RSA Conference 2016

Learning Labs

LAB3-W07 – Transforming Your Security Culture: From Awareness to Practice to Maturity

Post-Conference Summary

Lance Hayden

Lance Spitzner

Table of Contents

Introduction

Thanks for attending!

Both of us are very grateful and honored that you chose to spend some of your valuable time attending our Learning Lab, *Transforming Your Security Culture*, at RSA Conference 2016. There were so many great presentations and tracks, and your participation in our Lab means a lot to us. We hope you found it as engaging and educational as we did, and that it gave you everything you hoped it would.

This summary is designed to recap the discussions and topics that made up our time together in the Learning Lab. The issues of security training, awareness, and culture are complex and varied, and two hours was barely enough time to scratch the surface. That being said, we both felt that many people both contributed and took away key insights that will help them improve and mature their security awareness programs and their overall enterprise security posture. That includes both of us, and we couldn't have done any of it without the enthusiastic and insightful participation of each and every Lab participant.

Everyone should be proud of the work we did at the conference, and we hope that the rest of your RSA Conference experience over the week was as rewarding for you as collaborating on this Lab was for us. Until next year! Thank you again.

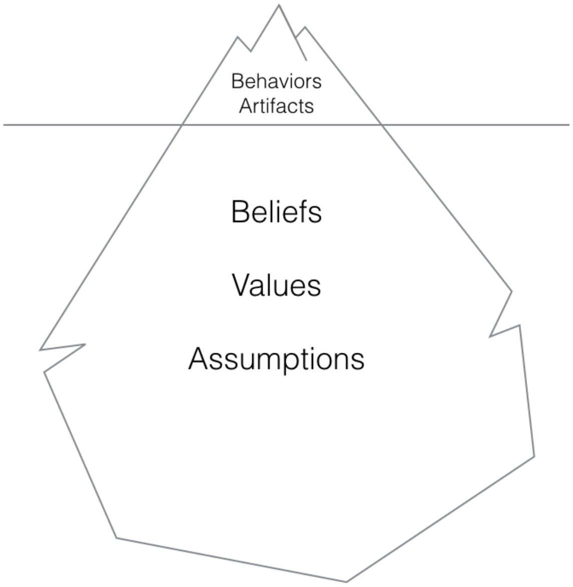
Lance Hayden and Lance Spitzner

Lab Summary

Key Takeaways

ORGANIZATIONAL CULTURE IS AN “ICEBERG” PRINCIPLE

Culture is a combination of what can be observed “above the surface” of organizational activity (visible behaviors, documents, dress codes, conversational styles, etc.), and those things that are driving the visible traits more or less out of our immediate attention. The bulk of the cultural iceberg are the beliefs, values, and priorities that people in the organization feel strongly about.



SECURITY CULTURE IS A COMBINATION OF BEHAVIORS AND BELIEFS

Security culture is a mix of behaviors and beliefs. People can debate which are most important (Lance and Lance often do), but the reality is that a strong security culture will address both the ways people behave and the things they believe. Security awareness programs cannot afford to neglect either in their efforts. Whether you are trying to influence “below the surface” cultural values by reinforcing good behaviors and providing effective engagement and training, or whether you are trying to change “above the surface” behavior by getting people to think differently about the problem, the results are the same. Security gets better, people feel more empowered, and the organization wins.

SECURITY AWARENESS IS HIGHLY DEPENDENT ON STRATEGY AND COMMUNICATION

People-centric security focuses, as you might imagine, on the "people" side of the people-process-technology security triad. While technology has done a lot for security, recent history is filled with powerful reminders that technology alone cannot solve our information security challenges. But organizations looking to take advantage of their human capital, their people, must deploy different tools and skills than technologists and engineers do. People-centric security relies more on skills and aptitudes for strategy and communication than for programming and administration of technology. And it is often these very skills that are lacking in security teams, which presents a profound opportunity for innovative security.

SUCCESSFUL SECURITY AWARENESS PROGRAMS OPERATE ON PRINCIPLES OF ENGAGEMENT

The most successful security programs incorporate principles of engagement in their training, awareness, and culture initiatives. This includes such innovations such as gamification and the development of champion programs to encourage those outside of information security to get more involved. When properly managed, engagement programs can exponentially increase the reach and power of the security awareness team, a necessary outcome in an environment of resource and budget constraints.

Lessons Learned

CULTURES CAN COMPETE

One of the reasons that security failures take place has little to do with technical vulnerabilities and everything to do with the fact that different organizational cultures have different priorities and values. For instance, if a security program focuses exclusively on control and standardization, seeking to lock everything down very tightly, the program may find itself in conflict with other parts of the organization for whom such measures makes it difficult to run the business. In these scenarios, conflicts may result in risk as different groups take different approaches to security, argue and compete with one another, or even neglect security completely as the security team is viewed only as "the party of 'no'…"

The best way to avoid security culture conflicts is to measure and assess the types of security cultures in place within an organization, and then to seek to deconflict problems and competition before they become security risks. One method for measuring and assessing security culture is the "Competing Security Cultures Framework" created by Lance Hayden in his book *People-Centric Security*. The CSCF allows organizations to measure and "map" the shapes of their security cultures in order to identify problems and define transformation strategies.

SECURITY AWARENESS PROGRAMS CONTINUE TO FACE CHALLENGES AND TO IMPROVE THEIR EFFORTS

Each year, the SANS Securing the Human program conducts a large survey of the security training and awareness community. This year's survey had the largest response rate yet, and revealed many insights into the state of the security awareness community. While we only reviewed the draft survey during the Learning Lab, the final survey results should be available by the time you read this summary. We encourage you to visit https://securingthehuman.sans.org/ and download a copy to dive into these fascinating results.

LEADING STRATEGIC AND CULTURAL CHANGE IS A LEARNED SKILL

There are many researchers and business leaders outside of security who have explored how to effectively drive change and cultural transformation in their organizations. Lance Spitzner shared one of his favorites, John Kotter, who has written extensively on the subject, and discussed companies that have put these techniques to productive use in their own security awareness programs. Kotter's work, along with other resources, can be found below.

Key Feedback

THE SECURITY CULTURE APP

During the Lab, Lance Hayden solicited feedback on BRG's cultural measurement app. The app, a mobile web site, is meant to provide a short, somewhat gamified, quiz that will give initial insights into where the organization's security culture fits in regards to the CSCF model discussed above. The feedback gained on the app was extremely frank and valuable, and we appreciate everyone's input. Your comments have gone directly into improving the content and usability of the app as it approaches public release.

Further Resources

You can find many resources for your security awareness campaign, including the Annual Security Awareness Report, at the Securing the Human website - https://securingthehuman.sans.org/

Lance Hayden's book *People-Centric Security* is available from Amazon, Barnes & Noble, and your local bookstore. You can download the first chapter, as well as security culture resources released under Creative Commons, at Lance's website – http://lancehayden.net/culture

You might want to check out some of the books we talked about during the Lab:

Leading Change by John P. Kotter

Organizational Culture and Leadership by Edgar H. Schein

Managing the Unexpected by Karl E. Weick and Kathleen M. Sutcliffe