THE STATE OF RISK-BASED SECURITY MANAGEMENT

COMMUNICATION, COLLABORATION AND CULTURE
US & UK
2013

Ponemon Institute LLC
RESEARCH REPORT
CHAPTER 6: COMMUNICATION, COLLABORATION AND CULTURE IN A RISK-BASED SECURITY MANAGEMENT ORGANIZATION

In Chapter 3 of this study conducted by Ponemon Institute, 81 percent of respondents said that their organization’s commitment to risk-based security management was significant or very significant. In this chapter, we dig deeper into the disconnect between an organization’s commitments to risk-based security management and its ability to develop the collaboration, communication styles and culture necessary to make risk-based security programs effective across the organization.

COLLABORATION EFFECTIVENESS

The key ingredient in the creation of an organizational culture that is security-aware is collaboration. Higher levels of collaboration ensure that security is not isolated from other areas of company operations and helps avoid information silos.

When asked to rate the level of security and risk management collaboration in their organizations, just 13 percent in the U.S. and 14 percent in the U.K. said it was ‘excellent.’ The majority of respondents (50 percent in the U.S. and 44 percent in the U.K.) said collaboration was adequate but can be improved, and a significant number (41 percent in the U.S. and 38 percent in the U.K.) rated collaboration as poor or nonexistent.

FIGURES 6-1A/B. What one statement best describes how security and risk management functions within your organization work together to support business objectives?

*This choice was not available in 2012
Although company cultures vary significantly, there are common barriers that impact collaboration. The most significant barrier in both the U.S. and U.K. is the lack of skilled or experienced personnel, followed closely by insufficient resources or budget (Figure 6-2A and 6-2B). These findings are not surprising, since resource limitations often mean that security resources are stretched very thin.

Based on these survey responses, it’s not possible to assess whether the skill gap is on the technical side or on the ‘soft skills’ side. However, given the deep technical background of many IT security professionals, it’s probably both.

**FIGURE 6-2A.** What do you see as the most significant barriers to achieving effective risk-based security management activities within your organization today? Please select your top two choices.

- Lack of skilled or expert personnel
- Insufficient resources or budget
- Lack of business’s understanding of the role and contribution of information security*
- Insufficient risk assessment enforcement
- Lack or leadership
- Lack of C-level support or buy-in
- Complexity of compliance and regulatory requirements
- Lack of effective security technology solutions
- Other

*This choice was not available in 2012
Lack of skilled personnel is a very significant problem for almost every organization. Studies conducted by the Ponemon Institute show that demand for skilled security professionals is four times greater than supply. Contributing to this problem, security engineers are expected to be generalists across many evolving, complex security disciplines. Successful cyber attackers, though, frequently specialize in a specific area.

Security skills take significant time and effort to develop, and it takes time and budget to find and hire security experts. As a result, the scarcity of skilled security professionals has become a systemic problem for most organizations. Effective information security professionals also need to develop business and communication skills, further compounding this problem.

On the bright side, both U.K. and U.S. figures indicate that lack of leadership is less of a barrier to effective risk-based security than it was in 2012. This was particularly true in the U.S.—2013 figures showed nearly a 29 percent gain in this area.
PROACTIVE COMMUNICATION OF SECURITY RISKS

The lack of proactive security posture communication that can be understood by nontechnical executives is a significant challenge for a majority of security professionals. In the U.S., 64 percent of respondents (and 60 percent in the U.K.) admit they either do not communicate security risks to senior executives or do so only when a serious risk is revealed (Figure 6-3).

The chain of communication to the senior executive team is definitely broken. Eighty-five percent of U.S. respondents and 89 percent of U.K. respondents don’t meet with senior executives routinely about cybersecurity risks. Obviously, the majority of security professionals are not able to effectively articulate the security risk or demonstrate clearly that security is aligned with the goals of the business.

FIGURE 6-3. When do you communicate the state of security risk to senior executives in your organization?

[Bar chart showing communication methods and percentages for U.S. and U.K. respondents]
In light of these findings, it is not surprising that half of respondents rated their own communication skills as ‘not effective’ (Figure 6-4).

It is apparent from these responses that security professionals are aware of the importance of building a bridge, yet about half of the respondents (51 percent in the U.S. and 47 percent in the U.K.) rate communication with senior executives as not effective. What is keeping them from being effective communicators? The following table helps explain the issues (Figure 6-5).

**FIGURE 6-4. Please rate your effectiveness in communicating all relevant facts about the state of security risk to senior executives?**
When asked why communication with senior executives was not effective, 68 percent in the U.S. and 57 percent in the U.K. said the information was too siloed, while 61 percent U.S. and 56 percent U.K. said the information was too technical to be understood by nontechnical management. This is understandable as Security has its own jargon—acronyms, technology and terminology—that can make it difficult for nontechnical executives to understand.

A more serious problem, particularly in light of the frequency and seriousness of cyberattacks, is that 59 percent of respondents say that negative facts are filtered before being disclosed to senior executives and the CEO, dramatically limiting the opportunity for effective communication and reducing the organization’s visibility into the urgency of security issues.

A small but still troubling percentage of respondents (16 percent of U.S. and 12 percent of those in the U.K.) say that senior executives are not interested in risk-based security management communications. Given the rising media profile of cybersecurity issues, these results are more likely an indictment of security professionals’ ability to communicate effectively than an accurate barometer of executive disinterest.
COMPANY CULTURE CAN MAKE OR BREAK RISK-BASED SECURITY MANAGEMENT

The key factors that affect an organization’s ability to support risk-based security management include openness to challenge assumptions and being proactive in addressing risk (Figure 6-6). However, given the other communication challenges listed in Table 6.5, it’s likely that most organizations are still struggling to establish a culture that supports the communication essential to risk-based security management.

FIGURE 6-6. The following is a list of eight factors that affect organizational culture. Which features are most critical to the success of a risk-based security management approach. Please select your top three choices.
LUCK FAVORS THE PREPARED

In business there exist degrees of randomness, ranging from perfectly predictable to dynamic chaos. Security lives in the middle—a stochastic zone of complexity, predictability and outcome, and where assumptions are constantly morphing. This means that even the most secure and sophisticated organizations are at risk because there are too many variables in play. Effective communication and collaboration are critical for mitigation when things awry.

As cyber attacks increase in sophistication and quantity, the need for security professionals and C-suite executives to effectively understand and exchange information is even more pressing. Good communication—both downstream and up—is an essential part of every good security program. In the same way that every company has a crisis communication plan, every organization also needs a security communication process in order to embed security in day-to-day operations.

Both sides have a responsibility to meet this challenge. Not only does IT security need to learn how to report actionable security information within a business context, executives must ask relevant questions and require adequate answers in order to progress from silent participants to informed leaders.

However, with buy-in and awareness from every level—from rank-and-file employees to the C-suite—organizations can mitigate security risks to critical assets such as high-valued data, customers, revenue and reputation.

If, as has been said, luck favors the prepared, then those organizations with the culture and communication to establish a solid security posture on risk-based security management principles are on the strongest footing.
ADVANCING RESPONSIBLE INFORMATION MANAGEMENT

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

As a member of the Council of American Survey Research Organizations (CASRO), we uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.

For more information about this study, please contact Ponemon Institute by sending an email to research@ponemon.org or calling our toll free line at 1.800.887.3118.

For more information about this study visit www.tripwire.com/ponemon/2013
and follow on twitter @TripwireInc