Japan its own enemy in push to improve cybersecurity

November 8 2015, byGerry Shih

In this Dec. 18, 2014 file photo, a man walks out from the headquarters of Sony Corp. in Tokyo. Improving cybersecurity practices has emerged as a top national priority for Japan, stung in recent years by embarrassing leaks at Sony Pictures, the national pension fund and its biggest defense contractor, Mitsubishi Heavy Industries, which possibly suffered the theft of submarine and missile designs. (AP Photo/Eugene Hoshiko)

Apart from rogue hackers, criminal organizations or even state-backed

cyberwarfare units, Japan's businesses and government agencies are facing a unique cybersecurity foe: themselves.

Even with the frequency and severity of cyberattacks increasing rapidly worldwide, efforts by the world's third-largest economy to improve its data security are being hobbled by a widespread corporate culture that views security breaches as a loss of face, leading to poor disclosure of incidents or information sharing at critical moments, Japanese experts and government officials say.

Improving cybersecurity practices has emerged as a top national priority for Japan, stung in recent years by embarrassing leaks at Sony Pictures, the national pension fund and its biggest defense contractor, Mitsubishi Heavy Industries, which possibly suffered the theft of submarine and missile designs.

Toshio Nawa, a top Japanese security consultant who is advising the Tokyo 2020 Olympics organizers, said he encountered a telling instance this summer when he was called to investigate a breach at a major Japanese government agency.

Nawa found that five different cybersecurity contractors employed by the agency had discovered the breach, but not one reported or shared their findings.

With evidence from the contractors pooled together, Nawa matched the digital fingerprints to a Mexican group that he believes was responsible for a previous attack on Japanese diplomatic servers. The breach was patched, but Nawa walked away flustered.

"In the U.S., if they find a problem, they have to report," he said. "The Japanese engineer feels he fails his duty if he escalates a report. They feel ashamed."

To be sure, the cybersecurity industry around the world, not just in Japan, frequently echoes the call for greater transparency within and among organizations. The U.S. Senate last month passed the Cybersecurity Information Sharing Act to ease data sharing between private companies and the government for security purposes, although civil liberties advocates warned it posed a threat to privacy.

But the problem may be particularly acute for Japan's private sector behemoths and government ministries. These sprawling bureaucracies are wrapped in a "negative culture that cuts against wanting to communicate quickly," said William H. Saito, the top cybersecurity adviser to Prime Minister Shinzo Abe.

While rank-and-file workers fear reports of security lapses may get them punished, the problem reflects a broad lack of understanding of cybersecurity among the top ranks of Japanese executives, Saito said in an interview on the sidelines of the Cyber3 conference in Okinawa.

"This is Japanese culture where in some situations the upper management doesn't know how to use email and IT integration is voodoo magic," said U.S.-born Saito, also an executive at Palo Alto Networks, a security firm. "The reality is companies either have been hacked or will be hacked. My message is, 'It's not your fault.'"

In 2013, the latest year of available data, the Japanese government network faced an eightfold increase in cyberattacks from two years prior, with attacks spreading into civil infrastructure, as well as the telecommunications and energy sectors.

Against that backdrop, the Abe administration has pinpointed the 2020 Tokyo Olympics as a chance to upgrade Japan's national security capabilities while calling for a more hands-on government role to nudge companies to take cybersecurity seriously.

A Cabinet-level cybersecurity agency in September published a strategy paper that proposed, among other things, extending government-run cybersecurity classes to companies, awarding financial incentives for firms that demonstrate improved security capabilities and requiring companies to fill a chief cybersecurity officer role.

The Cabinet report also highlighted the issue of disclosure, saying "it is essential to relieve (network) operators' psychological burden of possibly losing credit or ruining reputation of their business if providing information to others."

Jim Foster, a former U.S. diplomat and Microsoft Japan executive who heads the Keio International Center for the Internet and Society in Tokyo, said the fast-evolving threat of hacking poses a looming challenge for Japanese industry, which never developed a deep pool of cybersecurity expertise with active exchange of ideas and know-how.

"Japanese companies grew up too big too quick and didn't have to cooperate or rely on outside expertise," he said. "But now there's this new threat unlike anything else and things suddenly get difficult."

But changing habits is hard, said Nawa, the security adviser for the Olympics, who is now holding simulations and educational sessions around the country, where he emphasizes to security engineers—who do not necessarily lack technical chops—the importance of sharing findings and speaking up when they spot a problem.

He said he uses a simple mantra on the training circuit: "What I say is: 'Please remove your pride.'"