CYBERCRIME FACTS AND STATISTICS

STEVE MORGAN,
EDITOR-IN-CHIEF AT CYBERCRIME MAGAZINE

2021 REPORT: CYBERWARFARE IN THE C-SUITE

JAN. 21, 2021

PUBLISHED BY CYBERSECURITY VENTURES | SPONSORED BY INTRUSION, INC. | OFFICIALCYBERCRIME.COM

CYBERCRIME FACTS AND STATISTICS FOR C-SUITE EXECUTIVES

Cyberwarfare In The C-Suite is authored by Steve Morgan, Editor-in-Chief at Cybercrime Magazine, and published by Cybersecurity Ventures, the world's leading researcher and Page ONE for the global cyber economy, and a trusted source for cybersecurity facts, figures, and statistics.

We provide cyber economic market data, insights, and ground-breaking predictions to a global audience of CIOs and IT executives, CSOs and CISOs, information security practitioners, cybersecurity company founders and CEOs, venture capitalists, corporate investors, business and finance executives, HR professionals, and government cyber defense leaders.

Cybercrime Magazine publishes our annual and quarterly reports covering global cybercrime, cyberwarfare, hacks and data breaches, cybersecurity market forecasts and spending predictions, publicly traded cybersecurity companies and stock performance, M&A and VC funding activity, cyber defense employment, and more.

Steve Morgan
Founder of Cybersecurity Ventures
Editor-In-Chief at Cybercrime Magazine
steve@cybersecurityventures.com
Twitter.com/CybersecuritySF
Linkedin.com/in/CybersecuritySF

CYBERSECURITY VENTURES

INTRUSION
Protect everything. Trust nothing.

CYBERCRIME FACTS AND STATISTICS FOR C-SUITE EXECUTIVES

Cyberwarfare In The C-Suite is sponsored by INTRUSION, Inc., a cybersecurity innovator who has reframed the problem of failed network security to successfully address the depth and breadth of cyber attacks experienced every 3 seconds in the United States alone.

We believe your company network should be a safe place. Free from ransomware, theft of trade secrets, harvesting of corporate knowledge, insider threats, IoT extraction of data, and many other forms of cyberwarfare and cybercrime.

We leverage decades of experience and dynamic technology to offer your organization the best possible defense. We are passionate about winning the war on cybercrime. That's why we offer important insights and updates in the form of regular Threat Updates.

INTRUSION Shield™ is the newest Internet protection solution for all businesses: small, medium and large enterprises. INTRUSION Shield's primary role is to identify and block all dangerous and harmful traffic. Shield does this using a unique, patented process flow technology which analyzes all network traffic - incoming and outgoing - to keep your business safe.

For more information, visit intrusion.com.

CYBERSECURITY VENTURES

INTRUSION
Protect everything. Trust nothing.

If it were measured as a country, then cybercrime — which is predicted to inflict damages totaling $6 trillion USD globally in 2021 — would be the world's third-largest economy after the U.S. and China.

Cybersecurity Ventures expects global cybercrime costs to 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. 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.

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.

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 HITS HOME

The United States, the world's largest economy with a nominal GDP of nearly $21.5 trillion, constitutes one-fourth of the world economy, according to data from Nasdaq.

Cybercrime has hit the U.S. so hard that in 2018 a supervisory special agent with the FBI who investigates cyber intrusions told The Wall Street Journal that every American citizen should expect that all of their data (personally identifiable information) has been stolen and is on the dark web — a part of the deep web — which is intentionally hidden and used to conceal and promote heinous activities. Some estimates put the size of the deep web (which is not indexed or accessible by search engines) at as much as 5,000 times larger than the surface web, and growing at a rate that defies quantification.

The dark web is also where cybercriminals buy and sell malware, exploit kits, and cyberattack services, which they use to strike victims — including businesses, governments, utilities, and essential service providers on U.S. soil.

A cyberattack could potentially disable the economy of a city, state or our entire country.

In his 2016 New York Times bestseller — *Lights Out: A Cyberattack, A Nation Unprepared, Surviving the Aftermath* — Ted Koppel reveals that a major cyberattack on America's power grid is not only possible but likely, that it would be devastating, and that the U.S. is shockingly unprepared.

Billionaire businessman and philanthropist Warren Buffet calls cybercrime the number one problem with mankind, and cyberattacks a bigger threat to humanity than nuclear weapons.

A bullseye is squarely on our nation's businesses.

"Cybercriminals know they can hold businesses — and our economy — hostage through breaches, ransomware, denial of service attacks and more. This is cyberwarfare, and we need to shift our mindset around cybersecurity in order to protect against it," says Jack B. Blount, president and CEO at INTRUSION, Inc.

Organized cybercrime entities are joining forces, and their likelihood of detection and prosecution is estimated to be as low as 0.05 percent in the U.S., according to the *World Economic Forum's 2020 Global Risk Report*.

"Every American organization — in the public and private sector — has been or will be hacked, is infected with malware, and is a target of hostile nation-state cyber intruders," adds Blount, formerly the CIO at the United States Department of Agriculture (USDA).

RANSOMWARE

Ransomware — a malware that infects computers (and mobile devices) and restricts their access to files, often threatening permanent data destruction unless a ransom is paid — has reached epidemic proportions globally and is the "go-to method of attack" for cybercriminals.

A 2017 report from Cybersecurity Ventures predicted ransomware damages would cost the world $5 billion in 2017, up from $325 million in 2015 — a 15X increase in just two years. The damages for 2018 were estimated at $8 billion, and for 2019 the figure rose to $11.5 billion.

The latest forecast is for global ransomware damage costs to reach $20 billion by 2021 — which is 57X more than it was in 2015. We predict there will be a ransomware attack on businesses every 11 seconds in 2021, up from every 40 seconds in 2016.

The FBI is particularly concerned with ransomware hitting healthcare providers, hospitals, 911 and first responders. These types of cyberattacks can impact the physical safety of American citizens, and this is the forefront of what Herb Stapleton, FBI cyber division section chief, and his team are focused on.

Late last year, ransomware claimed its first life. German authorities reported a ransomware attack caused the failure of IT systems at a major hospital in Duesseldorf, and a woman who needed urgent admission died after she had to be taken to another city for treatment.

Ransomware, now the fastest growing and one of the most damaging types of cybercrime, will ultimately convince senior executives to take the cyber threat more seriously, according to Mark Montgomery, executive director at the U.S. Cyberspace Solarium Commission (CSC) — but he hopes it doesn't come to that

PODCAST: Mark Montgomery, Executive Director at CSC and Jack Blount, President & CEO at INTRUSION. [LISTEN]

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.

In 2013, IBM proclaimed data promises to be for the 21st century what steam power was for the 18th, electricity for the 19th and hydrocarbons for the 20th.

"We believe that data is the phenomenon of our time," said Ginni Rometty, IBM Corp.'s executive chairman, in 2015, addressing CEOs, CIOs and CISOs from 123 companies in 24 industries at a conference in New York City. "It is the world's new natural resource. It is the new basis of competitive advantage, and it is transforming every profession and industry. If all of this is true — even inevitable — then cyber crime, by definition, is the greatest threat to every profession, every industry, every company in the world."

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.

As a result of the COVID-19 pandemic, nearly half the U.S. labor force is working from home, according to Stanford University. As employees generate, access, and share more data remotely through cloud apps, the number of security blind spots balloons.

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.

Roughly 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.

By 2023, there will be 3X more networked devices on Earth than humans, according to a report from Cisco. And by 2022, 1 trillion networked sensors will be embedded in the world around us, with up to 45 trillion in 20 years.

IP traffic reached an annual run rate of 2.3 zettabytes in 2020, up from an annual run rate of 870.3 exabytes in 2015.

Data is the building block of the digitized economy, and the opportunities for innovation and malice around it are incalculable.

CYBERSECURITY SPENDING

Global spending on cybersecurity products and services for defending against cybercrime is projected to exceed $1 trillion cumulatively over the five-year period from 2017 to 2021.

In 2004, the global cybersecurity market was worth $3.5 billion — and in 2017 it was worth more than $120 billion. The cybersecurity market grew by roughly 35X during that 13-year period — prior to the latest market sizing by Cybersecurity Ventures.

"Most cybersecurity budgets at U.S. organizations are increasing linearly or flat, but the cyberattacks are growing exponentially," says CSC's Montgomery. This simple observation should be a wake-up call for C-suite executives.

Healthcare has lagged behind other industries and the tantalizing target on its back is attributable to outdated IT systems, fewer cybersecurity protocols and IT staff, extremely valuable data, and the pressing need for medical practices and hospitals to pay ransoms quickly to regain data. The healthcare industry will respond by spending $125 billion cumulatively from 2020 to 2025 to beef up its cyber defenses.

The FY 2020 U.S. President's Budget includes $17.4 billion of budget authority for cybersecurity-related activities, a $790 million (5 percent) increase above the FY 2019 estimate, according to The White House. Due to the sensitive nature of some activities, this amount does not represent the entire cyber budget.

Cybersecurity Ventures anticipates 12-15 percent year-over-year cybersecurity market growth through 2025. While that may be a respectable increase, it pales in comparison to the cybercrime costs incurred.

PODCAST: Cyberwarfare Roundtable featuring Fortune 500 Chief Information Security Officers and cybersecurity experts. Co-hosted by Steve Morgan, Editor-inChief at Cybercrime Magazine and Jack Blount, President & CEO at INTRUSION [LISTEN]

SMALL BUSINESS

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

"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.*

66 percent of SMBs had at least one cyber incident in the past two years, according to Mastercard.

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

Cybercrime Magazine

The editors at Cybercrime Magazine publish articles, reports, infographics, podcasts, videos and other resources for small businesses. Visit us at cybercrimemagazine.com

PODCAST: Cyberwarfare. Every American Business Is Infected With Malware. Steve Morgan, Editor-in-Chief at Cybercrime Magazine and Jack Blount, CEO at INTRUSION, Inc. [LISTEN]

AI AUGMENTS CYBER DEFENDERS

You don't bring a knife to a gunfight.

"The enemy is now using AI (artificial intelligence) against us," warns Blount. "It's critical for business and government to understand the average cyberattack is not coming from a person at a keyboard — instead it's coming from an AI algorithm running on a super-computer and it's going night and day attacking every IP address it can find on the internet. It doesn't care if you're small or big." As a result, Blount hasn't met one organization (out of hundreds) over the past five years who hasn't been a victim of malware.

The U.S. has a total employed cybersecurity workforce consisting of nearly 925,000 people, and there are currently almost 510,000 unfilled positions, according to Cyber Seek, a project supported by the National Initiative for Cybersecurity Education (NICE), a program of the National Institute of Standards and Technology (NIST) in the U.S. Department of Commerce.

Faced with a domestic worker shortage, the heads of U.S. cyber defense forces — CIOs and CISOs at America's mid-sized to largest businesses — are beginning to augment their staff with next-generation AI and ML (machine learning) software and appliances aimed at detecting cyber intruders. These AI systems are trained on big data sets collected over decades — and they can analyze terabytes of data per day, a scale unimaginable for humans.

The panacea for a CISO is an AI system resembling a human expert's investigative and reporting techniques so that cyber threats are remediated BEFORE the damage is done.

If enemies are using AI to launch cyberattacks, then our country's businesses need to use AI to defend themselves.

INTRUSION Shield

INTRUSION Shield™ is a combination of plug-n-play hardware, software, global data, and real-time Artificial Intelligence (AI) services that provide organizations with the most robust cybersecurity defense possible.

INTRUSION Shield uses the world's largest and most robust threat-enriched Big Data Cloud to identify threats before they can hurt you. Shield crawls the network 24x7 and incorporates over 270 data feeds to make sure it is as in-depth, complete, and current as possible. Shield identifies and instantly approves more than 3.7 billion IP addresses.

Learn more at intrusion.com

FOR THE BOARDROOM

Cybersecurity begins at the top.

CSC has an urgent message for boardroom and C-suite executives: The status quo in cyberspace is unacceptable, which is spelled out in its groundbreaking 2020 Report which proposes a strategy of layered cyber deterrence — to protect all U.S. businesses and governments from cybercrime and cyberwarfare. But, this is hardly the first warning. "Some of the same things we're recommending today, we were pushing 23 years ago," says Montgomery.

"Every company should have a CISO or cybersecurity expert on their board — because cybercrime is the greatest risk to business continuity that every company faces," says Blount. The idea is to put someone in the boardroom who will wave the red flag and get everybody paying attention to the severity of the risk. Montgomery agrees and says attention is the number one priority, not bringing in a new CISO — instead empower the CISO that you have.

The value of a business depends largely on how well it guards its data, the strength of its cybersecurity, and its level of cyber resilience.

If there's one takeaway from this report, then let it be this: Don't let your boardroom be the weakest cybersecurity link.

CYBERCRIME FACTS AND STATISTICS

Cyberwarfare In The C-Suite is authored by Steve Morgan, Editor-in-Chief at Cybercrime Magazine, and published by Cybersecurity Ventures, the world's leading researcher and Page ONE for the global cyber economy, and a trusted source for cybersecurity facts, figures, and statistics.

Cyberwarfare In The C-Suite is sponsored by INTRUSION, Inc., a cybersecurity innovator that has reframed the problem of failed network security to successfully address the depth and breadth of cyber attacks experienced every 3 seconds in the United States alone.