Preparing for Auditing New Risk, Part 2

Part 1 of this column explored domains of risk that are rapidly becoming apparent as they take unprepared organizations (in terms of policies on how to deal with them) by surprise. Social networks and bring your own device (BYOD) are two notable examples. This column addresses issues that are being talked about, but are largely in early stages of development, thus giving organizations a chance to analyze their strengths and weaknesses and develop appropriate policies.

This list is guaranteed to be incomplete, as are the many assumptions made in this column.

The Internet of Things

While, historically, vendors could remotely access data center equipment for diagnostic purposes, there are now many devices that can gain wireless access to the web. This will introduce significant new risk,[1] discussed in this section.

Some vendors have limited or no experience in security by design, quality assurance and other practices applied by the major software houses. Even the software of those major software houses is not always error free.

Ed Gelbstein, Ph.D., 1940-2015
Worked in IS/IT in the private and public sectors in various countries for more than 50 years. Gelbstein did analog and digital development in the 1960s, incorporated digital computers in the control systems for continuous process in the late '60s and early '70s, and managed projects of increasing size and complexity until the early 1990s. In the '90s, he became an executive at the preprivatized British Railways and then the United Nations global computing and data communications provider. Following his (semi)retirement from the UN, he joined the audit teams of the UN Board of Auditors and the French National Audit Office. Thanks to his generous spirit and prolific writing, his column will continue to be published in the *ISACA® Journal* posthumously.

Standards for exchanging information enable smart devices to control other devices, e.g., activating a camera and microphone the owner had previously disabled, or intercepting information from or that interferes with web-enabled medical devices such as pacemakers or insulin pumps.

The major "known unknown" is the swarm behavior of a large number of devices each with limited processing capacity but able to exchange data (i.e., identity, location, sensors, control functions). What is certain is that, if the behavior of swarms of insects and birds can be taken as a guideline, the impact of swarming devices could be much greater than imagined and huge amounts of data may be generated. Risk scenario planning[2] should consider these risk areas because "only the paranoid survive."

Research and development on how the the Internet of Things (IoT) will evolve already speaks of a next wave that will lead to an "Internet of Everything."[3] In this scenario, the Internet will link people, processes and objects and is seen as a major transformational initiative. The research predicts that global volumes of data will double every two years as everything becomes connected.

Big Data

Big data,[4] data analytics and business intelligence are much-used buzzwords. It seems some may have forgotten the many decision support systems that failed previously to meet managerial expectations.

The explosive growth of data without proper attention to its quality attributes (i.e., accuracy, timeliness, traceability, semantic description) leads to the risk of misuse and abuse and can result in garbage in, garbage out (GIGO).

Data management and data governance are likely to demand increased attention from data owners/data stewards, not only to strengthen the measures to protect the data, but also to ensure that legislation addresses retention, anonymization, encryption and disposal, in addition to protection.

Auditors have an educational role to play by making senior management (and, when appropriate, the audit committee) aware of weaknesses in data governance and management and the risk of using data where they may not be valid or relevant.

Beyond this, the convergence of the expanding role of mobile devices, the capabilities of the cloud in all its variants, the questionable quality of some apps and the expansion of IoT (or of Everything) will take us from big data to bigger data. The consequences of this convergence require, at present, a crystal ball to predict.

The Militarization of Cyberspace

It should not come as a surprise that the technologies described in this article (and many more) have been adopted to supplement and strengthen the technologies used in gathering intelligence and analyzing data, and for use in the field. Conversely, many innovations initially conceived for military use find their way into civilian consumer products, the most recent being drones.[5]

> **"Mutually assured disruption may end up only with losers and no winners."**

The military long ago recognized that critical infrastructures are dependent on information systems/information technology (IS/IT). These technologies are not covered by international treaties such as the Laws of Armed Conflict (LOAC),[6] which deal with warfare proper, or the International Humanitarian Law (IHL),[7] which addresses the impact of warfare on people and is better known as the Geneva Conventions.

These laws identify, among other things, protected targets such as hospitals and other critical infrastructures that would have a massive impact on civilian populations. The same applies to the concept of proportionality when responding to an attack. This means that critical infrastructures could become the target of a cyberattack until the LOAC or the IHL are updated to reflect the changing world (and even after that).

While these laws have been signed and ratified by most countries, this leaves nonstate actors free to continue to ignore them. "Nonstate actors" is a euphemism for those who describe themselves variously as liberators, freedom fighters or separatists, but never refer to themselves as terrorists.

The use of the Stuxnet[8] malware in 2009-2010 to interfere with the uranium enrichment facilities in Iran was never officially labeled an act of cyberwarfare, and there has been only speculation about the origin and use of this malware. This sort of activity creates exposures in:

- Systems control and data acquisition (SCADA) systems distributed over a large area, used extensively by utilities, refineries and manufacturing plants. Usually, these systems are not the responsibility of the IS/IT function and may not be audited regularly.
- Direct digital control that may not be connected to the corporate network or the Internet

Such systems perform vital roles. When they fail, it makes the front page in the world news. Recent examples include, in addition to the Stuxnet usage noted earlier, the electrical blackout in the northeastern United States in August 2003 and the attack of the Saudi Aramco network in August 2012. These are just the proverbial tip of the iceberg.

The capabilities to launch such cyberattacks already exist; cyberarmies are likely to exist, but they remain unacknowledged. Mutually assured disruption may end up only with losers and no winners.

Enjoying this article?

- **Learn more about, discuss and collaborate on audit tools and techniques in the Knowledge Center.** *www.isaca.org/it-audit-tools-and-techniques*

Over the Horizon

Other than the Internet of Everything, which is a potential future development, wearable devices, robotics and artificial intelligence (AI) have been around for some time. However, they have remained obscured to some extent by other, more pressing issues such as those raised previously in this column.

> **"Elon Musk, Bill Gates and Stephen Hawking have recently expressed concern about future developments in AI to the extent of referring to the potential of an 'existential threat.'"**

AI has been talked about since 1950, when Alan Turing formulated a test of a machine's ability to exhibit intelligent behavior equivalent to, or indistinguishable from, that of a human.[9] Since then, its development has shown some successes, such as a computer (Deep Blue) winning a chess match[10] in 1997 against a chess champion (Gary Kasparov) and, more recently, another computer system (Watson)[11] competing at the human champion level in real time on the US television quiz show, *Jeopardy*, and winning.

It may be worth noting that Elon Musk, Bill Gates and Stephen Hawking have recently expressed concern about future developments in AI to the extent of referring to the potential of an "existential threat."[12]

It is possible that these comments are comparable to the activities of Luddites and saboteurs of the 19th century, who attempted to damage and destroy the machinery that was automating their jobs. On the other hand, the achievements of Musk, Gates and Hawking suggest they may just be right.

Conclusion

Perhaps one of the variants of Murphy's Law is worth remembering: There is never anything so bad that it could not possibly get worse.

Audit strategy and corporate policies should consider these emerging risk issues and address them as early as practical in a manner consistent with national legislation. Two factors will be key to success: securing the buy-in and visible support of the board and executive management (tone at the top) and inspiring the willingness of staff to adopt and comply with appropriate policies.

Endnotes

1 Gonzalez, M. H.; J. Djurica; "Internet of Things Offers Great Opportunities and Much Risk," *ISACA® Journal*, vol. 2, 2015, *www.isaca.org/Journal/archives*

2 ISACA®, *Risk Scenarios: Using COBIT® 5 for Risk*, USA, 2015, *www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Risk-Scenarios-Using-COBIT-5-for-Risk.aspx*

3 Institut Montaigne, "Big data et objets connectés," April 2015, *www.institutmontaigne.org/res/files/publications/20150403_rapport%20objets%20connecte%C3%8C%C2%81s%20v8.pdf*

4 Press, G.; "A Very Short History Of Big Data," *Forbes*, 9 May 2013, *www.forbes.com/sites/gilpress/2013/05/09/a-very-short-history-of-big-data/*

5 Cavelty, M. D.; "The Militarisation of Cyberspace: Why Less May Be Better," 4th International Conference on Cyber Conflict, 2012, *https://ccdcoe.org/publications/2012proceedings/2_6_Dunn%20Cavelty_TheMilitarisationOfCyberspace.pdf*
6 International and Operational Law Department, *Law of Armed Conflict Deskbook*, The United States Army Judge Advocate General's Legal Center and School, US Library of Congress, 2012, *www.loc.gov/rr/frd/Military_Law/pdf/LOAC-Deskbook-2012.pdf*
7 International Committee of the Red Cross, "What Is International Humanitarian Law?," 31 December 2014, *www.icrc.org/en/document/what-international-humanitarian-law*
8 Farwell, J. P.; R. Rohozinski; "Stuxnet and the Future of Cyber War," *Survival*, January 2011, *https://www.scribd.com/document/57100263/Stuxnet-and-the-Future-of-Cyber-War*
9 Harnad, S.; "Minds, Machines and Turing: The Indistinguishability of Indistinguishables," Cogprints, 2001, *http://cogprints.org/2615/*
10 IBM, "Deep Blue," *www-03.ibm.com/ibm/history/ibm100/us/en/icons/deepblue/*
11 Ferrucci, D., *et al*.; "Rebuilding Watson: An Overview of the DeepQA Project," *AI Magazine*, Fall 2010, *www.aaai.org/Magazine/Watson/watson.php*
12 Sainato, M.; "Stephen Hawking, Elon Musk, and Bill Gates Warn About Artificial Intelligence," *Observer Opinion*, 19 August 2015, *http://observer.com/2015/08/stephen-hawking-elon-musk-and-bill-gates-warn-about-artificial-intelligence/*