C-Suite Library

eSENTIRE | CYBERSECURITY VENTURES

REPORT

2022 Official Cybercrime Report

Cybercrime to cost the world $8 trillion annually in 2023

A report by Cybersecurity Ventures, sponsored by eSentire
– Steven C. Morgan, Founder of Cybersecurity Ventures

Introduction

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

Steve Morgan,
founder of Cybersecurity Ventures

Cybersecurity Ventures predicts global cybercrime damage costs will grow by 15 percent per year over the next five years, reaching $10.5 trillion USD annually by 2025, up from $3 trillion USD in 2015.

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

Table of Contents

Cybercrime Impact

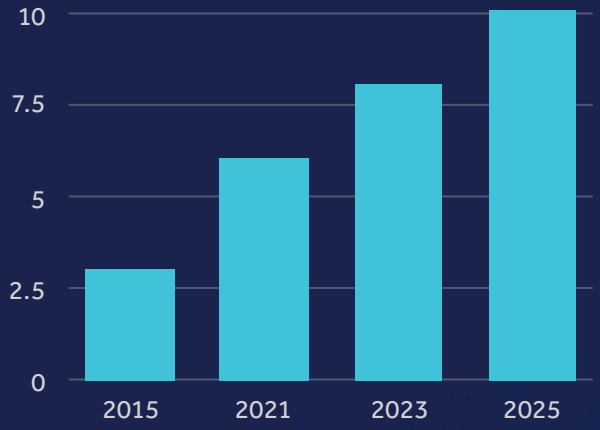
The global annual cost of cybercrime is predicted to reach $8 trillion annually in 2023. This represents the greatest transfer of economic wealth in history, risks the incentives for innovation and investment, is exponentially larger than the damage inflicted from natural disasters in a year, and will be more profitable than the global trade of all major illegal drugs combined.

Our estimations are 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 we expect to be an order of magnitude greater in 2025 than it was last year.

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.

Cybercrime Damage Costs

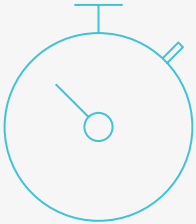
Cybercrime damage costs are predicted to grow from $3 trillion USD in 2015 to $10.5 trillion in 2025.



eSENTIRE | CYBERSECURITY VENTURES

A breakdown of global cybercrime damage costs predicted by Cybersecurity Ventures in 2023:

- $8 trillion USD a year
- $667 billion USD a month
- $154 billion USD a week
- $21.9 billion USD a day
- $913 million USD an hour
- $15.2 million USD a minute
- $255,000 USD a second



How much is cybercrime costing your organization annually?

> ***Cybercrime is impacting businesses of all sizes*** *and any business that wants to ensure its uptime, to ensure its reputation, to ensure the safety of its employee and customer data, has a responsibility to invest in cybersecurity and put themselves ahead of disruption.*
>
> **Erin McLean**, Chief Marketing Officer at **eSentire**

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 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.

"In my view [ransomware] is now the most 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.

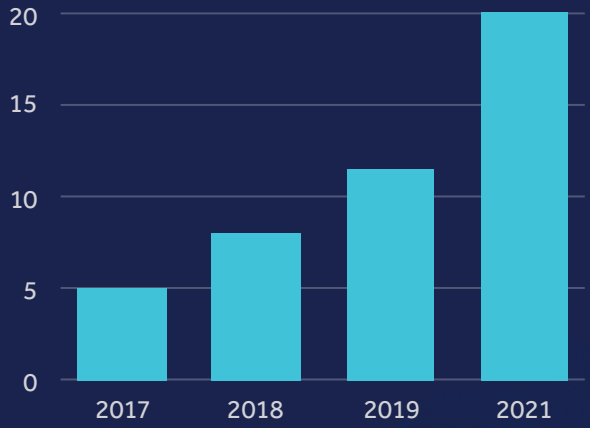
Some 92 percent of business executives surveyed agree cyber resilience is integrated into enterprise risk-management strategies; only 55 percent of cyber leaders surveyed agree. This gap between leaders can leave firms vulnerable to attacks as a direct result of incongruous security priorities and policies.

"Ransomware is continually evolving and it's really hard to keep track of all the different strains" says **John Moretti**, CISSP, CCSK & CEH, Principal Solutions Architect at eSentire. "While each ransomware variant has different ways of spreading, all ransomware variants rely on similar social engineering tactics to deceive users and hold their data hostage."

To pay or not to pay (a ransom) is all too often the question for organizations. And there is no one right answer for every case. “Paying that ransom unlocks all your corrupted data and makes you a prime target for a second attack” advises Moretti. “Paying that ransom doesn’t necessarily mean you’re going to be safe. It just opens that door again for those threat actors.”

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.

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.

Some of the biggest crypto hacks so far in 2022:

- Hackers Steal **$540M** in Crypto From 'Axie Infinity' Game
- Cryptocurrency Platform Wormhole Restores Funds After Suffering **$320M** Hack
- Victims Of **$200M** Hack Of BitMart Crypto Exchange Still Waiting To Get Their Money Back
- Hackers Drain Nearly **$200M** From Crypto Startup Nomad In 'Free-For-All' Attack

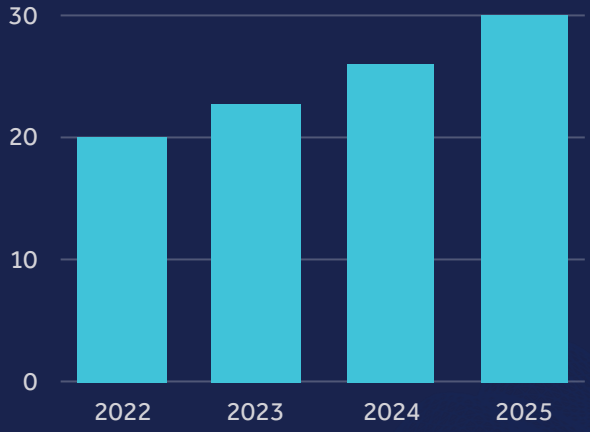
More crypto hacks so far in 2022:

- Hacker Steals **$182M** From Beanstalk Stablecoin Protocol
- Crypto Market Maker Wintermute Loses **$160M** In DeFi Hack
- Decentralized Crypto Exchange Maiar Offline After Hacker Steals **$113M**
- **$100M** Stolen From Binance In Blockchain Hack Crypto Hackers Steal **$100M** With Horizon Bridge Attack
- Hackers Have Stolen **$80M** In Cryptocurrency From The Qubit DeFi Platform
- DeFi 'Robin Hood' Hacker Exploits Crypto Worth **$52.8M** On Cashio
- Hackers Snagged **$36M** In Crypto In Breach Of IRA Financial
- Crypto.com Shares Details On Security Breach: 483 Accounts Compromised, **$34M** Stolen

Details on these crypto hacks and others can be found at **cryptocrime.com**.

Global Cryptocrime Costs

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



Cyber Attack Surface

The modern definition of the word "**hack**" was coined at MIT in April 1955. The first known mention of computer (phone) hacking occurred in a **1963 issue of The Tech**. Over the past fifty-plus years, the world's attack surface has evolved from phone systems to a vast datasphere outpacing humanity's ability to secure it.

Nearly a decade ago, IBM proclaimed that **data** promises to be for the 21st century what steam power was for the 18th, electricity for the 19th and hydrocarbons for the 20th.

The world will store 200 zettabytes of data by 2025, according to Cybersecurity Ventures. This includes data stored on private and public IT infrastructures, on utility infrastructures, on private and public cloud data centers, on personal computing devices — PCs, laptops, tablets, and smartphones — and on IoT (Internet-of-Things) devices.

It's predicted that the total amount of data stored in the cloud — which includes public clouds operated by vendors and social media companies (think Apple, Facebook, Google, Microsoft, Twitter, etc.), government-owned clouds that are accessible to citizens and businesses, private clouds owned by mid-to-large-sized corporations, and cloud storage providers — will reach **100 zettabytes by 2025**, or 50 percent of the world's data at that time, up from approximately 25 percent stored in the cloud in 2015.

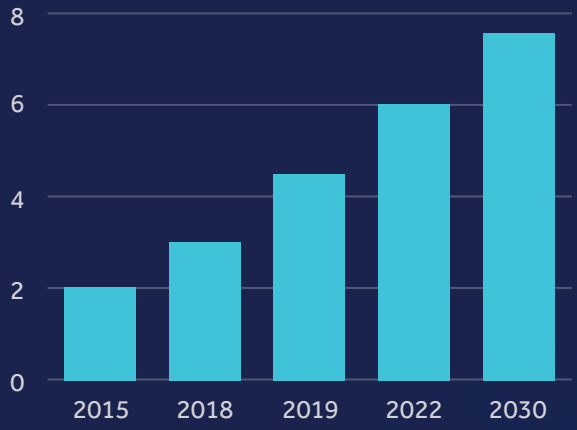
Around one million more people join the internet every day. We expect there will be **6 billion people connected to the internet** interacting with data in 2022, up from 5 billion in 2020 — and more than 7.5 billion internet users in 2030.

Cyber threats have expanded from targeting and harming computers, networks, and smartphones — to people, cars, railways, planes, power grids and anything with a heartbeat or an electronic pulse.

Many of these Things are connected to corporate networks in some fashion, further complicating cybersecurity.

Cyber Attack Surface

Cybersecurity Ventures predicts there will be
7.5 billion humans connected to the Internet in 2030.



Riskiest Industries

Around $22 trillion of global debt rated by **Moody's** has a "high" or "very high" exposure to the risk of cyber attack, the ratings agency said in a Sept. 29, 2022 report, with **hospitals and utilities seen as the greatest risk**. Out of $80 trillion worth of debt across 71 sectors that the rating agency monitors, more than a quarter — or 28 percent — featured in these two highest-risk brackets, according to a **press release** from Reuters.

Hospitals and infrastructure including electricity, gas and water utilities, are the most at risk, according to Moody's. The scores took into account the risk of exposure to hacks and mitigation measures taken. "We view not-for-profit hospitals as being highly attractive, data-rich targets with average mitigation measures in place to reduce the impact of a potential cyber event" the report said.

For its **Cyber Heatmap**, Moody's looks at two factors, exposure and mitigation, and weighs both across all of the sectors it rates.

Moody's scores each of the 71 sectors and rates them "low," "moderate," "high" or "very-high risk." According to this year's Heatmap, and perhaps unsurprisingly, **utilities rated the highest for cyber risk**, according to analysis by The Register.

Moody's names the **riskiest industries**:

- Critical infrastructure – including electric, gas and water utilities and hospitals – faces VERY HIGH cyber risk exposure.

- Banks, telecommunications, technology, chemicals, energy and transportation services face HIGH cyber risk exposure.

Cyber risk is rising. However, we are witnessing correlated growth in robust security program investments, as industries prioritize the need to assess and quantify the risk to inform key strategy decisions, mitigate supply chain risk, and ensure investor confidence.

- **Steven Libretti**,
Analyst and Lead Author of the recent Moody's report

A huge danger to utilities is the "**multiplier effect across an economy**" according to the Moody's report. For example, a cyberattack that knocks a regional power grid offline will impact more than just the utility itself, with potentially devastating consequences for hospitals that can't perform life- saving surgeries or access critical medicine for patients, or assisted living centers that can't turn on heat or air conditioning for their elderly residents in the middle of a heat wave or cold snap.

Not-for-profit hospitals also ranked "very high" in terms of their cyber risk. "We view not for profit hospitals as being highly attractive, data rich targets with average mitigation measures in place to reduce the impact of a potential cyber event" the Moody's report states. The rise in ransomware attacks against hospitals and healthcare organizations support this finding.

Small Business

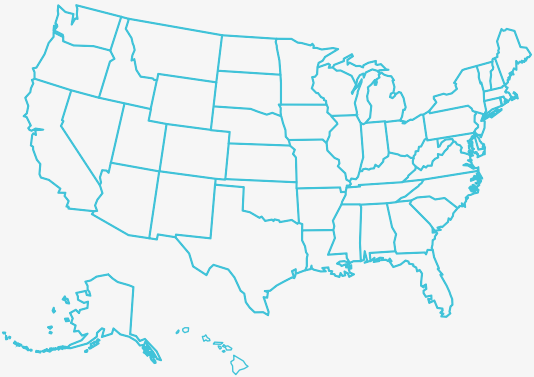
"There are 30 million small businesses in the U.S. that need to stay safe from phishing attacks, malware spying, ransomware, identity theft, major breaches and hackers who would compromise their security" says **Scott Schober**, author of the popular books "Hacked Again" and "Cybersecurity Is Everybody's Business."

More than half of all cyberattacks are committed against small-to-mid-sized businesses (SMBs), and 60 percent of them go out of business within six months of falling victim to a data breach or hack.

Small and medium sized businesses lack the financial resources and skill set to combat the emerging cyber threat.

- **Scott E. Augenbaum**,
Former supervisory special agent at the FBI's Cyber Division, Cyber Crime Fraud Unit, where he was responsible for managing the FBI's Cyber Task Force Program and Intellectual Property Rights Program

A Better Business Bureau survey found that for small businesses — which make up more than 97 percent of total businesses in North America — the primary challenges for more than 55 percent of them in order to develop a cybersecurity plan are a lack of resources or knowledge.



Ransomware attacks are of particular concern. “The cost of ransomware has skyrocketed and that’s a huge concern for small businesses — and it doesn’t look like there’s any end in sight” adds Schober.

Talent Crunch

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, 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.

Retention has proven to be as much of a challenge as recruiting in the highly competitive cybersecurity market.

In the U.S. the cybersecurity workforce has more than 1.1 million workers — with around 715,000 of them yet to be filled (as of Oct. 2022), according to CyberSeek, a project supported by the National Initiative for Cybersecurity Education (NICE), a program of the National Institute of Standards and Technology in the U.S. Department of Commerce.

The U.S. job market reflects a global supply and demand problem around recruiting candidates with cybersecurity certifications.

Nationwide, there are just over 90,000 CISSPs (Certified Information Systems Security Professionals), according to CyberSeek, but more than 106,000 job openings require the CISSP certification, our industry's gold standard. Or consider CISMs (Certified Information Security Managers), with just 17,000 people holding the credentials but nearly 40,000 advertised jobs requesting them. (figures as of Nov. 2021)

Women hold 25 percent of cybersecurity jobs globally in 2022, up from 20 percent in 2019, and around 10 percent in 2013.

We predict that women will represent 30 percent of the global cybersecurity workforce by 2025, and that will reach 35 percent by 2031. This goes beyond securing corporate networks and includes IoT, IIoT and ICS security, and cybersecurity for medical, automotive, aviation, military defense, and other.

Our latest research figures are based on in-depth discussions with numerous industry experts in cybersecurity and human talent, third-party reports, surveys, and media sources — and it reveals that while the situation is improving, it is nowhere near enough.

Women understand cyber. They understand technology. They are no less capable than men, but discrimination, a lack of awareness, and a failure to encourage the next generation to promote cybersecurity as an attractive career path all contribute to fewer women entering the field.

Charlie Osborne,
Top cybersecurity journalist and author of Cybercrime Magazine's Women Know Cybersecurity 2022 Report

The gender gap becomes a chasm when we consider the top roles in cybersecurity. For example, our research found that women held only **17 percent** of Chief Information Security Officer (CISO) roles at Fortune 500 companies. Said otherwise, women held only 85 of 500 available CISO positions.

Thankfully, the disproportion of men and women in cybersecurity roles has not gone unnoticed. As a result, scores of initiatives and grant programs targeting underrepresented groups in our field are now active.

Cybersecurity Insights

Cyber leaders face the impossible challenge of winning a game when the rules keep changing.

The only way to tackle emerging threats is to prioritize continuous improvement. That's why we speak about cyber resilience and taking a risk- based approach to cybersecurity. You've got to ask yourself - How are you as a leader continuing to improve, and harden your defenses? And how are your security partners adding value in helping you measure and demonstrate resilience?

Tia Hopkins,
Field CTO & Chief Cyber Risk Strategist at **eSentire**

The statistics presented in the 2022 Cybercrime Report demonstrate that there is no end to cyber risk so our executive board level conversations must shift to how we are actively improving cyber resilience, and putting our organizations ahead of disruption. Cyber-savvy boards are discussing topics like cyber risk appetite, cyber risk tolerance, cyber risk quantification and the risk-based approach to cybersecurity with increasing frequency.

As the Authority in Managed Detection and Response, eSentire proactively recommends a risk- based approach, allowing security leaders to prioritize building the appropriate controls for the worst vulnerabilities, to defeat the most significant threats. Risk-based approaches tend to be significantly more cost-effective than traditional maturity models since business leaders have the option to invest heavily in defenses for the vulnerabilities that affect the business's most critical areas.

Defending your organization against modern ransomware, social engineering, crypto crime and the level of state-sponsored attacks outlined here, requires a multi-layered defense strategy that includes 24/7 security monitoring, visibility and coverage over the complete attack surface, and an incident response plan in the event of a successful attack.

eSentire's Threat Response Unit recommends the following foundational security program elements:

- Adopting a **comprehensive vulnerability management program** that provides your team with continuous awareness of the threat landscape, enables a disciplined, risk-based patch management approach, and conducts vulnerability scanning to understand which systems are inadvertently exposed.

- Educating your employees to recognize the signs of phishing and social engineering tactics that state-sponsored adversaries may leverage to gain access into your environment through ongoing **Phishing and Security Awareness Training (PSAT)**.

- Engaging a **24/7 multi-signal Managed Detection and Response (MDR)** provider to ensure you have visibility across all your signal sources – endpoints, network, log, cloud, and identity – help your team to perform rapid threat investigation, containment, and remediation when an incident occurs.

- Leveraging a global threat hunting program that includes detection engineering driven by highly skilled threat hunters who can build proprietary detection content and runbooks mapped to the **MITRE ATT&CK framework**. The threat hunting program your team engages should have demonstrated expertise in investigating the latest threat actor Tactics, Techniques & Procedures (TTPs) through original research, leverage enriched threat intelligence, proactively identify threats, and streamline investigations using the best-of-breed platforms.

- Having an **Incident Response retainer** for post- incident support and emergency preparedness so your team can determine the precise extent of an attack and to investigate the threat with speed and efficacy.

Security leaders who can demonstrate the financial consequences of a cyberattack and business downtime to their executive teams are more than likely going to get the budget required to prevent business disruption and protect their customers' sensitive data. eSentire's Hopkins warns, "You can't speak to a CFO in bits and bytes when they understand things in dollars and cents." When comparing the average **daily cost of revenue disruption** to the cost of building out and maintaining a DIY security operation, or investing in an outsourced 24/7 extension of your security team, the choice to partner with trusted experts in cybersecurity is clear.

Cybercrime has evolved with threat actors modeling their strategies after enterprise organizations (for example: through role differentiation, as a service solutions, and sophisticated malware distribution). The best way to combat the dynamic threat landscape and continue to scale your business operations securely, is to partner with an organization who is AS focused in preventing threat disruption to help you reclaim the advantage, and improve your overall cyber resilience.

Sponsored by eSentire

At eSentire we pride ourselves on understanding your business and the challenges you're facing in protecting its operations and reputation.

Kerry Bailey,
CEO, eSentire

- Cyber attacks are getting more sophisticated, complex and destructive.
- The global talent shortage is severe requiring you to evaluate outsourcing IT and cybersecurity expertise.
- As you continue on your business' digital revolution, you will face greater risk but less control. More data – more scale – more pressure.

This is why we've partnered with Cybersecurity Ventures to bring the 2022 Official Cybercrime Report to life. Cybercrime damages are continuing to grow 15 percent year over year reaching $10.5 trillion USD annually by 2025. It's clear there is no endgame when it comes to cybersecurity – no such thing as perfection. Instead of accepting defeat, we have to work together to reclaim the advantage. Together, we can improve your business' cyber resilience and help you scale, securely.

You have been presented with every statistic possible to demonstrate the global threat of cybercrime and the potential revenue disruption your business faces. Let me be clear - it's how you choose to respond to these cyber threats, that will make all the difference - in your career, and in your business' ability to continue to compete at a global scale. As the Authority in Managed Detection and Response, **eSentire** is mission-driven to put your business ahead of disruption. We detect threats in seconds, and disrupt them in minutes - with a 15 minute mean time to contain as a matter of fact. We **respond** with speed, with expertise, and complete coverage - 24/7 full attack surface protection.

To build a more responsive security operation capable of keeping pace with the global cybercrime epidemic, you need more than alerts. You need a partner who goes further to prevent your business from ever being disrupted. More than 1500 organizations in 80 countries around the world count on eSentire to protect them from the impact of cybercrime. We take their protection personally and demonstrate each and every day – An Attack On You Is An Attack On Us.

Let us help you reclaim the advantage.

– **Kerry T. Bailey**, CEO at eSentire

About eSentire

eSentire is The Authority in Managed Detection and Response Services, protecting the critical data and applications of 1500+ organizations in 80+ countries from known and unknown cyber threats. Founded in 2001, the company's mission is to hunt, investigate and stop cyber threats before they become business disrupting events.

To learn more, visit **https://esentire.com**

2022 OFFICIAL CYBERCRIME REPORT is written by **Steve Morgan**, founder of **Cybersecurity Ventures**.

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