6

Measures to Maximize Your Corporate Security Strategy & ROI on a Tight Budget

Corporate security is no longer a local concern, but a global one. In today's age of high-speed connectivity and communication, security teams must keep track of distributed offices and facilities on an international scale—24 hours a day, seven days a week, with no window for error. The demand is unprecedented.

This shift increases the need for physical and technological assets that a corporate security operations center (SOC) requires to effectively mitigate any threats to a business and its people. Without a well-equipped SOC, the security of your enterprise remains vulnerable to risk, breach, and loss.

Here's the catch: Demand is higher but budgets are tighter, and many chief security officers are being instructed to rein in costs, while still delivering exceptional service. This raises the key question: How can you do more with less when the threats to your business are growing in number and complexity?

These six preventative measures will help you establish a cost-effective strategy, while maintaining—and even increasing—the effectiveness of your SOC. Though they may not show an immediate ROI, the long term benefits and preparations will prove to be explicit and invaluable over time.

1 Take Stock & Prioritize

Internal organization costs very little, but goes a long way. Begin by creating a detailed inventory of your existing projects and services and their prices and benefits. Ask yourself: What business areas are the recipients of each service? What metrics can we gather to demonstrate their value?

This investment of your time may seem tedious at first, but it will deliver vital insights into how your current budget is being used. Your findings will inform discussions with business leaders about their needs, goals, and priorities, and set in motion many of the following points.

2 Eliminate & Optimize

With a detailed inventory of your organization's services, in addition to stakeholder feedback, an obvious but significant opportunity will present itself: Decommission the services or tools that no longer serve a purpose. This will free up funds for applications that can deliver value, allowing you to provide a more optimal level of protection for new or growing threats.

3 Make New Investments Wisely

If you determine that new products are necessary for the security of your business, be sure your choices are prudent ones. The decision process is three-fold: First, take into account price and functionality. You need to be able to afford a new tool—it's that simple. Second, look for products that leverage the knowledge base of your staff and are compatible with your existing infrastructure. This will save on training, installation, and deployment costs. Third, keep in mind ease of integration. You'll want any new products to exist within your workflow and help improve the efficiency of your day-to-day operations.

Here's the bottom line: Investments are about cost, but they're also about implementation and functionality. Strive for innovation, but never at the expense of practical budgeting and smart strategic planning.

Find the right news before everyone else. The awareness will provide an unprecedented edge.

4 Leverage Social Media

Welcome to the 21st century: Public social media activity is a powerful informer of real-time events before they make headlines. Most corporations today rely upon social media tools, like Dataminr, Brandwatch, NetBase, or Lithium, for early notification of issues that are relevant to their business, from natural disasters near a regional office to terrorist activity at an executive's travel destination.

Find the right news before everyone else. The awareness will provide an unprecedented edge that allows you to respond quickly and more effectively to any threats to your business, personnel, or facilities, no matter where in the world they may arise.

5 Use Cloud-Based Technology

Old school servers are dinosaurs of the past. There's no hardware you need to maintain when using the cloud. Your business programs run at a single, off-premises location and are accessible to employees everywhere as long as they have access to the Internet. If software needs to be updated or replaced, your supplier takes care of that for you, while also providing a secure infrastructure and the latest-available protection for your sensitive business data.

Using cloud-based technology contributes to significant cost-savings when compared to performing the same functions in-house. According to Deloitte's 2016 Global Outsourcing Survey, 59% of respondents use the cloud as a cost-cutting measure, and 57% of respondents also say it enables them to better focus on their core business functions.

Similar to cloud computing, less advanced procedures may not require in-house execution. Training, alarm monitoring, travel security, and other services could be implemented by other firms at a lower price.

If software needs to be updated or replaced, your supplier takes care of that for you

6 Relocate

So much of security work is performed remotely that having a physical space is less of a priority. If your SOC pays a premium for real estate, consider cutting costs by relocating to a less expensive area. You don't need to be restricted to a corporate home office or high-priced city location. You may find a more economical space in a nearby town or a different region of the country.

There's no doubt that corporate security is expensive. But by carefully reassessing your services on an annual basis and making strategic, cost-effective choices, your strategy can deliver the preventive and defensive measures your business requires—without breaking the bank.