proofpoint®

Anyone can be a VAP

VERY ATTACKED PERSON

Protection starts with people.

Learn how Proofpoint can help you protect your remote workforce against today's biggest cyber threats at www.proofpoint.com.

INDUSTRY SPOTLIGHT

Why a People-Centric Approach to Security Has Become a Necessity

An interview with Bruce Brody, Resident Chief Information Security Officer (CISO), Federal Practice, Proofpoint

For years, cybersecurity experts have said that the weakest link in an agency's cyber defense is not a system but a human – the employee who clicks on a link in an email that introduces malware onto the network. Nonetheless, most organizations continue to think about security strictly as a technology issue.

A technology-centric approach to cybersecurity is essential, but not sufficient. Think about it from the attacker's perspective. What is easier: identifying and exploiting the vulnerability of a network, or tricking a user into clicking on a link opening an attachment? The nation's recent history of data breaches, many of which began with phishing attacks, suggests that agencies need to take a people-centric approach as well.

To learn more about the human dimension of security, GovLoop spoke with cyber experts at Proofpoint, which offers an integrated suite of FedRAMP-authorized cloud-based, people-centric solutions.

The key to people-centric security is to identify those individuals within the organization that are at the highest risk of being targeted. Proofpoint calls those individuals "Very Attacked Persons" (VAPs).

"Malicious actors have become very adept at using org charts, social media and other tools to identify people with desirable network privileges and engineer highly targeted attacks," said Bruce Brody, Resident Chief Information Security Officer (CISO) for Proofpoint's Federal practice. Brody also served as CISO at the Department of Veterans Affairs and the Department of Energy.

A VAP is not necessarily someone high on the org chart. Instead, it might be a lower-level employee whose responsibilities require them to have access to a wide range of network resources. To identify VAPS, Proofpoint developed an Attack Index that reflects the risk of a given threat, or set of threats, to a given individual.

The Attack Index assigns every threat a score of 0-1000, based on three key components:

- Actor type, which considers the criminal's level of sophistication. Does it appear to be a state-sponsored actor or typical small crime actor?
- Targeting type, which looks at the degree of targeting involved with the threat. Is it focused on a particular user, organization or sector, or is it a general-purpose attack with no particular target?
- Threat Type, which addresses the type of malware involved. Is it highly sophisticated or just garden-variety phishing?

In each case, the more sophisticated and targeted the overall threat, the higher the score. The index is based on a massive database of globally observed threats and malware analysis across corporate and consumer email, social media and other platforms.

Once the cyber team has identified their VAPs, they know where to focus their energies. From a technology perspective, that might mean adding security controls around those individuals. From a people perspective, the first step is to train VAPs to recognize phishing attempts and other socially engineered attacks.

The next step is to turn those VAPs into assets for the cyber team. Once an individual is recognizing threats, they can feed that information back to the team, said Brody. "Whereas before, they were one of the weakest links in the chain, we're going to make them one of the stronger links," he said.