Cybersecurity thoughts and issues from a political perspective

- Area: COMBINED INTERNET GOVERNANCE PRINCIPLES AND ROADMAP
- Entitled by: Gonzalo A Romero B
- Region: Colombia
- Organization: .CO Internet S.A.S.
- Sector: Private Sector
- Keywords: cybersecurity, awareness, capacity building, stability

Abstract

The daily life and economics of the global citizen depend each time more on a stable, secure, and resilient cyberspace; protection of intellectual property and business/personal sensitive information against illegal practices (theft and misuse, mainly) is getting critical within the high-level business and operational processes and capabilities. This short but concise paper puts forward a series of relevant issues we need to face in cyber-security in a short and mid-term; big data, the human factor, identification, false information published online, hacktivism, among others, are issues, terms, concepts and technologies we want to take into account sooner than later in regard to cyber-security as individuals, entities and enterprises. Only adopting a "forward looking" and innovative insight, continuously reviewing, rethinking and redesigning the security framework principles,as well as doing unknown risk exercises, the organizations will be able ensure service continuity.

Document

According to the ITU (Guadalajara Resolution 181, 2.010), “***cybersecurity***” is a “set of security tools, policies, concepts, drivers, risk management methods, actions, education, awareness, good practices, insurances and technologies to protect users and organization assets in cyberspace”.

As stated by the “Global Cybersecurity Center (GCSEC)”, “*DNS security, stability and resilience* (*DNS-SSR) have a direct and strong impact on the performance and dependability of nearly all aspects of interactions on the Internet, including Web applications, Service Oriented Architecture (SOA) based systems, cloud infrastructure and distributed applications in general, which constitute a foundation for high performance and scalable services computing, putting always more demands on the DNS infrastructure, by increasing requirements for higher performance and improved dependability*”. DNS-SSR needs more and better efforts on awareness and tech capacity building/training: “Gaps in talent always means Gaps in security”. ICANN SSR Working Group, as well as Global & Regional organizations like LACTLD, LACNIC and ISOC, and also ccTLD’s and TLD Registrars are working hard on this at this time.

“Big Data” rapid adoption, defined as exponential volume and complexity of data under management, is drastically changing the way “online privacy” needs to be handled and guaranteed. New generic TLD’s (nTLD's) economy and business will impose a lot of challenges to cybersecurity as well, in particular to the Internet’s Domain Name System (DNS).

The weakest element in information security is the HUMAN factor. As a result, organizations need to constantly improve their awareness programs (employees must be more conscious of their information security responsibilities and appropriate use of assets, IP data and technology; info-sec should be part of their performance assessment) and introducing new security instruments: examples can be (a) 2-step authentication for high visible enterprise (PR, marketing, channel management) profiles, (b) sharing passwords strongly prohibited (to avoid cases like Snowden gaining admin/social confidence with NSA workers). 80% of the solution is NON-TECHNICAL, it’s case of “good IT, Security, Operations and Business Governance”.

In terms of cybersecurity framework and strategy deployment, there are good ways for government, civil society and private sector to share information and work toward same goals and challenges: a strong and aligned cooperation effort involving relevant stakeholders is urgently needed globally, regionally and in-country, especially to work together on hardening critical infrastructures, fight against cyber-crime and cyber-delinquency, as well as stability and resilience issues.

“Identification” is one of the most relevant challenges in cybersecurity today (specially for Law Enforcement and National Security agencies): services helping individuals and organizations for “going dark” by handling network anonymity and identity, particularly in “domain names”, as well as advanced encryption and wiretapping techniques, give particular interest benefits but contribute fraudulent, illegal, abusive and malicious activity to increase in cyberspace.

False information published online, as a result of human mistakes or deliberate actions, could have complex social, political and economic consequences to actors involved (i.e., hacking to AP twitter’s account for publishing fake information about White-House explosion and U.S. President’s injury caused stock and marketing uncertainty).

Several countries recognize cyber-attacks more dangerous to their national security than terrorist ones, and face them as serious threats to the country safety from a political, economic, social and technological perspective.

“*Hacktivism*” seen as the usage of IT hacking methods to stage protests and make political statements, is another big challenge for today’s cybersecurity: political activists, cyber-insurgents and mischief makers continue to increase DDoS attacks and take advantage of IT vulnerabilities every day.

Individuals and organizations needs to understand cybersecurity is not just a technological and compliance issue; it’s a business risk that implies and requires an enterprise-wide approach and an innovative approach and response to the unknown challenges new technologies bring ahead.

Inaction or inappropriate preventive and proactive personal/corporate information security measures, as well as not making nor maintaining framework based and continuously reviewed, rethought and potentially redesigned policies, can lead to seriously affect the image/brand and reputation, disrupt business and operational continuity and lead to a host of financial and legal issues.

Every organization's member needs to fully understand and be conscious of the overall consequences of cybersecurity breaches: theft of funds, data leakage/loss, Intellectual Property (IP) are not the only inherent risks associated with; there are costs associated with losses of profits and business as well as the high expenses associated with remediation.

Breaches eventually could derail key objectives, undermine the confidence of shareholders, analysts and customers, and affect business and operational continuity, financial performance, ultimately reducing revenue and company's overall market value.

For as much progress as organizations have made, many of them still have a long way to go. As the rate and complexity of cybersecurity incidents continue to increase, they need to act quickly to avoid leaving themselves exposed to a costly and brand-damaging security incident that shakes the confidence of consumers and shareholders.

People and organizations aspiring to be "information security innovators" need to set their sights on new frontiers. They need to continuously review, rethink and potentially redesign their entire information security framework in order to be better prepared. In many cases, innovating may require a fundamental transformation of the information security program to proactively fortify against both the known and the unknown risks in the cyber risk environment: "the future".

Organizations need to be more "forward-looking" in cybersecurity. As being ready to handle security and risk considerations with "digital devices" (smartphones and tablets, software applications, web/mobile-based apps) and "social media" (a digital business enabler and networking facilitator), they should have been preparing for current technologies as they were appearing on the horizon.

Finally, if resources are still working to improve capabilities for emerging technologies and trends that are right in front of organizations or already behind them, then they will have no time to prepare a defense that proactively protects the organization from technologies that are just (a) "*around the corner*": *big data*, *enterprise app store* (which encompasses associated costs vs. increased productivity of employee request for apps), *supply chain management* (in the context of how external assets like customers, suppliers, vendors, contractors and partners impact security), *cloud service brokerage* (how brokers/partners

manage cloud security, privacy and compliance issues), "*bring your own cloud*", as well as those which about to appear (b) "*on the horizon*": *in-memory computing* (data storage in RAM instead of DB's allowing real-time analysis of high-volume data), *Internet of things*, *digital money* (and regulations and legislation required to address fraud and money laundering issues related with mobile money services) and *cyber-heavens* (where countries provide data hosting without onerous regulations).