help source

Q I have heard from vendors that cognitive technologies such as machine learning can assist in my risk management and security efforts. Is this the case? If so, how do I measure and evaluate their performance? Are there any standards, tools or information sources that can help?

A An effective risk management process requires a risk response decision that is based on earlier knowledge about the possibility of threats exploiting vulnerabilities within the system. A normal risk management process identifies a threat and assesses it for relevance to the organization. Based on these assessment results, the organization makes a decision on how to respond. However, with the automation of information management, the speed of information processing is continuously increasing and the organization requires faster responses. The challenge the normal risk management process presents to organizations today is its ability (or lack thereof) to meet the need for timely detection of risk materialization and response to those risk items.

Detection of risk materialization is currently being done using structured data analysis. A good example is security incident and event management (SIEM) tools used for log analysis and determining possible risk materialization. Another good example is financial institutions using transaction analysis and unstructured (text) data analysis utilizing tools with analytics capabilities to detect possible fraud or attacks. However, these technologies suffer from false-positive alerts, and human intervention is required to make a response decision. To date, there have been two distinct eras of cyber security: perimeter controls[1] and security intelligence. These serve as building blocks as we enter the third era—cognitive security.

Cognitive systems are self-learning systems that use data mining, machine learning, natural language processing and human-computer interaction to mimic the way the human brain works. If used for detecting risk materialization, these systems can learn from the decisions made by humans and update their knowledge engine.

There are a few products for the financial sector being used for detecting possible fraud; however, these products are still not mature enough to be used for risk management in all sectors. Another challenge is that the review of new threats and risk that forms the basis for risk management is not yet mature enough for cognitive technologies to adopt. There are some tools available that can understand the updated risk database and provide dashboards to management for review, but risk assessment, which is human judgment based on experience, will take more time to be available for self-learning systems.

Today, the use of cognitive technologies in risk management and security is limited to:

- Analyzing security trends and distilling enormous volumes of structured and unstructured data into information and then into actionable knowledge to enable continuous security and business improvement[2]
- The use of automated, data-driven security technologies, techniques and processes that support cognitive systems' having the highest level of context and accuracy[3]

In the future, cognitive systems could analyze interactions, their nature and susceptibility, to develop risk profiles for organizations, corporate actions, training and reeducation. Cognitive systems could also use natural language processing to find and redact sensitive data in an organization.

Q How important is threat intelligence to my risk management efforts? Is this something that we should implement? If so, how do I do this?

A Organizations suffer attacks every day and are able to respond to most of them with the knowledge available. However, the adversaries are always ahead and keep devising new attacks using new techniques. The result? Organizations miss the attack and come to know about it only when

Sunil Bakshi, CISA, CRISC, CISM, CGEIT, ABCI, AMIIB, BS 25999 LI, CEH, CISSP, ISO 27001 LA, MCA, PMP

Has worked in IT, IT governance, IS audit, information security and IT risk management. He has 40 years of experience in various positions in different industries. Currently, he is a freelance consultant and visiting faculty member at the National Institute of Bank Management, India.

the damage is done. Zero-day attacks or advanced persistent threats (APTs) are known examples. In other words, organizations are defenseless against new attacks.

Threat intelligence, in simple words, is information an organization can use to enhance its detection capabilities. It helps to detect an attack before it materializes. Primitive examples of threat intelligence can be heuristic scanning by antivirus tools, intrusion prevention system (IPS) or the virus signature update provided by the antivirus vendor. In other words, threat intelligence is information that helps organizations in enhancing the ability to detect, prevent and/or investigate possible attacks before an attack actually takes place or in the early stages of an attack before it impacts business.

Because early detection of an attack helps organizations control the attack's impact and threat intelligence supports earlier detections, organizations would be wise to consider implementing threat intelligence. However, they should also understand that implementing threat intelligence is not a one-time project. It is an ongoing endeavor, as new threats are constantly emerging. To implement threat intelligence, these steps may be considered:

- Build a threat profile that includes possible perpetrators/attackers. This can be done by building possible risk scenarios (refer to *COBIT® 5 for Risk*[4] for generic IT risk scenarios).
- Collect information, particularly about past incidences, within the organization and within the industry: malware indicators and incidents, Internet Protocol (IP)/URL reputation, information from command and control networks, and so on. There are a number of data sources available that can provide this information.
- Form an internal group that analyzes information received from internal and external sources for relevance for the organization.
- Aggregate and analyze the data received, particularly considering the volume and duplicate information. Identify the data that might prompt actions such as updating the existing controls or implementing new controls, and identify possible false-positives. The information posted by possible attackers can especially mislead the response decision.
- Based on information analysis, identify the areas that require changes, particularly the policies, processes, rules for monitoring the events (risk indicators/risk thresholds), firewall rules, etc.
- Validate the rules and implement processes for ongoing threat intelligence information gathering and updating rules and processes.
- Automate the process. For example, in the event of a data breach, lockdown or zero-day attack, implement temporary blocks automatically based on predefined policies. Or, if a device starts behaving abnormally, have it automatically removed from the network for investigation.

> **“Because early detection of an attack helps organizations control the attack's impact and threat intelligence supports earlier detections, organizations would be wise to consider implementing threat intelligence.”**

The key point to be noted is that implementing threat intelligence is a mammoth task, so it must be undertaken in small steps.

Endnotes

1 IBM, *Cognitive Security White Paper*, USA, 2016, *http://cognitivesecuritywhitepaper.mybluemix.net/*
2 *Ibid*.
3 *Ibid.*
4 ISACA®, *COBIT® 5 for Risk*, USA, 2013, *www.isaca.org/COBIT/Pages/Risk-product-page.aspx*