SEC
SECURITY EXECUTIVE COUNCIL
A research and advisory firm

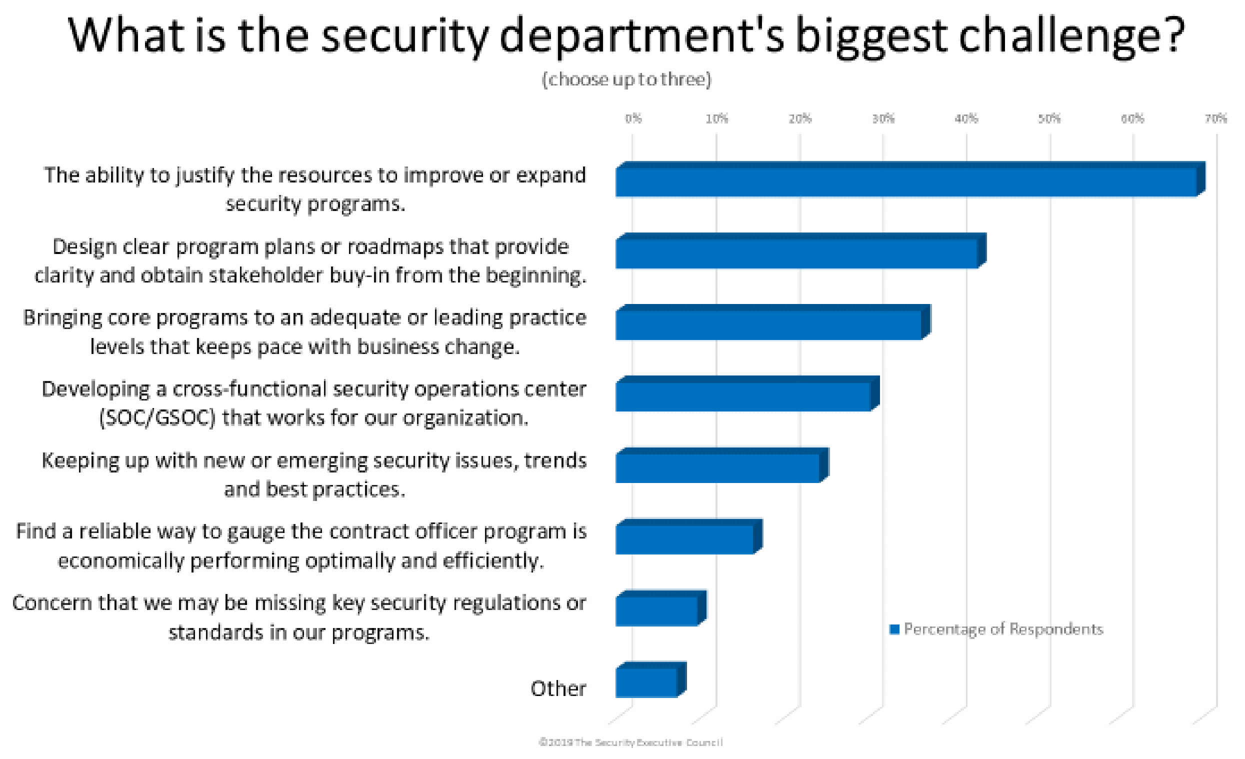
Security Program Strategy & Operations > Strategic Planning/Management >

Security Barometer Results: What is the Security Department’s Biggest Challenge?

By the Security Executive Council

Leading security programs is a difficult job. Not only does the risk environment evolve but the organization's managing business leaders bring their own challenges to the job.

This security barometer sought the top challenges security leaders are facing within their own organization.



Some selected “Other” answers [edited to preserve privacy] include:

- Lack of regulatory clarity
- Consensus decision making at the top echelon
- Embedding security throughout the enterprise
- Gaps silos and disconnects
- Staffing: Labor pool is empty. Cannot get qualified applicants
- Compliance by employees
- Technical issues with access control and CCTV
- Obtaining leadership buy-in to fund critical security infrastructures to protect people and operations
- The ability to integrate technology with different proprietary standards
- Aligning competing security strategies with other security entities within the corporation to into a common framework rather than competing interests
- Budget to operate effectively
- Physical security combined with Cyber, not just a focus solely on cyber
- Achieving corporate goals for operational excellence, continual improvement, and risk mitigation while concurrently delivering on cost reductions.
- Challenge: creating a structured communications framework for strategic messaging/reporting/analysis that incorporates well-defined triggering incidents/events/timelines.
- Meaningful and quantifiable metrics for preventative measures or security systems investments, aimed at the C-Suit level management group.

- The security industry keeping pace with technology and individual security groups being able to implement that technology in a timely manner.
- There is so much information about so much new technology, that it can be quite difficult to navigate through it all to what is operational and pertinent.
- The various agencies have so many rules and regulations that is can be challenging to ensure we are compliant on each issue and in every way.
- Keeping our programs adaptable and not focused on mitigating risk the same way we have for the past 10 years.

We received a lot of insightful commentary from participants in the survey and wanted to share some selected comments [edited to preserve privacy] with you.

- Cybersecurity and anti-money laundering are in the forefront and what general counsels hear. There is a lack of clarity at the legal and regulatory levels which leads to tone deafness and deniability.
- Our organization empowers every business division to be "collaborative," to the extent that security is often challenged to prove why such things as online training prior to international travel is important, especially when compliance isn't enforced. Sometimes decisions at the upper echelon are made by consensus among executives who prefer to please everyone rather than support unpopular programs.
- The security sector evolves slower than the criminal network
- Many of us are challenged with reduced budgets so we have to ensure we use technology efficiently. It's inefficient to have 10 different systems that do not talk to each other. The security industry should develop tech standards to ensure developers deliver products which can be fused to meet an organization's specific needs.
- I think the biggest challenge I have is clearly communicating how our security programs and strategies affect the bottom line and bring value to the company as a whole. Company BUs are always competing for resources. Finding effective ways to measure performance, communicate what we are doing, reflect how it benefits the company either in cost savings, risk avoidance or improved efficiencies is the key to unlocking additional resources or expanding programs.
- It's becoming more difficult to justify additional head count to support increased volume of Security engagements that's supported by the continuous effort of HR, Compliance and Business Continuity programs that advise folks to engage with Global Security for various reasons. In addition, like many corporation's stance of taking on less risk, it requires adhoc enhanced security practices & measures that have yet to mature to fully or partial automation resulting in more manual labor from a security professional.
- There are often other high priorities in our company for resources. This makes it challenging to partner with key stakeholders to gain support for security initiatives. I don't want our company to be in a position of expediting a security improvement because a serious incident has happened, we need to be proactive in addressing potential risks.
- Providing a logical explanation of our organizational value to leadership is our biggest

hurdle. If we can't accomplish this, we're left with just enough funding to provide "security theatre" and not the robust security posture required to protect the company.

- I think most security leaders struggle to quantify resources when metrics are absent or misleading. Even when available (accurate) data exposes gaps or vulnerabilities, business leaders tend to minimize or marginalize the results. Recently, we worked to gain approval for a comprehensive and much needed incident management reporting system. During conversations with the decision maker to gain approval the question was asked, "how often would you have used this in the past year and what benefit would it have served?" The answer was simple, of course, but not reasonable in the decision maker's opinion. The same can be said for spending money to purchase software to reduce the risk of insider threat. When asked, "how many times have we had data stolen, because we need to consider that before we buy anything?" Again, the answer is simple… we don't know how much data has been stolen because we lack the technology to detect it. Sometimes, it requires the cart before the horse to identify (and quantify) the need.
- My organization though leading in technological advancement, lacks the understanding of enterprise risk management where security management could have calculated approaches including safety cultures that can be developed in embedded in to the core business. More and more awareness is required to beat complacency at senior management levels so security management integrates well in to all levels from design, planning and rolled out in to the field.

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/