

Building Brand or Re-Branding the Security Function

When You Know Security's "Brand" Might be Less than Optimal

- ❑ Imposed budget reductions are made without consideration of increased risks
- ❑ There is a realignment of Security to a lower level, which impacts unfettered access to the top
- ❑ There is an increased frequency of inadequate first-response to security incidents; and management is taking notice
- ❑ Security is thought of as specific stereotypical tasks ("gates, guns and guards") – not a business function that mitigates risks
- ❑ Internal customers do not know what services Security provides or cannot list services provided to them specifically in the last 12 months
- ❑ Security is not included in business decisions that have risk considerations
- ❑ Senior management does not understand the correlation between risk and costs and security's cost to reduce risks

Things to Consider When Re-Branding Your Department

- ❑ Know what your current brand value or image is and have a vision of what you want it to be
- ❑ Identify the steps to take you from where you are to your goal and line up the needed resources
- ❑ Develop the messaging to communicate the intended change for your brand image
- ❑ Communicate Security's role and value in a way resonates with the business side
- ❑ Fully identify security risk mitigation-related costs by customers and by services
- ❑ Develop key performance indicators – this is more than just “counting” events. What is the contribution to the organization?
- ❑ Be an organization of influence versus an organization of “doing”
- ❑ Understand business units are the risk owners – Security needs to partner with BUs to provide the services they want to mitigate risks to employees and assets

A Start: Organizational Security View via SWOT (Example)

| Strengths | Weaknesses |
|---|--|
| <ul style="list-style-type: none"> • Organizational readiness • Business / cultural demand • Base physical security program in place locally • Infrastructure investment • Global footprint / recognized industry role • Ethics & Compliance programs | <ul style="list-style-type: none"> • Industry standards & disciplines • Security business accountability • Role of security • Vendor management & services • Position resources • Enterprise readiness and response • Enterprise services (physical / threat / crisis) |
| Opportunities | Threats |
| <ul style="list-style-type: none"> • Enable business strategy • Contribute to increased employee engagement • Public-private partnerships • Increased level of enterprise security services • Expense control and vendor service • Organizational role clarity • Consolidation of services and standards | <ul style="list-style-type: none"> • False perception of safe & secure environment • Compliance standards • Increasing threats with business growth without needed capabilities • Site safety standards and response • Speed and accuracy of services without enterprise approach • Speed of investment to competency as business strategy changes |

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 and 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 us to start a discussion on building brand for your security department: contact@secleader.com

