Security Leadership Solutions Executive Council

The Roadmap for Security Leadership Success

Ten trends based on research of successful leaders

The following 10 insights are based on our observations and research encompassing the last 10 years of working with successful security leaders. The Council has helped leaders reach their goals by accurately identifying fundamental changes in the security industry through research and our wide-ranging relationships with practitioners, academia, the vendor community and trade media. We have analyzed many organizations that have effectively managed the changes in the industry; most of the security practitioners of these organizations are horizon leaders that have been on the bleeding edge.

We have learned a lot in the last decade. Our research shows the following best practices are becoming the success markers in security. It is time for you to choose if you want to be a fast follower or play catch-up to an inquiry from management about a negative incident or the latest media hype. Your decision point is whether you want to be a proactive leader or a reactive manager.

The 10 Most Common Decisions Highly Accomplished Security Leaders Make

1. They have the right tools/assets/people in place *before* an incident happens and these resources are focused on the right things.

Why is this important?

Our research has shown that the determining factor of successful programs is not dependent on the size of the budget, the quantity of staff or the sophistication of technology installed. What is critical is understanding that the resources you have are directed toward validated issues, needs and goals of the organization.

In order to fully support the goals of the business, you need to be proactively positioned. The programs and services Security builds need to be those that are used within the organization effectively. To accomplish this, you must understand where the business is now and where it is going. Take the time to understand, classify and document for your own needs what the culture of the organization is and how it impacts decisions. Pay attention to internal trends. Start to intuit what is next on the horizon for your organization to stay viable. Use this information to understand what resources need to be in place

Being a true business partner is not a matter of doing what management tells Security to do, instead it is about being in tune with what the business needs as it grows. This proactive focus on the business and its operating culture will put Security in position to more effectively respond to and divert threats. Consequently make sure information about your efficiencies gets communicated in front of those in the organization that are at a level of influence.

Additional Resource:
Improving the Way Risk Management is Perceived by the Enterprise

2. They build the right relationships – internally and externally.

Why is this important?

There are a lot of very intelligent people in the security industry but over the last 10 years of interacting with recognized successful security leaders we have concluded that a critical element of success is how well they are connected to their network - both internally and externally. This assists with finding winning solutions for the obvious reason that you have more trusted resources to draw from. Internally, this means building a network comprised of strategic stakeholders, cross-functional team members, and key people from support services. Strategically seek out those that can help you do what you think needs to be done for the good of the organization. Strive to create "win-wins."

Externally, build a network of both peers from within your industry and outside. The latter is in part for cases when you are lacking a resolution to a problem in your sector or industry – an answer may be found through examination of a similar problem in a different industry or sector that you can adapt to form your solution.

Develop relationships with the public side if you are from the private side and vice-versa. One of the most important benefits of partnership between the corporate world and the public sector is related to business continuity. A strong relationship between the groups ensures that in an emergency the corporation security team is ready to work quickly and effectively with law enforcement and public agencies to provide the best response to protect both the organization and the citizenry.

Also tap into the academic world to stay up-to-date with risk and business theories, and research. If you can - become involved. You never know something as well as you can until you need to teach it to somebody else.

Additional Resource:
What is the Most Important Characteristic of an Outstanding CSO/CISO?

3. They foster an environment of sharing and create useable ways of documenting what they learn from others.

Why is this important?

Security since its inception has done a poor job of doing this. We have been reinventing wheels for decades. This does not help security grow as a function and be valued as it should be. The only way to evolve is to share what can be shared. Put aside egos or ways you've learned to engage from previous organizations and be open to input from team members and colleagues. This type of process, that the Council uses and calls Collective Knowledge™, brings multiple experiences, various viewpoints and options to a project. It's not always easy and someone needs to be the lead to synthesize the best of the best into a cohesive solution. But its whole is always better than the sum of its parts; plus it builds faith and trust amongst those who work together.

Sharing also needs to happen not only within an individual organization but across the industry. The Council gets requests for industry benchmarks and metrics on a weekly basis. But not enough practitioners are contributing their data. Therefore, as an industry, the answers to questions by way of reliable data are just not there. But on the other hand, understand that having the data in hand is not a magic bullet. If a request was made from

senior management to come up with comparison data to peer companies - dig into why? Are they questioning Security's value?

Additional Resource:
Benchmarks Aren't Magic, They're Tools

4. They are lifetime learners and continually push programs to the next level.

Why is this important?

The risk landscape changes all the time. Your organization is continually evolving. Business models shift. If you are not pushing your leadership skills and security program organizational fit and maturity level – you are in maintenance mode at best, or slated to be let go after the next big incident, at the worst. The Council's most successful members of its community are continually seeking new knowledge. They are open to recognizing when they don't know something well and will reach out to others to learn more.

As companies look into their futures, more and more are seeing themselves as global, lean, connected organizations. Security professionals must reach out to their organizational leadership to clearly and objectively articulate the risks that may impact their strategies as they move into this landscape. They must also remain cognizant of the organization's risk appetite and understand that as business changes, so must security.

Make sure you keep up on information and events outside of security that can impact security and risk mitigation. This includes business theories and processes, business leadership/management trends and world events. Watch what senior management is watching.

Additional Resource:
Driving Excellence in Enterprise Security

5. They focus on leadership issues.

Why is this important?

No matter where you are in your career or what sector or industry you practice in, this is a key consideration. It crosses over all of the services and programs you provide your organization. At the end of the day it's not about a particular technology, process, standard or solution. It's about thinking how to move your department and your company ahead. The most successful security leaders the Council has worked with make use of the following 9 leadership practices:

- Creates a robust internal awareness program for the security department, including formal marketing and communication initiatives
- Ensures that senior management is made aware of what security is and does
- Walk-and-talk methodology—regularly talking to senior business leaders about their issues and how security can help
- Converses in business risk terminology, not "security"
- Understands the corporate culture and adapts to it
- Wins respect by refusing to exploit fear, uncertainty and doubt
- Bases the Security program goals on the company's business goals
- Has top-level support from day one

- Portrays Security as a bridging facilitator or coordinator across all functions

Additional Resource:
9 Practices of the Successful Security Leader

6. They discuss risks and mitigation strategies in terms the Board "gets."

Why is this important?

This is not just a matter of being able to use business terminology or having a business degree. This is about understanding what the Board (or senior management) identifies as "risk." Start here and identify the business processes in these risk areas with security components. Map what the security department does to mitigate these security risks. In this exercise you have created a dotted line to what Security does and the concerns of the board. It is an "ah-ha" moment. The Council's Board Level Risk diagram has been used by dozens of its members to successfully articulate their contributions in terms the board resonates with. See Managing Enterprise-Wide Board Risk listed below to learn more on the how-tos of this exercise and how it creates value.

In a similar vein, understand Security is not the sole owner of anything security-related anymore. There needs to be a unified communication and coordination process. Security can step-up and take the lead on this. Agree what risks the organization wants to take on. Agree on the boundaries for specific functions on a particular security issue. Coordinate the mitigation strategies so there are no gaps. Make sure the right information is communicated to the right stakeholders. Strive to all communicate on the same level across the organization. The Council has found a risk-based approach to be the best.

Additional Resources:
Managing Enterprise-Wide Board Risk
Unified Risk Oversight™

7. They run security as a business.

Why is this important?

Many organizations think of Security as something "outside" standard business functions (finance, sales, marketing, HR, etc.). How did this happen? It's because often the security department does not use the basic business processes everyone else relies on such as:

- Understanding all of your internal customers and what "products" they want or need
- Where security efforts fit into the BIG ultimate goal – creating revenue
- KPIs (key performance metrics) and other ways to measure activities are working as planned and adding value
- Cataloging what Security offers and it's perceived value
- Constant communication to stakeholders on where Security is and where it is going

Regarding the last point, work on your communication strategy to the business side. This is different than your communication and management strategy to security colleagues and staff. If you only remember one thing around this topic make it this – at the end of the day security may provide value to the organization, but are you valued? Your communications to the business side should always expose the insight you have on what the business is trying to do and that you are helping the company get there.

More business executives are expecting business leaders that have expertise in security and not the other way around.

Additional Resource:
Using Business Research to Increase the Effectiveness of Security Leadership

8. They take care of staff and help them grow.

Why is this important?

Yes, it takes work and resources. But one of the biggest blocks to success is having a security team where only the top person is thinking strategically and knows the ins and outs of the business they are supporting. A strategically thinking staff helps them with their own careers, helps you get the job done and has additional benefits like having the organization think of your staff as experts they can consult with when they have a risk-based issue.

Also help staff learn how to measure Security's performance against company-based metrics, how to appropriately interface with internal and external customers and be on the look-out for possible revenue opportunities. This will foster the vision of a security leader who has a team of leaders. The Council has seen this often creates strong relationships that tend to last even if team members move on.

Additional Resource:
Next Generation Security Leader Program

9. They recognize their organization is different from any other, even from peer companies.

Why is this important?

If you don't understand this you risk applying the wrong security solutions for your organization. The Council has seen more people let go for this, even if it is not overtly articulated, than any other reason. Don't assume you can apply something in a new organization just because it was successful somewhere else. Our research shows there is no one "best" model for the security department. It's very dependent on organizational-specific factors including differences related to industry, sector, organizational structure, corporate culture, and executive drivers.

The Council uses a process called OPaL+ to identify the elements that need to be understood to start or enhance security programs within an organization. OPaL+ stands for:

- Organizational State of Readiness: what "is" security to the organization, which impacts the willingness to accept your strategic vision of Security
- Program Maturity: where your program is now and where do you want it to be?
- Leadership Continuum: what is your leadership style and how does it fit the organization?
- The "Plus": Corporate Culture and Organizational Risk Appetite

Knowing this informs your strategic plan and future states. You will need to do the internal research necessary to make these elements align.

Additional Resource:
The OPaL Assessment Executive Summary

10. They prepare for future trends.

Why is this important?

All of the considerations above have emerged over time. Security has seen some major shifts including the expectations of the security leader. We have moved from the early days of a law enforcement and military mindset to a business value perspective. Today's most accomplished security leaders acquire four capabilities that define the next generation security leader:

1) A security head must understand his or her industry and company.
2) A security leader must develop a skill set that blends security, IT, business expertise and the ability to identify and evaluate emerging issues.
3) A security leader must grow with his or her company.
4) Finally, he or she must possess an imagination capable of exploring for opportunities that will add value to the company.

Are you ready for the next wave?

Additional Resource:
The Evolution of the Security Executive Council

Selected Additional Resources

From One Winning Career to the Next

Measures & Metrics in Corporate Security: A Workbook for Demonstrating How Security Adds Value to Business

Not A Moment to Lose: Influencing Global Security One Community at a Time

Security's 2012 Accomplishments and 2013 To-Do List

Wanted: A New Type of Security Leader

About the Security Executive Council

The Security Executive Council (www.securityexecutivecouncil.com) is a leading problem-solving research and services organization focused on helping businesses build value while improving their ability to effectively manage and mitigate risk. Drawing on the collective knowledge of a large community of successful security practitioners, experts, and strategic alliance partners, the Council develops strategy, insight and identifies proven practices that cannot be found anywhere else. Our research, services, and tools are focused on protecting people, brand, information, physical assets, and the bottom line.

Contact: contact@secleader.com