Cyber Security in the Wake of Innovation: *Will Technological Innovation Break Cyber Security As We Know It?*

If you rely on enterprise technology in any form, you already know that the lifeblood of cyber security is vulnerabilities. In general, vulnerabilities are the result of three conditions: a susceptibility, oversight or 'flaw', unauthorized access to the flaw and the capability to exploit the flaw. With new, malicious capabilities being developed everyday, its prudent to regard today's flaws as tomorrow's vulnerabilities.

Vulnerabilities have spurred a multi-billion dollar industry over the past decade, spanning hardware, software, devices (phones, tablets, sensors, Smart appliances, etc.), networking, architectures and other domains, as well as people, processes and policies. All of which have the potential to present avenues for exploits of varying complexity and impact.

Although improvements have been made in the ICT industry in design, quality assurance, standards and patch and update management, the foundations of cyber security are not in the ICT industry wheelhouse. Recognizing this, our current cyber security challenges and ICT's focus on speed, interoperability, markets and innovation, the 'Semantic Web' (Web 3.0) stands to disrupt cyber security as we know it.

The current Web environment is a conglomeration of fragmented content - chunks of information whose context is only valid unto itself and that was subjectively verified by an author, moderator or, increasingly, a service. The horizontal relationships between these chunks of information were created, not from micro-level data within the content, but by association, subject matter or correlations.

This is why the Semantic Web, the next version of today's media-rich, socially-networked environment, is so exciting. It will allow for content sharing from user-created data stores driven by rules, vocabularies and contexts beyond the constraints of applications and websites. Eventually, it will result in a filtered catchment of data that is effectively a *fluid continuum* without borders or edges. Current document-to-document (or website-to-website) structures will evolve to datum-to-datum relationships that leverage meta-data and Big Data, creating rich, complex and highly specific contents.

While the axioms of *prevent, deter/refuse, detect, respond* and *recover* may still ring true, the need for tighter, agile iterations and cycles to address vulnerabilities on a hyper-spectral scale will be crucial - something we've yet to master. Adding to this complexity, ubiquitous connectivity, all-access/open technologies, more robust network computing, open identity and neural capabilities (artificial intelligence and machine learning) will stretch conventional cyber security approaches thin.

As an example, ubiquitous connectivity will evolve from *anytime/anywhere* to an *always on* multi-device connectivity, increasing broadband adoption, enhancing mobile Internet access and creating multiple cross-platforms for mobile devices. On its own, this will increase the need for autonomous alerting, complex decision-making, such as switching and transferring systems to isolated environments, and more rigid authentication and authorization controls that maintain the integrity of these connections.

Open and portable identity will allow you to 'carry' your user account and its features from one service to another, creating a unique challenge to maintaining individual reputation, identity and access to personal data. Protecting and validating the "portable you" will require not only tactical safeguards and countermeasures, but strategic governance in the form of privacy regulations and legislation.

New software-as-a-service business models and all access/open technologies (open APIs, protocols, software platforms, data and data licenses) will depend on distributed, grid and cloud computing, mesh nets and extended enterprise environments that offer exclusive, controlled architectures and coordinated platforms. To meet security challenges of open technologies in preventing, detecting, monitoring and responding to threats, network security, especially for third party services, will need to be extraordinarily robust.

To the last point, this is where the technologies of the Semantic Web can be capitalized on: natural language processing, machine learning and autonomous agents - the same functional concepts that found the new environment - can contribute to all phases of the security lifecycle to counter cyber threats through intelligent and adaptive *thinking*, *associating* and *learning*.

New concepts, such as block-chain, may solve issues related to sustained asset confidentiality and integrity, but other methods will be to be explored to assess and protect the uniqueness, value and criticality of data and other assets in this dynamic and autonomous environment.