SecTor 2015: Make detailed incident reports public, CISOs told

Howard Solomon - October 22, 2015

When there's a serious aircraft incident in the United States, the National Transportation Safety Board investigates and issues an exhaustive public report and recommendations to the aviation industry.

By contrast, details about high-profile data breaches — think Target, Home Depot, Sony — are closely held, or smothered in leaks and speculation, with organizations reluctant to divulge what really happened for fear of lawsuits or damage to their brands.

But the aviation model is what infosec pros should strive for to improve IT security, Trey Ford, a private pilot and global security strategist at incident response firm Rapid7 told the SecTor conference in Toronto on Wednesday.

Trey Ford. ITWC photo by Howard Solomon

Public reporting would spread knowledge, increase public confidence in IT security and improve the infosec profession, he argued.

In the early years of aviation "when a plane crashed… (pilots) worked together to forward the profession. Their failures, their lessons learned weren't kept secret, they were shared."

Similarly infosec pros have to learn to share de-personalized threat and incident information if the IT industry is ever going to get ahead of attackers, he said.

Across the industry analysts and vendors have increasingly been calling for more threat sharing as private attackers and criminal gangs become richer and nation-states bolder in their campaigns.

Some industries, such as financial, are better organized than others. In this country the Harper government has encouraged critical industries to share cyber threat information, with some more ahead than others. Similarly, in the U.S. there are an increasing number of private and public sector information sharing and action centers (ISACs) in critical industries. But that leaves huge numbers of organizations who aren't in critical sectors alone.

Some of that gap may be filled by organizations offering to host threat information sharing platforms.

RELATED ARTICLES

New threat information sharing platform includes data privacy controls

Canadian CSOs need to share more threat information,

say experts

There are worries threat information sharing could lead to lawsuits, although experts say if the information has no personal identifying data it should be OK. On the other hand, wrongly warning about a particular Web site could be actionable.

Ford admits that not all the kinks have been be worked out for the kind of threat information collaboration he'd like to see. That's why he encouraged attendee to at least adopt the VERIS (Vocabulary Event Recording and Incident Sharing) methodology for describing any incident in a repeatable way.

"You'll know what's working and what's not, what incidents you're stopping and what's taking a little longer to get control of. That may be more effective in the short term" than sharing technical information like suspicious IP addresses. "Maybe today we can't share information," he said, "but that doesn't mean you can't prepare to."

Publicly sharing details of attacks is vital, he argues, to meeting threats and sharing what's been learned. Attackers will be able to adapt, he admitted, "but I ask you to consider that every time we force the attacker to work, to buy more exploits to buy more tools, every action raises their visibility, raises their cost and makes it more difficult for them to operate."

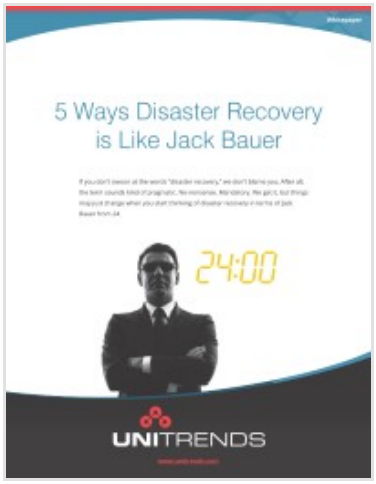
In an interview Ford said CSO and CFOs not already in formal information sharing groups are starting to get together for tentative collaboration. But, he complained "it's all behind closed doors."

–"I think the profession has a lot of room to mature," he said. "A lot of lessons we learn are going to come from sharing mistakes." However, "a lot of people are re-inventing the wheel."

"I think we have the opportunity to make this change," he told the conference, "and even if we can't share (incident) data, I want you to prepare to share it. I want you to think about how you can encode this data so at some point you can partner with data scientists, partner with statisticians to help measure risk and help the

business make informed decisions."

Related Download



Sponsor: **Unitrends**

5 Ways Disaster Recovery is Like Jack Bauer

5 Ways Disaster Recovery is Like Jack Bauer, a fun and informative whitepaper from Unitrends, looks at how to start thinking of disaster recovery in terms of the butt-kicking hero of 24.

Register Now

Privacy, **Security** **data breach**, **security strategies**

About Howard Solomon

Currently a freelance writer, I'm the former editor of ITWorldCanada.com and Computing Canada. An IT journalist since 1997, I've written for several of ITWC's sister publications including ITBusiness.ca and Computer Dealer News. Before that I was a staff reporter at the Calgary Herald and the Brampton (Ont.) Daily Times.