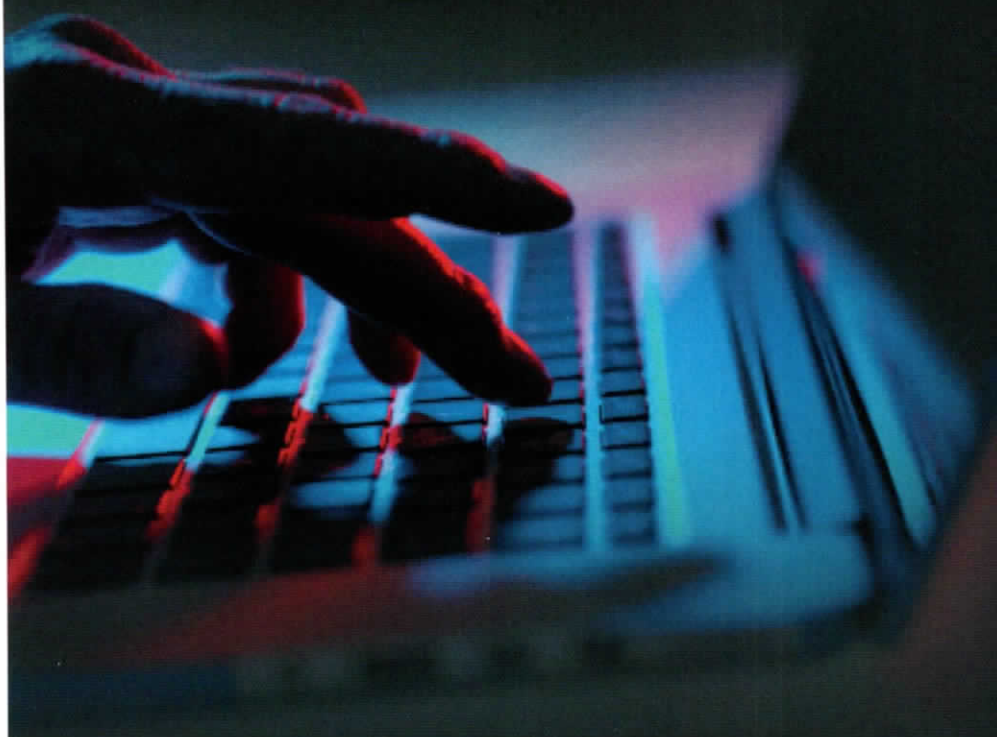

An Insider's Look at Personal Security, Online and Off

Frank Rodman has spent his career protecting diplomats, CEOs and billionaires. Think Princess Diana, Nelson Mandela, Michael Dell, Madeleine Albright. Not to mention the many others who work hard to keep their names out of the headlines.

Today Rodman is president of New York-based TorchStone Global, a consultancy that he started with several security veterans, including Eljay Bowron, a former director of the U.S. Secret Service. Its mission is managing the security risks of the world's wealthiest organizations and individuals.

William Blair advisor Bob Fix has worked with Rodman since TorchStone was founded in 2010.

From advising on cybersecurity to terrorism scares, this business is growing. The world seems to become more risky by the day.

Rodman says clients are concerned about their physical security. But as the collection and storage of data mount, they increasingly worry about their online security, especially identity theft and fraud.

"Protecting yourself from cybercriminals is actually not that much different than protecting yourself from traditional criminals," Rodman says. "Both require adopting good security habits both online and in the physical world. Unfortunately, most people don't change bad habits until they have a compelling reason."

The sad lesson for victims, he says, is that "a cybercrime can be just as personal and invasive and violating as a physical crime."

TorchStone encourages companies interested in evaluating their cybersecurity safety to start with assessing real-world physical security issues—doors, drawers, locks, windows, luggage, purses, wallets, papers.

Even if a client has the most sophisticated software on the planet, he says, it won't help if someone can get hands-on access to your computer, network or old-fashioned paper documents.

Rodman tells the story of a client whose laptop bag was stolen while he was traveling. The client later recovered the laptop bag but he came to Rodman very upset that someone might have gained access to his computer.

The stolen bag, the client said on questioning, had also contained his driver's license, checkbook, a letter from the IRS about an audit that included his Social Security number, and a letter from his divorce attorney outlining how his assets might be divided.

"'You're concerned about your laptop?'" Rodman told him. "They had everything they wanted in physical documents," Rodman recalls. "It's a really good example of how we focus too much on technology than on our own behavior."

The importance of being prepared—expecting the unexpected—is vital, he says.

Rodman says many of the most common-sense safeguards for cybersecurity are obvious once the individual becomes aware of how technology becomes vulnerable.

Rodman has learned over the years that people usually follow three approaches in handling security risk.

1. The first is "hope." People live in the moment and hope they remain safe, he says. So if their identity or security is compromised, they hope someone swoops down and saves them. They think they don't need a plan.

2. The second approach is to deal with a problem when it happens. They push the panic button and assume help will arrive. But the speed and effectiveness of that strategy, Rodman says, depends on the availability of the help at the time.

3. "The third strategy and the one we promote is the integrated approach where you combine awareness of your environment, thoughtful plans, training and testing against those plans," Rodman says.

He highly recommends using credit monitoring services, which will flag whether someone's identity has been stolen. Changing and keeping passwords secret is also key but so is keeping software, especially antivirus software, current.

"Software is the only industry known that's allowed to sell us something that needs to be fixed on a weekly basis," he says. "So we need to keep our software patches current and our antivirus software up to date. New viruses are constantly being developed and deployed."

Criminals will continue to increase their use of social networking sites to identify targets, says Rodman, recalling the kidnapping of hedge fund manager Eddie Lampert in Greenwich. His kidnappers went online first to find the wealthiest people in Connecticut. Lampert was listed and he was then chosen as a target because he was accessible.

Security and awareness while traveling are also important.

"In some countries it's a physical security threat. In other places like China, for example, people are more worried about the security of their digital information while traveling," Rodman says. "So we've designed a program of essentially bringing clean devices to those places—stripped of any proprietary or personal information. When those devices are turned back in they are swiped clean again."

Vigilance is the key for every user of online devices.

"We all rely on the Internet and use it for everything. But it creates a lot of vulnerability. We try to help clients understand those vulnerabilities and put some good security practices in place," Rodman says.

Beginnings in the U.S. Diplomatic Security Service

Rodman began as a special agent for the U.S. Diplomatic Security Service in the late 1980s after the Beirut embassy was bombed. Congress decided to expand security for embassies worldwide. One of his many postings was heading diplomatic security for the U.S. embassy in Tokyo in what he thought would be a "quiet" assignment given Japan's reputation for public order and respect for authority.

Then the Tokyo subway system was attacked by terrorists using poison gas, a Philippine airliner was bombed, and the Kobe earthquake killed 5,000 people and destroyed the consul general residence.

"So you can't tell what risks are around the corner regardless of where you are," Rodman says.

That rule holds not just in the real world but everywhere online.

"As a former government employee, I received a notice recently that my personal information was compromised in a hacking incident. So if even the government can't secure our data appropriately, what makes us think we will be able to do it on our own?" he says.