SEC
SECURITY EXECUTIVE COUNCIL
A research and advisory firm

Risk-Based Security > Risk Assessment >

Reimagine Risk and Security: Evolving Beyond COVID

By the Security Executive Council

A recent SEC Security State of the Industry event for Tier 1 leaders explored how practitioners must reimagine risk and security to envision a post-COVID future.

Here are some of the highlights of the discussion, which featured Bob Hayes, SEC Managing Director; Kathleen Kotwica, EVP and Chief Knowledge Strategist; Dan Sauvageau, Emeritus Faculty - Executive Influence; Francis D'Addario, Emeritus Faculty - Strategic Innovation; and Jim Hutton, Emeritus Faculty - Strategy and Leadership Development.

Security Success

If we want to adapt to an uncertain future, we first must look at what we're doing now, why and how we're doing it, and then examine whether that model matches the reality we are facing.

It's useful to first revisit how we achieve security success in any environment.

- Success requires you to recognize Security's current conditions, culture, circumstances, and resources (your C4R). You may have great plans, but if you don't consider the C4R, you'll likely fail to gain traction.
- Successful leaders develop a compelling story for Security. They set expectations and give examples of what success looks like. They use it as a tool to gain strategic input. Now, more than ever, our story is important; however, it is likely to change due to the current environment.
- We need to understand the entire realm of Security. The SEC has outlined the Universe

of Security Success (see figure 1). This is the accumulation of 15 years of research and collaboration with thousands of leading security practitioners. Not all elements in this universe are necessary for everyone. The trick is to find the elements that will provide your organization the most value.

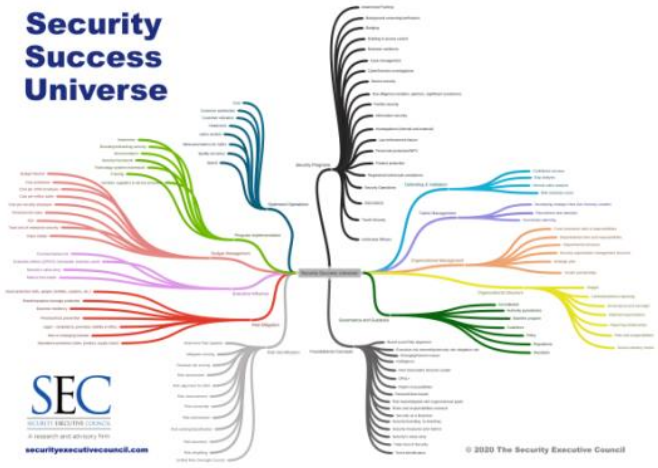

Figure 1 The Security Success Universe

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.

Why Reimagine Risk and Security Now?

A worldwide pandemic of this scale has not been seen in our lifetime. It has produced a tremendous amount of change. Organizations and security departments clearly have their hands full reacting to twists and turns. But we need take the time to be prepared for an alternative future state.

Your company today is not the same company it was last year. A recent McKinsey report claimed that a majority of businesses have changed how they go to market since the pandemic started.

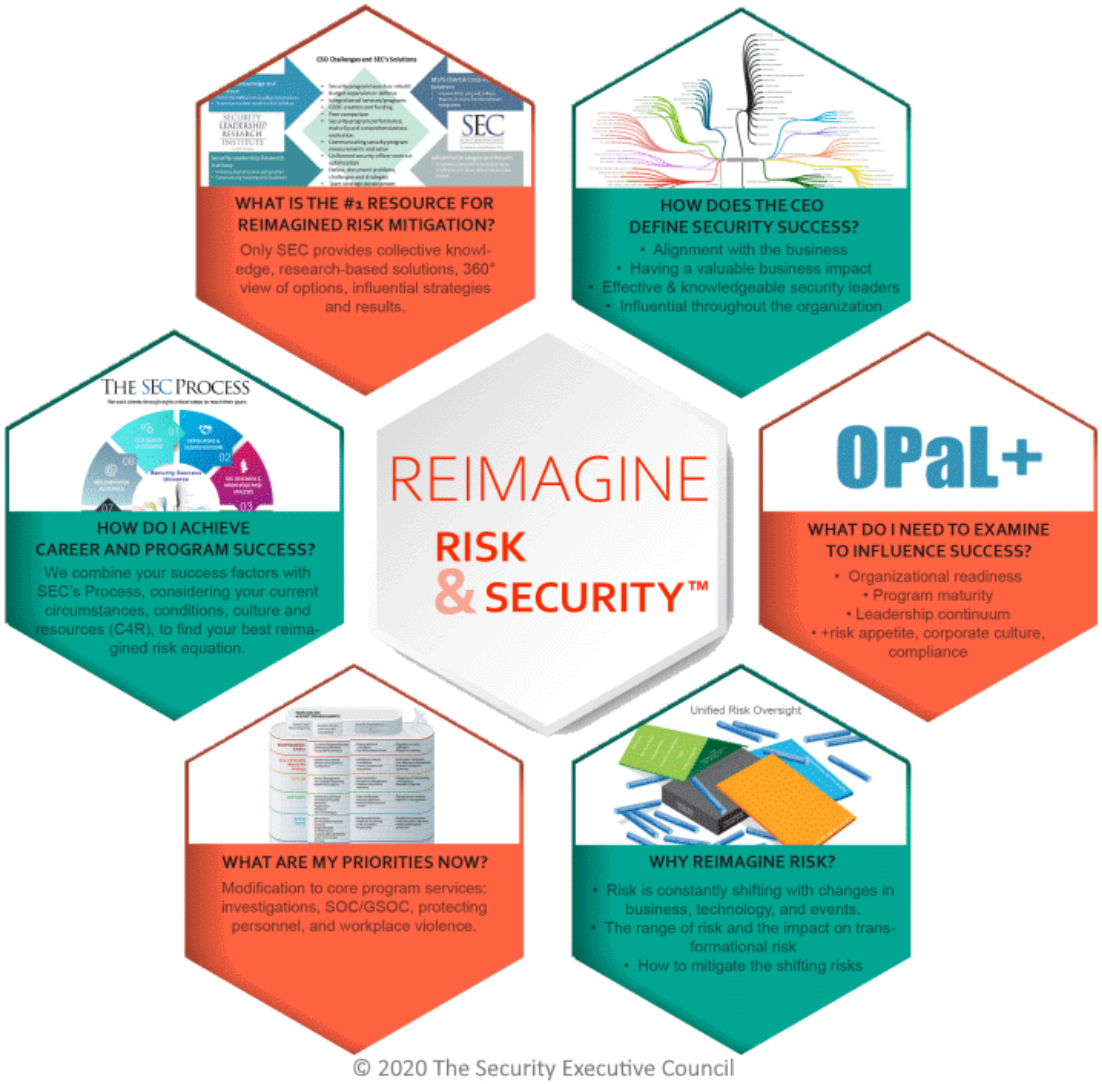

Figure 2 Reimagine Risk and Security

Reimagining risk and security (figure 2) means:

- recognizing risk shifts based on current events, company changes, social, economic, and political changes.
- re-assessing your organization's security risks and revisiting your programs, services, and mitigation strategies informed by these changes.
- prioritizing any modified plans while aligning with the organization's new directions and goals.

Security needs to look ahead. What may permanently change, and how will core security programs adapt in a VUCA (Volatile, Uncertain, Complex, and Ambiguous) world?

Executives are Looking for Opportunities

According to McKinsey's Innovation Through Crisis survey, most executives see new opportunities for growth right now, but few feel confident they'll be able to harness them. Security can be a partner in this endeavor. Opportunities exist in moving fast and taking on more risk. Security can help in the reimagining process by doing what we do – objectively articulating the potential security risks that may derail new growth.

Security must adapt its core programs to meet the company's new requirements and the need to leverage new opportunity.

Risks from Continued Work from Home

The continuing work from home model brings both physical and Information risk.

On the information protection side:

- Employees working from home are unlikely to use safe practices on their own.
    - A CyberArk study shows that 60% of remote workers use unmanaged BYOD to access company assets; 89% use the same password across platforms; and 57% insecurely store passwords in browsers.
- Vendors are also using remote workers.
    - Are you comfortable with their workers' remote security?
    - Do you trust they will contact you in the event of a breach?
    - Do they have the capacity to meet your security requirements at all?
- Insider threats
    - In the brick and mortar environment, security often gets tips on insider risk from coworkers who see red flags. In a work-from-home environment, that resource is lost. How do we replicate that informal environment in a remote world?

On the physical security side:

- The economic forecast shows a potential increase in crime; should companies install home security systems to keep staff and assets safe?
- Hiring concerns - the intuitive behavioral signals that occur during an in-person interview will be harder to assess on video meetings. Perhaps we will be able to use automated behavioral analysis applications?
- What will access control, video surveillance or medical emergency procedures look like? How do we accomplish that in a work from home environment? Or can we?
- The security control center (SOC) or GSOC is one tool that could help you reimagine some risk processes. Will it take calls from all employees? Will the GSOC take on situational awareness, coordinate responses, or send individualized advisory

information to help remediate potential issues?
- Investigations – how will we handle hostile interviews, equipment recovery, or searches for material or information? Do employees sign a condition of employment document that ensures Security can come and get the equipment if the employee does not return it?
- Risk mitigation is the responsibility of many functions across the organization. Working from home will make cross-functional teams even more important for coordinating handling events. This may also include updating or developing new policies.

At-home employees continue to share responsibility for security. It's important to communicate that responsibility and articulate exactly what they need to do to manage security in their workspace. It's also important to solicit their feedback. Companies are pivoting –from auto parts to ventilators, distillers to sanitizers – and those solutions may be coming from the shop floor. Find out what employees are thinking and what they need. Be culturally relevant. Use apps to let them provide input and feedback about their own safety, security and health.

Further Resources

For more information about some of the foundational concepts of security mentioned in Figure 2:

Unified Risk Oversight

Board-Level Risk

OPaL+

Program Continuums

Security's Value Potential

Maturity Model

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/

