Risk Based Security > Risk Assessment >

Security Risk Assessment: What Not to Do

By the Security Executive Council

In 2017, the Security Leadership Research Institute (the SEC's research arm) asked security practitioners to choose from a list which activities their security department performed. We asked the question to see what kind of risk assessment activities security leaders were conducting.

The results raised new questions.

Most respondents were identifying security countermeasures to mitigate risk and identifying specific threats, but fewer were identifying assets, and even fewer were identifying and communicating with risk owners.

At a high level, risk assessments would include most or all of these elements in equal measure. Why was there such variance?

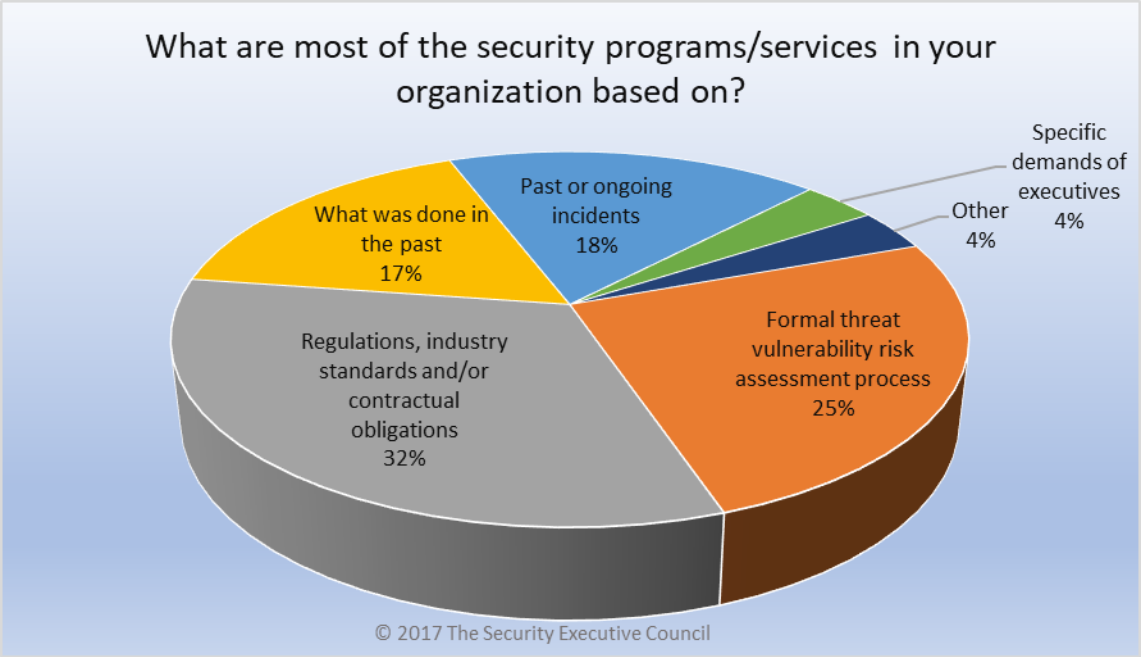
These questions and other research have led us to see that there are a variety of approaches to risk assessment, as well as confusion regarding process and proven practice.

Here are some common missteps to avoid.

Lacking a formal, comprehensive process.

Over our 20 years working with security and risk practitioners, we've recognized that a comprehensive risk assessment is the ideal first step to beginning a new program or inheriting a new security position. We've also recognized that it often doesn't happen.

In a 2017 survey conducted by the Security Leadership Research Institute, only 25% of participants based their security programs and services on a formal risk assessment process. In contrast, nearly 40% based them on "the way it's always been done," past incidents, and specific demands from executives.



Building or revising the program around a comprehensive assessment is the only way to ensure that all risk, not just familiar risk or common risk, is addressed.

Basing the risk assessment solely on your background or expertise.

Risk assessment in the United States has a long history, beginning with the Army Physical Security Field Manual in the 50s and moving through residential and small business crime prevention surveys in the 70s, the ASIS Protection of Assets Manual, and finally to the Securities and Exchange Commission's 10K requirements.

Notice that this history crosses over from military and law enforcement to small business and multinational corporations. It also crosses over a couple of generations, and an unprecedented shift in technology and its integration into common culture.

Because of all this, it's important to ask yourself how your approach to risk assessment is colored by not only its history, but your own. If you were trained in the military, for example, are you relying on the concepts of that original 1950s field manual to the exclusion of other perspectives? If you started out in cybersecurity for a multinational, are you neglecting the fundamentals of physical security?

Oversimplifying.

Risk is complex and assessments can be highly specialized.

Business has evolved, as has risk. Staff work from remote offices. Services are delivered through a variety of models, most of which require at least some contractors to have access to sensitive information or assets. The rapidity of technological innovation creates new risks every day.

Globalization has created new risk. Product development is often done offshore where regulations and monitoring may not meet local standards of care. Laws and customs in local countries must be considered carefully because what is acceptable practice in one location may not be in others. Where are your products and components coming from? What is the level of due diligence of the companies you do business with?

Regulatory requirements now add their own layer of risk as well: the risk of noncompliance.

The risk to the organization generally goes well beyond what one might see at first glance. Always look further.

Not aligning with organizational strategy.

What is your company's strategy? What is its risk appetite? What are its growth priorities?

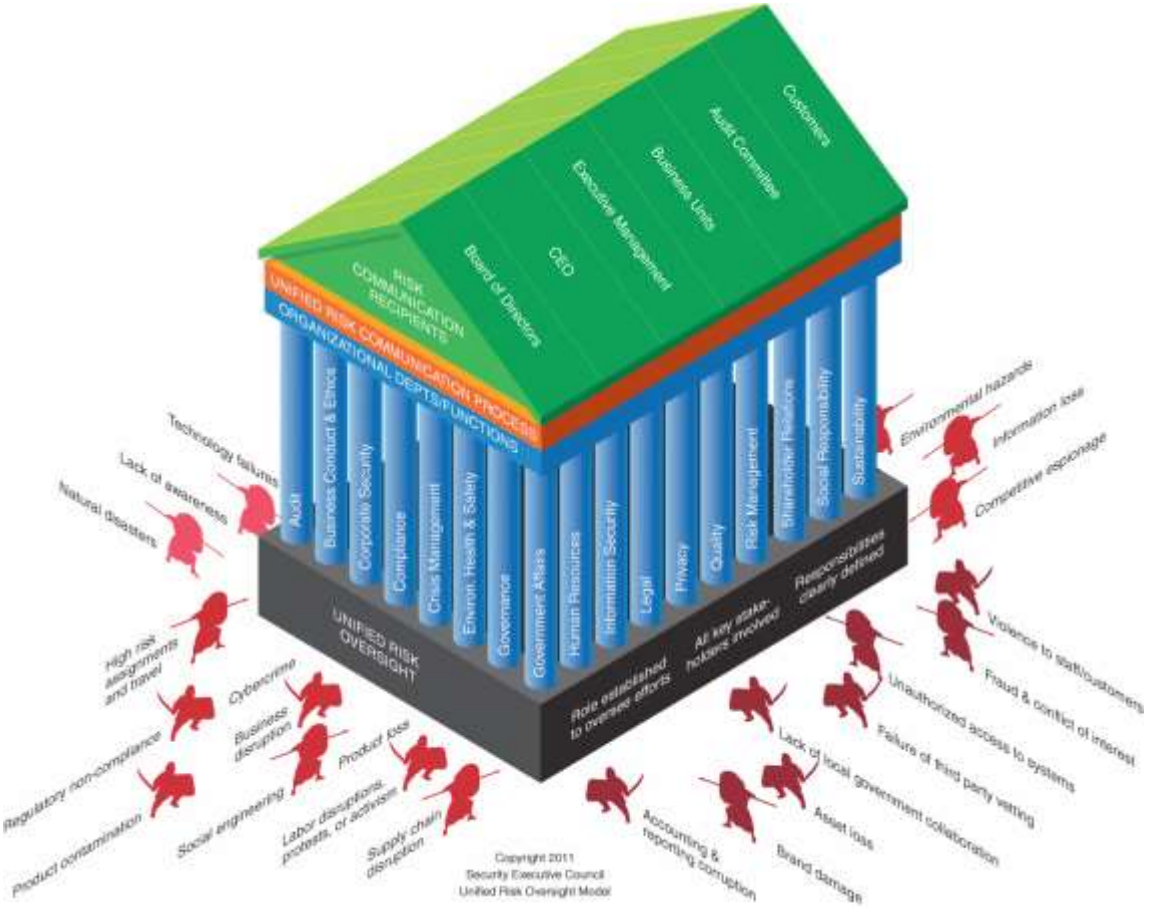
These questions should go hand in hand with a security risk assessment. Knowing the answers will help identify risk and guide risk mitigation, avoidance, or acceptance.

If your organization has done an enterprise risk assessment, that's a good place to start. Look at the business of your organization from a high level, understand it, and ensure that your assessment incorporates the organization overall.

Working in a vacuum.

Risk impacts executive management and other leaders across the organization. Integrating their input and concerns into the risk assessment process will make its results more accurate and more effective.

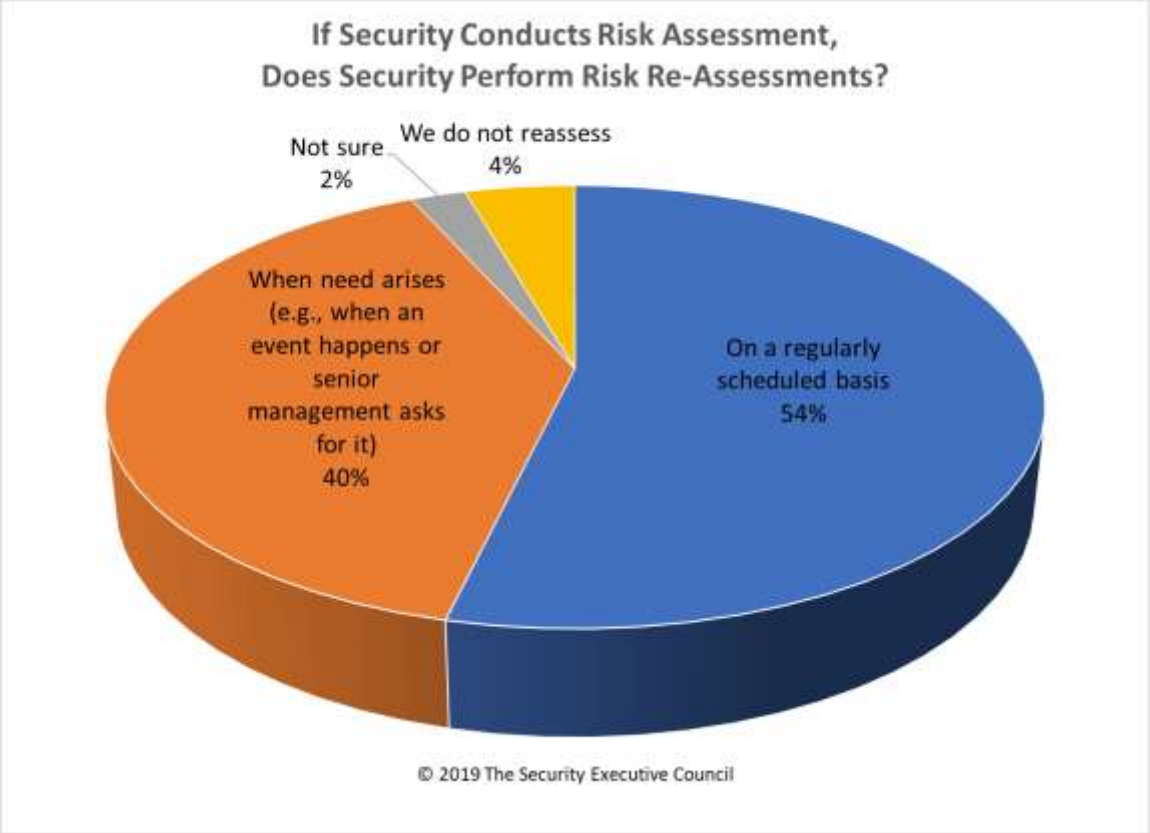
It's also important to remember that other functions often have risk mitigation roles. Reaching out to them can make security aware of possible synergies and prevent the silo effect, in which multiple functions are operating alone and often duplicating efforts.



Communicate to upper management throughout the process that Security is the risk mitigation organizer, but they are the risk owners.

Failing to re-assess regularly.

Even when you are in tune with the changing and wide-ranging risks to your organization, do you regularly re-assess them? Only about half of practitioners we surveyed in 2019 said yes.



If it seems that nothing ever changes at your organization and annual reassessments are unnecessary, think again. Local crime trends change, new technologies emerge, creating new threats. Regular assessment can also create opportunities. For instance, if a risk that you've budgeted to mitigate is no longer a significant risk, those funds can be reallocated.

Visit the Security Executive Council web site to view more resources in the Risk Based Security: Risk Assessment series.

About the Security Executive Council

The SEC is the leading research and advisory firm focused on corporate security risk mitigation solutions. Having worked with hundreds of companies and organizations we have witnessed the proven practices that produce the most positive transformation. Our subject matter experts have deep expertise in all aspects of security risk mitigation strategy; they collaborate with security leaders to transform security programs into more capable and valued centers of excellence. Watch our 3-minute video to learn more.

Contact us at: contact@secleader.com
Website: https://www.securityexecutivecouncil.com/

