

Program Best Practices > Resilience >

# Top Security Practices for a Resilient Business

By the Security Executive Council

A group of security leaders recently gathered in Calgary, Alberta, to share the lessons they've learned from challenging experiences. The themes that emerged form a set of best practices (the SEC prefers to use the term "proven practices") that can inform any security practitioner aiming for business continuity excellence. Here's what we heard time and again.

## Exhaustive and Creative Crisis Planning

Resilience requires in-depth knowledge of your community, its service providers, its businesses, and its needs.

- What role can and will each of these entities fulfill in a crisis?
- Look beyond the police force and governmental partners. What are the resources and capabilities of local and regional NGOs? Business organizations like the Chamber of Commerce?
- Your duty of care for your community requires that you even consider your own competitors as potential partners in crisis. Explore this possibility in advance of a critical event.
- Build agility and adaptability into your resilience and organizational framework. If security cannot adapt to new internal and external challenges, security will not succeed.

## Clear Risk Ownership

Recognize, and ensure management recognizes, that you are a risk advisor, not a risk owner.

- Identify and communicate risk, then step back and allow executive management to make the risk decisions.
- Sometimes they will make tough choices and you will end up picking up the pieces. That is part of the job.
- This is also why postmortems are so important. They allow the organization, as the risk owner, to learn from the results of its past risk decisions.

## **Actively Enabling the Business**

Remember that security is ultimately a service enabler. Therefore:

- Make it a priority to develop active, listening relationships with business units.
- Conversations with other business units need not begin: “Security must accomplish X so the unit must do Y.” As a service enabler, security may lead with “What do you as a service line require, and how can we help you accomplish your goals safely and securely?”
- Request long- and short-term strategic plans from business units and use those to inform your own strategies. When security or business units request investments or projects, begin by determining whether they align with those strategic plans.

## **Change Management**

When you propose change in any part of the organization, engage in change management.

- If your organization has a low level of readiness or program maturity, you may be able to rapidly increase that through extreme socialization – that is, by dedicating extensive time up front to listening to and involving all internal partners
- Don’t assume that individuals who resist your proposed changes are naysayers or saboteurs. Ask questions. “What can I do to facilitate this change?”
- The goal is not to eliminate resistance. It’s to understand what underlying issues people are communicating through their resistance, why, and how you can address it.
- People resist change because they feel a loss of control or uncertainty. So, have coffee with your resisters. Have a candid, salient, and succinct conversation about their concerns. Ask, “How can we make this benefit you?”
- Once you’ve instituted a new program, give the organization time to catch up, time to be validated and heard. Do not launch and leave.

These insights and more were shared at the SEC’s Next Generation Security Leader (NGSL) program, which brought together security professionals from a multitude of industries and backgrounds for two days of learning and peer engagement. Presenters from the City of Calgary alongside other leaders from public and private organizations in cyber and corporate security, covered a diversity of topics.

For information on NGSL: <https://securityexecutivecouncil.com/spotlight/?sid=29593>

Interested in the hosting at NGSL event? Want to implement some of these best practices? Need a little help? The SEC can assist you with this. Contact us today to discuss your needs.

**Visit the Security Executive Council web site to view more resources in the [Program Best Practices : Resilience](#) 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](mailto:contact@secleader.com)

Website: <https://www.securityexecutivecouncil.com/>