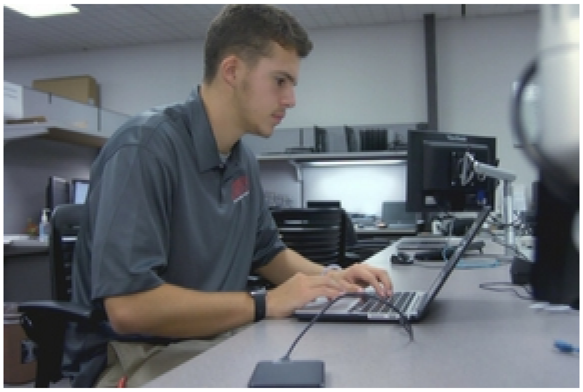
2-28-2018

Is Your Organization Cyber-Mindful?

Thomas D. Skill

Is Your Organization Cyber-Mindful™?

udayton.edu/blogs/cybersecurity/2018/2018-02-28-social_engineering_threats_skill.php



Wednesday February 28, 2018

By Thomas Skill, Ph.D., Associate Provost and CIO

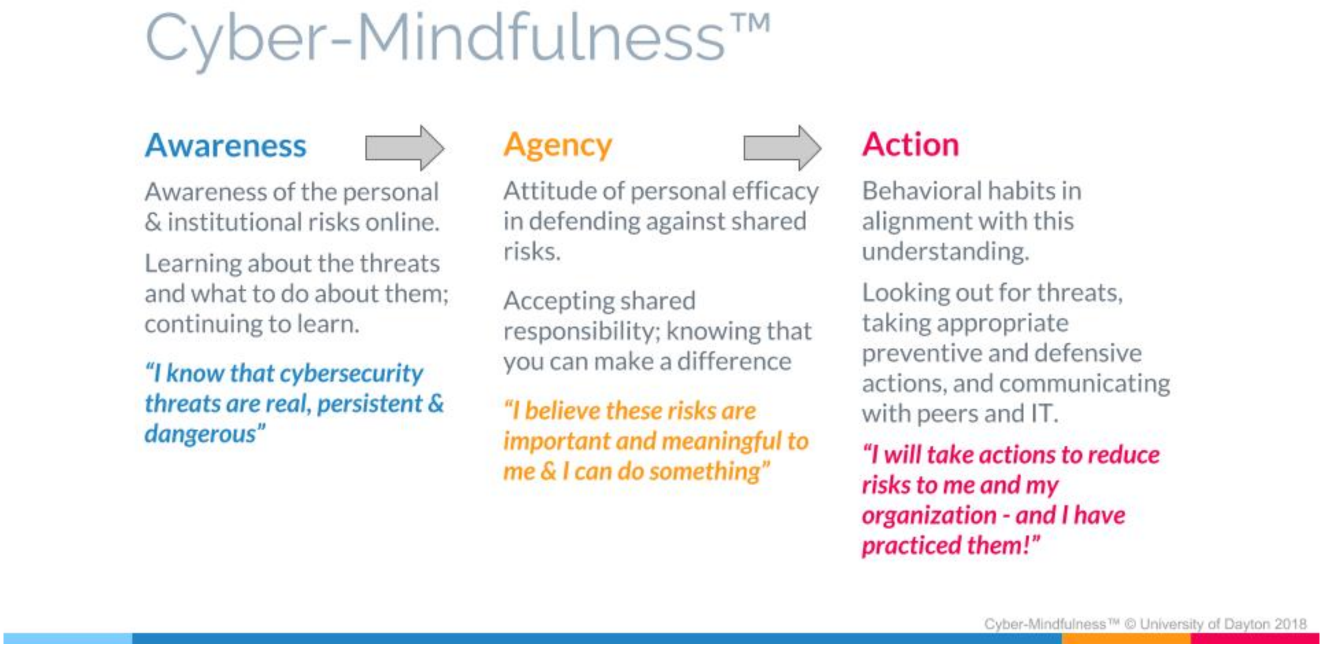
Let's face it, cybersecurity isn't going to get any easier in 2018. As long as there is a financial or geo-political incentive, the threats will keep coming and the level of exploit sophistication will keep rising. Winning this battle truly requires a change in our approach. If you have been scanning the popular media or reading our professional publications, you'll notice that the attack vectors are shifting from technical exploits to human vulnerabilities. Like most businesses, even the bad guys are striving to be more efficient, and it is very cost-effective to socially-engineer a way into your system rather than deploying a technical exploit. Thus, in addition to maintaining our technical vigilance, we now must strengthen our cybersecurity awareness training just to keep up with the bad guys. Cybersecurity "human factors" is an area that many organizations are not fully prepared to do effectively.

This new reality demands that we develop and deliver more powerful cybersecurity education programs that are engaging, sustainable and continuous. Toward this goal, our team at The University of Dayton Center for Cybersecurity & Data Intelligence has pioneered an engagement model called "Cyber-Mindfulness™." This approach emphasizes three critical elements that significantly enhances the responsiveness of our stakeholders: *Awareness, Agency* and *Action*.

Most cybersecurity training programs begin and end with *awareness*. It goes something like this: Information is provided about personal and professional cyber risks, a few horror stories are shared regarding mistakes people have made and the session concludes with a list of things to avoid. In some cases, attendees complete a quiz and the results are logged for HR tracking purposes. This "one and done" model is great for avoiding liability when a breach happens, but the evidence suggests that it is generally ineffective in helping organizations avoid most social engineering exploits.

Our Cyber-Mindfulness™ model engages stakeholders in continuous learning about exploits and threats. A successful "*awareness*" phase results in users being able to affirm that *"I know cybersecurity threats are real, persistent and dangerous."* The next and perhaps most critical stage is "*agency*." This phase seeks to establish a sense of ownership and shared responsibility for cybersecurity by our users. Successful results at this step might be characterized as *"I believe these risks are important and meaningful to me and I can do something."*

Finally, we must move our users from *awareness* and *agency* to *action*. It is not unusual to discover that many users feel extremely inadequate in responding to cyber threats. Identifying "doable actions" that users can practice and achieve on their own are critical to a successful cybersecurity program. Cyber-Mindfulness™ can best be expressed at this phase with the *statement "I will take actions to reduce risks to me and my organization – and I have practiced them!"*



Cyber-Mindfulness™

Awareness

Awareness of the personal & institutional risks online.

Learning about the threats and what to do about them; continuing to learn.

"I know that cybersecurity threats are real, persistent & dangerous"

Agency

Attitude of personal efficacy in defending against shared risks.

Accepting shared responsibility; knowing that you can make a difference

"I believe these risks are important and meaningful to me & I can do something"

Action

Behavioral habits in alignment with this understanding.

Looking out for threats, taking appropriate preventive and defensive actions, and communicating with peers and IT.

"I will take actions to reduce risks to me and my organization - and I have practiced them!"

Cyber-Mindfulness™ © University of Dayton 2018

Translating the concepts of Cyber-Mindfulness™ into effective engagement tactics requires that we approach cybersecurity as a marketing communications challenge. With that in mind, we must build and sustain a trusted relationship with our user communities. Here are six engagement strategies for establishing a *Cyber-Mindful*™ user community:

1. Invite users into the cybersecurity educational program with friendly messaging – absence of IT jargon and the "arrogance of expertise."
2. Appeal to both personal and work-related cybersecurity needs. Helping users better secure their personal information assets will strengthen trust.

3. Stop “shaming and blaming” users for mistakes – instead, recognize and reward all efforts by users to engage with IT around security issues.
4. Share frequent communications with your stakeholders that blends serious and humorous information on good practices, effective behaviors, and emerging threats. Offering games and prizes are great ways to keep folks thinking about cybersecurity.
5. Phish your stakeholders at least monthly – but not as a “gotcha” program. Frame this activity as our exercise for getting and staying in shape so that we can beat the bad guys. Also, be sure to report back to the community on what the “tells” were and how your team is performing.
6. Train your IT staff on how to be “user friendly” with your stakeholders. Welcoming “false positives” and encouraging users to engage early and often with your IT service team is critical to long term success.

Cyber-Mindfulness™ seeks to build awareness, shape attitudes and impact behaviors in significant and measurable ways. Empowering users with useful information, a sense of shared responsibility and frequent opportunities to practice their cyber-defense skills will greatly assist organizations in shifting the role of users from victim to early alert agent. The goal is not to make our stakeholders into cybersecurity experts but rather to create a culture of shared responsibility around the protection of our information assets – and it all begins with Cyber-Mindfulness™.

For more information on our work, please visit our site at http://go.udayton.edu/cybermindful

Work originally published in Tech First Magazine's January 2018 Edition.