Advancing the Mission of Security:
Reduce security risks to acceptable levels, at an acceptable cost.

Rate Your Security Program

Business Alignment

For more than a decade now *business alignment* has been an increasingly common security management objective. Research performed by the Security Executive Council presents an interesting picture of the security profession today, and the security programs that security practitioners have developed.

The research shows the relative percentages of CSOs who have in place or are working on programs that can be characterized as shown below:

- **75% – Core Security Programs:** traditionally common security measures, such as basic policies & procedures, investigations, risk assessment process, workplace violence prevention, awareness programs, reporting policies, access control and so on

- **15% – Sector Security Programs:** business sector-specific security programs tailored for the specific risk or incidents of the industry such as retail, manufacturing, higher education, electrical energy, hospitality, oil & gas, etc.

- **8% – Business Alignment Programs:** where the senior security manager or executive is at the leadership table discussing the security implications of new business strategies and are becoming influential in the business

- **2% – Future Security Programs:** future-focused and very well-aligned with the business, the security leader is involved in its evolution and planning for the emerging risks the horizon and not yet here

Most security programs are not 100% in one category. Usually there are many common core security program elements, along with some that are business sector-specific and some that are specifically aligned with the business and the specifics of each facility type.

 One way to apply these research results is to create a summary chart (a full size example follows on the next page) that can be used to brief both company management and security personnel, and which can serve as a year-to-year metric depicting the continuing progress in security program development. Don't underestimate the value of such a simple presentation of information. In some cases, senior executives have asked, "What would it take to make faster progress and get us all the way up to the top of the chart, where we have better risk mitigation?" Of course, you should be prepared to answer such a question—but not with a barrage of technical details or a large budget request. The most easily understood and most quickly communicated answer is one that characterizes the approach that should be taken to perform the required risk assessments, determine potential business risk impacts, and then incorporate the appropriate people, process and technology measures to reduce security risks to acceptable levels, at an acceptable cost.
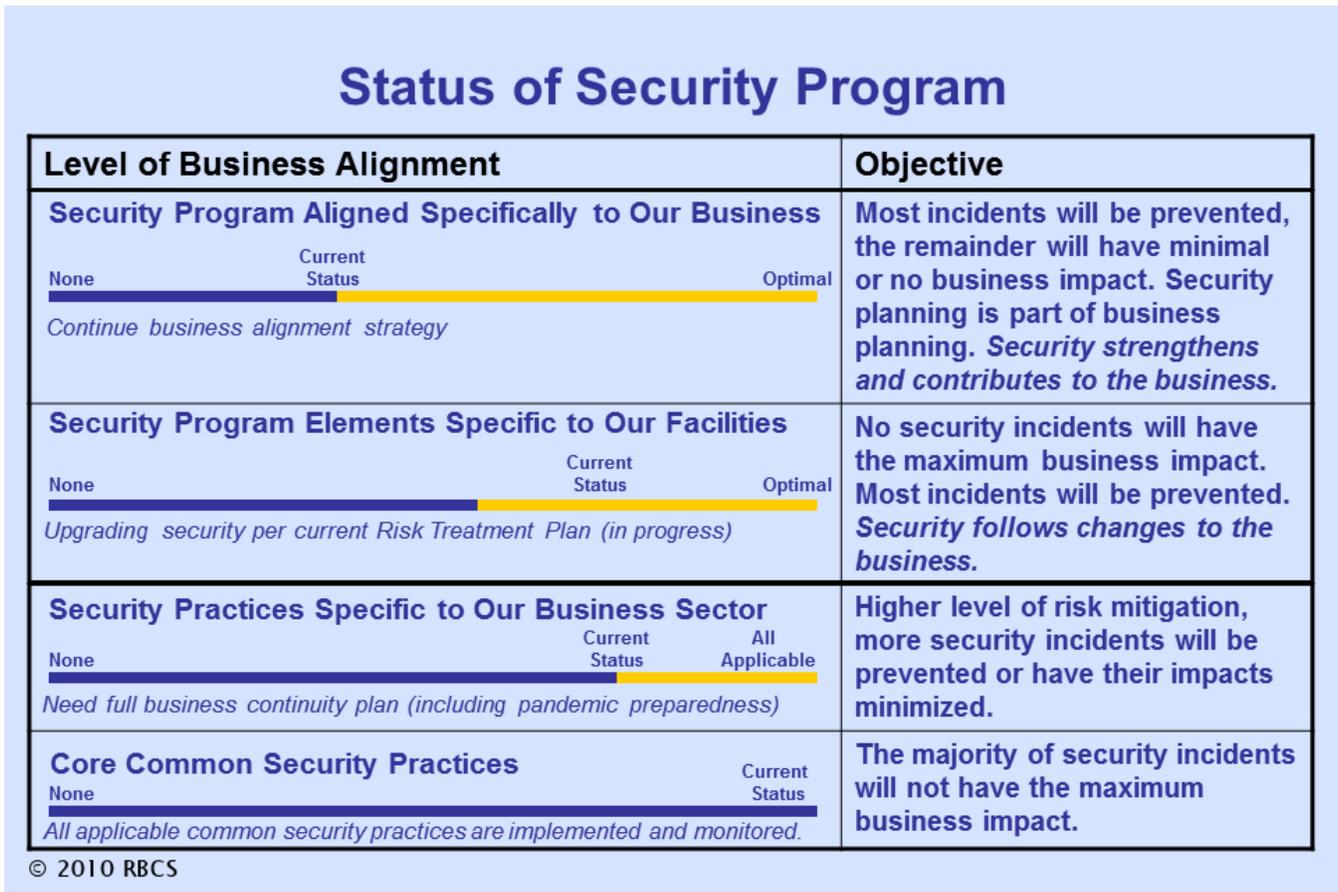
Figure 1. A Example Summary Status Chart Depicting Security Program Development

The chart above is just an example. A similar chart can be used developed to show the status of a comprehensive approach to address any particular risk or provide protection for a category of critical assets. For your own use, you would have more detailed lists and planning materials that identify what you have in place and are monitoring, and a high-level schedule based upon risk priorities of security program elements to put in place going forward.

The four security program categories are also are helpful in identifying additional elements that would advance the business alignment of the security program.

Application Tips

Here are some ways to apply these categories in examining your current security program, and in considering future security program elements.

1. **Create four pages** in a word-processing document (use four pages on a writing pad), and title each page in this sequence:

   - Core Common Security Practices

   - Business-Sector Specific Practices

- Company-Specific and Facility-Specific Practices

- Business Planning and Future Trends

2. **Core Common Security Practices:** Identify and list the security program elements such as card access control, visitor management, security officer patrols, intrusion detection, and so on that are common to most businesses.

3. **Business-Sector Specific Practices:** If any of the core elements you listed are strongly tailored for the specific business sector of your organization, move them into this category.

4. **Business-Sector Specific Practices:** Identify and list the security program elements that are common specifically to your business sector, such as shrinkage reduction (retail) or container screening and tracking (supply chain). Include business-sector security conferences participation.

5. **Company-Specific and Facility-Specific Practices:** Identify and list the security program elements that are specific to your organization or to specific facilities. For example, it may be a practice in some facilities to escort employees that work after hours to and from parking areas. There may be special cash handling procedures in place, or special audits or security reviews. Your security metrics may be very organization-specific.

6. **Business Planning and Future Trends:** Identify and list the ways that you and your security program take into account planned changes to the business and future trends impacting your business. Do you participate in quarterly and annual management planning actions? Do you have metrics that are leading indicators to business changes (that advance warning instead of after-the-fact reporting)? In some organizations the security function is not actively included in business planning, but is simply informed of changes after-the-fact.

This is an exercise that is a cross between list-building and idea-capturing. Typically there are more items in the first two categories than in the second two.

After walking through this exercise once, repeat it again but this time adding onto each page the security program additions or improvements that you think would be valuable. Consult with your security colleagues for those categories where you think outside input would be helpful.

This is not a one-hour exercise. One successful approach has been to go through the list several times, each time writing down what comes to mind quickly, and then putting the work away for a day or more and letting new thoughts occur in between work sessions. Usually the initial ideas—whether many or few—are followed by more thoughts that occur in the days following the first pass at this exercise. Commonly it's a process of iterative development, where first thoughts lead to others, and ongoing thinking expands the original picture.

The primary purpose for this exercise is to provide a way of examining your current security program and considering it from new perspectives and to bring to light opportunities for improvement. *Even without a summary status chart, the concepts and ideas make productive talking points for meetings and on-on-one discussions.*