The Big Risks to Technology Growth

"Defense Against the Dark Arts" Grows in Importance

Dale Ford, Chief Analyst

Issue

After exploring the "Next Big Thing" expected to drive future growth in the electronics industry – the technology triumvirate of 5G, IoT and the Cloud – it is appropriate to consider the forces that present the most significant risks to the exciting future envisioned for technology and electronics. Success in combating the risks presented by "dark forces" around the world will require an aggressive defense and offense on multiple levels and multiple fronts ranging from corporations and governments to individual employees and consumers. To develop an effective strategy that will protect the health of the electronics industry it is necessary to identify the key areas of risk facing the global technology economy. In reviewing the potential threats to the electronics industry, the following eight challenges emerge as the most significant risk factors:

"Big Risks" Impeding Growth

- Cybersecurity Risk
- Inadequate Intellectual Property Protection
- Counterfeit Components
- Collapse of Global "Free Trade"
- Regulatory Paralysis
- Health Concerns
- Balkanization of the WWW

In identifying the risks listed above it is important to note that other potential challenges to industry growth should not be ignored including overall economic health, technology hurdles, adequate business investment incentives, etc. However, these are challenges that the electronics industry has successfully managed throughout its history and productive strategies and policies have already been widely implemented to address these areas. The risk factors highlighted in this analysis are either relatively new in their emergence/size or continue to bedevil industry players and require reinvigorated efforts and innovative approaches to deal with the ever-changing and growing danger they present.

While each risk represents a major topic on its own, the purpose of this analysis is to briefly highlight these key areas of concern and provide perspective on the threat they present. The creation and implementation of intelligent solutions in each of these areas will be needed to protect the bright future enabled by electronics technology.

Analysis

1- Cybersecurity Risk

The most significant threat to the future of technology and electronics comes from cybersecurity as it both drains all industries financially and undermines trust in use of critical networked technologies that will form the foundation for future products and services. Lost confidence in cybersecurity could seriously undermine adoption of new technologies and cripple the strong value propositions enabled by networked technologies. Certainly, the number and frequency of reports about major cyber crimes has reached dizzying levels. However, the significant concern regarding cybersecurity would seem to be counter intuitive - complacency. According to Robert Herjavec, founder and CEO at Herjavec Group, a Managed Security Services Provider with offices and SOCs (Security Operations Centers) globally, "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."

To highlight the challenge facing us, Cybersecurity Ventures has presented compelling statistics and projections related to the size of the challenge we face in protecting the enormous value being created in the digital world. A wealth of data can be found at their site, cybersecurityventures.com. The critical forecast emerging from their analysis is highlighted in the quote below:

> "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." - *Cybersecurity Ventures*

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 cyberattack 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.

Some key statistics from Cybersecurity Ventures that provide context regarding the size of the challenge and key industries at risk are presented in the following bullet points:

- Today there are nearly 1.9 billion websites. There were nearly 4 billion Internet users in 2018 (over 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

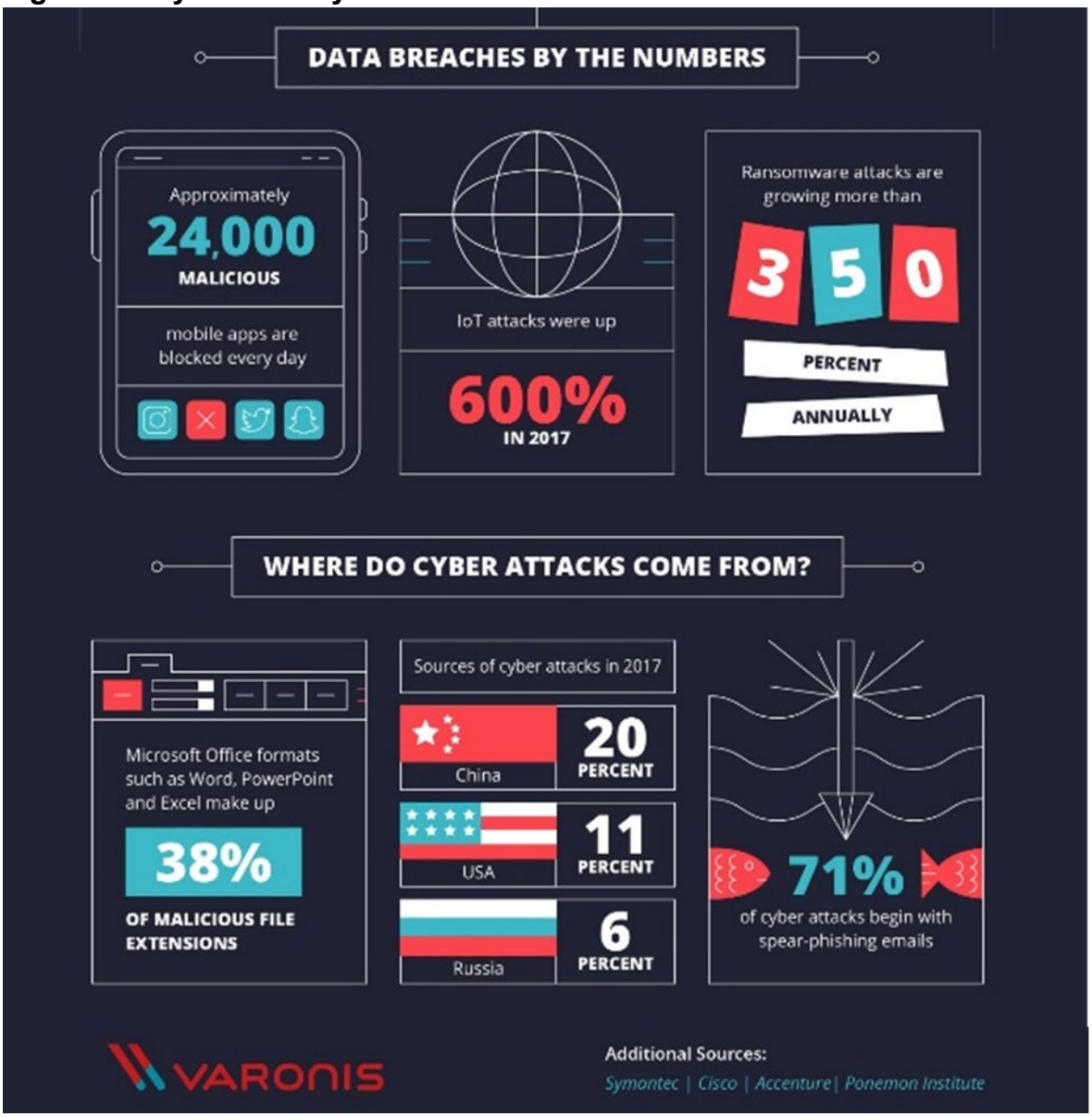
Internet users by 2030 (90 percent of the projected world population of 8.5 billion, 6 years of age and older).

- 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 confirms that cloud data center traffic will represent 95 percent of total data center traffic by 2021.
    - 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.
- 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.
- Dr. Janusz Bryzek, previously 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), hyper imaging, macroscopes, medical "labs on a chip," and silicon photonics.
- Worldwide spending on information security (a subset of the broader cybersecurity market) products and services reached more than $114 billion in 2018, an increase of 12.4 percent from last year, according to 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.
- Healthcare providers have been the bullseye for hackers over the past three years. Ransomware attacks on hospitals are predicted to increase 5X by 2021."
- Manufacturing has become the new healthcare in 2018.
    - 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 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.
- 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."

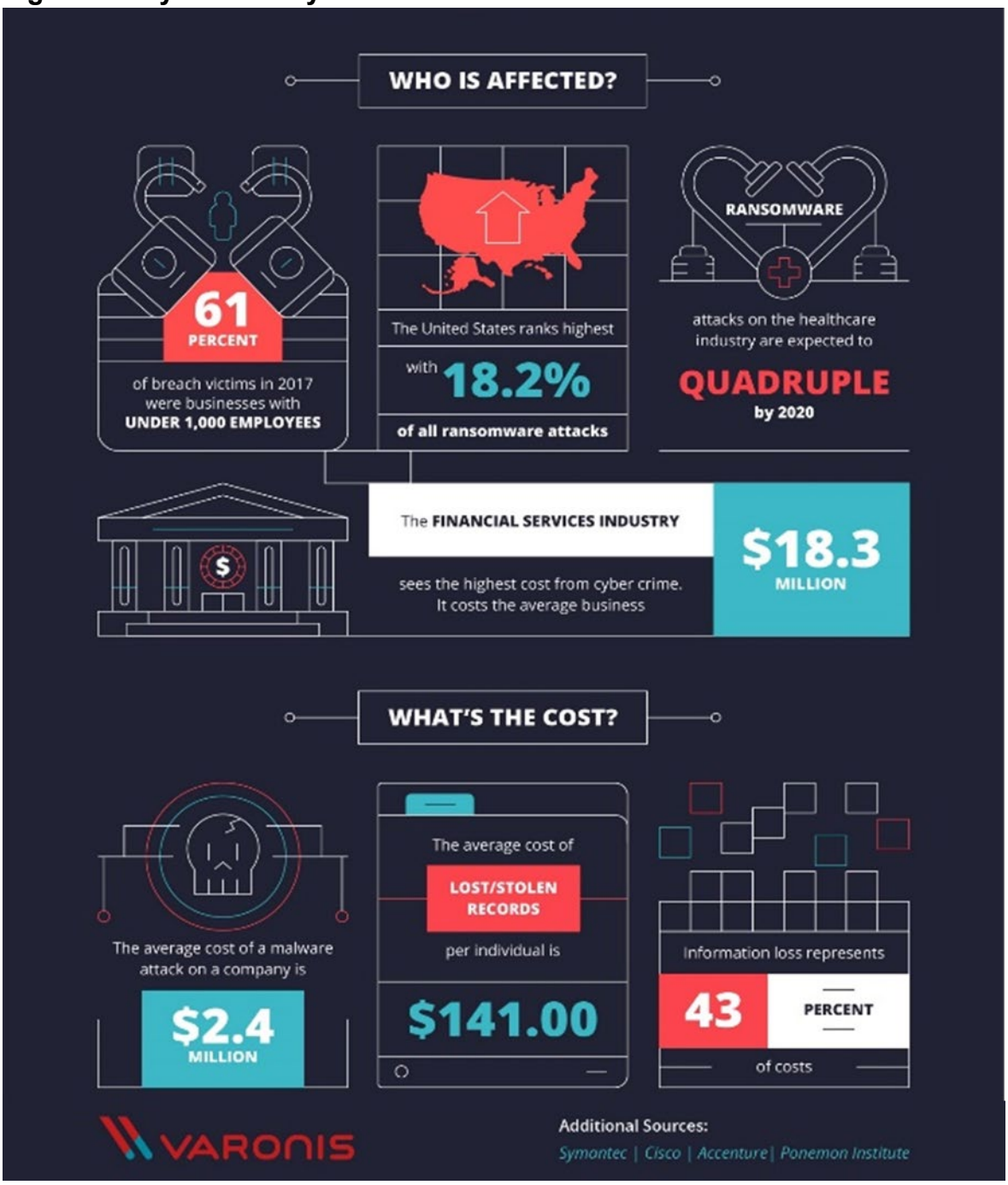
Additional perspective is provided by Varonis in an Infographic that is presented in Figures 1, 2 and 3 below:

Figure 1 – Cybersecurity Statistics for 2019 – Part 1



Source – Varonis

Figure 2 – Cybersecurity Statistics for 2019 – Part 2



Source – Varonis

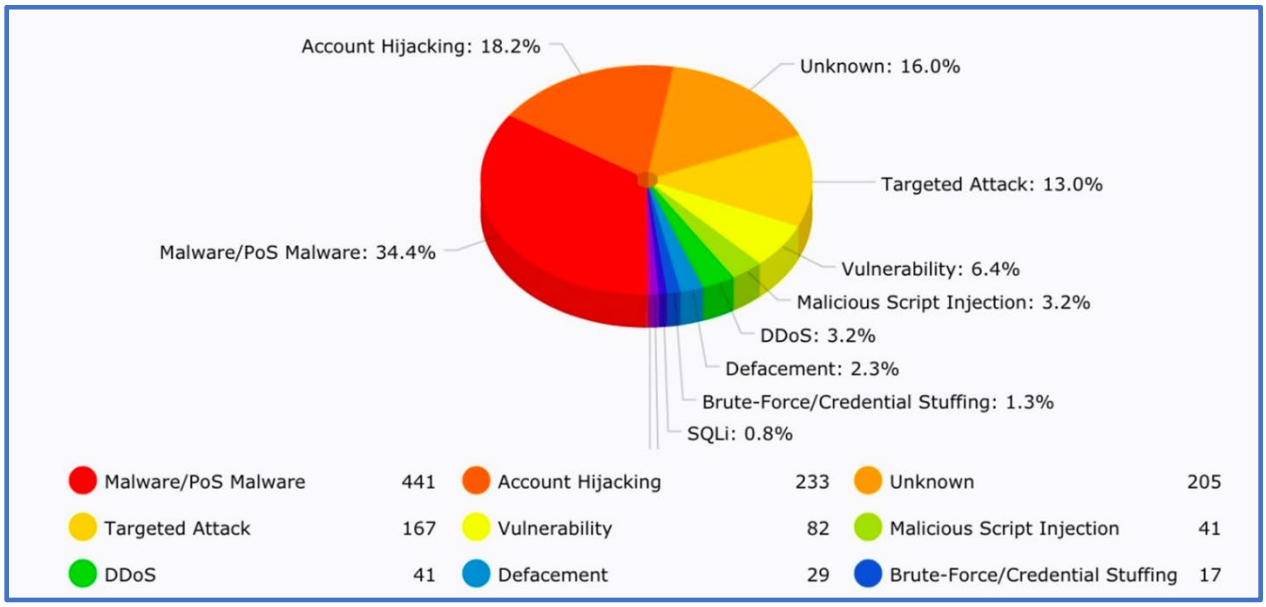
Figure 3 – Cybersecurity Statistics for 2019 – Part 3

Source – Varonis

Finally, Hackmageddon.com has tracked the hacking activity around the world on a weekly basis for a number of years and presents a comprehensive list of attacks on its website. Figures 4 and 5 present a summary of the hacking activity in 2018.

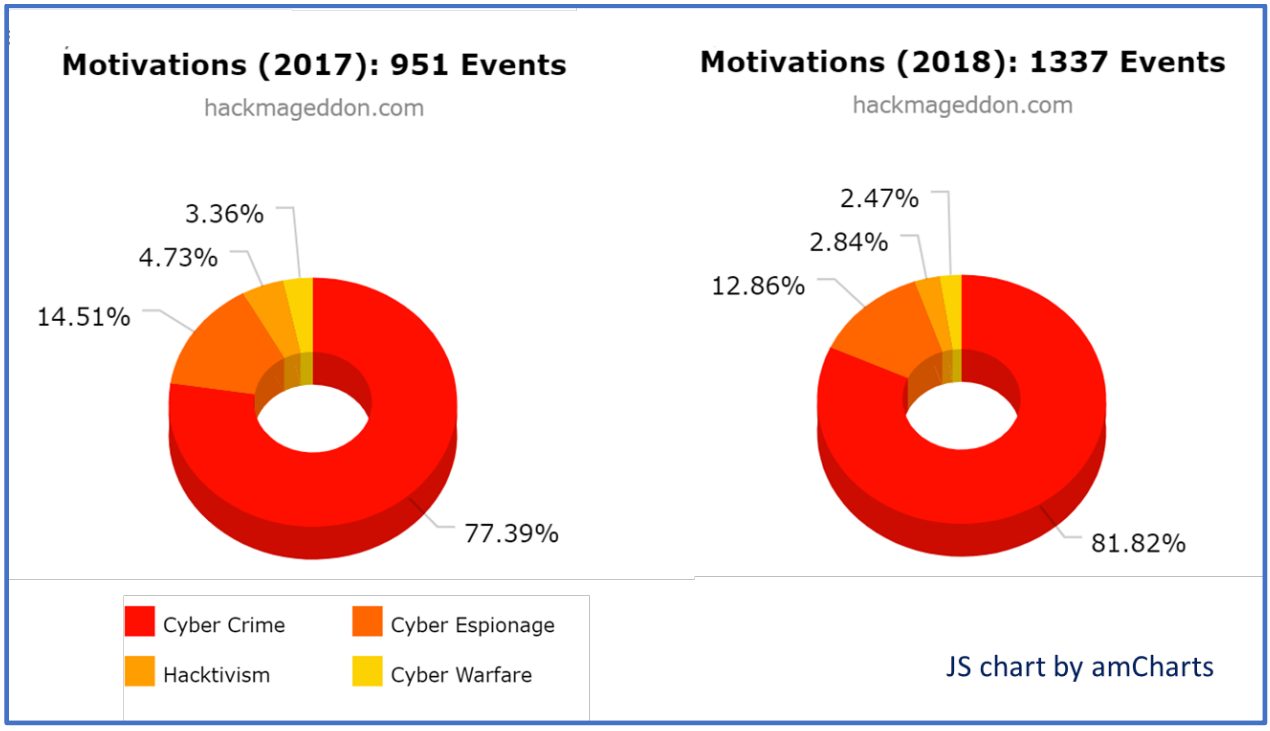
To return to the claim made at the beginning of this section, the data presented by organizations tracking cybersecurity show a clear and present danger to the technology industry future from cyber-crime. The need for aggressive strategies and investment in solutions is critical if we are to successfully fight forces that threaten the bright prospects enabled by the exciting technologies that will achieve critical mass over the next few years.

Figure 4 – Attack Distribution – Top 10 for 2018



Source – Hackmageddon.com

Figure 5 – Hacking Motivations – 2017 / 2018



Source – Hackmageddon.com

2- Inadequate Intellectual Property Protection

The United States has long said that intellectual property theft has cost the US economy billions of dollars in revenue and thousands of jobs. So just how much damage has it done?

An article published on CNN.com reports that, “The United States Trade Representative, which led the seven-month investigation into China's intellectual property theft and made recommendations to the Trump administration, found that ‘Chinese theft of American IP currently costs between $225 billion and $600 billion annually. Those numbers are in line with a 2017 report from the Commission on the Theft of American Intellectual Property.” Theft of intellectual property takes many forms ranging from outright espionage to forced technology transfers and mandatory joint ventures.

According to a CNBC survey published in March 2019, just under one-third of CFOs of North America-based companies on the Global CFO Council say Chinese firms have stolen from them at some point during the past decade. One in five North American-based corporations on the CNBC Global CFO Council says Chinese companies have stolen their intellectual property within the last year. The CNBC Global CFO Council represents some of the largest public and private companies in the world, collectively managing nearly $5 trillion in market value across a wide variety of sectors.

Negotiating an agreement related to intellectual property protection is a central issue in the ongoing trade negotiations between the U.S. and China. In its report on CFO concerns and IP issues between the US and China CNBC noted, “After the December 2018 G20 meeting in Buenos Aires, Argentina, China took a step that conservative think tank American Enterprise Institute described as significant, when the Chinese government issued a memo that set out some 38 punishments for IP violators, including denial of access to government funding. ‘The mere publication of the memo (which explicitly referred to American complaints) was an important concession: Until quite recently the Chinese government had officially denied that significant IP theft occurred in China,’ AEI’s Claude Barfield wrote in a blog post. But the issues are complicated by, among other things, blurred lines between cyber espionage committed by the Chinese government against corporate and military targets and the passing on of those secrets to Chinese companies.”

The creation and development of intellectual property is the life blood of the technology industry. If the industry hemorrhages this vital energy through theft it will risk its ability to attract future investment and lose in the global competitive arena. At some point, if investment in IP is significantly diminished due to an inability to protect it, the market competition will spiral down to a contest of who can produce and deliver a product for the lowest cost. Markets that compete on cost alone stagnate and lose both the talent and financing that enable meaningful growth.

3- Counterfeit Components

An issue that has been at the front of concerns of all manufacturers of electronics components is the challenge of counterfeiting. Fortunately, several initiatives have shown positive results in combatting this pernicious activity. ECIA continues to lead in many areas in the fight against counterfeiting. However, the war is far from won and counterfeit activity impacts economic activity across a wide range of industries as shown in Figures 6 and 7.

Figure 6 – The Economic Impacts of Counterfeiting and Piracy – Part 1

Figure 7 – The Economic Impacts of Counterfeiting and Piracy – Part 2

Table 1 shows that electronics is one of the most heavily impacted areas from counterfeiting activity. If Software Piracy is combined with Electronics losses to represent “Technology” it suffers the largest losses accounting for over 36% of lost value due to counterfeiting.

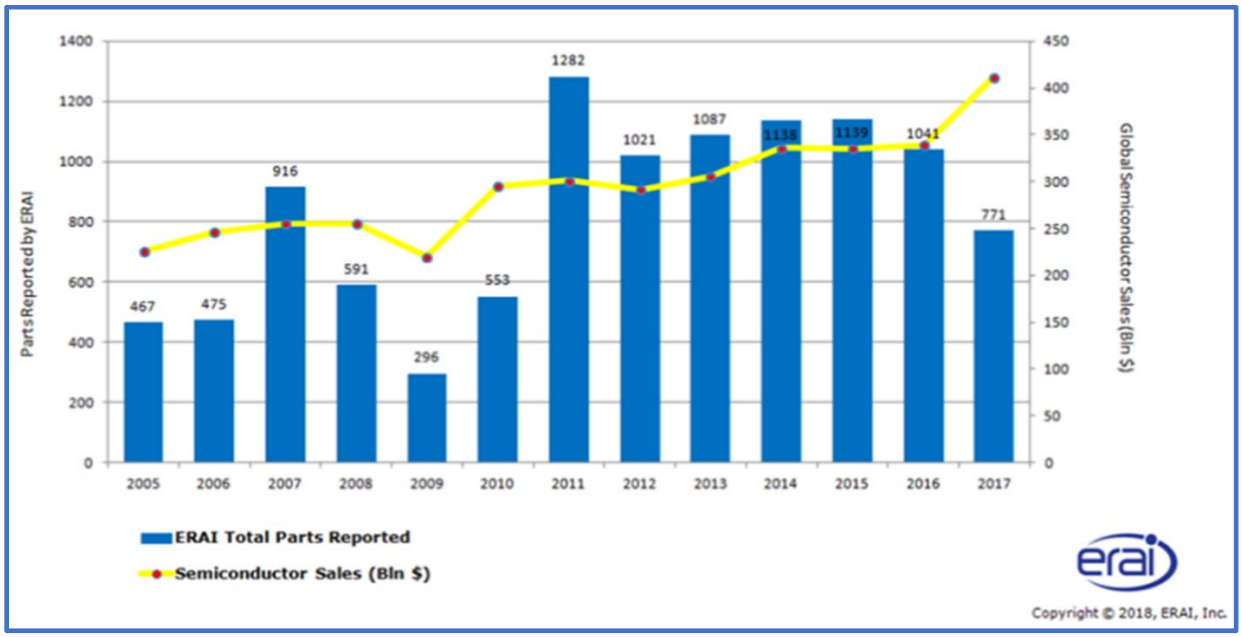
Table 1 – Rank Value of Counterfeit Goods

CATEGORY	$ Billion
Counterfeit Drugs	200.0
Counterfeit Electronics	169.0
Software Piracy	63.0
Counterfeit Foods	49.0
Counterfeit Auto Parts	45.0
Counterfeit Toys	34.0
Music Piracy	12.5
Fake Shoes	12.0
Counterfeit Clothing	12.0
Cable Piracy	8.5
Video Game Piracy	8.1
Counterfeit Sporting Goods	6.5
Counterfeit Pesticides	5.8
Mobile Entertainment Piracy	3.4
Counterfeit Cosmetics	3.0
Movie Piracy	2.5
Counterfeit Aircraft Parts	2.0
Counterfeit Weapons	1.8
Counterfeit Watches	1.0
Fake Diplomas and Degrees	1.0
Book Piracy	0.6
Fake ID	0.1
Counterfeit Money	0.081
Counterfeit Purses	0.070
Counterfeit Lighters	0.042
Counterfeit Batteries	0.023

Source – Havocscope.com

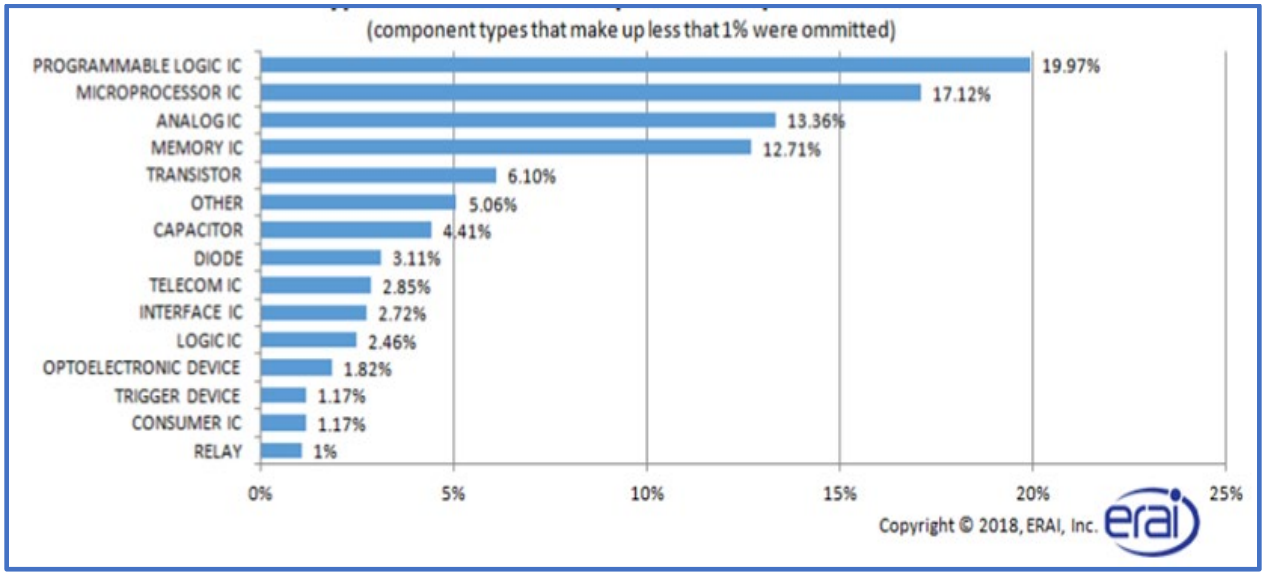
Accurate data regarding the scope of counterfeit electronics is limited. One source of such data is ERAI whose last publicly reported data is shown in Figures 8, 9 and 10. Most recent anecdotal reports show an uptick in counterfeit capacitors and the growing sophistication of counterfeiters. Again, the battle is far from over.

Figure 8 – Reported Counterfeit Parts vs Global Semiconductor Sales 2005 - 2017



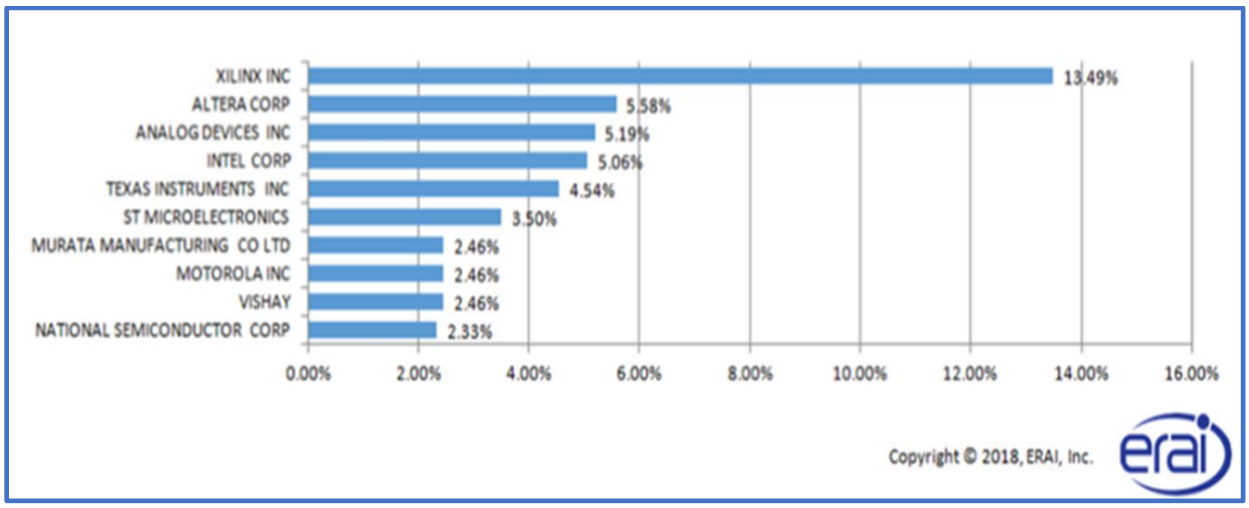
Source – ERAI

Figure 9 – Types of Electronic Components Reported in 2017



Source – ERAI

Figure 10 – Top 10 Manufacturers' Brands of Reported Parts in 2017



Source – ERAI

4- Collapse of Global Free Trade

The electronics industry has been one of the greatest beneficiaries of the stable "free trade" environment over the past two decades. Synergies developed across regions and countries in the design and production of electronics products at compelling consumer price points has driven revenues to dramatic heights and supported strong economic growth on a global basis.

The conflict between the U.S. and China with the reciprocal escalating tariffs has captured headlines over the past year and impacted supply chains throughout Asia. However, this is not the only trade conflict with negative implications. The U.S. congress continues to drag its feet in approving the USMCA trade accords that are vital to healthy relationships in North America. Of course, Brexit has created tension between the U.K. and its European partners with negotiations seeming to go nowhere. Serious concern regarding lost trade and economic damage swirl around Europe. In Asia, Japan and South Korea are engaged in their own trade battles with barriers going up between those two important electronics systems, components and materials producers.

The global electronics industry is at a critical crossroads where the outcome of diplomatic and economic negotiations could reshape trade relations and supply chains around the world. If a win-win solution can be found in these negotiations it could actually strengthen the electronics economy. However, there is a very real possibility of a dramatic downside if barriers go up and the supply chain value creation that has enabled historic growth is damaged.

5- Regulatory Paralysis

The development of many important new markets requires timely and productive support from government regulatory bodies. For example, the success of autonomous vehicles will require the creation of regulations that will support safe market development. Other market opportunities ranging from communications to drones rely on the establishment of related regulations. While technology advances at an accelerating pace, the typical government processes move at a glacial rate. In addition, the adoption of common rules that are accepted across multiple areas is a major challenge.

While it is common for each country to have its own regulations that meet local needs there are times when it is difficult for governing bodies in various jurisdictions within a country to agree. As companies invest in new products, they want to be careful that they do not go down a path that could be blocked by future rules. As a result, even product development cycles can be dragged out by the external force of government regulation. While the often-slow process of regulation development is not likely to kill new technologies/products it can impede the rate of market growth.

6- Health Concerns

A variety of health concerns have accompanied the advancement of electronics markets from the beginning. In the early days of television parents were concerned about possible damage to the eyesight of their children if they sat too close to the TV. The growth of mobile handsets and smartphones has been accompanied by various studies about possible cancer risks. In addition, the serious challenge of distracted driving has prompted the often-ignored laws against texting and driving. The concerns even range to concerns about mental health at the individual, family and societal level due to the powerful influence of social media and the near-addictive behavior patterns that can develop. Even privacy rights are an element of “health concerns” as governments pass “right-to-be-forgotten” laws that are intended to protect consumers.

Health concerns related to technology can result in varying levels of backlash ranging from societal pushback to actual government regulation. In some cases, individual companies such as Google and Facebook have such a dominant influence that they must take a lead role in addressing health concerns. However, in most cases, the need for shared responsibility in addressing concerns motivates necessary participation in industry standards and policy setting activities.

7- Balkanization of the WWW

From its beginning, the development of the WWW has followed principles that might be described as supporting the ideals of civil rights. For example, the rights of free-speech, freedom of association, freedom of the press and other important liberties have been championed by the movers and shakers in the online world. However, the emergence of China as an economic powerhouse and powerful internet force has also been accompanied by a philosophy that communication is not a civil liberty, but a privilege granted by the government.

China has taken a diametrically opposed approach to the WWW from the Western world as it censors online information, requires internet search providers to manipulate results and block access to “sensitive” material, blocks websites, monitors communications activities and even creates “social media scores” that govern privileges of its citizens. China is promoting its own vision of the WWW and the right of a government to enforce internet control within its boundaries. This view is attracting other countries that share this nonconformist Internet-with-borders idea. As a result, the much bigger question of internet governance between two world powers of diametrically opposing visions is coming to a head.

The risk of adopting China’s WWW philosophy is the possible balkanization of the WWW with the free flow of communication across borders being limited or eliminated. This could harm the commercial development of XaaS services & blockchain implementations and create major hurdles for content storage, tracking, dissemination, etc. A large share of the value creation around technology builds on the backbone of a robust and open communications infrastructure. The balkanization of the internet could damage global economic development that relies on an open WWW philosophy.

Action

- Join the upcoming “Data Privacy by Design” webinar on October 18 at 11:00 am EDT. You can register for this webinar at ecianow.org. You can also listen to a recording of the webinar after this date.
- Develop a strategy to invest in cybersecurity assets and talent to protect your company, your products and customers.
- Actively participate in industry associations that enable the creation of standards and regulations that enable cybersecurity, IP protection and counterfeit detection & prevention.
- Work with legislative, regulatory and law enforcement bodies to combat IP theft, cybersecurity and counterfeiting threats
- Develop scenarios and solutions to be implemented based on varying outcomes of trade negotiations.
- Act early to promote the development and adoption of regulations that are required for the creation and development of emerging markets.
- Develop a balanced and productive approach to health issues related to technology.
- Prepare market solutions that anticipate a more fragmented cyber world.