Professor Richard Theodor Kusiolek is the President/CEO of TransGlobalNet and GlobalMilComm Communications. He is an American scholar and professional experienced in technical communications research, strategy, and international business management in the areas of Information Technology, Supply Chain Management, Aerospace and Defense, and Cyber Security.

He has been an active thinker of strategic development of revenue opportunities to ensure organizations' continual growth. A seasoned leader with experience in information systems and technologies who knows the techniques to ensure an organization's economic and product market dominance. Professor Kusiolek is accredited by the US Department of Defense as a journalist interviewing American NASA Astronauts: USAF Colonel Robert L. Behnken and Michael Lopez-Algeria.

He has been teaching courses in management, marketing, and economics at several U.S. universities. Richard Kusiolek is the author of the book "Angels in the Silicon: How Silicon Valley Changed Forever America's Sociopolitical and Global Technology Paradigms".

The article of an American visionary, professor and journalist discusses a vital issue of global cyber-security, analyzing the threats across industries and through time, focusing on growing mobility as a new challenge. The author quotes examples of various countries, including Ukraine, allocates the major problems and offers solutions. The author's ideas and findings may be of great interest to different stakeholders in Ukraine, from governmental institutions to scientists and IT engineers.

Стаття американського мислителя, професора та журналіста присвячена надзвичайно важливій проблемі глобальної кібербезпеки. В ній подано аналіз загроз в різних сферах економіки та в різні часові періоди, зосереджено увагу на поширенні мобільних пристроїв і технологій як новій проблемі. Автор наводить приклади різних країн, зокрема України, виділяє основні проблеми та пропонує рішення. Авторські ідеї та висновки можуть представляти значний інтерес для різних зацікавлених сторін в Україні, від державних установ до науковців та інженерів-фахівців з інформаційних технологій.

SECURING AN ORGANIZATION’S NEW MOBILE INFRASTRUCTURE©®

Richard Theodor Kusiolek

Preface

The advancement and challenges of mobile security, the unlimited potential of mobility, and how to determine which type of mobile device is best suited for the user and organization are extremely important issues. We all are aware that our work is more mobile. Laptops and notebook computers are being integrated into the mobile infrastructure but the challenges of managing and securing these mobile platforms remains a priority. However, mobility cybersecurity has been overlooked and under-played by three key domain sectors; namely, Global Central Governments, Global Commercial Sectors, and Defense. With more mobile applications being developed for downloading to mobile platforms and Operating Systems, the risk has become very real. What are the 2018–2023 Cybersecurity Strategy issues and can they be addressed?

Real Global Cybersecurity Threats

It is far to conclude that the Global Media has tended to report major cyber incidents and thus create a hyper- attention beam that distorts the magnitude of the frequency, magnitude, and the likelihood of the threat to an organization be it industry, government, or defense. In late 2014, the Sony Pictures Entertainment and Target breach (netted 40 million credit and debit card numbers and 70 million customer records and was largely responsible for the company’s 46 percent drop in profit in Q4 of 2013 when compared to 2012), Anthem BlueCross, and the U.S. Office of Personnel Management were hacked as well. In 2017, malware was spread through a Kiev Ukrainian tax preparation software program originating out of Kiev and compromised both U.S. and Ukrainian firms.

Cyber Security is simply difficult for the following realities:

(1). Networks are not smart and do not communicate with other networks or the multiple nodes.

(2). Old point to point old technology is totally incapable of providing security capabilities for today's cyber-attack landscape.

(3). Service (SaaS) providers, cloud computing, mobility, the Internet of Things, and other macro technology trends have the impact for security professionals giving them less and less control over data. The advanced integrated security and automated outcomes must be the same whether the network is on premise, in the cloud, or has data stored off the network in third-party applications.

(4). The 2017 U.S. National Security Strategy report stated, "the ability to meet these challenges of the cyber domain will determine our future prosperity and security."

Tom Farley, President of the New York Stock Exchange, wrote in October 2015, "No issue today has created more concern within corporate C-suites and boardrooms than cybersecurity risk. With the ability to shatter a company's reputation with their customers and draw criticism from shareholders, lawsuits from affected parties, and attention from the media, the threat of cyber risk is ubiquitous and insidious. No company, region, or industry is immune, which makes the responsibility to oversee, manage, and mitigate cyber risk a top-down priority in every organization." Europe and the United States have relied on the Internet Data and Systems within cyberspace. The reliance leaves the West vulnerable to dangerous cyber threats from both state and non-state players. Using hacking to steal a business's intellectual property undercuts both the technological and military superiority. In 2015, the Ukraine electrical grid was hacked resulting in all power supply denied to 225,000 customers. In 2016, the U.S. dropped "cyber-bombs" that forced ISIS fighters to abandon their command post and flee to other outposts, thus revealing themselves from satellite connected drones.

Cybersecurity Threats

By definition, Cybersecurity is "the process of protecting information by preventing, detecting, and responding to (cyber) attacks." As part of cybersecurity, (private and government) organizations should consider the management of internal and external threats and vulnerabilities to protect information assets and the supporting infrastructure from technology-based attacks." Once anyone enters the “Cyber World” they soon learn that this cyber world also consists of cyber criminals, State sponsored cyber espionage trade craft, recreational hackers, identity thieves, industrial spies, and just private companies wanting to gain personal information to sell. Adam Segal in his book, Hacked World Order, sees the Internet as a freeway on-ramp for “economic espionage for China, Iran, Russia, North Korea, and Israel; are stealing global defense secrets, tool for information warfare, and future asymmetric global wars.” California’s Silicon Valley firms pushed the Internet on a global basis as a means to promote democracy and as future streams of cash-flows. When the “the greatest transfer of wealth in history” was happening, company presidents and politicians all look the other way knowing that it would eventually cripple the strongest engine of USA’s economic growth and military power; namely, information technologies and the internet.

Mobility has taken on a new risk reality

Mobility has increased and with it the cyber risk. In 2017, global mobile subscribers reached 5 billion. During the same period, Mobile Broadband Networks increased by 69%. In America, 90% of the populations have a cell phone and 58% own a smartphone. The number of unique mobile subscribers will reach 5.9 billion by 2025, equivalent to 71% of the world's population. Smartphones are now outselling PCs. In 2016, technology hardware companies like Dell and HP were scrambling to refocus their hardware platforms toward the Global Mobility Market. Landline and Satellite Broadband spectrum is running out and hence the global networks are latency is growing and the speed of the Global IP networks is lowering decision making. Mobility to mobility connections will reach one billion by 2020 and it is clear that the weakest link of the network “edge” are mobility platforms. Also, cars such as Tesla Motors are being connected with WiFi and Bluetooth and the Internet of Things has penetrated private areas of a business and homes.

Action Now

Organizations must step up to meet these challenges and risk associated with cyber mobility as well as fixed platforms that will determine the prosperity and security of a commercial or government related entity. A strategy must be in place that understands the network landscape that exists now and in the future. Further, the strategy must outline how to deter or prepare for future cyber threats to the assets and liabilities of the organization. Business must work closely with government policy makers to set the course and engage in mutual funding in an environment that is owned and unregulated by a few oligopolistic market power brokers. Cybersecurity of mobility is a critical issue that crosses business, public, and international sectors. Now is the time to act!

Article published: November 06, 2018