Study determines why organizations fight data breaches differently

July 9 2015

In the wake of recent high-profile security breaches at retail stores such as Target and Neiman Marcus, a new study from The University of Texas at Dallas determines why differences exist in the level of information security control resources among organizations.

Since digitalization began, organizations have understood how valuable their information is, said Dr. Huseyin Cavusoglu, the study's lead author and an associate professor of information systems at UT Dallas. More recently, dependency on the Internet has made it difficult for organizations to secure and protect this asset.

Protecting information initially was viewed as a technology-related problem, he said, and was solved by investing in technology-based solutions.

"But over the years, it has become clear that technology-based solutions are not foolproof or sufficient," said Cavusoglu, a security management researcher in the Naveen Jindal School of Management. "In light of this observation, we were interested in identifying a coherent set of organizational resources for information security controls that organizations should invest in to protect their information assets."

For the study, published in the June edition of *Information & Management*, the researchers surveyed senior and midlevel IT managers about information security practices and operations in their organizations. The analysis was based on responses from 241

organizations of varying industries and size.

The study found that organizations should invest in three distinct resources to better protect their information: security technologies, qualified information security personnel and security awareness of organizational users.

- Security technologies—Preventive and detective technical solutions to address vulnerabilities within IT structure in which critical information assets reside.
- Qualified information security personnel—Professional staff members who can define, execute and maintain the information security program of the organization.
- Security awareness of organizational users—Employees interacting with the information assets of an organization are fully informed, well-trained and aware of security-related issues and assume security as their everyday responsibility.

Because organizations perceive security risks differently, they invest in information security controls at different levels. The researchers also examined the drivers of these investments.

"We found that coercive pressures—stemming from business partners or industry and government regulations—and normative pressures—rooted in information security practices of partners, as well as the firm's exposure to security best practices through professional organizations, trade shows, conferences and security publications—largely impact the firms' investments in security control resources," Cavusoglu said.

Cavusoglu said the findings have several implications for public policymakers, security vendors and individual organizations.

The study advises public policymakers to continue to support

government-sponsored security groups and to work closely with professional security associations and councils to design regulatory rules on security and promote best security practices.

Cavusoglu said the study shows that information security is not solely about technology and that to ward off security threats, organizations should invest in both technology-based solutions and knowledge-based assets.

The study advises organizations to consider information security as an issue that can be managed with a combined portfolio of control mechanisms consisting of information security technologies, qualified information security personnel and security awareness of organizational users.

"Employees should understand that they play an important role in safeguarding the information assets of their organizations and keep themselves up-to-date with the contemporary security threats," Cavusoglu said. "Businesses should pay close attention to security education, which can change employees from being the weakest link in security to the biggest safeguard for security."

More information: *Information & Management*, www.sciencedirect.com/science/ … ii/S0378720614001499

Provided by University of Texas at Dallas