SEC
SECURITY EXECUTIVE COUNCIL
A research and advisory firm

Risk-Based Security > Risk Assessment >

Six Questions to Ask Yourself About Security Risk Assessments

Getting back to basics to align your security risk process with the rest of the business

Created by the Security Executive Council

Businesses are more in tune to risk than ever before – it has become a part of corporate culture. Corporate leaders have improved their understanding of the role risk assessments play; however, Security and the rest of the business are not always in agreement on the "why" and the "how." Therefore, Security's risk assessment activities may not be in line with the rest of the organization.

This paper is designed to help security executives evaluate their current risk assessment program. The SEC has found that while many security leaders are performing risk assessments, they are not being conducted at the enterprise level; instead they are assessing at the site or building level. Although there are practitioners that are advanced in the practice of risk assessments, our research shows that as more people are moving into corporate security leadership roles, many are not starting with the basics – like conducting an enterprise-level risk assessment related to security issues.

The SEC has found that conducting a risk assessment at the enterprise level is a first and essential step for successful programs. In a recent Security Barometer poll on risk assessment, security practitioners shared the steps they use to assess risk and how well they feel their organization is tackling significant security risks overall. The results can be found here.

To evaluate where your risk assessment program is, begin by answering the following questions:

- Do you have a working definition and process for risk assessment?
- Is there a risk assessment program in place that's embraced and followed from the top down within your organization?
- When was the last time you did a risk assessment? And how frequently are they updated?
- Do you re-evaluate and update your program on a regular basis—especially, but not limited to,

  after incidents or threats?
- Do you review the results with senior management and obtain concurrence on the risks?

If you can't answer these, or if the answer is "no," it's time to examine what you are doing and how you can improve the risk assessment program for the betterment of your organization. Creating a common risk definition and language between security professionals, security executives and senior management is critical.

Risk Management Definitions

For security and business to be a truly unified discipline, there needs to be a shared language for defining risk and mitigation and articulating the success or failure points for any given initiative. The common language needs to be accessible and inclusive to all units within an organization, including executives, human resources, legal, finance and security.

There are plenty of definitions to be found for risk, threat and vulnerability. But an example is useful to clarify the terms.

For illustration purposes we chose an example that can impact several areas of risk: event security, which has become of importance in many companies based on recent incidents. This example highlights the complexity of risk.

Corporate Events (sponsored or held at a Corporate location)

We'll start with examples of general categories of risk and the threats:

People Risk

Threat = Personnel death or injury at a corporate event

Brand Risk

Threat = Brand name associated with a catastrophic incident at an event (e.g., the Mandalay Bay Resort and the Las Vegas shooting)

Product Risk

Threat = Products used/featured at an event cause damage (e.g., food contamination)

Property Risk

Threat = Fire or riot at an event at a company facility
The vulnerabilities and mitigation are basically the same for all four risk areas listed:

Vulnerability = Lack of adequate planning, contingencies, preparedness and inappropriate contractual requirements

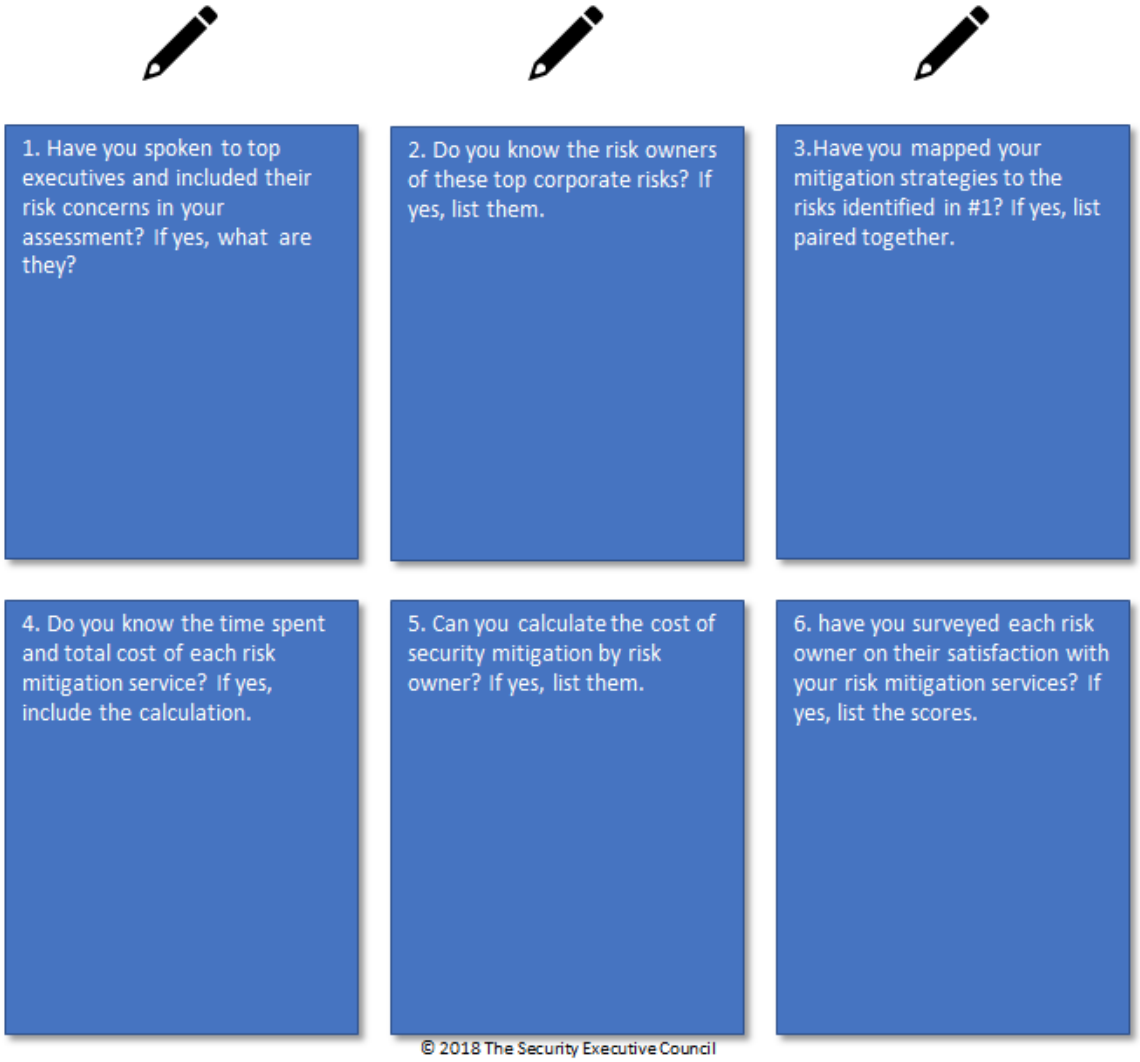
Mitigation = Pre-event risk ranking, attendees risk analysis, appropriate contractual requirements for security and crisis management, risk assessment/emergency response plan, and adequate security measures in place.

Of course, probability and impact levels of any risk will need to be determined as well.

It's important for security executives to establish and maintain an ongoing process of risk assessment to drive security and resource planning. Risk assessment statements ultimately should represent key risks to the organization and characterize a measurable, effective security program.

Six Critical Questions

Can you answer these questions about your company's business/security risk alignment? Write down your answers in the boxes below. This can also be used to document progress.



If you gave the same **six critical questions** to each member of your security leadership team, would they come up with the same results?

The goal of this exercise is to provide a resource that solidifies and documents key success factors and provides assurance your program is working. It's also a way to determine if the plan and processes you have in place are significant enough to mitigate the risk.

There are other targeted questions that can be posed internally to conduct this exercise:

- Is the mitigation program run uniformly throughout the company so you are providing the same services throughout the organization?

- Have criticality, profitability and single points of failure been incorporated into the risk assessment to make sure that adequate mitigation has been provided to those sites or businesses?

- If security is not a main provider of risk assessment and mitigation—what support should you provide?

Failure Points

The SEC has found the five most common failure factors for a security risk assessment:

1. Risks aren't aligned with the enterprise risk assessment that executive management has completed.
2. There is no stakeholder input and concurrence.
3. Security executives don't map and align their mitigation strategies to risks.
4. Security executives don't prioritize risks.
5. There is no identified process.

Many times, there is too low a level of scope in the risk assessment, and potential risks are missed. Or, personal opinion was applied, and security executives only look at the process from their perspective and not from the perspectives of other business units within the organization. There are additional variables, such as outside contractors. If they don't have the right foundational knowledge of risk and the organization, there is no cumulative quality, only "currency."

Security executives need to regularly reassess their established risk assessment plan to determine if it is up to date. Do elements need to be added? Have you determined what has been effective and what has not? There may be a better, more targeted program than the one currently in place. In reality, this type of deep thought and analysis on risk assessment is not taking place at many organizations – but it should.

What is your plan? Contact us at contact@secleader.com if you want to discuss how to align your security risk process with the rest of the business.

Visit the Security Executive Council website for other 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/

