THE CENTER FOR LEADERSHIP STUDIES®

THE GLOBAL HOME OF SITUATIONAL LEADERSHIP®

SITUATIONAL LEADERSHIP®

CREATING A CULTURE OF CYBER RISK AWARENESS

Major General (Retired) Brett Williams and Dr. Sam Shriver

THE CENTER FOR LEADERSHIP STUDIES®
THE GLOBAL HOME OF SITUATIONAL LEADERSHIP®

Situational Leadership®

Creating a Culture of Cyber Risk Awareness

By: Major General (Retired) Brett Williams and Dr. Sam Shriver

Change (viewed through the lens of Situational Leadership®) can have a tendency to look very much like *regression*. In that regard (and in the context of Organizational Behavior), when you change, you *disrupt*. When you change, you ask people that have developed an acceptable cadence for the manner in which they perform their duties and contribute to the cause to start doing something new or stop doing something that, over time, has become some manner of personal habit.

The imperative to change is especially prominent as companies deal with the real and serious business risks related to cybersecurity. The first step required in most organizations (regardless of size) is to cultivate a culture where every employee understands that managing cyber risk is an essential component of his or her job. Any enterprise-wide change initiative, particularly a culture change, succeeds or fails based on how well the most visible and influential leaders in the organization establish the priority, set the tone and (at least initially) adopt a leadership style characterized more by strategic and tactical guidance and support than by collaboration or empowerment.

Creating a culture of cyber risk awareness begins with leadership efforts in these three areas:

- Cybersecurity training
- Accountability and management of cyber risk
- Adoption of cybersecurity counter measures

Training: The primary objective of cybersecurity training is to create a shared sense of understanding, awareness and appreciation for the role users play in creating and sustaining a secure network environment. The average employee must internalize the fact that their seemingly routine actions can create significant vulnerabilities due to the sophisticated methods attackers

use today. Establishing this shared sense of responsibility is not an easy task. As is the case with any training that matters, key leaders and managers throughout the organization must be the drivers of training transfer. Driving to success starts with those leaders personally establishing post-training expectations for behavior change with each employee *before* the formal training starts.

As for the training itself, all aspects of contemporary design must be considered. The training experience must be both relevant and engaging with attention placed on situations and scenarios with which employees will both recognize and identify. Key leaders should attend training as active members of multilevel employee groups as a means of reinforcing the priority of the overall initiative.

Accountability: Once a company has implemented and validated that they have an effective cybersecurity awareness training program, key leaders must be willing to hold themselves and others accountable. Just as in all other aspects of their work, employees must understand their jobs may be at risk if their actions on the network put the company at risk. Expectations should be reflected in employee agreements that clearly state the company takes information security seriously and there will be consequences for generating unnecessary risk to the company. A well-documented certification process for operating on the company network must be established and effectively communicated if employees are to be held accountable.

Key leaders should also remain acutely aware of the fact that accountability has a positive side as well. Employees should be encouraged to report suspicious emails, hostile websites or gaps in company security policy. Leaders should find creative ways to reward people who are taking cybersecurity seriously and making positive contributions.

Counter Measures: The third area of responsibility is to implement specific cybersecurity counter measures that feature key leaders taking active roles in execution. The concept is for the key leaders to be the ones who introduce a new security habit or protocol that many might initially resist but, when implemented, has a measurable effect on increasing the company's security. Consider Multifactor Authentication (MFA) as an example.

We know the most dangerous cyberattacks start with the hacker getting access to the user name and password of an authorized user. Once they have that digital ID, the hacker can move around the company network masquerading as someone who belongs there. MFA provides perhaps the biggest "bang for the buck" in terms of reducing this threat. A user still starts the process by entering their user name and password, but they must also enter a separate numeric code that is

provided to their cell phone or through other means such as an authenticator app. After entering that code, the user is granted access. This extra level of security has been proven to be highly effective since the chances that the hacker will have access to a stolen set of credentials, as well as the user's personal phone, is remote.

The challenge with implementing counter measures like MFA is that, in the absence of proper positioning, it can be perceived as a "time-consuming, inconvenient additional step that doesn't really matter." However, if leaders approach the introduction of this counter measure in a directive manner that also emphasizes explanation of benefits and clarity of purpose, users quickly realize that what they are being asked to do really is not much of an inconvenience, and, in the end, is actually well worth the effort. Success is a function of key leaders being directly involved in selecting the solution, then "owning it" and setting the tone for enterprise-wide adoption and compliance primarily through their personal example.

As we bring this brief overview to a close, we wouldn't be surprised in the least if the little voice inside your head is screaming something like:

"Well, this is all just 'common sense!'"

We also doubt you would be surprised to know that both of us wholeheartedly agree. In fact, when Dr. Hersey introduced Situational Leadership® way back in the early 1970s, he himself described it as "organized common sense." But the challenge we continue to face on an ever-recurring basis with change initiatives of significance is that *common sense* is far removed from *common practice*. And, in that regard, if nothing else, the very real threats imposed by the pervasive reach of all that is "cyber" provides leaders with true opportunities to lead!

Biography:

Major General (Retired) Brett Williams is the President of Operations, Training and Security at IronNet Cybersecurity. Brett is an accomplished keynote speaker and consultant to corporate boards on cyber risk oversight. In his last active duty position, he served as the Director of Operations at U.S. Cyber Command.

Dr. Sam Shriver is the Executive Vice President of Research and Development at The Center for Leadership Studies (CLS). In that capacity, he serves as a senior thought leader, subject matter expert and author. Sam has over 35 years of direct experience with Situational Leadership®,