COLLABORATIVE, TECHNICAL AND COMPREHENSIVE SECURITY BUSINESS CONSULTING, LLC

White Paper on "The False Sense of Security and the Associated Risk."

Every industry is plagued with detractors and the security industry is no exception. When you think of this industry you think of extra measures being taken to protect different forms of assets and the financial investments that are made to reach security goals. You also think of security professionals possessing certain levels of competence when implementing security measures. While the security industry tries to reduce/eliminate its unique detractors, it very often overlooks some of the key causes of security vulnerabilities. These vulnerabilities are often caused by personal goals to remain employed and the need to turn a profit; ultimately, transferring risk to the unaware stakeholder.

> *"The progression of error has become the rite of passage!"*
> *Calvin James Daniels*

Personnel Skill Sets

How do you know if you have gained beneficial advice that eliminates/lowers security risk? The security industry consists of sub-trades that are comprised of Information Security, Personnel Security, Physical Security, Management Security and Security Officers (formally labeled "Guards"). Each of these sub-trades make unique contributions to the security industry. Information Security professionals are skilled in the field of protecting an organization's intellectual property (both tangible and intangible). Personnel Security professionals are skilled in the field of background investigations and assist Human Resources during employment evaluations. Physical Security professionals are fluent in designing Physical Protection Systems and in creating response plans. Management Security professionals possess the skill sets that help develop and promote organizational security requirements. Security Officers possess the skill sets needed to enforce security requirements and aid response plan efforts. With so many sub-trades in the industry the question could be asked "Are there specialist who possess experience within each sub-trade?"

The competence level of security professionals is often highlighted by tenure, certifications and training courses. Employee tenure is gained when personnel remain employed at an organization for an extended period of time, usually performing the same tasks. Without consistent training, tenure employees are normally not exposed to industry standards and very

often utilize skill sets that have been gained by on the job training. This on the job training is not frequently evaluated to see how it conforms to industry standards.

Certifications within the security industry are created by organizations that focus on the personal growth of sub-trade professionals. In some cases, certifications are misused in an effort to gain employment or increase profit. An example of this would be when a management security certification is used to promote physical/information security experience; management security, physical security and information security are very different. Management Security is centered on promoting security requirements in an effort to reach security goals. Physical Security is centered on designing and implementing Physical Protection Systems. Information Security is centered on protecting electronic networks and access to these networks. Misapplied skill sets can contribute to unique security vulnerabilities, which often exposes stakeholders to higher levels security risks.

Installation/Monitoring companies also contribute to industry detractors. When the workforce of installation/monitoring companies is evaluated you often find a skill set lapse that contributes to security vulnerabilities. Vulnerabilities are often created because installation/monitoring companies often do not focus on the science of risk management and very often only focus on the installation of components (which drives cost). This is evident when you evaluate the hiring practices of these installation/monitoring companies and the skill sets needed to fill positions within their workforce.

The industry also is filled with training courses for each sub-trade. These courses often last days or weeks; and can be taken online in most cases. The detractor associated with training courses is that they do not take the place of experience that is gained through industry exposure. A one day or two-week training course could never provide a security professional with the experience that is needed to manage a security program. Position skill set requirements and experience are two factors that are the backbone of the security industry.

Risk Transfer

As a stakeholder have you conducted a thorough security risk assessment?

Stakeholders are always interested in cost savings and decision makers often want some form of return on investment when it comes to investing in security measures. Installation/Monitoring Companies offer services that are 'low cost' and that are less intrusive on organizational operations. These same installation/monitoring companies offer services that can be completed over the phone and in 'easy steps' which seems to attract the unaware stakeholder. When did the security of critical/valuable assets become easy? Can $1K of an annual security investment properly security $1M of assets without transferring high levels of risk to stakeholders?

There are numerous pitfalls that exist within the security industry. These pitfalls contribute to design flaws and administrative oversight which both are the results of a lack of sub-

trade knowledge. This lack of sub-trade knowledge is often passed on to stakeholders and exposes them to new forms of liability. An example of this liability transfer exists when installation/monitoring companies do not understand the needs of clients and provide profit driven security system that do not reduce security risks.

Another liability that stakeholders are faced with is cost exposure as a result of a security liability transfer. Cost exposure is created when installation/monitoring companies make stakeholders liable for design flaws, leave assets exposed (for up to six months), provide limited warranties, limit their system monitoring liability and when they implement legal terms that stakeholders are not familiar with. Many false alarms are linked to design flaws and poor space planning. Costs associated with false alarm response is transferred directly to stakeholders. Installation/Monitoring Companies have also exposed stakeholders to additional risk by implementing grace periods that allow them to isolate system problems within six months. Six months is a long period of time to have vulnerabilities within a Physical Protection System. Do you know what is your security system outage tolerance?

Another cost exposure that is transferred to stakeholders exists with warranties. Most installation/monitoring companies give a 90-day warranty on the components that they install; however, the manufacturers of these components give a 12-month factory warranty on the components they produce. The applied 90-day warranty substantially reduces the liability of installation/monitoring companies. New component and service call costs are transferred directly to stakeholders.

Most installation/monitoring companies have established liability policies that limits their liability when it comes to system monitoring. These companies have implemented a $500 clause that limits their liability during the system monitoring effort and have implemented response clauses which gives them the ability to decide if/when alarm responses are needed. As a stakeholder do you know if you have given an installation/monitoring company the ability to make decisions for you that contradicts your asset protection/loss prevention goals? Installation/Monitoring Companies have also adopted legal statutes from other states that restrict the legal rights of stakeholders. As a stakeholder do you know the 'color of law' that governs the operation of your security system? or the 'color of law' that installation/monitoring companies have adopted?

Way Forward

As a stakeholder how do you overcome the risk associated with personnel skill sets and the unknown risk that has been transferred from installation/monitoring company's? The first step that should be taken to overcome these issues is to identify what are the overall goals of your security program. After the goals of your security program are identified, you should then

identify if in house personnel possess the skill sets that are needed to conduct in-depth risk assessments. Stakeholders must remember that most security professionals do not have experience within the numerous security sub-trades to conduct a detailed risk assessment. If in house personnel do not possess certain security skill sets you must seek outside help; the more critical (valuable) the asset, the more urgent the need.

Fortunately, there are industry specialist available that can help you identify your security risks and that can provide you with recommendations that help mitigate these risks. These Industry specialists are referred to as 'Security Consultants.' Security Consultants are committed to promoting positive changes within the security industry. CTCH's Lead Consultant is board certified through the International Association of Professional Security Consultants (IAPSC) and the American Society for Industrial Security (ASIS) International. These certifications culminate 22 years of experience and exposure within the security industry. CTCH's business model is centered on 'listening' to clients, identifying true security risk and providing clients with recommendations that help them implement security measures that reduce risk (with a return on investment). If CTCH can help you meet your security goals, contact us. We look forward to working with you.

References

Industry Observation

Installation/Monitoring Company websites (Legal/Liability polices)

Installation/Monitoring Company Employment Pages