A FEW TIPS FOR A MORE SECURITY-CONSCIOUS LIFESTYLE

By Judge Henry E. Hudson and John Muffler

The intensity of litigation in today's world is unprecedented. An unfortunate byproduct is the potential for retribution against lawyers and judges. When it occurs, the aftershock touches the lives of every member of the legal community. News coverage of assaults on judges, prosecutors, and practicing attorneys typically engenders moments of introspection—what if it happened to me—or, worse, my family? Unfortunately, when tragedy strikes, it is too late to adopt a protective strategy. Interest in security reaches its peak in the days immediately following an act of revenge against a lawyer or judge. Regrettably, as memories fade, so does interest in security.

Project 365, developed by the U.S. Marshals Service, in league with the Administrative Office of the U.S. Courts and the Judicial Conference Committee on Judicial Security, is designed to foster security awareness 365 days a year. It strives to promote a security-conscious lifestyle at work, at home, en route, and even while on vacation. In today's high-stakes litigation, the emotions of litigants and affected persons sometimes reach a flashpoint. Acts of retaliation are unpredictable, so every member of a judge's or lawyer's staff and family should be trained to react in a crisis. This preparation should include periodic training exercises to ensure quick response. Remember, even momentary chaos can give a potential assailant the edge.

Disorder in the Court—Remember Your ABCs

Disruptive incidents in the courtroom can take many forms—from an obstreperous observer in the gallery to a violent prisoner charging the bench. Each such incident may require a different response by security personnel. But, in the heat of the moment, courts rarely have the opportunity to instantaneously craft a protective strategy. That's why advanced planning is critical. The plan should be simple with firmly established practices and procedures.

Absent the most extraordinary of circumstances, such as protecting life from imminent danger, attorneys, judges, and court staff should never attempt to intervene. Court security personnel are trained to handle such incidents and the trial judge's first task is to summon them immediately. If the courtroom is equipped with an emergency alarm, it should be activated without delay. Otherwise, notification should be made by telephone if it is safe to do so. The presiding judge should next determine if evacuation or protective cover is the most feasible option. Unless the situation is prohibitively dangerous, exiting the courtroom is the preferred action unless directed otherwise by the judge or a security officer. Doing so will deescalate the situation and also preclude the judge from becoming a witness.

Always remain in a secure location until authorized by security personnel to return to the courtroom. If directed to take cover, remain concealed under a table or bench until the disruption is brought under control. It is important to keep in mind that oftentimes crisis situations can be averted—or at least contained—by advanced planning and preparation. Senior Chief Inspector Christopher Parks of the U.S. Marshals Service captures it succinctly: (A) activate **a**larm; (B) get **b**ehind a barrier; and (C) **c**all for security.

Threatening Communications and Suspicious Behavior

An integral part of security awareness is the development of a sensitivity for inappropriate communications and behavior. Keep in mind that there is no demonstrated correlation between a direct threat and an attack on a public official. This does not mean, however, that such communications are not a factor in assessing the possibility of a threatening encounter, particularly if there is a pattern of such activity. All inappropriate or threatening communications should be taken seriously and reported to law enforcement officials. Experience has taught law enforcement agencies with protective responsibilities to adopt a behavior-based approach in assessing whether an individual is on a predicable path to violence.

Michael J. Rose, chief inspector, U.S. Marshals Service, and a former Secret Service agent, has found from experience that, while most assailants do not make direct threats, they frequently reveal their intentions to family members, friends, colleagues, and associates. Often they write their thoughts or ideas in journals or diaries. The unexpected purchase of a weapon or firearm is obviously significant in a multifactor evaluation procress. Also, research has indicated that assailants do not necessarily fit any one demographic profile or age group.

Despite impressions to the contrary, mental illness only rarely plays a key role in assaults on public officials. Case studies reveal that a person can be mentally ill and still have the organizational skills to develop an elaborate attack plan. The most recent example is Jared Lee Loughner, who, in 2011, killed six people in Tucson, Arizona, including Chief U.S. District Judge John Roll, and wounded 14 others, including U.S. Congresswoman Gabrielle Giffords. Subsequent to his arrest, Loughner was diagnosed as schizophrenic, but his condition proved to be no impediment to his merciless attack on 20 people.

Individuals who plot assaults on public officials harbor a range of motives. Typically, these include a wish to achieve fame or notoriety, to avenge a perceived wrong, to enable law enforcement–assisted suicide, or to bring national attention to an alleged injustice. Surprisingly, a review of recent case histories reveals that few assailants had prior arrests for crimes of violence.

To safeguard against assaults or dangerous encounters, persons in the legal community should immediately report to law enforcement officials any oral, written, or gestured threats and inappropriate communications. Likewise, any suspicious behavior or activity suggestive of uncontrollable anger or contemplated revenge warrants reporting.

Restricting Access to Personal Information

One of the first steps in cultivating a secure lifestyle is containing your personal profile or the level of personal information publicly available about you and your family. Because disgruntled litigants and potential antagonists can tap an infinite well of personal information from the Internet or other social networking services, a judge or lawyer should never assume that his or her activities are private.

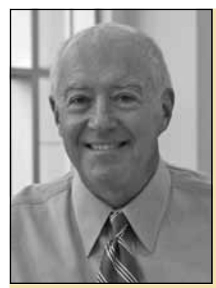
Social networking has become an increasingly popular form of communication, but precautionary measures are necessary to minimize the dissemination of personal information. Keep in mind that once such information is launched into cyberspace, it is difficult to retrieve. Few Internet-based media services are willing to remove personal information from their sites, even when requested by a public official. Therefore, the public dissemination of personal information is best controlled at its source—you, your family, and friends. When merchants ask for your name, address, and telephone number in connection with a purchase, when possible, simply say "no." Moreover, when stores invite you to become a preferred customer, or add your name to their mailing list, remember the information you provide will most likely be sold to an information aggregator. Information aggregation services sell mailing lists and phone numbers to thousands of individuals and vendors throughout the country. Always be skeptical when merchants claim that they do not sell their customer lists.

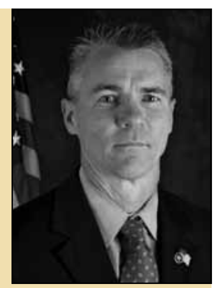
You also should avoid accepting unsolicited "preapproved" offers of credit or related services. Acceptance of such offers may facilitate uncontrollable dissemination of personal information. To preclude such offers, you can contact legitimate opt-out services by calling 1-888-567-8688 or at www.optoutprescreen.com.

Another fertile source of personal information often tapped by data marketers is your credit card. The black magnetic strip on the reverse side of your card is a treasure trove of personal identifiers, including your home address, phone number, credit card number, and often more. Many merchants market these data to information brokers. As an enhanced security measure, some so-called smartcards have encrypted microchips rather than magnetic strips. While most U.S.-based credit card issuers find conversion to encrypted data too costly, it has become common in European markets.

Another wise information control measure is to use your business telephone number and address on publicly available documents. Many states allow judges to use their office address on voter registration and motor vehicle–related documents. By separating your personal and professional life, you can often form a protective firewall.

Chief Inspector John Stark, U.S. Marshals Service, an expert in cybersecurity, recommends the same practice





Judge Henry E. Hudson is a U.S. district judge for the Eastern District of Virginia and a member of the Executive Advisory Committee of the National Center for Judicial Security. He formerly served as the director of the U.S. Marshals Service, U.S. Attorney for the Eastern District of Virginia, and Commonwealth's Attorney for Arlington County, Virginia.

Chief Inspector **John Muffler**, administrator of the U.S. Marshals Service's National Center for Judicial Security, manages a program that assists federal, state, local, tribal, and international stakeholders on best practices within court and judicial security and has oversight of academic and operational programs.

with respect to social networking. When signing up for Internet services or joining networks, beware of requests for intrusive information. Aside from your user name, password, and e-mail address, the balance of questions are typically optional. Avoid providing your home address and telephone number, employment history, and, of course, personal identifiers. When responding to additional questions, always determine whether they are based on a legitimate need. Stark cautions that your answers are not private despite the network's representations to the contrary. There is no guarantee that the data you share with any social media site will be kept confidential.

Beware of social engineering ploys. These are tactics that involve the deceptive use of personal information to elicit more valuable information, such as passwords, travel plans, and perhaps even details about your home security system. Stark suggests the use of privacy settings on your social networks, limiting the amount of personal information you share, and staying clear of risky online neighborhoods, such as free games. Over 9.2 million customers annually are tricked into submitting personal data, such as bank account and credit card numbers, to sinister websites that appear on their face to be established companies. If you learn that your account has been breached or that data have been stolen, promptly notify your bank or credit card provider and, of course, discontinue use.

If you enjoy socially interacting with a large network of people, Stark recommends that you consider developing two discrete media accounts—personal and professional. The first should be in your real name with access limited to verifiable friends and relatives. Alternatively, if you prefer a wider network, this account could be in a false or non–readily identifiable name. This nickname account allows you to communicate with strangers without compromising your identity or identifying your connection with family members. The second account can portray your public identity and be used for professional contacts. A secondary advantage of this type of system is that it allows you to limit the amount of spam you receive in your primary personal account.

As an additional security precaution, vary your user names and passwords—don't use the same one for all of your online accounts. If you store a significant amount of personal information on your cell phone, you may wish to activate the password feature on your phone's menu. After purchasing computer hardware or software, always change the default user ID or password provided by the manufacturer.

Additional Cybersecurity Tips

According to Jeff M. Spivey of Security Risk Management, Inc., a former president of the American Society of Industrial Security, cybersecurity is now considered the nation's number one security challenge. Malware, which is short for malicious software, and other forms of spyware can be remotely embedded in your computer and place data at risk. Some malware programs can clandestinely transfer data in your system to a third party. More virulent strands can cause significant damage to servers and networks. Even legitimate websites can host malware embedded by a hacker. When accessed unwittingly, the malware can quickly infect a visitor's computer.

The Security Operations Center of the Administrative Office of the U.S. Courts recently reported an e-mail scam that can potentially infect the recipient with a computer virus. The e-mail directs the recipient to attend a bogus court hearing on a specific date and time. Such e-mails may also instruct recipients to view an attached virus-infected document. Use caution in opening documents that do not appear related to a familiar case. You may wish to contact the court before wading into potentially malware-infested waters.

Another frequently encountered form of data piracy is referred to as phishing. Spivey describes phishing as the act of attempting to acquire information, such as user names, passwords, credit card information, and so forth, by appearing to be an e-mail from a recognized or trustworthy source. This technique typically employs a seemingly legitimate decoy website, perhaps simulating a bank or investment firm. To enhance the likelihood of duping the target, so-called spear phishing attacks are usually focused on specifically selected individuals who are often identified by illicitly hacked data. The mere act of opening the e-mail allows malware to be surreptitiously installed in a visitor's computer.

Spivey suggests a few specific countermeasures to deter invasive spyware. He recommends the use of firewall software on your home computer. You should also use antivirus software and scan your computer weekly to detect malware. Avoid using obvious or easily guessed passwords. Instead, Spivey advises the use of random combinations of letters, numbers, and symbols in both upper- and lowercase. Always change the default name on your wireless router before placing it into service and adopt an effective wireless security protocol.

Needless to say, confidential business should never be conducted over public wireless networks. If you store sensitive information, such as interview notes or privileged communications, equip your device with a feature that allows for the GPS tracking and remote destruction of data if lost or stolen. If you regularly transmit confidential information on your computer, you may wish to explore encryption. Systems that enable this function are not difficult to install. Always avoid using public computers for sensitive or confidential information.

Enhancing Security of the Home

Because courthouses and legal offices are relatively secure environments, most assaults on judges and lawyers occur at their residences. A recent study (1950–2012) by Santa Clara County, California, Detective Glen McGovern, "Murdered Justice: An Exploratory Study of Targeted Attacks on the Justice Community," concluded that 51 percent of all targeted attacks against justice personnel occurred at their homes and a disturbing 68 percent were fatal. McGovern also determined that only 20 percent of assailants actually entered the victim's residence. Typically while at home, people feel more detached from the pressures of the workplace and less vigilant of danger. Providing a secure residence for you and your family involves more than security systems, sound locks, and entry-proof windows. The security footprint of your home starts beyond the brick and mortar of the home's exterior. It begins at the street, curb, and tree line. It involves multiple layers of security—the interrelationship of each is critical for optimal effectiveness.

The exterior is an important consideration because a significant number of predators conduct surveillance before selecting their intended target. Therefore, landscaping and outside lighting form the first layer of home protection. Remove hiding places and keep the structure visible from the street. The less dense the landscaping, the better. Shrubs near the house should be trimmed to a height of no more than three feet. Bushes should be maintained at a height of around seven feet; planting thorny shrubs under windows can act as a further deterrent. Trunks of larger trees should be pruned to seven feet to preclude concealment. These measures will ensure good lines of sight from inside the house. External visibility can also be enhanced by illuminating trees and shrubs. Motion-activated lights serve a dual purpose of both illuminating large areas and providing early warning of encroachment by trespassers. Lamp posts and timer lights are also advisable. Statistics confirm that a well-lit home is less likely to be burglarized.

Sound locks and sturdy doors are critical elements of home security. Exterior doors should preferably be composed of either solid wood or metal without low-level glass. To maximize effectiveness, the door must be flush with the frame and the bolt should penetrate at least an inch into the frame. Locks secured by a thumb-turn device inside the residence should never be used in close proximity to windows that can be broken. Doors with low-level windows should be equipped with double-cylinder deadbolts that require a key to disengage the lock from the interior. Although convenient, never leave the key in the internal portion of the lock.

And, remember, windows are the weakest and most vulnerable part of your residence. The simple act of drawing curtains or closing blinds will prevent a potential assailant from learning the number and location of occupants. Always keep windows locked or insert a pin or nail in the sliding portion of the frame as an added countermeasure. Dual-pane windows that require multiple blows to shatter are strongly recommended. The last two sounds a burglar wants to hear are the shrill of an alarm or the sound of breaking glass. Intruders often put tape on windows to suppress the noise caused by breakage.

When arriving at your residence, particularly after dark, be keen to your surroundings. Watch for vehicles or service trucks that are out of place or have been parked for an extended period of time. Be alert to individuals on foot that you do not recognize or a vehicle that has been following you for several blocks. If you observe unusual or unsettling activity, take a moment to drive around the block to see if the activity continues. If it does, consider contacting your local police department. If you choose to exit your vehicle, keep your cell phone in your hand to summon help quickly. Do not hesitate to press the alarm button on your remote key if a suspicious person approaches in a menacing fashion.

It's a fact that a home without a security system is three times more likely to be burglarized than one with an alarm. Home intrusion detector systems provide an unparalleled layer of protection and security, particularly for those times when your family is at home alone. At a minimum, a security system should consist of control panels in the primary bedroom and lower level, glass break detection, door and window contacts, motion detection, and an alarm annunciation. It is also advisable to include a cellular backup feature that allows your system to function in the event your landline is severed or out of service. Closed circuit television systems and self-monitoring Internet/smartphone features are also available options. Needless to say, even the most advanced alarm system is worthless if you don't use it regularly.

Precautions for Handling Suspicious Packages

While developing a secure home environment can provide a protective barrier against intruders, it's important to note that some assailants choose to avoid a direct encounter. These disgruntled litigants opt for packages or letters containing hazardous or explosive substances. Learning the characteristics of suspicious packages is critical, particularly for young members of the family.

Because of the diverse variations of suspicious packages, their characteristics are difficult to concisely capture. As Senior Inspector Heather Walker of the U.S. Marshals Service points out, identifying a suspicious package is not only subjective, but often depends on the environment in which it is encountered. So your initial question should be, "does it appear out of place?" If so, before touching the letter or package, Walker recommends close inspection for the following characteristics: (1) excessive postage; (2) handwritten or poorly typed address labels; (3) incorrect or improper titles; (4) omitted names; (5) lopsided, uneven, or bulky packaging; (6) disproportional weight given size of package; (7) misspellings; (8) oily stains and/or strange odors; (9) no return address or postmark that differs from return address; (10) leaking powder or sloshing sounds; (11) excessive tape, string, or wrappings; (12) restrictive endorsements such as "Personal" or "Confidential"; and (13) protruding wires.

If you receive a suspicious package, err on the side of caution. Do not touch the item, warn others in the area, and, if possible, place a barrier between you and the package. Immediately summon law enforcement. If powder is visible, wash your hands with soap and water and shut off the ventilation system.

Final Thoughts

While the recommendations offered above are important in heightening your security awareness, the critical element is personal commitment. Statistics confirm that the threat is real. Your life, and those of your family and staff, may depend on it. And always remember, security starts with you! ■