



PRIVATE SECURITY

In every interaction with members of the public, security guards engage in risk. Unlike most other vocations, it is often the very risk of bodily injury that causes workers in the security field to take action, and this requires that judgments be made on the fly in changing and sometimes confusing situations. In virtually every lawsuit against a security company, the thinking and particular actions of the security company employee are questioned. Their employers are exposed to liability by virtue of the master and servant relationship. Much can be done to insure that when a security guard is called upon to respond, he will do so in a way that limits the risk of injury - because of either inadequate response or overzealous response - to members of the public, himself, and his employer.

Private Security

Risk Management

C&F RISK ENGINEERS UNDERSTAND YOUR BUSINESS

Since 1822, Crum & Forster has successfully anticipated what's next. Our insurance policy is our promise to help you - the policyholder - in the event of a loss. It gives you a future benefit that you can count on. But C&F offers something more. Our Risk Engineers can help your operation right now.

Before you ever encounter a claim, our Risk Engineers can meet you and identify actual and potential loss sources. We'll conduct a thorough study of your company that includes exposures, hazards and accident trends. Together we'll review your current loss prevention efforts, physical location, loss information and other business records to pinpoint fundamental loss causes. Then we'll create an action plan with practical recommendations to strengthen existing safety programs. We can maintain an ongoing review of it to evaluate progress and effectiveness. We can even conduct a legal exposure review of your company's agreements. Everything we do is aimed at putting into place an effective loss control strategy that works consistently over time to lower your operation's risk of loss.

Our highly specialized Risk Engineers are strategically located throughout the country and have the experience, training and professionalism to provide risk management solutions to meet your business needs and contribute to your success. They have on average more than 20 years industry experience, many with roles dedicated to safety and training. And we invest not only in our insureds, but in the industry. We are members of and participate in many state associations and regularly present at industry conventions and events. These connections and experience are invaluable, and are key in assisting you in developing and deploying a modern, up-to-date safety and training program.

Our solutions are both innovative and established. Whether it's Accident Event Recorders (AERs) to help identify vehicle accident causes and tailor safety training, digital tracking systems, or online video training to assure OSHA compliance, we bring you the latest technology. Matched with the experience of our Risk Engineers, your operation benefits from the engineering awareness built over a lifetime and cutting edge safety science.

Know the employee

Employment background checks are now the norm, and they are especially useful when the employee can be called upon to contain or repel physical force exerted by members of the public. If a security company employee interacts with a member of the public and injury results, can it be said that the injury is something that could have been foreseen by his employer? With background checks, an employer is able to answer the question, and when done properly, an employee background check can help avoid liability for negligent hiring.

State and local regulations may affect how and when a potential employer performs a background check. These regulations generally control how notice is to be given to the applicant, how confidential information is to be handled, when and how written permission to perform the background check is to be obtained from the applicant, the scope of the information to be obtained, and how it is used once obtained.

The scope of the background information sought is important. In 2012, the Equal Employment Opportunity Commission published Enforcement Guidance on the Use of Arrest and Conviction Records in Employment Decisions under Title VII of the Civil Rights Act of 1964. The document sets forth standards for the use of prior criminal convictions in hiring decisions and makes clear that what is relevant in one employment context might not be relevant in another. It seems reasonable that not every criminal conviction suggests that a potential employee is prone to violence. The definition of a crime of violence used in the U.S. Code is helpful. 18 U.S.C. Sec. 16 states:

The term "crime of violence" means—

(a) an offense that has as an element the use, attempted use, or threatened use of physical force against the person or property of another, or

(b) any other offense that is a felony and that, by its nature, involves a substantial risk that physical force against the person or property of another may be used in the course of committing the offense.

The same might be said of the potential for employee theft and a prior conviction of a theft or burglary offense.



Private Security

Risk Management

Know the employee (continued)

State laws control to some degree what criminal activity can and cannot be used in making a hiring decision. Some states do not permit consideration of arrest at all. Some do not permit use of active prosecutions that have not yet resulted in conviction. It's important to know what is permissible in the state in which the security company operates. The hiring of a qualified background screening company can help guide security company employers on what types of activity can be considered in their hiring decisions.

Note also that in the U.S., there are at least 51 different criminal jurisdictions. What shows up on a California state criminal records check is unlikely to show up on a Florida state criminal records check. This underscores the importance of the multijurisdictional, comprehensive criminal records check. Hiring an applicant that has a clean New Mexico record two months after he is released from serving an 18-year sentence for murder in Arizona is something that can be easily avoided when the right steps are taken.

Use of force training and written company policy

The vast majority of lawsuits against security company employers center on the use of force by the security employee. Not every security company employee is authorized to use force, or even to touch a member of the public, as these things frequently depend on customer needs and employee qualifications. Some security company employees are licensed to carry weapons and are not prohibited from using them (e.g., off duty police officers). But every security company employee should be trained in the use of force so that it is deployed properly when authorized. An example of a use of force continuum for police officers, published by the National Institute of Justice, follows:

Officer Presence

- No force is used. Considered the best way to resolve a situation.
- *The mere presence of a law enforcement officer works to deter crime or diffuse a situation.*
- *Officers' attitudes are professional and nonthreatening.*

Verbalization

- Force is not physical.
- *Officers issue calm, nonthreatening commands, such as "Let me see your identification and registration."*
- *Officers may increase their volume and shorten commands in an attempt to gain compliance. Short commands might include "Stop," or "Don't move."*

Empty-Hand Control

- Officers use bodily force to gain control of a situation.
- *Soft technique. Officers use grabs, holds and joint locks to restrain an individual.*
- *Hard technique. Officers use punches and kicks to restrain an individual.*

Private Security

Risk Management

Use of force training and written company policy (continued)

Empty-Hand Control

Officers use less-lethal technologies to gain control of a situation.

- *Blunt impact.* Officers may use a baton or projectile to immobilize a combative person.
- *Chemical.* Officers may use chemical sprays or projectiles embedded with chemicals to restrain an individual (e.g., pepper spray).
- *Conducted Energy Devices (CEDs).* Officers may use CEDs to immobilize an individual. CEDs discharge a high-voltage, low-amperage jolt of electricity at a distance.

Lethal Force

Officers use lethal weapons to gain control of a situation. Should only be used if a suspect poses a serious threat to the officer or another individual.

- *Officers use deadly weapons such as firearms to stop an individual's actions.*

A variety of non-firearm weapons are capable of exerting lethal force or sub-lethal force that produces severe injury (extensible metal batons, for example). Consequently, a written weapons policy is a key tool for limiting the unauthorized use of force. Prohibition of personally owned non-lethal weapons can have a great impact on employee behavior, and it also puts the security company employer in a much more defensible position when a member of the public is injured by an employee's personally owned, prohibited non-lethal weapon.

Command communication and supervisory oversight in emergencies

The media spotlight on multiple shooting incidents in shopping areas and melees after sporting events often emphasizes the actions of security and first responders. Whether onsite security guards participate in the response to such an incident depends greatly on post orders; indeed, security's only duty might be to call 911. But where command communication falls within the responsibility of security personnel, up-to-date training and clearly defined roles can have a great impact on outcomes.

For all jobs where participation in emergency response falls within the duty of security personnel, each shift should have a defined Incident Commander, who identifies and assesses the problem, a defined Incident Command Post, and a defined Staging Area. Interoperability of communications (the ability of security personnel to hear and communicate with law enforcement personnel) is also valuable in emergencies.

Incident investigation and reporting

The incident investigation and report is essential not only to law enforcement, but to the defense of the security company employer if it is sued for bodily injury or property damage. When taking a statement, it may be appropriate to draw the witness's attention to other information that appears to conflict with what the witness is saying and the taker of the statement is entitled to indicate that a court may find a particular piece of information difficult to accept. But if the witness maintains that the information is accurate, it should be documented in the investigation file.

In every investigation, the following information should be obtained, while never admitting liability to any party with whom there is contact:

Incident investigation and reporting (continued)

The Witness

- Their full name
- Their date of birth
- Their gender
- Their address
- Their occupation
- The identity of their “anchor contact,” a person who will always know the whereabouts of the witness so that contact can always be re-established.

Incident Facts

- When (on what date and at what time of day or night) did the incident take place?
- Where was the witness at the time? What was he or she doing?
- Who was the witness with at the time of the incident?
Identify each person as best they can, e.g. give:
 - Their name
 - Their date of birth
 - Their relationship with each person there, e.g. neighbor, brother, friend
 - If they did not know them, any identifying features or unusual characteristics.
- What did the witness see?
- What did each person present say or do?
- What happened as a result of the incident?
- Was any damage caused or harm suffered?
- What did each person present say or do?
- If so, who or what caused it? Include as much identifying information as possible about those involved including:
 - Any names used
 - Any other identifying characteristics such as facial hair, scarring, etc.
 - Any vehicles used, including make, model and markings
 - Any weapons or other instruments used
- What did the witness and other persons present do immediately after the attack?
- Are there any other witnesses to the events that have not previously been identified? If so, do you know how we can contact them?

Effect of the incident on the victim

- What was the state of health of the victim prior to the incident?
- What was the effect of the incident on the victim? Did the victim suffer physical harm?
- If the victim suffered physical harm, provide details of when, where and what harm was suffered.
- Did the victim seek any medical or other treatment? If so, from whom? What was the nature and cost of the treatment?
- What ongoing treatment has been recommended?

Private Security

Risk Management

Contractual risk management

At its most basic, the contract and post orders agreed to between a security company and its customer provide a clear understanding of the work to be performed, and hence the duty owed to the customer and the public. The location or geographical area where the work is to be performed, the number of security guards, whether they are able to interact or touch a member of the public – or only observe and report to law enforcement – should all be addressed.

Security companies are frequently asked to defend and indemnify their customers – the corporations and individuals for whom they provide security services. The variety of indemnity agreements that security companies are asked to sign by their customers is notable.

- A limited indemnity agreement typically mandates that the security company indemnify the customer for the security company's direct negligent acts while performing agreed upon duties. The security company is not responsible for the passive or active negligent acts of its customer (for example, requesting an insufficient number of security personnel after developing its own security plan). Sometimes limited indemnity agreements restrict the security company's exposure to the proceeds of its insurance policy.
- In an intermediate indemnity agreement, the security company agrees to indemnify its customer for damage caused in whole or in part by the security company's negligence, and indemnity can extend to covering the negligence of the customer.
- A broad indemnity agreement extends all liability arising out of an incident, whether caused by the security company's own employees or employees of the customer, and whether the damage was caused intentionally or negligently. Broad indemnity agreements are to be avoided.

Employee licensing

A growing number of states mandate licensing of security guards after completion of state-approved training. Some states prescribe the content of security guard training, but do not mandate that every person working in the state complete the training and obtain a security guard license. Some states require security guard training only if the guard is to carry a weapon. It is important that a security company employer be familiar with the licensing requirements for the states in which it operates.

The states that mandate security guard training and licensing frequently set a minimum age and require that applicants for a license undergo a criminal records check and provide fingerprints. Some criminal convictions will render an applicant ineligible for a license. In some circumstances, the hiring of a person who lacks a needed license can support a finding of negligent hiring.

Private Security

Risk Management

Any users of these training materials signify their understanding of and assent to the following: These materials are not intended to reduce a user's burden in training personnel. Each user engaging in such training activities bears full responsibility for his, her or its own training, education and accompanying materials to ensure both the accuracy of the training and materials and compliance with all applicable local, state, and national laws and regulations. These materials are not intended to replace any training or education that users may wish or need to provide to their personnel. The companies of Crum & Forster, their directors, officers, employees, technical personnel, advisors, consultants, agents and staff (collectively, "Representatives"), shall not be held liable for any improper or incorrect use of these training materials and assume no responsibility for any use of them. In no event shall Crum & Forster or their Representatives be liable for any damages however caused and under any theory of liability arising in any way out of the use of these training materials, even if advised of the possibility of such damage. This disclaimer of liability applies to any damages or injury. Information in the training materials may include technical inaccuracies or typographical errors. The companies of Crum & Forster or their Representatives may make improvements and/or changes in the products, services and/or job aids described in these materials at any time without notice. These training materials are provided 'as is' without warranty of any kind, either expressed or implied, including, but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement. Some jurisdictions do not allow the exclusion of implied warranties, so the above exclusion may not apply in such jurisdictions. Neither the companies of Crum & Forster nor their Representatives warrant or make any representations regarding the use or the results of the use of the materials, or the accuracy, adequacy, completeness, legality, reliability, or usefulness of the training materials.



This material is provided for information purposes only and is not intended to be a representation of coverage that may exist in any particular situation under a policy issued by one of the companies within Crum & Forster. All conditions of coverage, terms, and limitations are defined and provided for in the policy.

The C&F logo, C&F and Crum & Forster are registered trademarks of United States Fire Insurance Company.

Version 2.0 2016.05.18