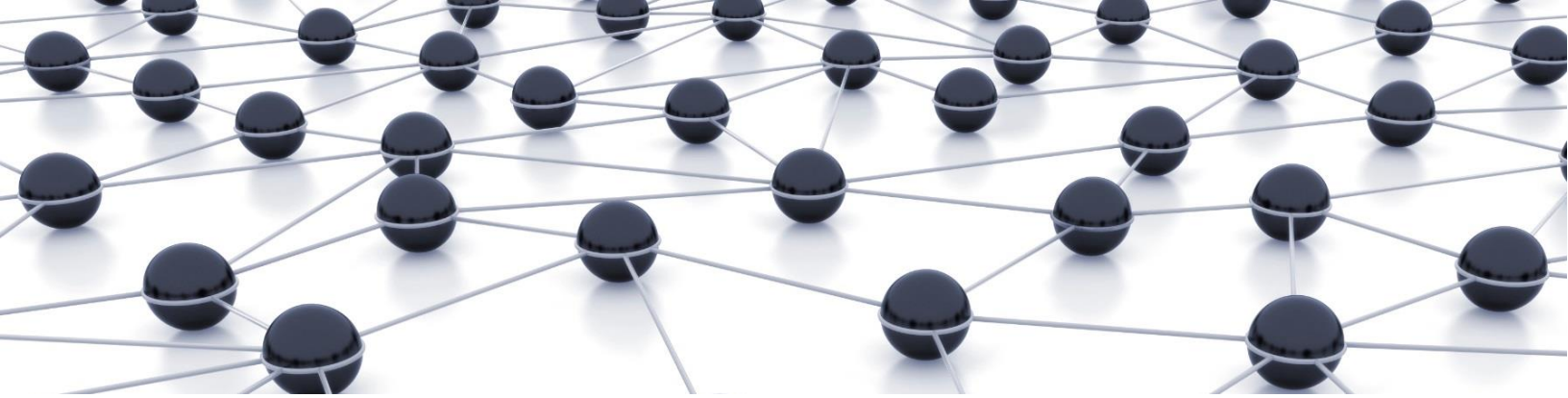

IntelliSyn

Desktop-to-Cloud Business Communications

When IT Is Only An Asset When Protected Against Future Artificial Intelligence Computer Threats

By Merv Perry MBA MSc CISSP CIS

Information Technology is only an asset when the content data is adequately protected; however, there are growing threats to the use of artificial intelligence (A.I) as a tool that cyber criminals will use to assess an asset's value and vulnerability, making it a target for almost unimaginable chaos. A.I will be nearly unstoppable once an IT system is penetrated with the use Internet of Things (IoT) devices. It may work with total impunity within a cloud structure unless there is a better countermeasure. We will see a complete transformation on how businesses operate, whom they hire, and how they handle sensitive information.

While the implications and opportunities of cloud computing may afford large amounts of data being available for business analysis, some risks must be managed to assure citizens of secure and accurate engagement. Regardless of the means access, mobile computing or other ways to citizen's data, the operating model for an entirely digital data value driven business and the analysis of the data they hold has must be secure: even if this service is outsourced. To combat the threat will require the use of a behavioral analytics engine to interpret and provide the insight needed to investigate IT system threats due to A.I.

The integration of social sciences
is our best approach to defending our cloud structures and the sensitive data they hold.

There is an S-curve in the development of IT protection that is reaching a plateau and is potentially threatened by artificial intelligence, unless we all get beyond our reliance on technology alone for an IT defense. The integration of social sciences (i.e. psychology, sociology, anthropology, philosophy, and

related neurological behavioral sciences with A.I computing models) is our best approach to defending our cloud structures and the sensitive data they hold. The major premise is to understand a user's actions from information and data they use in performing their work as a predictor of their behavior and intent.

The Internet of Things (IoT), which puts distributed and highly connected devices via the Internet, can access other networks under intelligent control for both good and bad intent. The use of neural networks with powerful algorithms will gather IoT data that compares good intent from bad intent when access attempts are made by a user. This can be accomplished by examining what content is being accessed and a machine learning's use of a baseline of background data of every user as a means of protection of an asset. The background data is obtained from the history of interaction with social networks. The corporate people's network will gather huge amounts of employee data, which they freely throw off from social networks to the keystrokes, grammar composition of emails, vocal tones, and expressions they make in conversation. It constructs a new social protection profile used to determine when an emerging threat is developing prior to accessing an asset's sensitive data. A password and user identification will no longer be enough to gain access to corporate network if it is deemed that you might be threatened based on the accumulated actions from the data that is gathered from Facebook, Google, Match.com, blogs, credit history, college grades, mobile phone metadata, facial recognition, genetic profiling, and more.

An artificial neural network is a system of interconnected and advanced electronic neurons which exchange messages with each other to formulate the intent.

The neural network uses ongoing feedback to learn good intent versus bad intent through the application of a family of models inspired by the human brain's neural structure. It attempts to estimate behavioral functions that can depend on a large number of unstructured inputs that may or may not be related to good or bad intent. An artificial neural network is a system of interconnected and advanced electronic neurons which exchange messages with each other to formulate the intent. The connections have numeric weights that can be tuned based on experience, making neural nets adaptive to inputs and capable of learning. The learning is applied to revise security as individuals evolve over time.

The combining of different platforms into one platform with the core capabilities to digitize complex business processes: business process management (BPM), robotic process automation (RPA), workforce orchestration, and machine learning-powered cognitive automation with behavioral analytics engine will determine the ongoing protection required for an asset's sensitive data content. This single platform must be sensing and observing not only individual behaviors, but how each individual is making a contribution to an entire organization's operations and processes. The idea is to derive a daily

organizational level of behavior that fits within what is referred to as being normal, expected, and predictable. If this gathered information shows a deviation that infringes a law, policy, procedure, guideline, or best practice, then it is treated as an emerging threat to one or many appropriately identified or related assets that can do harm.

To further safeguard the IT system, different individuals within an organization are asked for their separate input.

A.I is the threat agent that will require another smart A.I to counter its capability by assessing who is behind the attack and determining if their actions are of a good or bad intent. If at any point in the assessment the defending neural machine is undecided or unsure from conflicting probabilities in forecasting good from bad intent, then it moves to a higher level request for human input. To further safeguard the IT system, different individuals within an organization are asked for their separate input without each of them knowing who has been asked. This action is to prevent collusion to gain access while the machine's learning capability determines what action to take.

Companies like Google and Facebook will have accumulated a vast amount of personal information that current efforts in A.I will use as the baseline for determining intent. They will marry A.I with cognitive behavior analysis engines that forecast your intent on a daily basis. This is being proposed initially as a means of evaluating projects and matching employees to tasks.

Machines like IBM's Watson will interact with a user to determine what information they can have or not have access to. It will use natural language processing to understand more than grammar and context alone to evaluate what is being asked based on supporting evidence and the quality of information it finds in order to protect the system. A.I will reveal insights, patterns, and relationships across data and your relationship to the data in terms of creation and use before you are allowed to access it.

"All of these tech companies are now exploring a particular type of deep learning called convolutional neural networks, aiming to build web services that can do things like automatically understand natural language and recognize images."

--Wired

Information access and misuse will be prevented by what A.I determines and learns from its understanding of your intent, which will be evaluated on a minute by minute basis. Those A.I machines that do not know your daily behavior and intent will not able to penetrate another A.I machine and access sensitive information.

While the implications and opportunities of cloud computing may afford large amounts of data being available for business analysis, the operating model for an entirely digital data value driven business and the analysis of the data they hold must be secure by convolutional neural networks to combat the threats by interpreting intent with behavioral analytics engine and provide insight on users when needed.

IT is only an asset when protected against future artificial intelligence computer threats and when artificial intelligence is programmed to manage good intent only and restrict access if the bad intent is recognized and blocked based on user profiles.