CYBERSECURITY VENTURES

HERJAVEC GROUP

# 2017 Cybercrime Report

**Cybercrime damages will cost the world $6 trillion annually by 2021.**

Steve Morgan, Editor-in-Chief
Cybersecurity Ventures

A 2017 report from Cybersecurity Ventures
sponsored by Herjavec Group.

# Table of Contents

# Introduction

## Cybersecurity Ventures predicts cybercrime will cost the world in excess of $6 trillion annually by 2021.

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

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.

Last year, 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 year, it has been corroborated by hundreds of major media outlets, universities and colleges, senior government officials, associations, industry experts, the largest technology and cybersecurity companies, and cybercrime fighters globally.

The 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.

Cyberattacks are the fastest growing crime in the U.S., and they are increasing in size, sophistication, and cost.

The Yahoo hack was recently recalculated to have affected 3 billion user accounts, and the Equifax breach in 2017 — with 143 million customers affected — exceeds the largest publicly disclosed hacks ever reported. These major hacks alongside the WannaCry and NotPetya cyberattacks which occurred in 2017 are not only larger scale and more complex than previous attacks, but they are a sign of the times.

Herjavec Group Founder & CEO, Robert Herjavec

"We are edging closer and closer to seeing Cybersecurity Ventures' $6 trillion in costs attributed to cybercrime damages globally," says Robert Herjavec, Founder and CEO of Herjavec Group, a Managed Security Services Provider with offices and SOCs (Security Operations Centers) globally.

"DDoS attacks, ransomware, and an increase in zero-day exploits are contributing to last year's prediction becoming a reality," adds Herjavec, a Shark on ABC's Shark Tank. "It's concerning that all of 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. We all have a role to play in how we protect our businesses from the accelerating threat of cybercrime."

# Expanding Attack Surface

HERJAVEC GROUP

The World Wide Web was invented in 1989. The first-ever website went live in 1991. Today there are more than 1.2 billion websites.

There are 3.8 billion Internet users in 2017 (51% of the world's population of 7 billion), up from 2 billion in 2015.

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

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

'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 include smartwatches, head-mounted displays, body-worn cameras, Bluetooth headsets, and fitness monitors.

**Cybersecurity Ventures predicts that there will be 6 billion Internet users by 2022, and 7.5 Billion Internet users by 2030.**

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 finds that the world will need to cyber protect 300 billion passwords globally by 2020.

There are 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 zettabytes last year to 96 zettabytes by 2020 (this is how big a zettabyte is).

The far corners of the Deep Web — known as the Dark Web — are 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.

# Expanding Attack Surface

HERJAVEC GROUP

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.

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.

# Cybersecurity Spending

HERJAVEC GROUP

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

The latest forecast from Gartner Inc. says worldwide information security (a subset of the broader cybersecurity market) spending will grow 7 percent to reach $86.4 billion (USD) in 2017 and will climb to $93 billion in 2018. That 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 next five years, 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 over the next five years, 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.

"From our optics, if you define cyber as data collection, storage, security, analysis, threat intelligence, operations, and dissemination, then the $1 trillion market forecast from Cybersecurity Ventures barely scratches the surface," says Jeremy King, President at Benchmark Executive Search, a boutique executive search firm focused on cyber, national, and corporate security. "Cyber will never go away as the bad guys will never stop exploiting this new medium."


**Cybersecurity spending will grow from $86.4 billion in 2017 to $93 billion in 2018.**

# Ransomware Rising

The U.S. Department of Justice (DOJ) recently 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.

Every 40 seconds a business falls victim to a ransomware attack. Cybersecurity Ventures predicts that will rise to every 14 seconds by 2019.

The FBI estimates that the total amount of ransom payments approaches $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 are skyrocketing.

Global ransomware damage costs are predicted to exceed $5 billion in 2017, up more than 15X from 2015.

"Ransomware is a game changer in the world of cybercrime," says Marc Goodman, author of the New York Times best-selling book Future Crimes, founder of the Future Crimes Institute and the Chair of Policy, Law and Ethics at Silicon Valley's Singularity University. "It allows criminals to fully automate their attacks. Automation of crime is driving exponential growth in both the pain felt by businesses and individuals around the world, as well as in the profits of international organized crime syndicates."

**Cybersecurity Ventures predicts that organizations globally will suffer a ransomware attack every 14 seconds by 2019.**

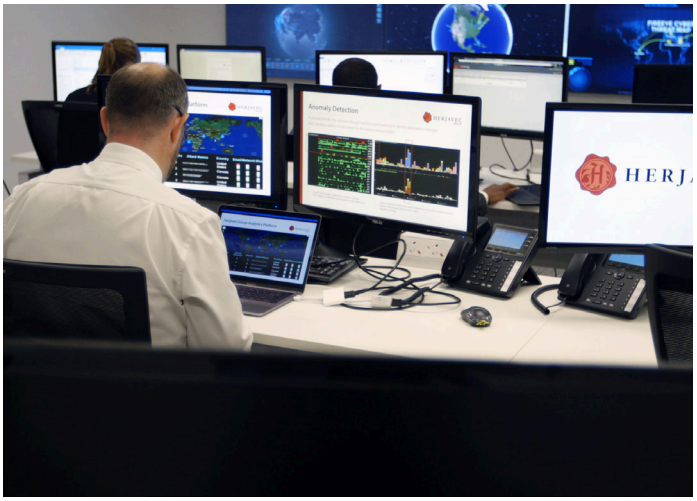
# Labor Crisis

The sheer volume of cyberattacks 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 recently wrote. "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.



> Cybersecurity Ventures predicts there will 3.5 million unfilled cybersecurity jobs by 2021, up from 1 million openings in 2014.

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

"Unfortunately the pipeline of security talent isn't where it needs to be to help curb the cybercrime epidemic," says Robert Herjavec. "Until we can rectify the quality of education and training that our new cyber experts receive, we will continue to be outpaced by the Black Hats."

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.

The cybersecurity workforce shortage has left CISOs (Chief Information Security Officers) and corporate IT security teams shorthanded and scrambling for talent while the cyber attacks are intensifying.

# Security Awareness Training

Cybersecurity Ventures expects 2018 to be the "Year of Security Awareness Training" — the breakthrough year when organizations globally take the (financial) plunge and either train their employees on security for the first time or double-down on more robust and ongoing security awareness programs.

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.

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.

**Training employees on how to recognize and react to phishing emails and cyber threats may be the best security ROI.**

Kevin Mitnick — the world's most famous hacker — who's now a security consultant and Chief Hacking Officer at security awareness training provider KnowBe4, adds, "You could spend a fortune purchasing technology and services, and your network infrastructure could still remain vulnerable to old-fashioned manipulation."

"If humans are the primary targets of cybercriminals, they ought to be prepared, informed, and weaponized as the first line of defense" according to Anuj Goel, co-founder of Cyware Labs.

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

# Looking Ahead

Healthcare providers have been the bullseye for hackers over the past two years.

"Healthcare is the most hacked vertical we're seeing right now and what makes this industry different is that it affects everyone not just financially but personally," says Atif Ghauri, VP at Herjavec Group and Adjunct Professor – Cybersecurity at Drexel University.

"In 2017 we have seen more focus on cybersecurity investment from healthcare providers," says Robert 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."

"We will see more and more traction next year 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 will be the new healthcare in 2018."

To Herjavec's point, 40 percent of the manufacturing security professionals responding to a recent Cisco survey said they do not have a formal security strategy.

IoT (Internet of Things) devices will be the biggest technology crime driver in 2018. Cisco estimates that the number of IoT devices will be three times as high as the global population by 2021.

"In the next year we anticipate more exploits related to IoT related devices," says Ghauri. "The divide is softening between personal and corporate devices and many organizations struggle to get ahead of this curve. This is the lowest hanging fruit for attackers."

"Manufacturing will be the new healthcare in 2018."
– Robert Herjavec, CEO at Herjavec Group.

The construction industry is 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.

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.

The 5 most cyber-attacked industries in 2015 — healthcare, manufacturing, financial services, government, and transportation — are the same in 2017 and predicted to remain so for 2018, although the rank order may change. The small business sector will see a bump in cybersecurity next year.

# Looking Ahead

In 2018, a legion of small businesses will wake up to the reality that they are under cyber-attack — and take preventative security measures.

Many companies with 100 or fewer employees have learned the hard way that if they wait until after being hacked to deal it — it may be too late. Nearly half of all cyber attacks are committed against small businesses, and the percentage is expected to rise next year.

Finally, consumers are expected to pay more attention to security in 2018 in the aftermath of the Yahoo hack and Equifax breach — plus newer vulnerabilities such as the Krack Attack, which puts every Wi-Fi connection in the world at risk… including wireless routers in homes.

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.

"In the next year we anticipate more exploits related to IoT related devices. The divide is softening between personal and corporate devices and many organizations struggle to get ahead of this curve. This is the lowest hanging fruit for attackers."

–Atif Ghauri, VP, Herjavec Group

# Safety in Numbers

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

For example, 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 acquisition in 2017, 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.

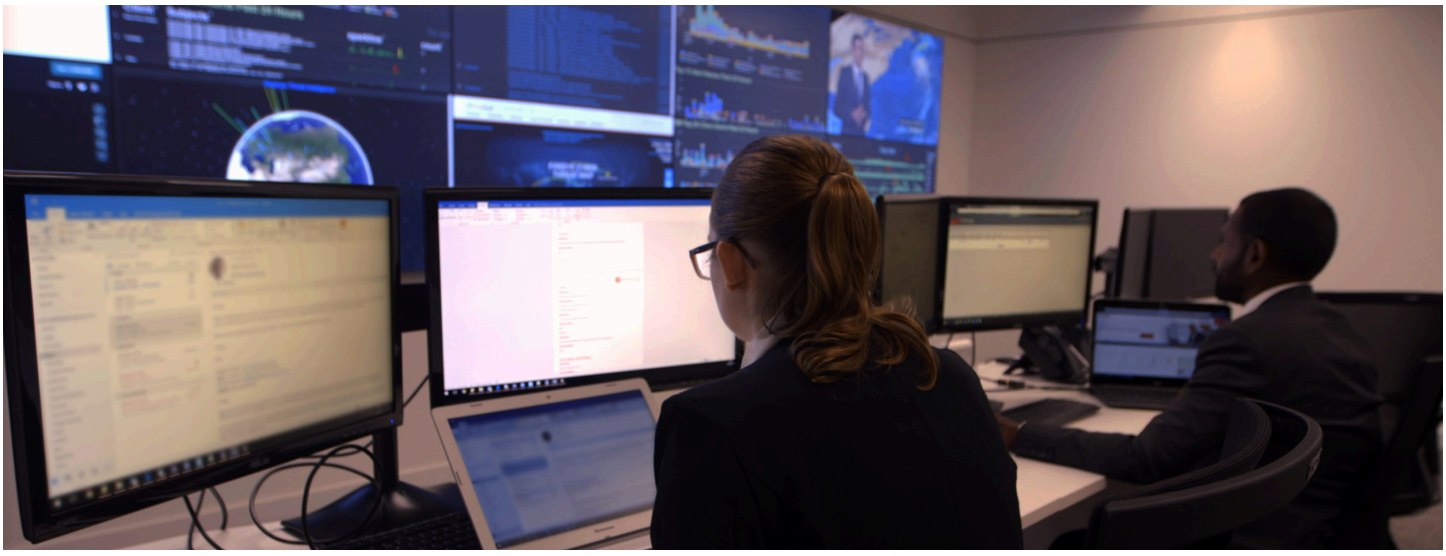
## Security M&A: Intel parks in the collision avoidance space with its acquisition of Mobileye.

Cyber entrepreneurs globally are hard at work on combating and reducing cybercrime.

Hundreds of top cybersecurity companies are innovating cutting-edge products and creating new services in the war against cybercrime.

A growing number 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 protecting themselves.



# Cybercrime Statistics

HERJAVEC GROUP

Nearly half of all cyberattacks are committed against small businesses.

Cybersecurity Ventures predicts that a business will fall victim to a ransomware attack every 14 seconds by 2019, increasing from every 40 seconds in 2017.

Ransomware damages are up 15X in the past 2 years.

Ransomware attacks on healthcare organizations are expected to quadruple by 2020.

According to the FBI's Internet Crime Complaint Center (IC3), the BEC (Business Email Compromise) scam has seen an increase of 1,300 percent in identified exposed losses, totaling over $3 billion, since Jan. 2015.

Cisco put the total amount of loss due to BEC — from Oct. 2013 through Dec. 2016 at more than $5 billion, and the losses continue to mount.

**91 percent of attacks by sophisticated cybercriminals start through spear phishing emails.**

A global survey conducted last year indicates two out of three people have experienced a tech support scam in the previous 12 months, according to the Microsoft Digital Crimes Unit.

Cyber criminals are creating an average of around 1.4 million phishing websites every month with fake pages designed to mimic the company they're spoofing.

The average size of distributed denial-of-service (DDoS) attacks is 4X larger than what cybercriminals were launching two years ago — and more than 42 percent of DDoS incidents in 2017 exceed a whopping 50Gbps, up from 10 percent of cases in 2015.

Cybersecurity Ventures predicts that newly reported zero-day exploits will rise from one-per-week in 2015 to one-per-day by 2021.

"In 2017 we have seen more focus on cybersecurity investment from healthcare providers. 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."

–Robert Herjavec, Founder & CEO, Herjavec Group

# 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 CybersecurityVentures.com.

---

# About Herjavec Group

At Herjavec Group, we take our role as your trusted advisor in information security very seriously.

Information Security Is What We Do. Full Stop.

We are laser-focused on protecting the infrastructures of our customers globally and will take every measure possible to learn and engage with security experts worldwide to ensure we remain on the cutting edge of this rising threat landscape.

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 players, and excel in complex, multi-technology environments. Our service expertise includes Consulting, Installation & Architecture, Identity & Access Management, Managed Security Services and Incident Response. Herjavec Group has offices globally including across the United States, the United Kingdom and Canada.

For more information, visit HerjavecGroup.com.

## Follow Us

Herjavec Group
@HerjavecGroup