CYBERSECURITY VENTURES

HERJAVEC GROUP

2019 Official Annual Cybercrime Report

Cybercriminal activity is one of the biggest challenges that humanity will face in the next two decades

Steve Morgan, Editor-in-Chief
Cybersecurity Ventures

A 2019 report from Cybersecurity Ventures sponsored by Herjavec Group.

Introduction

Cybersecurity Ventures predicts cybercrime will cost the world in excess of $6 trillion annually by 2021, up from $3 trillion in 2015.

Cybercrime is the greatest threat to every company in the world, and one of the biggest problems with mankind. The impact on society is reflected in the numbers.

In August of 2016, Cybersecurity Ventures predicted that cybercrime will cost the world $6 trillion annually by 2021, up from $3 trillion in 2015. This represents the greatest transfer of economic wealth in history, risks the incentives for innovation and investment, and will be more profitable than the global trade of all major illegal drugs combined.

The cybercrime prediction stands, and over the past two-plus years it has been corroborated by hundreds of major media outlets, academia, senior government officials, associations, industry experts, the largest technology and cybersecurity companies, and cybercrime fighters globally.

Frank W. Abagnale, an FBI consultant for over 40 years and one of the world's most respected authorities on forgery, embezzlement, and secure documents, concurs with the $6 trillion cybercrime damage cost prediction. "I'm very concerned with cyber starting to turn very dark," says Abagnale, the inspiration for Steven Spielberg's 2002 film, Catch Me If You Can, starring Leonardo DiCaprio as Abagnale and Tom Hanks as the FBI agent fast on his heels. "Up until now it's just a financial crime for the purpose of stealing money – or stealing data that is money – but we have the ability now to turn someone's pacemaker off."

Cybersecurity Ventures' damage cost projections 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 cyber attack surface which will be an order of magnitude greater in 2021 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.

"This dramatic rise (in damage costs) only reinforces the sharp increase in the number of organizations unprepared for a cyber attack," says Robert Herjavec, founder and CEO at Herjavec Group, a Managed Security Services Provider with offices and SOCs (Security Operations Centers) globally.

Introduction

Cyber attacks are the fastest growing crime in the U.S., and they are increasing in size, sophistication and cost. A major data breach — the second largest ever — suffered by Marriott and disclosed near the end of 2018, is estimated to have exposed 500 million user accounts. The Yahoo hack — the largest ever — was recalculated to have affected 3 billion user accounts (up from an earlier estimate of 1 billion), and the Equifax breach in 2017 — with 145.5 million customers affected — exceeded the largest publicly disclosed hacks ever reported up until that time. These major hacks alongside the WannaCry and NotPetya cyber attacks, which occurred in 2017 are not only larger scale and more complex than previous attacks, but they are a sign of the times.

The cybercrime epidemic has hit the U.S. so hard that a supervisory special agent with the Federal Bureau of Investigation 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 now on the dark web.

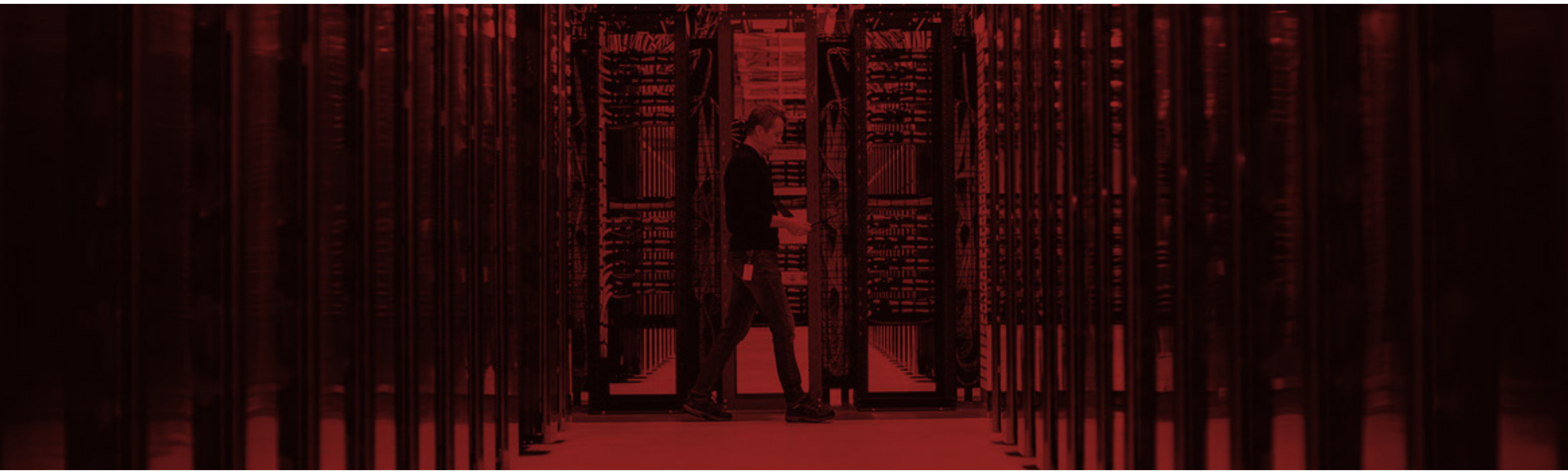
"DDoS attacks, ransomware, and an increase in zero day exploits are contributing to the cybercrime damages prediction becoming a reality," adds Herjavec. "What really worries me though, is that all the hype around cybercrime – the headlines, the breach notices etc. – makes us complacent. The risk is very real and we can't allow ourselves to be lulled into a sense of inevitability."

"This dramatic rise (in damage costs) only reinforces the sharp increase in the number of organizations unprepared for a cyber attack."

-- Robert Herjavec, Founder & CEO at Herjavec Group

Cyber Attack Surface

HERJAVEC GROUP



Our entire society, the Planet Earth, is connecting up to the Internet – people, places, and Things. The rate of Internet connection is outpacing our ability to properly secure it.

The World Wide Web was invented in 1989. The first-ever website went live in 1991. Today there are nearly 1.9 billion websites.

There were nearly 4 billion Internet users in 2018 (nearly half of the world's population of 7.7 billion), up from 2 billion in 2015.

Cybersecurity Ventures predicts that there will be 6 billion Internet users by 2022 (75 percent of the projected world population of 8 billion) — and more than 7.5 billion Internet users by 2030 (90 percent of the projected world population of 8.5 billion, 6 years of age and older).

Like street crime, which historically grew in relation to population growth, we are witnessing a similar evolution of cybercrime. It's not just about more sophisticated weaponry; it's as much about the growing number of human and digital targets.

"The degree of difficulty in protecting businesses from cyber attacks grows in proportion to a number of factors," says Herjavec. "Emerging threat actors, the prominence of interconnected devices and the most critical in my opinion – the VAST amount of data that needs to be secured – are all adding to this complex challenge."

Microsoft helps frame digital growth with its estimate that data volumes online will be 50 times greater in 2020 than they were in 2016.

Cisco confirmed that cloud data center traffic will represent 95 percent of total data center traffic by 2021. Or to put it another way – cloud computing will wipe out data centers altogether over the next 3-4 years.

Cybersecurity Ventures predicts that the total amount of data stored in the cloud – which includes public clouds operated by vendors and social media companies (think AWS, Twitter, Facebook, etc.), government owned clouds that are accessible to citizens and businesses, and private clouds owned by mid-to-large-sized corporations – will be 100X greater in 2021 than it is today.

'The Big Data Bang' is an IoT world that will explode from 2 billion objects (smart devices which communicate wirelessly) in 2006 to a projected 200 billion by 2020, according to Intel.

Gartner forecasts that more than half a billion wearable devices will be sold worldwide in 2021, up from roughly 310 million in 2017. Wearables includes smartwatches, head-mounted displays, body-worn cameras, Bluetooth headsets, and fitness monitors.

Despite promises from biometrics developers of a future with no more passwords — which may in fact come to pass at one point in the far out future — a 2017 report found that the world will need to cyber protect 300 billion passwords globally by 2020.

There are more than 111 billion lines of new software code being produced each year — which introduces a massive number of vulnerabilities that can be exploited.

The world's digital content is expected to grow from 4 billion terabytes (4 zettabytes) in 2016 to 96 zettabytes by 2020 (this is how big a zettabyte is).

The far corners of the Deep Web — known as the Dark Web — is intentionally hidden and used to conceal and promote heinous criminal 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, according to one report.

ABI has forecasted that more than 20 million connected cars will ship with built-in software-based security technology by 2020 — and Spanish telecom provider Telefonica states by 2020, 90 percent of cars will be online, compared with just 2 percent in 2012.

Hundreds of thousands — and possibly millions — of people can be hacked now via their wirelessly connected and digitally monitored implantable medical devices (IMDs) — which include cardioverter defibrillators (ICD), pacemakers, deep brain neurostimulators, insulin pumps, ear tubes, and more.

Dr. Janusz Bryzek, Vice President, MEMS and Sensing Solutions at Fairchild Semiconductor predicts that there will be 45 trillion networked sensors in twenty years from now. This will be driven by smart systems including IoT, mobile and wearable market growth, digital health, context computing, global environmental monitoring, and IBM Research's "5 in 5" — artificial intelligence (AI), hyperimaging, macroscopes, medical "labs on a chip," and silicon photonics.

Cybersecurity Spending

Cybercrime is creating unprecedented damage to both private and public enterprises, and driving up IT security spending.

Worldwide spending on information security (a subset of the broader cybersecurity market) products and services will reach more than $114 billion (USD) in 2018 *, an increase of 12.4 percent from last year, according to the latest forecast from Gartner, Inc. In 2019, the market is forecast to grow 8.7 percent to $124 billion.

* The Gartner forecast doesn't cover various cybersecurity categories including IoT (Internet of Things), ICS (Industrial Control Systems) and IIoT (Industrial Internet of Things) security, automotive cybersecurity, and others.

Cybersecurity Ventures predicts global spending on cybersecurity products and services will exceed $1 trillion cumulatively over the five year period from 2017 to 2021. Taken as a whole, we anticipate 12-15 percent year-over-year cybersecurity market growth through 2021.

Global spending on cybersecurity will exceed $1 trillion cumulatively for the 5 year period from 2017-2021, according to Cybersecurity Ventures.

IT analyst forecasts remain unable to keep pace with the dramatic rise in cybercrime, the ransomware epidemic, the refocusing of malware from PCs and laptops to smartphones and mobile devices, the deployment of billions of under-protected Internet of Things (IoT) devices, the legions of hackers-for-hire, and the more sophisticated cyber attacks launching at businesses, governments, educational institutions, and consumers globally.

"Problem is (for tracking cybersecurity spending), tech giants — with the exception of IBM and Cisco Systems — don't always break out cybersecurity revenue figures and a large cut of consumer security spending on mobile malware and virus removal and data recovery is never reported. Much like corporations, consumers are spending time and money as a result of cyber attacks," according to a story in Investors Business Daily, which helps explain part of the delta between spending forecasts from some industry analysts and the trillion dollar 5-year market prediction by Cybersecurity Ventures.

Ransomware Rising

Cybersecurity Ventures predicts that a business will fall victim to a ransomware attack every 14 seconds by 2019, and every 11 seconds by 2021.

The U.S. Department of Justice (DOJ) has described ransomware as a new business model for cybercrime, and a global phenomenon.

Ransomware — a malware that infects computers and restricts their access to files, often threatening permanent data destruction unless a ransom is paid — has reached epidemic proportions and is the fastest growing cybercrime.

At the end of 2016, a business fell victim to a ransomware attack every 40 seconds. Cybersecurity Ventures predicts that will rise to every 14 seconds by 2019 — and every 11 seconds by 2021.

Last year, the FBI estimated that the total amount of ransom payments was approaching $1 billion annually.

Cybersecurity industry experts and law enforcement officials have been advising organizations not to pay ransoms. While the percentage of ransom victims who pay bitcoin to hackers in hopes of reclaiming their data appears to be on the decline, the total damage costs in connection to ransomware attacks is skyrocketing.

Global ransomware damage costs were predicted to exceed $5 billion in 2017, up more than 15X from 2015. Ransomware damages are now predicted to cost the world $11.5 billion in 2019, and $20 billion in 2021.

“Ransomware attacks are in the process of morphing from spray-and-pray phishing blasts to highly targeted and extremely damaging network-wide infections that can cause days or weeks of downtime for a whole organization,” says Stu Sjouwerman, founder and CEO at KnowBe4, a company that specializes in training employees on how to detect and respond to ransomware attacks. “It is an unfortunate fact of life that ransomware is here to stay and that traditional software-based endpoint protection is not able to protect well against this type of malware.”

Labor Crisis

The sheer volume of cyber attacks and security events triaged daily by security operations centers continues to grow, making it nearly impossible for humans to keep pace, according to Microsoft's Global Incident Response and Recovery Team.

Security is a people problem. People are committing the cybercrimes. And we need qualified people to pursue and catch the perpetrators.

Technology is essential and we are making a lot of progress there, but without a sufficient army of white hats (good guys) to go up against the growing army of black hats (bad guys), we will not be able to bring down the cybercrime rate.

"The greatest virtual threat today is not state sponsored cyber-attacks; newfangled clandestine malware; or a hacker culture run amok," states John Reed Stark, former Chief of the SEC's Office of Internet Enforcement, in a guest blog post he wrote last year. "The most dangerous looming crisis in information security is instead a severe cybersecurity labor shortage."

The demand for cybersecurity professionals will increase to approximately 6 million globally by 2019, according to some industry experts cited by the Palo Alto Networks Research Center.

Cybercrime will more than triple the number of job openings to 3.5 million unfilled cybersecurity positions by 2021, and the cybersecurity unemployment rate will remain at zero percent.

Every IT position is also a cybersecurity position now. Every IT worker, every technology worker, needs to be involved with protecting and defending apps, data, devices, infrastructure, and people.

"Historically, there's been a line drawn in the sand between an IT organization, and its security team," says Herjavec. "In fact, aside from a CIO, the only other IT 'Chief' title is CISO (Chief Information Security Officer). But it's the larger group of IT workers that can be your future cybersecurity pros. The challenge across the board is in recruiting and retaining new security hires."

The cybersecurity workforce shortage has left CIOs, CSOs, and CISOs shorthanded and scrambling for talent while the cyber attacks are intensifying. Security leaders must recognize how to prioritize, and how to sacrifice, when it comes to limited human capital.

"Mostly, my job (and this is true of any cybersecurity professional) is to determine how to allocate scarce resources to the highest risk," says Jim Routh, Chief Security Officer at CVSHealth, the largest pharmacy healthcare provider in the U.S., with 246,000 colleagues across all 50 states, Washington, D.C., Puerto Rico and Brazil. "You never have enough resources to do everything, so you have to pick and choose where you want to make investments in terms of the allocation of resources," adds Routh (previously CSO at Aetna before being acquired by CVSHealth).

While the annals of hacking are studded with tales of clever coders finding flaws in systems to achieve malevolent ends, the fact is most cyber attacks begin with a simple email. More than 90 percent of successful hacks and data breaches stem from phishing, emails crafted to lure their recipients to click a link, open a document or forward information to someone they shouldn't.

"People are the weakest link in the security chain," says Kathy Hughes, VP and CISO at Northwell Health, one of the nation's leading healthcare systems and New York's largest private employer with 68,000 people. "You can have all the wonderful technologies and layers of security protections in place, but ultimately it comes down to the person — to people being really aware of the threats and knowing how to detect them and how to report them," adds Hughes, who has helped create a culture of security awareness at the healthcare giant.

2018 was a breakthrough year when many organizations globally took the (financial) plunge and either trained their employees on security for the first time, or doubled-down on more robust and ongoing security awareness and phishing simulation programs.

Training employees how to recognize and defend against cyber attacks is the most under spent sector of the cybersecurity industry.

Northwell may be the poster child for how a large enterprise can implement and benefit from training employees on cyber threats. Hughes led the organization's initiatives, which included hiring a security awareness training manager and dedicated staff, and orchestrating a phishing campaign that includes simulated attacks on users (and groups of users) that are more susceptible to scams — including new hires.

Making sure there is a security aware culture is a top priority at Xerox, which has offices in over 160 countries around the world. "How large is the security organization at Xerox?" asks Dr. Jay, VP and CISO at Xerox, and former White House Deputy CIO. "The security organization is 30,000 people… every single employee at Xerox," she says, answering her own question.

"The bad guys are using the same $2.99 (hacking) tools to get to Xerox as they were to get to the White House," adds Dr. Jay. A 'Hacker's Tool Kit', as seen in Fortune, offers a cybercrime price list with tools ranging from $1 to $200 — many of which can be utilized by complete novices — for injecting ransomware to stealing personally identifiable information (PII) to hacking into email accounts, and other nefarious purposes.

Global spending on security awareness training for employees is predicted to reach $10 billion by 2027, up from around $1 billion in 2014. Training employees how to recognize and defend against cyber attacks is the most under spent sector of the cybersecurity industry.

Employee training may prove to be the best ROI on cybersecurity investments for organizations globally over the next 5 years.

Looking Ahead

“Every company will be hacked,” according to Roger Grimes, a Computer Security Columnist for Infoworld, and 30-year tech industry road warrior who spent 11 years as a Principal Security Architect at Microsoft.

Healthcare providers have been the bullseye for hackers over the past three years. “In 2017 and 2018 we saw more focus on cybersecurity investment from healthcare providers,” says Herjavec. “They’ve felt the pain of their antiquated systems and have had to step up out of necessity to do more to protect their infrastructures and patient data. Ransomware attacks on hospitals are predicted to increase 5X by 2021.”

“We saw more and more traction this year (and we’re expecting the same for 2019) in what I call ‘traditional industries,’” adds Herjavec. “Particularly in the manufacturing space where compromises like cryptolocker have done some real damage, we will see organizations maturing their security programs and investing in order to keep up with ever changing exploits. Manufacturing has become the new healthcare in 2018.”

To Herjavec’s point, 40 percent of the manufacturing security professionals responding to a Cisco survey said they do not have a formal security strategy. Due to a general lack of investment in cybersecurity, yet a growing reliance on modern technologies, the manufacturing sector is one of the most vulnerable and targeted industries, according to Process Industry Informer, a magazine for the manufacturing sector.

The construction industry was another hot target for cyber attacks in 2018. As construction companies begin to standardize on IoT devices including thermostats, water heaters, and power systems, a whole new attack surface will emerge for hackers.

IoT (Internet of Things) devices were the biggest technology crime driver in 2018 — and all indications are that it will remain the same in 2019.

Consumer products companies have emerged this year as another industry that is challenged around cyber attacks and recruiting cybersecurity talent. Millennial and Generation Z workers may find young technology or investment banking companies more attractive as potential employers, according to a story in The Wall Street Journal.

The 5 most cyber-attacked industries in 2016 — healthcare, manufacturing, financial services, government, and transportation — have remained largely the same, although the rank order has been changing. Every industry has gone “Tech” — AdTech (advertising), FinTech (financial services), EdTech (educational technology), GovTech (government), LegalTech (law firms), etc. — and they all need to scale their cyber protection.

Looking Ahead

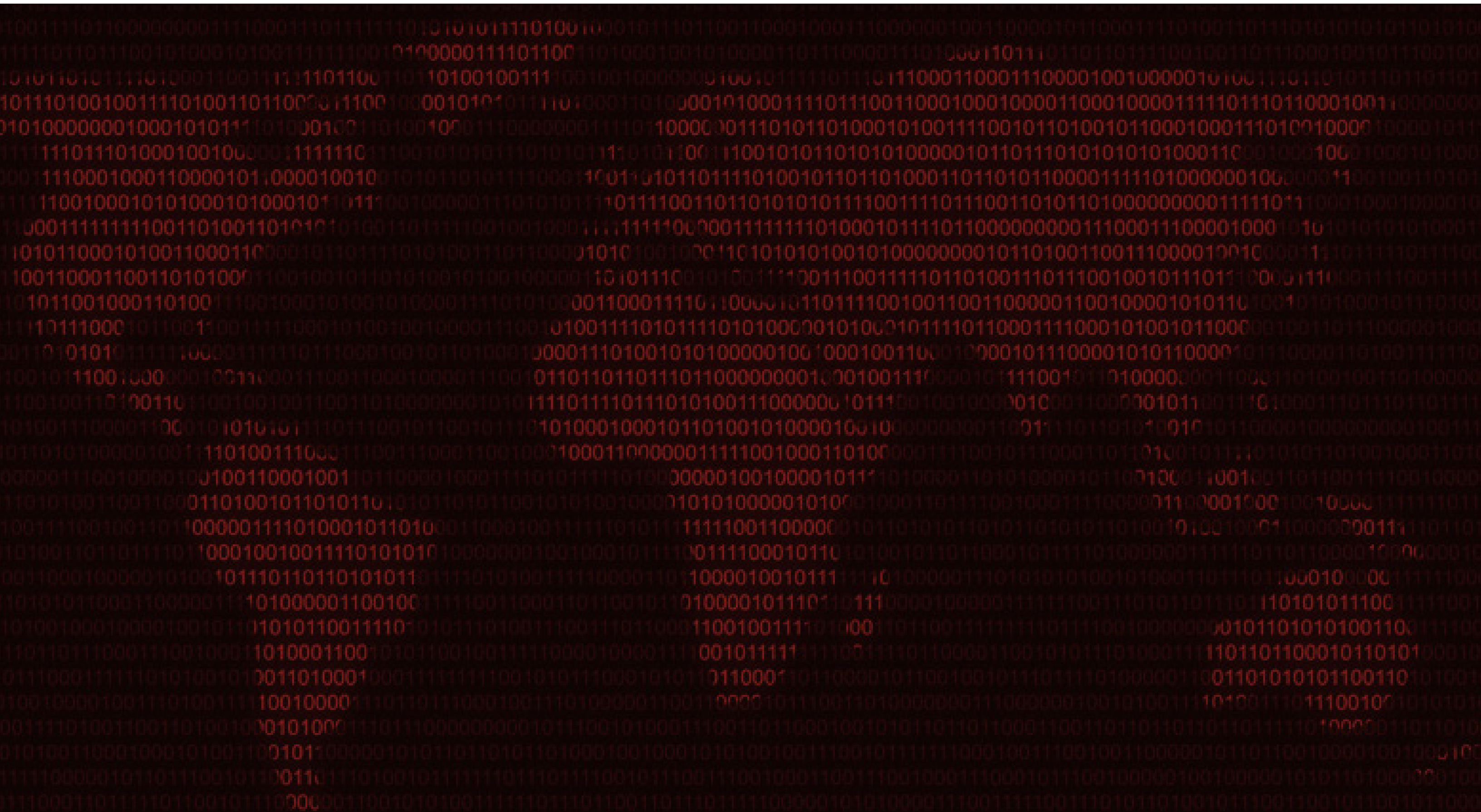
The small business sector saw a bump in cybersecurity this year. A legion of small businesses woke up to the reality that they are under cyber attack — and need to take preventative security measures. Many companies with 250 or fewer employees have learned the hard way that if they wait until after being hacked to deal with it — it may be too late. Nearly half of all cyber attacks are committed against small businesses, and the percentage is expected to continue rising.

One cybersecurity expert has a warning that CEOs at organizations of all types and sizes should heed: "It's just like preparing for hurricanes, earthquakes, any type of natural or man-made disaster that could create business continuity issues — same thing with the digital cyber event," says Theresa Payton, CEO at Fortalice Solutions, and former White House CIO.

Industries aside, IoT (Internet of Things) devices were the biggest technology crime driver in 2018 — and all indications are that it will remain the same in 2019 and for the foreseeable future. Cisco estimates that the number of IoT devices will be three times as high as the global population by 2021. "The IoT devices were really built with just pure functionality in mind," says Northwell's CISO, Hughes. "They have very small operating systems and security is more of a 'bolt-on' than a 'built-in' to those devices."

Finally, consumers are expected to pay more attention to security in 2019 in the aftermath of the Yahoo, Marriott, and other data breaches.

The thought of stolen email addresses and PII (personally identifiable information), and hackers being able to read private text messages and listen to baby monitors may be the things that get people motivated to fight back by switching to more secure email providers, turning on 2-step verification, and buying their first cybersecurity products.



Safety in Numbers

Despite the cybercrime epidemic, technology promises to make the world a much safer place.

Traffic authorities see nearly 300,000 lives saved over the next 10 years from a vast reduction in traffic fatalities using autonomous vehicle technology.

Intel announced the largest security related acquisition last year, a whopping $15.3 billion acquisition of Mobileye, an Israeli automotive technology company focused on collision avoidance — with approximately 450 engineers and an installed base of nearly 15 million vehicles.

Overall crime statistics could drop by more than 20 percent when metropolitan sensors and cutting edge home security remote monitoring begin to work seamlessly together through the IoT.

Cyber engineers and entrepreneurs globally are hard at work on new solutions to combat and reduce cybercrime. Hundreds of top cybersecurity companies are innovating cutting edge products and creating new services in the war against cybercrime. A growing list of MSSPs (managed security service providers) are assuming responsibilities for the most daunting cyber risks faced by organizations of all sizes and types globally.

Cybercrime is a natural outgrowth of the expanding cyber attack surface, and it should be expected. A realistic view of the risks and threats we face will help organizations and consumers to do a better job of protect themselves.

About Cybersecurity Ventures

Cybersecurity Ventures is the world's leading researcher and publisher covering the global cyber economy. Our firm delivers cybersecurity 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.

For more information, visit **www.cybersecurityventures.com.**

About Herjavec Group

At Herjavec Group, cybersecurity is what we do. Dynamic IT entrepreneur Robert Herjavec founded Herjavec Group in 2003 to provide cybersecurity products and services to enterprise organizations. We have been recognized as one of the world's most innovative cybersecurity operations leaders, and excel in complex, multi-technology environments. We have expertise in comprehensive security services including Managed Security Services (SOC Operations, Threat Detection & Security Technology Engineering) and Professional Services (Advisory Services, Identity Services, Technology Implementation, Threat Management & Incident Response). Herjavec Group has offices and Security Operations Centers across the United States, United Kingdom and Canada.

For more information, visit **www.herjavecgroup.com.**

Follow Us

in Herjavec Group

@HerjavecGroup