AWARENESS IS KEY to Today's Cybersecurity

by Jenny Mangelsdorf

Life is full of surprises. In IT, few know that better than those in cybersecurity. As the world becomes more connected and organizations experience massive increases in infrastructure access points due to innovations like the cloud, mobile devices, the new Internet Protocol (IPv6), and "x" as a service offerings, the ability to rapidly counter threats to an operation continues to challenge even the best technologists.

That's why many stress the importance of awareness. It's an idea moms have touted for millennia — 'be aware of your surroundings'— and something just as relevant to IT. Referred to as "situational awareness," this level of alertness is all about knowing what's happening within your enterprise as well as in the outside world.

"You cannot think about situational awareness strictly within the confines of your own network or enterprise any longer," says Carlos Solari, CSC vice president, Cyber Technology and Services. "The challenge is how to correlate the threat information that's available in the larger picture with the sensor information you have from inside your own network."

This is especially true as new sophisticated threats emerge, like Stuxnet. This malware, which targets industrial equipment, has infected at least 24 of Siemens' industrial customers' systems worldwide[1], including the centrifuges used in Iran's uranium enrichment program. And while this isn't the first case of cyber sabotage — Stuxnet was discovered in mid-2010 — some say it's a game changer because of the amount of resources used for its development and its sophistication.

"Stuxnet has received the attention of industrial manufacturers and power producers worldwide who now realize their operational systems may be more vulnerable than they had thought," says Sam Visner, CSC vice president and lead cyber executive. "Because of malware like Stuxnet, public awareness has increased and people are beginning to realize that having situational awareness is even more important — not just for general IT systems, but also to protect against threats to the IT embedded in and used for critical infrastructure."

Many nations believe these threats are real, as are their consequences. For example, the UK's 2010 National Security Report lists "hostile attacks upon UK cyber space by other states and large-scale cyber crime" as one of the top four risk areas that should be the highest priority for action, taking account both likelihood and impact.[2] Evidence of the UK's cyber emphasis is the fact that even with last year's deep budget cuts, it has committed £650 million over the next four years to cybersecurity "to give Britain a real advantage in cyber resilience."[3]

Increasingly, governments are also viewing the cyber world as a domain unto itself and one that needs protection because if that domain is crippled, it can have far-reaching repercussions.

This view comes from the Stuxnet attacks as well as other cyber events, such as the cyber attacks that flooded Estonian websites in 2007 and the numerous Georgian and Azerbaijani website attacks in 2008.

"In the case of Estonia, cyber was treated absolutely as its own domain," says Visner. "The perpetrator's message was clear, 'Within the cyber domain, you're isolated and within our sphere of influence.'

"It was clear that for a few days what happened in Estonia was not up to the Estonians; it was up to someone else, and whoever it was, was physically invisible, but clearly influential. Situational awareness in this case is about managing what happens to you inside of cyber as its own domain."

As organizations continue to gain first-hand cyber crime experience — the U.S. Department of Defense's systems are probed by unauthorized users more than six million times per day[4] — public and private sectors are increasingly working together to create stronger cybersecurity capabilities. For example, more than 500 participants from the public and private sector, including specialists outside the U.S., have formed a Cyber Security Working Group to create cybersecurity guidelines the U.S. can use as it begins to transform its electric power infrastructure into a Smart Grid infrastructure.[5]

A key challenge, says Visner, is taking this collaboration a step further and sharing threat information. Private and public sectors, as well as nations, are increasingly evaluating potential cybersecurity partnerships, especially as they relate to securing global or continental infrastructures, such as transportation, financial, and energy.

"Effective situational awareness requires data gained through stronger international cooperation and the selective use of intelligence that relates to threats to global infrastructures, supply chains, and the international system," says Visner. "The global cyber environment has grown beyond the control of any single nation. Broader intelligence capabilities related to emerging threats are needed to successfully combat them."

One misconception to which organizations cling is the belief that if their systems are separate from the Internet, they are safe from attack. That complacency further dampens any urgency in developing a strong situational awareness capability.

"Even if you use a separate network, without situational awareness you may not know that someone has gone in, plugged a device into the network, and is communicating to the outside," says Solari. "Physical isolation can be breached readily. So the isolation you think you may have because you have a separate physical network is an assumption; you can take no comfort in that whatsoever."

Stuxnet was reportedly introduced using removable drives, like USB flash drives, and allegedly attacked Siemens' industrial control systems via private networks. Some organizations, however, still operate as if security is about stopping a cyber attack from coming in the door, at the ingress points. They don't pay enough attention to the threat inside and instead focus solely on securing their networks — a view that Solari says has to change.

"The IT industry has miscalculated by its network-centric focus, and continues to do so by its lack of attention on the applications and data, including metadata. These areas still get so very little attention and is why we have the issues we do," Solari says.

To achieve awareness today takes continuous monitoring, says Solari. Before, the focus was on inspecting an organization's systems on some annualized cycle. However, because the cyber landscape changes so rapidly, organizations need to monitor their systems constantly, as well as what's happening in the world outside.

For example, to monitor clients' systems, CSC uses managed security services on a 24x7 basis to provide information about external threats and identify and protect against potential vulnerabilities. However, today's tools need to be stronger, says Solari, to keep pace with the continually increasing amount of threat data and turn it into accurate, timely intelligence.

"The ability to deal with the volume of data, and find the exposures and threats inside of all that data, is one of the most significant challenges facing the world of situational awareness," he says. "That is a big part of the technical challenge, and we are working with our partners to solve that." ■

JENNY MANGELSDORF is a writer for CSC's corporate office.

[1] http://support.automation.siemens.com/WW/llisapi.dll?func=cslib.csinfo&lang=en&objid=43876783&caller=view

[2] http://www.direct.gov.uk/prod_consum_dg/groups/dg_digitalassets/@dg/@en/documents/digitalasset/dg_191639.pdf

[3] http://www.fco.gov.uk/en/news/latest-news/?view=News&id=23074623

[4] http://www.military-information-technology.com/mit-home/261-mit-2010-volume-14-issue-6-july/3142-mission-success-in-cyberspace.html

[5] http://csrc.nist.gov/publications/nistbul/october2010-bulletin.pdf

CSC Secures Systems Globally

Our nearly 2,000 cyber experts serve public and private sector clients worldwide, providing a full range of cyber services — from vulnerability analysis, penetration testing, and data-loss prevention to a full range of managed security services. Our global StrikeForce team responds to cybersecurity incidents and provides cyber forensics training and analysis. We also operate Common Criteria Test Laboratories in the U.S., Europe, and the Far East, and have a worldwide infrastructure of Security Operations Centers.

To learn more, visit www.csc.com/cybersecurity.