Information Security & the Business: Changing the Conversation

James J. Cusick, PMP
Chief Security Officer & Director IT Operations
Wolters Kluwer, CT Corporation, New York, NY
j.cusick@computer.org

Introduction

A roundtable discussion focusing on the relationship between security objectives and business support for those objectives was held as part of the Spring 2016 Security Leaders' Summit [1] organized by Executive Alliance. This technical note documents the planned scope of the discussion and the outcome in terms of key points agreed to by the participants. The group was made up of one dozen seasoned security Executives, CISOs, managers, and engineers. The participants represented financial institutions, defense contractors, security solution vendors, information services providers, and more.

Roundtable Topic Defined

Conversations with business stakeholders typically focus on risks and rewards. But often, there are disconnects in terms of communication between information security leaders and business units on the amount of risk and the perceived rewards. In engaging with the business units, security organizations often face the dilemma of putting together content that is relevant to the business units for their decision making and but also provides insight into their accountability and impacts [2].

In this roundtable a discussion with industry peers was intended to focus on several core questions:

1. When engaging with the business units, what is being done by your security organization in advance to prepare for the conversations? (i.e., Understanding their goals and priorities, their top customers, their stake in delivering revenue to the company, etc.)

2. From an experience standpoint, typically where do conversations bog down with the business units and why?

3. From an organization perspective, how is your team maturing their conversations with the business units? How did you get there?

4. How do you know you are successful in engaging with the business units in terms of them understanding their role, accountability and impacts?

Additional Discussion Questions

In addition to the core questions above the author develop several further points of discussion to pursue as follows.

1. The reason the author was interested in leading this topic was that three years ago I was asked to build out our security program. This year I am expanding this to two additional business units within our division. At each step we have needed to incrementally justify investments in staffing and tools to meet the program objectives. It is often a case of 2 steps forward and 1 step backward in getting funding even if mindshare is there. I often find that it is through customer requirements that we finally decide to invest more in security. What makes you interested in this topic? How can we do better?

2. What is working well in getting business stakeholders to support security investments? What are the main business drivers to support advances in security? How do regulatory requirements play a role? Risk reduction? Countering threats?

3. What are the typical sand traps in these discussions? What are the barriers? From an experience standpoint, typically, where do conversations bog down with the business units and why?

4. Are there certain areas that tend to be more acceptable investment areas for the business? For example, security tools, sales support, vendor assessments?

5. What are the key themes from this discussion to share with others?

Roundtable Discussion Summary: Major Themes to Apply

Over the course of approximately 90 minutes the group discussed the above topics in some depth. Nearly all participants had a point of view to share as well as specific experiences and practices from their companies. The discussion was wide ranging and in most cases interlocking, that is, the experts often agreed with each other's points even if they came from a different industry or experience base. What emerged from the discussion were a core set of 8 concept areas or themes which we documented and shared with the broader conference gathering. These themes are provided below with some explanations from our discussions.

1. **Culture Matters**: The leadership of an organization sets its tone and culture. If the leadership makes a priority of security so will the overall organization. If instead the leadership does not take an active role or plays lip service to security people will pick up on that and act accordingly. The action here is to explicitly move the risk up to senior management so they can embody security awareness in their thinking, communications, and decisions. IT is really only the custodian of security. Security is in fact the responsibility of the leadership and each functional area in the company. Moving awareness and risk ownership upwards can be done through reviews of security plans and risks as well as a formal acceptance of risk (RA) process. It is also important to factor in the reality that risks can vary across the business. Thus, while pushing the risk upward the CISO should be sensitive to the localized needs within the business where security needs may vary

calling for an adaptive security framework per business area. This adds complexity to security operations but this customizability also builds stakeholder buy-in.

2. **Be the Department of Yes**: All too often security officers are seen as a veto on progress and speed to market. Sometimes CISOs are dubbed "Dr. No" as they only reject implementation requests on the first run. Instead, it is critical to turn the security function into the "Department of Yes". This means anticipating the needs of the business and building a ramp through the security compliance requirements to better enable success for the business. This creates a virtuous cycle as the security team pushes business efforts forwards and the business sees the value add. In turn the business returns to the security team ever earlier to get up front guidance and consultation to ensure continued speedy successful changes.
3. **Pre-Enlist Stakeholders**: As with many efforts it is always advisable to work with stakeholders in advance to help them understand the value proposition of a given program or investment proposal. This can be done through one-on-one interactions over the phone, via email, or face to face. By selling each key stakeholder up front and defusing any concerns or addressing gaps or requirements they may see the program will proceed with less friction. One way to approach this is to understand the business strategy and it's supporting technical strategy. From there the security strategy should dovetail with the goals of the business and the tactics of engineering. Once the full group comes together people will already be on the same page and ready to provide support.
4. **Early & Continuous Engagement of Business**: Our security experts emphasized that a significant challenge remains in getting engaged with the business early and staying engaged. It is often the case that security requirements and the security team are brought in late on projects. When this happens delays can occur forcing rework and refits to the project to meet security compliance requirements. One complicating factor is that IT traditionally does not make it easy for the business to understand technology requirements or how to engage with IT and security for maximum effect. Some participants of the roundtable explained that they actually embed security personnel in the business units to combat this issue. Such embedded experts can more effectively champion projects with the central security staff than can purely business knowledgeable staff.
5. **Leverage the Organization as a Whole**: It is often the case that within large organizations the left hand does not know what the right hand is doing. This is due to such causes as specialization, organizational separation, scale, geographic separation, and financial alignment. However, what makes the most sense is to develop a global security function and tie each business unit effort into that global function (even loosely). This improves standardization, sharing of best practices, reduced redundancy, improved reuse, and realization of economies of scale. In fact the author is currently working on building out an existing security program to cover multiple business units and simultaneously coordinating with the company's global security team. Such approaches are key to responding in a robust fashion to the ever increasing complexity of the security landscape. In our discussion we also focused on the need to leverage the non-security experts in the organization. It is important that all personnel are engaged in security awareness and practices.
6. **Define Security Responsibilities (RACI)**: With all the competing demands placed on the business it is important to be clear about the roles and responsibilities people have around security. Our

experts urged the definition of these responsibilities in a very clear manner. A classical means of doing this is the RACI (Responsible, Accountable, Consulted, and Informed) matrix often developed as part of projects or process definitions [3]. Application of this technique can help clarify for everyone involved what is expected of them in the security process.

7. **Emphasize Continuous Training**: It is often said that the majority of security breaches are due to the weakest link in the system – the human being. Thus training is extremely important. Simple awareness around not opening an unwanted or unexpected link in an email are vital to security. Going further, these awareness programs need to be repeated and there needs to be continuous training to remind people through repetition both around policies in place but also best practices on how to respond to potential threats. In some companies represented in our discussion there were defined penalty ladders for employees not following these procedures. In some companies security teams actually test employees by sending suspicious emails to see how many will fall for the bait.
8. **The Business wants to make Money – Enable It To Do So**: In the final analysis and even from the very first principle the business is interested in revenue growth, profitability, and providing customer satisfaction to attain these two measures. Thus it is critical to always keep in mind that the business as a whole is interested in making money and the security executive and their team needs to do whatever is possible to enable this. An example of this is in anticipating customer security requirements and building infrastructure to meet these needs in advance so as to not introduce drag on the business. Additionally, security can be a sales advantage if properly built into a company's product line. This can be emphasized to business leaders especially in product management or sales. Furthermore, it is positive to always pitch the ROI for he needed technology or capability in relation to the business growth and not simply as a new expense. In some cases the business may appear to be pennywise and pound foolish as they are trying to optimize bottom line results. On the flip side technology teams sometimes acquire tools which end up as shelf-ware. Avoiding this adds credibility to the next request. Conquering this collective push requires the CISO to be able to talk in business terms not just technical terms.

Conclusions

The roundtable provided for a lively discussion of this topic. Marshalling business support for security is difficult in most companies and will most likely remain to have its challenges. This is especially true as most business leaders still view security as a default option that should come with their IT environment. Unfortunately this is not the case. Unless security is planned for and designed in to environments, software, and operations including staff training risks will always remain. By following some of the expert wisdom documented here it is hoped that it will be easier for the reader to map out a plan to attain the security program support and funding they require.

Acknowledgements

The author is indebted to the Executive Alliance organization for hosting the conference and inviting the author to participate. In particular the author wishes to thank Mary Lou Heastings the CEO of Executive Alliance for her support. In addition, this technical note would not have been possible to create without the input of the members of the roundtable.

References

[1] **Security Leaders' Summit**, Executive Alliance, New York, NY, April 14, 2016, http://itsecurityleaders.com/security-leaders-summit-2016-spring/.

[2] Cusick, J., et. al., "*Who is Responsible for Information Security? IT or Business or Both*", **Premier CIO Forum**, Society of Information Management, At New Brunswick, NJ, October 2014.

[3] Meredith, Jack R., Mantel Jr. Samuel J., **Project Management: A Managerial Approach**, 8th Edition, Wiley; August 23, 2011.