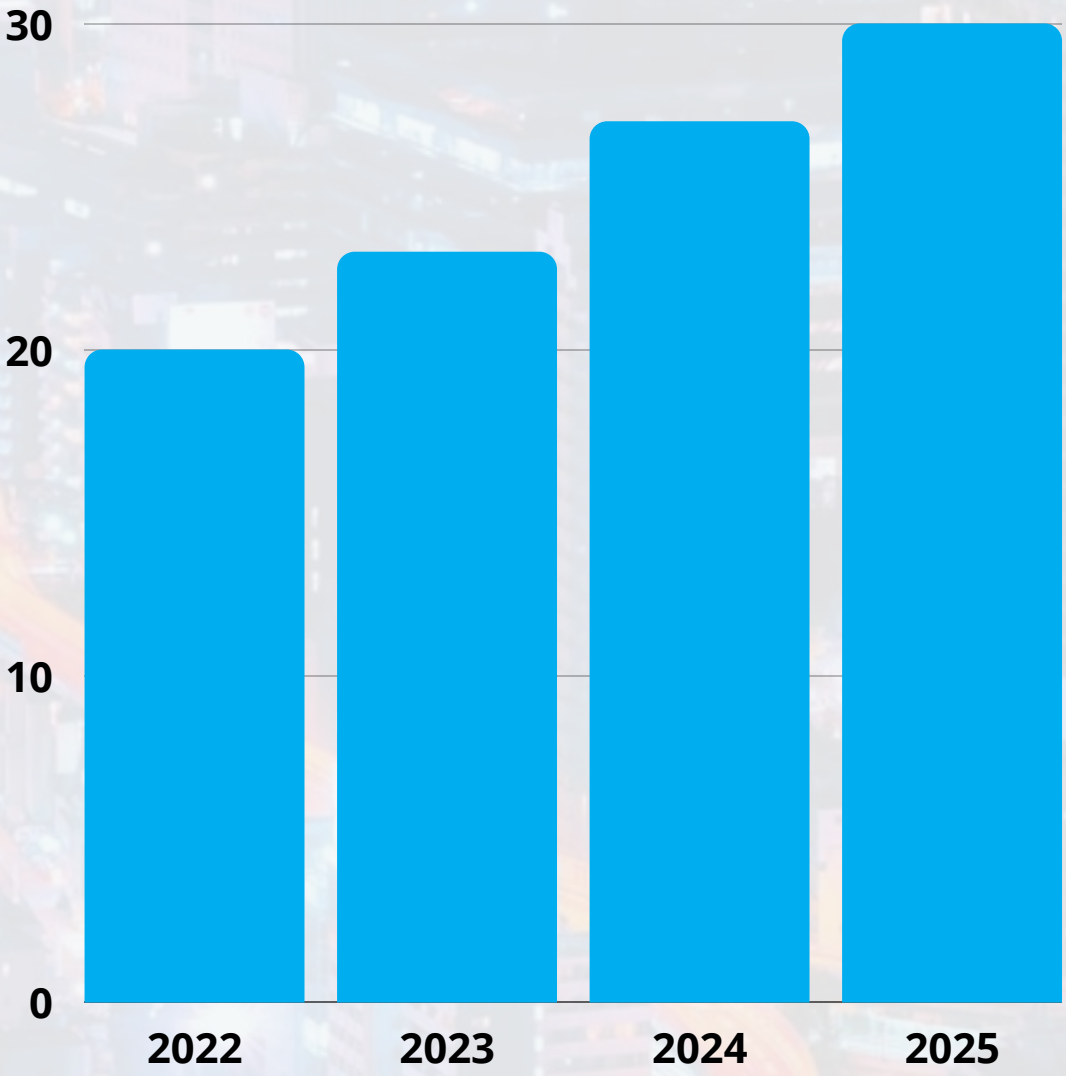
In early 2022, the U.S. Department of Justice appointed a first-ever Director for the National Cryptocurrency Enforcement Team (NCET), a new unit it launched last year tasked with investigating cryptocurrency-related crimes.

It is important to know that cryptocrime is uniquely different from other types of cybercrime.

Does your board have a go-to cryptosecurity expert?

GLOBAL CRYPTOCRIME COSTS

Cybersecurity Ventures predicts cryptocrime will cost the world $30 billion annually by 2025.



CYBERSECURITY SPENDING

In 2004, the global cybersecurity market was worth just $3.5 billion and now it's one of the largest and fastest-growing sectors in the information economy.

The imperative to protect increasingly digitized businesses, Internet of Things (IoT) devices, and consumers from cybercrime will propel global spending on cybersecurity products and services to $1.75 trillion (cumulatively) for the five-year period from 2021 to 2025, according to Cybersecurity Ventures. The figures reflect, in part, the dramatic change that the COVID-19 pandemic has wrought.

We predict expenditures for cybersecurity products and services globally will grow to nearly $459 billion (annually) in 2025.

Buoyed by the need to execute digital transformation initiatives faster than ever over the last year, businesses have doubled down on online services — overhauling existing products and developing entirely new ones based in the cloud.

CYBERSECURITY SPENDING

Yet even as these services took priority in companies' digital transformations, they also became lightning rods for cybercriminals who sensed the opportunity to find new forms of disruption — whether through profitable ransomware attacks, or by exploiting vulnerabilities to infiltrate and manipulate company networks.

Little wonder that CEOs now identify cybersecurity as the most significant risk their businesses face.

While all other tech sectors are driven by reducing inefficiencies and increasing productivity, cybersecurity spending is driven by cybercrime.

Cybersecurity is the only line item that theoretically has no spending limit. There is a budget before a company suffers a cyberattack or a series of them, and then there's the actual spend that takes place afterwards. What business isn't going to do and spend whatever it takes to recover from being hacked?

CYBERSECURITY SPENDING

In 2015, Bank of America CEO Brian Moynihan declared that the nation's second-largest lender had an unlimited cybersecurity budget. Moynihan was brutally honest. But really, what he said then is true now and in the future for Fortune 500 and Global 2000 enterprises all the way down to Main Street businesses. He just had the courage to say it without worrying about the repercussions. It's no surprise that in 2021 BoA's spending on cybersecurity eclipsed $1 billion for the year.

Look no further than ransomware, the fastest-growing type of cybercrime, to reinforce the notion of unlimited budgets when it comes to cybersecurity. Organizations can not possibly anticipate their spend in response to a ransomware attack and they'll never say there's no more budget to deal with it.

Markets aren't sized by unlimited budgets or the extraordinary lengths that companies are willing to go to if push comes to shove, but it is one of the dynamics in the burgeoning cybersecurity space.

CYBERSECURITY SPENDING

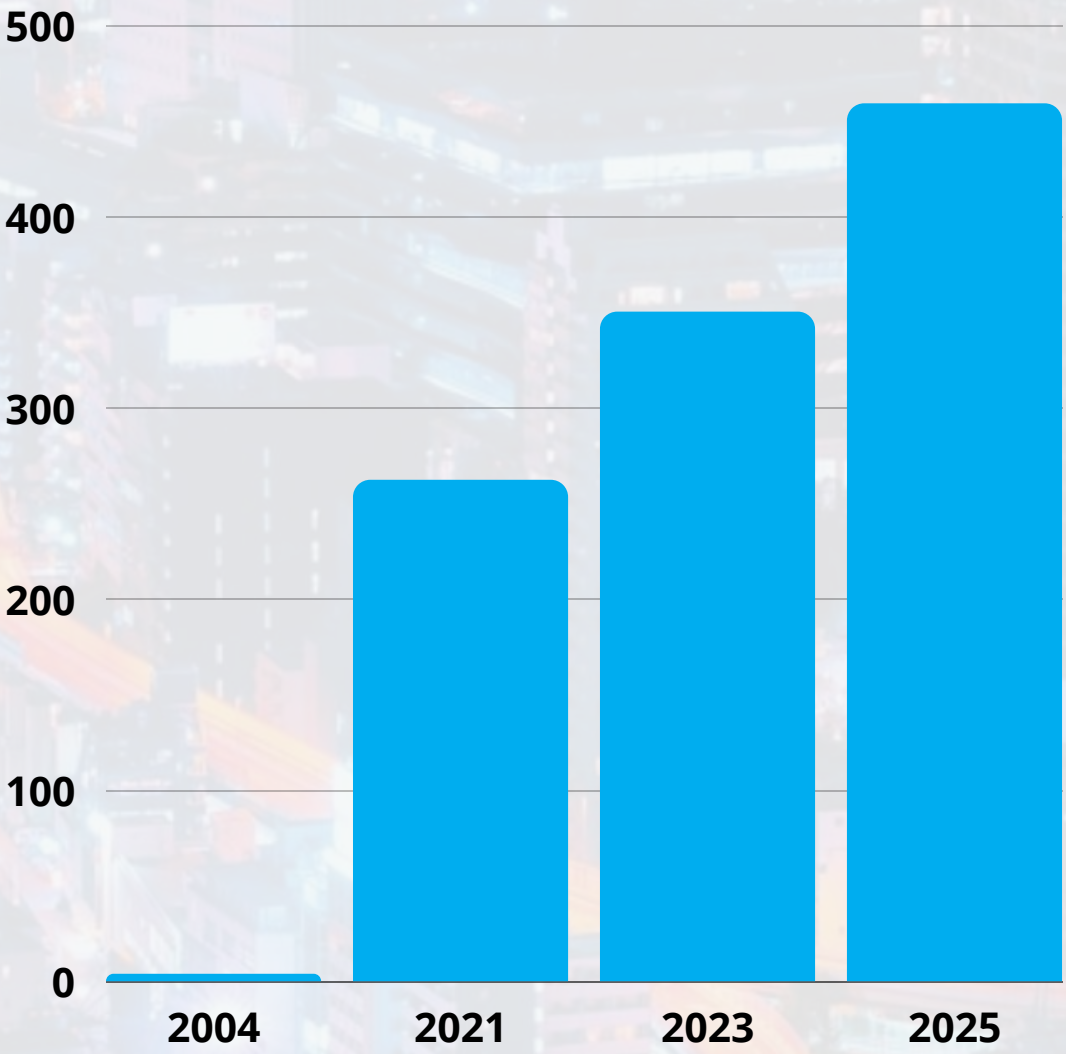
A boardroom sanity check on a realistic cybersecurity budget should take unexpected cyberattacks into consideration.

The cost of falling victim to a cyber or ransomware attack can be exponentially greater than the cost of investing in the people and technology that can prevent incidents in the first place – not something a boardroom should realize when it's too late.

“There’s a lot of money being spent on this (cybersecurity), and I think one of the things our industry has done a great job of is working together,” BoA’s Moynihan told CNBC last year.

CYBERSECURITY SPENDING

Cybersecurity Ventures predicts global spending on cybersecurity will hit $459 billion annually by 2025.



CYBERINSURANCE

Cyberinsurance has evolved rapidly in recent years, driven by the growing threat of cybersecurity compromise and awareness of corporate responsibility around breach prevention. Yet as the market's natural growth continues to be distorted by its untenable exposure to large ransomware payouts, changes to its operation and risk parameters will drive fundamental change through every aspect of the market.

For all its benefits in supporting a business response to conventional data breaches, the cyberinsurance industry is still far from resolving its increasingly enmeshed relationship with ransomware — and the future of the market will be shaped by the changes insurers make to cope with it in coming years.

The issue, of course, revolves around the payment of ransoms — a contentious topic that may, depending on where your business operates, range from perfectly acceptable, to inadvisable, to illegal.

CYBERINSURANCE

Back when ransoms were still in the four and five-figure range, insurers were broadly happy to cover their payment — seeing the payments as a cost of building up the sector's premiums base.

With ransomware artists now routinely demanding six and seven-figure sums — and victims of major attacks like JBS and Colonial Pipeline normalizing their payment as ransomware groups like REvil push claimed revenues past $100 million — cyberinsurers have been rapidly tweaking their exposure to ransomware extortion.

Since insurers aren't generally in the business of going bankrupt, increasing ransomware payments have driven a rapid surge in cyberinsurance premiums.

Broader efforts to reduce their exposure — especially in the face of an insufficient and fast-draining premium pool — are likely to drive many insurers to shift to a more proactive model in which they will put

CYBERINSURANCE

the onus on insured companies to substantiate their efforts to avoid ransomware compromise.

Demand for cyberinsurance is surging, according to Moody's Investors Service.

Maya Bundt, head of Cyber & Digital Solutions at Swiss Re, said last year cyberinsurance rates had increased by 30 to 40 percent in 2021, and at the time Marsh McLennan expected rates to rise 50 percent.

Munich Re's cyber premium volume alone was set to soar past the $1 billion mark in 2021. The insurance giant maintains that writing cyber policies is key to survival for major players in its space.

The cyberinsurance market opportunity is not lost on venture capital firms.

Specialty cyberinsurer Coalition has been on a fundraising tear. The five-year-old San Francisco

CYBERINSURANCE

company has raised a new round every year since 2018 including two last year — a $175 million Series D and a $205 million Series E. On Jul. 8, 2022, it announced $250 million in new funding from a Series F round that boosted its valuation to $5 billion from $3.5 billion at the end of 2021.

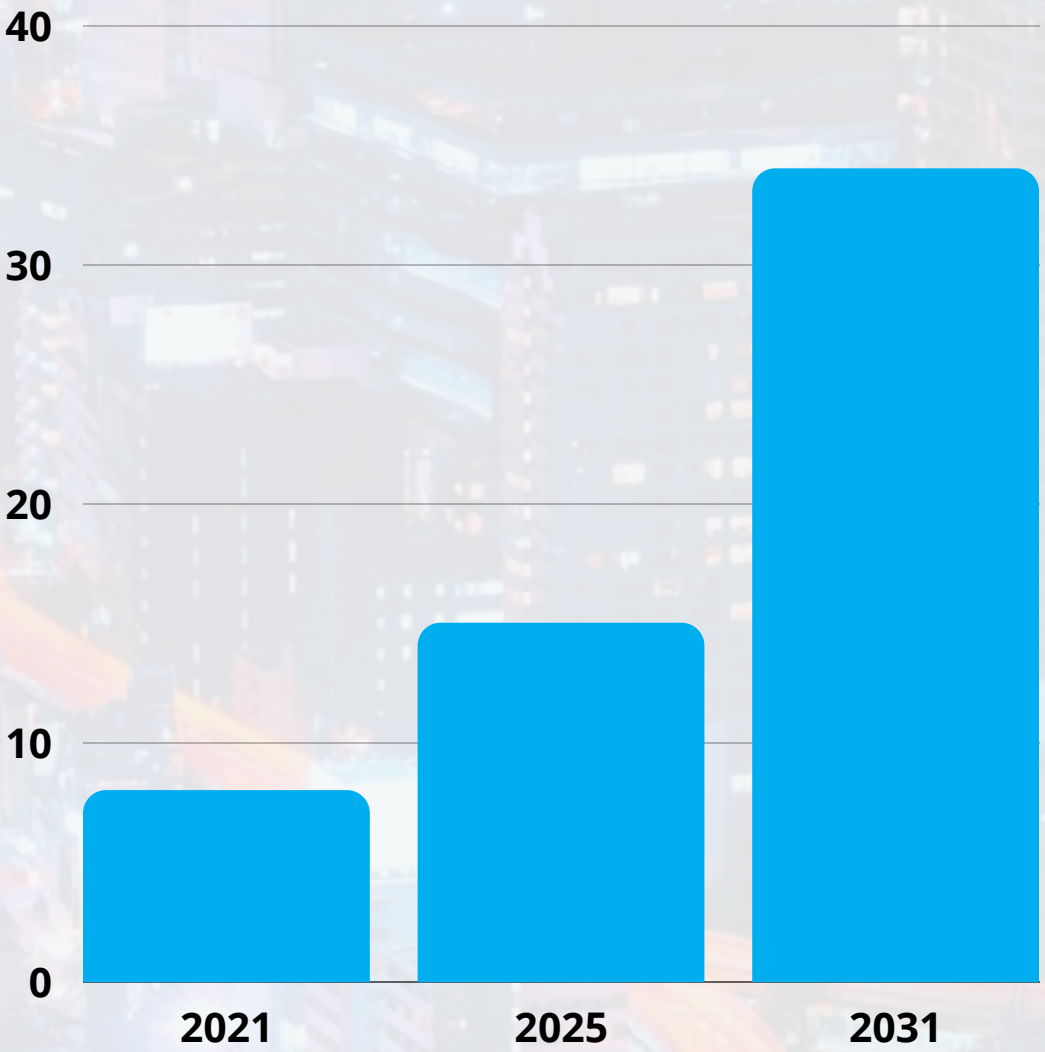
Emerging cyberinsurers have been pushing into an ever-crowding market. At-Bay, Cowbell Cyber, and Resilience collectively raised around $135 million in the past year.

Cybersecurity Ventures predicts the cyberinsurance market will grow from approximately $8.5 billion in 2021 to $14.8 billion in 2025, and exceed $34 billion by 2031, based on a CAGR (compound annual growth rate) of 15 percent over an 11-year period (2020 to 2031) calculated.

With this data in hand, a board should scrutinize its cyberinsurance policies and be vigilant investigating what the market has to offer.

CYBERINSURANCE MARKET

Cybersecurity Ventures predicts global spending on cyberinsurance will hit $34 billion annually by 2031.



CYBER FIGHTERS

The need for cybersecurity professionals has been growing rapidly, even faster than companies can hire —and that demand is expected to continue.

The number of unfilled cybersecurity jobs worldwide grew 350 percent between 2013 and 2021, from one million to 3.5 million, according to Cybersecurity Ventures. We predict that in five years from now, the same number of jobs will remain open.

More than 700,000 cybersecurity workers are needed to fill positions in the U.S. alone, notes Fortune Magazine.

Despite industry-wide efforts to reduce the skills gap, the number of open jobs in our field is enough to fill 50 NFL stadiums.

CISOs and security leaders are well aware of the labor crunch and ramifications, but what about boardroom and C-suite executives?

CYBER FIGHTERS

“Organizations can make great strides in cost savings by gaining the support of company CEOs and boards of directors to champion efforts that close the cyber skills gap such as investing in educational programmes and curricula that expand access to IT and cybersecurity skills,” wrote Aongus Hegarty, President International Markets, Dell Technologies, during the 2022 World Economic Forum Annual Meeting.

The more time an organization’s board and C-suite executives spend with its CISO, the more informed and cybersecure they’ll be.

Rich Baich, who previously served as SVP and CISO at AIG, and before that EVP and CISO at Wells Fargo, recently told Cybersecurity Ventures that boards should be hearing from their CISOs minimally annually but oftentimes quarterly.

“The board should have an educational meeting annually where the CISO provides them with an

CYBER FIGHTERS

understanding of the threat, an understanding of what has changed in the environment... really a general understanding of (their) information security," says Baich. "The most important thing is truth. How do you get truth to the board?"

Truth be told, most organizations are at risk, in part, because recruiting and retaining cybersecurity professionals is a daunting challenge. This is true of the CISO role.

Numerous studies have shown that CISOs, the lead cyber fighters in large enterprises, are job-hopping faster than most — with Cybersecurity Ventures finding 24 percent of Fortune 500 CISOs have been working in their roles for just one year on average.

That being the case, boards should know who their Deputy CISO or number two in cyber command is. C-suite executives should be planning for the inevitable turnover of their CISO.

BOARDROOM ACTION

You're a board member or CEO and you've read this report. Now what?

- Share this report with other members on the board and your C-suite executives. Then have a discussion about it at your next board meeting.
- Add cybersecurity experience to your board. This will help your board better understand cyber risk and your ability to mitigate that risk.
- Put a ransomware incident response plan in place that is approved by the board.
- Revisit your cybersecurity budget and be sure that it allows for swift action around unexpected cyberattacks and intrusions.
- Review your cyberinsurance policy and consider inviting your cyberinsurer to a board meeting.
- Put a succession plan in place for your CISO.

BOARDROOM CYBERSECURITY REPORT

SPONSORED BY SECUREWORKS©

“Tackling cybercrime must be a collective endeavor,” says Wendy Thomas, President and CEO at Secureworks©.

Wendy Thomas, President & CEO at Secureworks©

“Individual companies or governments cannot be effective if they operate alone. Threat groups work together to share knowledge and resources; that’s how they thrive, adapt and survive. We must face our adversaries as a united global community to strengthen our collective security, to enable us all to reduce cyber risk and optimize our investment of time and money in cyber defense. Imagine how

robust our cyber resilience could be if we came together to share our knowledge and insights, allowed victims to come forward and share their experiences without disadvantage, and we all benefited from the learnings. We would empower a global ecosystem that was agile, proactive, and responsive. Collaboration is key to changing the security playing field."

ABOUT SECUREWORKS©

Secureworks© protects organizations with battle-tested, best-in-class cybersecurity solutions that reduce risk, optimize IT and security investments, and fill security talent gaps. We deliver solutions by security experts for security experts to prevent, detect, and respond to continuously evolving and diversifying threats.

To learn more, visit https://secureworks.com

BOARDROOM CYBERSECURITY REPORT

BOARDROOM CYBERSECURITY 2022 REPORT is written by Steve Morgan, founder of Cybersecurity Ventures. David Braue, Editor-at-Large at Cybercrime Magazine, contributed.

Cybersecurity Ventures
83 Main Street, 2nd Flr., Northport, N.Y. 11768
info@cybersecurityventures.com