SORENSEN & WILDER Associates

Specialists in Safety & Security Solutions

A recently terminated employee returns to his place of employment and shoots his ex-supervisor and two co-workers. Fingers point in several directions. Meetings are held. <u>A scapegoat must be found!</u>

Violence erupts in the break room. Several employees, including a security officer, are injured while trying to intervene. Again, meetings are held.

An infant is abducted from its mother's room at a hospital. Fingers point first toward the nursing staff, then at security, safety, and risk management. The safety committee calls a special session. By now, there are numerous "security experts", all well-intentioned, making scores of comments and recommendations, including:

- ***Where was security***
- ***We need more security***
- ***How could security let this happen***
- ***If we only had an access control system***
- ***We need to install closed-circuit television cameras***
- ***Why don't we have an alarm system***
- ***Employees need to be trained to detect and prevent violence***
- ***Why weren't the police notified***
- ***Security should have known…..***

The incidents may be different, but it's the same old story at many companies: Everyone becomes a "security expert" immediately following an incident. Recommendations are plentiful, blame is abundant, and a "quick-fix" is needed to make it appear as though something is being done to prevent future incidents. That's all well and good for the media and the onslaught of concerned citizens demanding that something be done about this problem. However, quick fixes only temporarily mask the problem. The real solution is to be proactive in your approach to security. Identify your weaknesses early through a comprehensive security assessment, and put together a "Plan for Improvement."

The Security Assessment

A comprehensive security assessment must include, at a minimum, the following areas:

SORENSEN & WILDER Associates

Specialists in Safety & Security Solutions

Human Resources

- *In developing it's security program, the company performs an appropriate assessment that includes:*
    - Guidelines for hiring security officers
    - Decisions on contract vs. proprietary security
    - Background screening
    - Criminal history checks
    - Exit interviews

Security Staffing

- *The company has determined appropriate staffing levels for security based on:*
    - Crime in surrounding area
    - Crime in immediate vicinity
    - Crimes on company grounds
    - Police support and availability
    - Types of goods and services offered
    - After hour events
    - Number of perimeter entrances and exits

The assessment must also include:

- Access Control and CCTV technology
- Security Policies and Procedures
- Physical Security Measures
- Access Control
- Alarm Systems
- Parking Lot Security
- Perimeter and Grounds
- Security Training and Education
    - *The company has developed a security training program that:*
        - Is based on established skill sets for:
            - Security officers
            - Other staff
        - Provides security officer training consistent with duties:
            - New employee
            - Annual refresher
            - Certifications
        - Meets applicable:
            - State requirements
            - Federal requirements
            - Industry standards

- Is consistent with mission of the company
- Is appropriate for the position:
  - New employees
  - Annual refresher
- Includes laws of arrest, search, and seizure
- Includes uses of technology
- Tests competency of security staff, non-security staff, and management

- Security Training for Non-Security Staff

- Quality Management
  - *A quality improvement program for security that includes:*
    - A mechanism for determining performance indicators
    - A mechanism for establishing performance standards
    - A system for collecting and evaluating data, including:
      - Incident reports
      - Staff surveys
      - Industry practices
    - An annual evaluation of efficacy of security program
    - A system for setting and revising goals related to security performance
    - Staff Interviews
  - Physical Plant Assessment

- *The security program is designed to include:*
  - Integration into an Information Collection and Evaluation System to analyze data
  - Programs designed to lessen the risk of Workplace Violence
  - Response to emergency situations
  - Response to non-emergencies
  - An access control system to control access into security sensitive areas
  - A system for identification control that includes:
    - Employees
    - Visitors
    - Vendors
    - Guests
  - A traffic control program that includes provisions for:
    - Pedestrian traffic
    - Vehicular traffic

    - Emergency traffic
    - Fleet vehicles
- Adequate security controls in all parking areas
- Confidentiality of sensitive information
- Response to disaster situations:
    - Internal
    - External
    - Off site
- Response to hostage Incidents
- Response to bomb threats
- Media control
- Crowd control
- Response to sever weather conditions
- Response to chemical / hazardous material spills or leaks
- Fire response
- Evacuation procedures
- Utility failures
- Communications failures
- Computer failures

The security assessment should follow the P2T2® approach to security management. For a security program to be truly effective, all facets of the P2T2© system must be fully met. These are:

- **PEOPLE**
- **PROGRAMS**
- **TRAINING**
- **TECHNOLOGY**

In the assessment phase, each of these four areas must be assessed. If the security program in any of these four areas proves to be deficient, then the program itself is weakened, and security is proportionately compromised.

The Plan for Improvement

When performed by a qualified professional, the assessment will open a lot of people's eyes on how security can be improved. It eliminates the "quick fix" approach previously identified, and eliminates the slew of "outside experts" who seem to have all your answers!

SORENSEN & WILDER Associates

Specialists in Safety & Security Solutions

After completion of the assessment, you are left with a long list of recommendations on how your program can be improved. Some are simple, and can be almost immediately implemented. Others are not so simple; they require substantial financial investments, or significant changes in work practices. How can you decide what to do?

The Plan for Improvement (PFI) allows you to develop a "strategic plan" for improving security, based on the assessment outcomes. A good PFI breaks corrective actions into one of four categories:

1. **HIGH RISK / HIGH COST**
   These are corrective actions that need to be taken in order to correct a high risk vulnerability, but require a substantial monetary investment to accomplish. They require planning and budgeting, and may have to be implemented over time.
2. **HIGH RISK / LOW COST**
   High risk / low cost corrections are just what the name implies. These are corrections which can be made to reduce a high risk vulnerability without requiring a large investment. Often, these are work practice adjustments; they are met by changing the way people perform as opposed to a large capital investment. These are changes that should be made as quickly as possible.
3. **LOW RISK / HIGH COST**
   Here, we have improvements that require a large investment of capital, but may not be a value based approach based on the severity of risk. Serious consideration must be given to the value of acting on these, and other alternatives should be considered.
4. **LOW RISK / LOW COST**
   Again, low risk / low cost corrections are just what the name implies. They are corrections which can be made to reduce a low risk vulnerability without requiring a large investment. Again, these are typically work practice adjustments. These changes should also be made as quickly as possible.

Conclusion

A security assessment performed by a qualified security professional will prove to be an invaluable resource. As more and more litigation develops alleging inadequate security, companies are taking their approach to security management more seriously than ever. The days of "doorknob shakers" and "night watchman" may be gone forever. Today's security management demands require a well organized, well managed program that addresses all aspects of facility security, and refuses to be compromised.

SORENSEN & WILDER Associates

Specialists in Safety & Security Solutions

About The Author

Steve Wilder, BA, CHSP, STS *is President and COO of Sorensen, Wilder & Associates (SWA), a safety and homeland security consulting practice based in Champaign, IL. SWA provides services to hospital, long term care facilities, schools, colleges, universities, and industry. For more information, contact SWA at 800-568-2931 or e-mail Mr. Wilder at swilder@swa4safety.com.*