



IAPSC FORENSIC COMMITTEE

A FORENSIC SECURITY CONSULTANT'S FRAMEWORK

for Assessing Threats and Developing Standard of Care Opinions

Karim H. Vellani, CPP, CSC and Tina S. Kristof, Esq.

October 2026



IAPSC

International Association of
Professional Security Consultants

Table of Contents

ELEMENTS OF NEGLIGENT SECURITY	3
The Four Elements.....	3
Standard of Care Opinion Development.....	3
Research and Evidence-Based Practices.....	5
THE THREAT ASSESSMENT	6
Elements of a Threat Assessment.....	6
Actual Threats	6
Inherent Threats.....	7
CONCLUSION	8
BIBLIOGRAPHY/REFERENCES	9
AUTHORS	10
ABOUT THE IAPSC	11

ELEMENTS OF NEGLIGENT SECURITY

When a customer, visitor, or employee is hurt in a criminal attack on a business's property, the business owner can be sued. These claims, known as negligent security lawsuits, are a form of premises liability. Settlements and verdicts can reach millions of dollars. Victims often sue the property owner. Security contractors, property managers, and surveillance vendors are often named in the lawsuit in addition to the owner.

The Four Elements

To prevail in such a lawsuit, the plaintiff must prove duty, breach, causation, and damages.

Duty turns largely on foreseeability. Courts generally use one of three tests:

- **Specific harm:** The specific harm test (also called the imminent harm test) is the narrowest of the three foreseeability tests. It asks whether the business knew, or had reason to know, that a particular person or group faced a particular, probable harm. General knowledge that crime happens in the area, or even at the property, is not enough. A plaintiff typically must show that the business actually knew of a specific, likely threat to a particular person, had time and means to respond, and failed to act reasonably before the attack.
- **Prior similar incidents:** There is evidence of comparable crimes at or near the property. Jurisdictions differ on how similar, how recent, and how geographically close those incidents must be.
- **Totality of the circumstances:** Under the totality of the circumstances test, courts look beyond prior similar crimes to a broader array of conditions. Relevant evidence might include prior dissimilar crimes, the level of crime in the neighborhood, criminal activity at other business locations, the location and visibility of the business on the property, security personnel, cameras, lighting, property maintenance and physical barriers, and crimes at other places in the area.

Breach means failing to provide adequate security against foreseeable crime, failing to inspect, or failing to warn of a known hazard. No comprehensive law prescribes what "adequate" means, so juries rely heavily on expert testimony about the standard of care.

Standard of Care Opinion Development

The standard of care is the level of care that a skilled, careful person in a certain field or business would use in the same situation. If someone falls below that level, they have breached their duty. In security, this level is not the same everywhere or forever. It depends on the place, how likely crime is, and changes in technology, crime patterns, and research on what works to prevent crime.

As described by Kristof (2025), Forensic Security Consultants base their standard of care analysis on five sources: industry consensus standards, community practices, self-imposed standards, mandatory standards, and learned treatises. Each has limits.

- Industry consensus standards bind a defendant only if it adopted them. To determine if the defendant adopted an ASIS standard, for example, the Forensic Security Consultant might ask the following:
 - a. Do the defendant's written policies, procedures, and manuals cite an ASIS standard or mirror its requirements?
 - b. Do the security services contracts and vendor agreements require compliance with an ASIS standard?
 - c. Do the defendant's corporate designees testify that it adopted an ASIS standard?
 - d. Do the defendant's insurance policies or lender agreements require compliance with an ASIS standard?
- Community practices are the prevailing practices commonly seen within a specific geographic region or industry sector that, while not formally codified, reflect a shared understanding of what is reasonable or expected, though they are not always grounded in evidence-based research. For example, video surveillance at garden-style apartments is common, but research has not shown it prevents violent crimes.
- Self-imposed standards are the written policies, procedures, and guidelines an organization chooses to adopt. They are not legally required, but they show what the organization itself considered necessary for reasonable care.
- Mandatory standards are legally binding requirements set by statutes, ordinances, or codes. For example, a property code that requires deadbolts on apartment entry doors makes the deadbolt mandatory, and an owner who leaves a door without one has failed a legal requirement, not just a best practice.
- Learned treatises are scholarly books, peer-reviewed articles, and other authoritative writings that courts may treat as persuasive evidence of what is known in a field; for example, a recently developed violent crime typology, which classifies violence as predatory, dispute-related, targeted, or risk-detached along a continuum from most to least preventable, gives a Consultant a published framework for supporting an opinion on whether a subject incident could have been prevented.

Research and Evidence-Based Practices

Evidence-based practice means grounding standard of care opinions in what research shows works, not only in what is commonly done. The distinction matters because a measure can be widespread, intuitively appealing, and still unsupported by the evidence. Security Officers are a good example. Security Officers are a common and costly countermeasure, yet Perez et al. (2025) report that research has found little evidence they reduce crime. They cite a study of U.S. shopping centers that found no significant evidence Security Officers reduced violent, property, or disorder crimes (Lee et al., 1999), and a study finding that "observe and report" patrols were ineffective (Fabbri & Klick, 2021). They also note that Security Officer findings parallel the research on police patrol, where effects diminish after initial implementation and typically last only six to eight weeks (Novak et al., 2016; Ratcliffe & Sorg, 2017; Rydberg et al., 2018). They further note that deterrence-oriented patrols may help with disorder and property crime but have little to no impact on violent crime. For the Forensic Security Consultant, the lesson is to ask what the research says a measure can achieve against the specific type of crime at issue. This applies equally when opining that a measure was required and when opining that its absence would have prevented the incident. Where such research exists, it should shape the opinion. Where it does not, the Consultant should say so plainly.

Causation requires that the deficiency was a substantial factor in the harm. The plaintiff need not prove the crime would certainly have been prevented, only that the deficiency more likely than not contributed to it. Damages include economic and noneconomic losses, and punitive damages are possible for gross negligence.

THE THREAT ASSESSMENT

Many Forensic Security Consultants follow the IAPSC Forensic Methodology, which has three parts: evidence review, security risk assessment (threat and vulnerability), and analysis and opinions. The analysis is retrospective, limited to conditions up to the date and time of the subject incident. Consultants typically opine on three topics: foreseeability, standard of care, and preventability. We discussed standard of care above. For preventability, Vellani, Kaufer, and Army (2024) developed a framework that places predatory, dispute-related, targeted, and risk-detached violence on a continuum from most to least preventable.

Elements of a Threat Assessment

The Forensic Methodology defines a threat assessment as “an evaluation of events that can adversely affect operations and/or specific assets.” The Consultant must consider two categories of threat: actual and inherent.

Actual Threats

Actual threats are the crime history at the subject property, based on data reflecting actual crime. The Methodology treats this as the quantitative element of the threat assessment.

- **Records.** The available crime records depend on the police jurisdiction serving the property. Calls for Service and offense lists are the most common record type used at the beginning of a crime risk analysis. Its accuracy varies by jurisdiction, and changes to incident management and dispatch systems can affect accuracy even within one jurisdiction.
- **Validation.** Calls for Service and offense lists should not be used alone. Offense/Incident Reports are necessary to validate the Calls for Service data on three elements: the crime type, the crime location, and whether a crime actually occurred. In many jurisdictions Calls for Service alone is insufficient on all three. The Forensic Methodology makes clear that Offense/Incident Reports are required to assess the crime risk at a property.
- **Time frame.** The consultant may consider relevant crimes on the subject property for the three to five years before the date of the incident.
- **Immediate vicinity.** The consultant may consider relevant crimes in the immediate vicinity over the same period. No single definition of “immediate vicinity” or “neighborhood” exists, and what can be evaluated often depends on the law enforcement agency’s software and staff capabilities. The Methodology also recognizes that “criminology studies and related research have generally found that crime in the area may not be relevant to the subject property.”

- Offender-victim relationship. The consultant may consider whether the relationship was interpersonal, domestic, targeted, or otherwise.

The Forensic Methodology frames each of these as considerations “deemed relevant by the security expert.” That leaves the selection of relevant crimes to the consultant’s judgment, so the basis for that judgment should be explained in a report, if written, and during deposition and trial testimony.

Inherent Threats

Inherent threats are the crime risk at the property as determined by the Forensic Security Consultant. The determination rests on four sources: the property’s characteristics; the consultant’s research and experience in similar environments; information gathered through discovery; and a site inspection, if one is conducted. This element is not tied to the property’s own crime history. It addresses the risk that comes with the type of property and operation. A bank, for example, carries inherent robbery risk, and a healthcare facility carries inherent risk of patient-on-staff assault.

CONCLUSION

Negligent security cases can turn on the quality of the Forensic Security Consultant's opinions, so those opinions need a sound foundation. Three points deserve particular care.

First, build the standard of care deliberately. It is tempting to point to an industry guidance document, such as those published by ASIS, and call it the benchmark. An industry consensus standard generally holds a defendant to account only when there is evidence that the defendant voluntarily adopted it into its own policies, practices, or procedures and then failed to follow it. Before citing an ASIS standard against a defendant, confirm whether that adoption actually happened. Where it did not, the standard may still be useful context, but it is not the defendant's yardstick. The same discipline applies to the other sources. Mandatory standards bind by law. Self-imposed standards depend on what the organization itself adopted, and some jurisdictions give them limited weight. Community practices should be checked against available research rather than assumed to work.

Second, validate the crime data before relying on it. Raw crime counts and Calls for Service are a starting point, not a finding. The IAPSC Forensic Methodology is clear that Offense/Incident Reports are necessary to confirm those three elements. Pulling the reports takes extra effort, but it makes the threat assessment far more defensible.

Third, support your opinions with evidence-based practices. Because a security measure that is common or intuitive is not necessarily one that works, Consultants who anchor their standard of care and preventability opinions in evidence-based research give courts opinions that are more reliable, more defensible, and more useful to the fair resolution of the case.

Security programs are judged on what was foreseeable and what was reasonable at the time of the incident. Consultants who trace each standard to its source, confirm adoption where it matters, and verify their data against Offense/Incident Reports give judges and juries opinions they can trust.

BIBLIOGRAPHY/REFERENCES

- International Association of Professional Security Consultants. (2025). Forensic methodology (Rev. January 23, 2025). <https://www.iapsc.org>
- Kristof, T. (2025). Security liability. In K. Vellani, Strategic security management: A risk assessment guide for decision makers (3rd ed.). CRC Press. <https://a.co/d/06kTxdk2>
- Perez, K. L., Kaufer, S., Silva, M., Vellani, K., & Zajic, A. W. (2025). Place management for apartment crime prevention (EBSP-25-02). <https://iapsc.org/ebsp/>
- Vellani, K., Kaufer, S., & Army, C. (2024). A refined violent crime typology: Analyzing and solving specific types of violence. ASU Center for Problem-Oriented Policing. <https://popcenter.asu.edu/content/recommended-readings-problem-solving-tools>

AUTHORS

Karim Vellani, CPP, CSC

Karim Vellani is a security consultant at Threat Analysis Group, LLC. He holds Board Certifications in Security Management (CPP) and as a Certified Security Consultant (CSC). He has more than 30 years of expertise in security management, crime analysis, and forensic security consulting. Karim earned a bachelor's degree in Criminal Justice with a focus on Law Enforcement and Police Science and a master's degree in Criminal Justice Management. He is the author of Applied Crime Analysis, Strategic Security Management, and Unraveled: An Evidence-Based Approach to Understanding and Preventing Crime, and has contributed to various other security publications and journals. He can be reached at (281) 494-1515 or kv@threatanalysis.com.

Tina S. Kristof, Esq.

Tina Kristof is an attorney in Houston, Texas. She earned her J.D. with a Health Law Specialization from Boston University School of Law, and her B.A. from the University of California at Los Angeles. Tina is admitted to practice law in Texas, California, and Massachusetts. She is a Consultant specializing in Workplace Violence Prevention in healthcare environments. She previously served as Assistant General Counsel for Walmart Stores, Inc., Staff Attorney at Donoghue, Barrett & Singal, and Health Policy Manager at Wellpoint Health Networks. Tina authored two research papers for the IAHS Foundation and a book chapter on Security Liability.

ABOUT THE IAPSC

Founded in 1984, the International Association of Professional Security Consultants (IAPSC) is a widely recognized and respected association committed to establishing and maintaining the highest standards for security consultants in the industry.

IAPSC members are independent, non-product affiliated consultants who are required to meet strict educational, experience, and practice requirements, ensuring that they uphold the IAPSC code for professionalism and ethical conduct. For more information, to find an IAPSC security consultant, or to become a member of the association, visit www.iapsc.org.