RSA Conference 2018

Peer2Peer

Nudging: Can We Use Behavioral Economics to Drive Better Security?

P2P2-T10: Nudging: Can We Use Behavioral Economics to Drive Better Security?

Michael Waters, Director of Cyber Security, Control Risks

Cyber security has been described as an attempt to solve a non-technical problem through technical means. The non-technical problem is human behavior. People are often considered the weakest link in the security problem whether it is clicking on suspicious emails, choosing bad passwords, sharing credentials or failing to apply needed software upgrades – humans can find a way around technical controls. As a result, all the time and money invested in technical solutions can be undercut by a single individual doing something the security community does not want them to do.

The field of Behavioral Economics (BE) is the study and practice of affecting human decision making. At its core it recognizes that people do not always make *rational* decisions, but they very often make *predictable* decisions. If we can use BE to understand and guide the decision-making process we may be able to guide people to make decisions that enhance, rather than undermine, cyber security.

The RSA 2018 Peer2Peer session *Nudging: Can We Use Behavioral Economics to Drive Better Security?* hosted an active group of about thirty Information Technology (IT) professionals to discuss the topic of using BE to enhance security. Participants had a variety of experience levels and organizations represented including health care, finance, consulting and manufacturing. Several attendees had used BE successfully in at least one environment. Many were quite unfamiliar with the topic.

One of the key concepts that appeared to be most commonly and successfully used was using positive reinforcement statements for desired behavior. For instance “95% of all employees have already completed their annual security refresher” was more effective at getting people to comply than the negative version like “you are part of the 5% who has not…” Similarly, richly worded emails thanking staff for reporting suspected phishing emails had a very positive reinforcing effect versus bland generic responses.

While everyone held that at some level there had to be a ‘stick’ if the ‘carrot’ was not effective it was clear that positive reinforcement was preferred.

Gamification – where people are rewarded for completing security tasks or security training with badges or ranks – has been successfully used by several of the participants. Employees can become “InfoSec Advocates” by completing information security training over and above the minimum annual required training. This sort of personal branding was effective and long-lasting. Statistically, InfoSec Advocates were involved in fewer security incidents and tended to have a positive effect on their coworkers and peers as well.

This last point was reinforced by another part of the discussion: who should push training and awareness efforts? It was broadly agreed that while getting executive buy-in is important, a request from a line manager in close proximity in the organization chart was far more effective than from a distant C-level executive. A request from someone directly linked was far more useful than from someone far up the organization structure.

This same concept applied to decentralized decision making. Pushing approval decision making down to people close to the situation (whether it was granting access or approving software installation) resulted in decisions that more appropriately supported the business and security at the same time.

Some key concepts from this session include:

- Positive reinforcement is more effective than negative
- Gamification, badging, and personal branding can help people identify themselves as part of the security solution
- Requests for security compliance are more effective when they come from someone know to the user

Additional recommended resources:

- *Predictably Irrational* by Dan Arielly
- *Nudge* by Richard Thales (winner of the Nobel Memorial prize for Economics)
- The www.behavioraleconomics.com website