SEC
SECURITY EXECUTIVE COUNCIL
A research and advisory firm

Security Program Strategy & Operations > Strategic Planning/Management >

How Firm is Your Security Foundation?

By the Security Executive Council

Assessing these eight elements can help you ensure that your strongest programs aren't undermined by a weak foundation.

Quite often we meet security practitioners who’ve put a great deal of genuine care and hard work into developing strong security programs and services, only to end up baffled by executives’ lack of engagement, sidelined by negative feedback on risk management decisions, or battling internal customers’ unwillingness to comply with policies.

Why, when the function’s programs are so well-considered and solid, does everything seem like such an uphill battle?

The answer might be in the question. What if they are building on a hill?

Sometimes security leaders get so focused on rolling out the “right” programs that they don’t stop to think about the foundations those programs will be built upon. Some fall into this trap when they are building a brand-new security department. More often it happens when they are inheriting an existing function and hoping to improve.

To extend the foundation metaphor, imagine building a new house and deciding to begin with the second floor. Or imagine embarking on a renovation without knowing when the house was built, what the codes are, what features the occupants really care about or how much they have to spend. Sounds ridiculous, but that’s exactly what happens when security leaders fail to analyze their foundations before they develop programs. Everything may look great at first, but before long the cracks will start to appear and widen, until they successfully undermine all that hard work.

So, what are the elements of a firm security foundation, and what is the status of yours?

The SEC has identified an entire universe of security success elements [see Figure 1], but we've recently pinpointed eight specific foundational factors that can be analyzed and aligned to help security practitioners understand their foundations so they can either work to stabilize them or build programs that fit successfully atop them as they are.

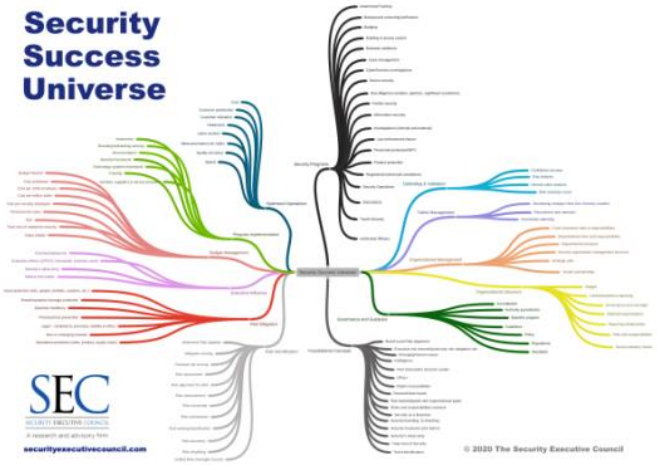
Security Success Universe
SEC
Security Executive Council
A research and advisory firm
securityexecutivecouncil.com
© 2020 The Security Executive Council

Figure 1 The Security Success Universe

Security Success Universe

The image to the left contains the universe of possible elements for security practitioners to consider. Our research based on security thought leaders' key success elements resulted in 13 categories:

- Foundational Concepts
- Risk Identification
- Governance/Guidance
- Risk Mitigation
- Executive Influence
- Organizational Structure
- Organizational Mgmt.
- Budget Management
- Program Implementation
- Talent Management
- Optimized Operations
- Defending/Validation
- Security Services/Programs

In total there are 115 unique elements to consider for your success equation. Consider implementing the ones that can bring value to your organization.

1. Security Leadership Level

Are you new to security or new to your industry? Are you now learning a facet of security you haven't previously worked in (corporate security or IT)? Are you creating or recreating a security department, maintaining an existing function, or urgently expanding the function in response to incidents or organizational changes? Are you able to be future-oriented, or to push the bounds and roles of security to innovate and build alignment? Where you are now as a leader impacts what you can do to bridge gaps and resolve foundational issues.

2. Service Delivery Model

There are several models of service delivery in security. In a centralized model, security resides primarily in-house, with a large central staff and a security leader over it. In a governance and oversight model, the majority of security services are outsourced under the oversight of a very small in-house security function – often an army of one. A distributed model can take many forms but combines elements of these first two.

Often security leaders enter new positions assuming that the delivery model will provide them in-house resources, only to discover they are expected to be an army of one. How does your organization expect security services to be delivered, and how does that align with your own expectations and plans?

3. Program Defensibility

In the case of a catastrophic negative impact from a risk event, could you and your security team be held legally accountable? Recent changes in case law allow for security programs to be found negligent for not meeting “professional security standards.” What about other types of defensibility? Would your actions be defensible to victims and their families, to employees, shareholders, or the media in the court of public opinion? These questions all point back to documentation, communication, and duty of care.

4. Program Maturity

Where does your program fall on a spectrum from reactive to optimized and value-adding? Is it in start-up mode? Does it offer consistency of service? Is it well defined and documented? Is the function an integrated part of the business? Is it measurable? Does it contribute to revenue or help build new business? Just as your leadership status impacts your foundation, so does the maturity of the function itself. (You can assess the maturity of individual security programs here.)

Your C4R - Make the Most of What You Have

The 8 foundation elements listed are things you can have some influence over. However, your current conditions, culture, circumstances, and resources (C4R) are your operating environment, and they are generally outside your sphere of influence. You can't control your organizational culture, your budget, or the trajectory of current events. However, assessing them will inform your risk decisions and priorities, and it will help you to make the most of what you have.

5. Executive Influence

Have executives been educated about the security function, the value it brings, and the results you have achieved? Is there a mechanism to effectively and quickly communicate the services the organization finds valuable? Can you demonstrate how each area of the company (audit, sales, comptroller, marketing, R&D) uses and benefits from security services? Do executives expect you to brief them on risk issues? What story are you telling to each internal and external audience you engage?

6. Security Metrics

Do you have an established program for identifying, developing, and deploying security metrics? Are your metrics primarily concerned with counting, or do they tell a story? Are they being used to enhance operational excellence? Do you have a process by which to communicate them to show business value? As SEC subject matter expert George Campbell often says, if you aren't measuring, you aren't managing. Meaningful measurement is central to performance assessment and resource management.

7. Board-level Risk Alignment

When was your last risk assessment? All publicly owned businesses are required to identify significant risks in their 10-K statements. Have you reviewed your company's 10-K? Did you contribute to it? How do your existing or projected security services and programs line up with the risks the board cares about? Do you articulate security's contribution to managing significant risks, or use the board's concerns to influence risk awareness? Developing risk-based programs – rather than programs designed to meet historical risks or executive mandates – is a critical foundational element.

8. Unified Risk Oversight

How is risk managed across the organization? Who has oversight over enterprise-wide risk management? Does the security function interact significantly with risk stakeholders to discuss and share risk information? Is there a centralized communication process? How does the organization understand and define its own risk appetite and residual risk, and who is responsible for reinforcing that understanding?

Next Steps

Assessing these eight elements can give you an idea of how firm your foundation is today and what you need to shore up in order to reach the goals you or your organization have set for security.

This process can be difficult to do on your own. If you would like a free assessment of the state of your foundation, contact us. The assessment takes only about an hour. Our subject matter experts help you to define your current foundation state and compare it with where you would like it to be. They can also provide some early ideas to help you close the gaps. If you'd like an abridged online self-assessment, we hope to release one at the start of the new year.

Visit the Security Executive Council web site to view more resources in the Security Program Strategy & Operations: Strategic Planning/Management 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/