UMD researchers formulate cyber protection for supply chains

October 21 2014

The supply chain is ground zero for several recent cyber breaches. Hackers, for example, prey on vendors that have remote access to a larger company's global IT systems, software and networks.

In the 2013 Target breach, the attacker infiltrated a vulnerable link: a refrigeration system supplier connected to the retailer's IT system.

A counter-measure, via a user-ready online portal, has been developed by researchers in the Supply Chain Management Center at the University of Maryland's Robert H. Smith School of Business.

The portal is based on a new management science called "cyber supply chain risk management." It combines conventionally-separate disciplines cybersecurity, enterprise risk management and supply chain management .

Funded by the National Institute of Standards and Technology, the UMD researchers developed the formula, in part, after surveying 200 different-sized companies in various industries.

"We found that, collectively, the cyber supply chain is fragmented and stovepiped, and companies are ill-prepared to sense and respond to risks in real time," said research professor and center co-director Sandor Boyson, who collaborated on the study and portal design with faculty-colleague/center co-director Thomas Corsi, research fellow Hart Rossman and UMD-Smith CIO Holly Mann. "Just half of our subjects

used an executive advisory committee such as a risk board to govern their IT-system risks."

The findings are published as "Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems" in the peer-reviewed industrial engineering journal *Technovation*. http://ter.ps/73f

The researchers leveraged the study into the portal. Companies can log on, cost-free, at http://cyberchain.rhsmith.umd.edu and track developing threats, plus map their IT supply chains and anonymously measure themselves against industry peers and NIST standards.

The benchmarking covers operations and allocating for cyber insurance via separate functions:

- A self-evaluation exercise shows a company's structure for cyber protecting the supply chain. For example, users reply to: "To what degree is your CIO and-or IT shop isolated from, or collaborative with, your supply chain specialists who actually procure the hardware and software for your IT system?"
- A special formula measures the risk levels of each company asset. The Common Vulnerability Scoring System – standard for analyzing software systems – is adapted to analyze the entire range of assets connected to the cyber supply chain.
- Firms can compare corporate disclosures, exposures and vulnerabilities to those of peer companies via an insurance-risk analysis framework provided by The Willis Group. The global insurance broker's database of aggregated SEC-reported cyber attacks—mandated for public companies – supports this tool.

The portal is scalable. About 150 various-sized companies have completed at least one or more of the aforementioned functions. Fifteen of those firms completed all three assessments and represent industries

including high-tech aerospace manufacturing, telecommunication, real estate, and medical and professional services.

"The portal not only helps individual organizations understand their risk and how they can better manage it. By doing so, this bolsters the resilience and security posture of the entire ecosystem of the U.S. economy," said Jon Boyens, senior advisor for information security in NIST's computer security division. "While this ecosystem has evolved to provide a set of highly refined, cost-effective, reusable products and services that support the U.S. economy, it has also increased opportunities for adversaries and made it increasingly difficult for organizations to understand their risks."

The study is entering a fifth phase focused on federal agency-private contractor supply chains. The UMD-Smith researchers subsequently will update the portal and train managers of participating agencies and contractors to efficiently and effectively use the separate functions.

Provided by University of Maryland