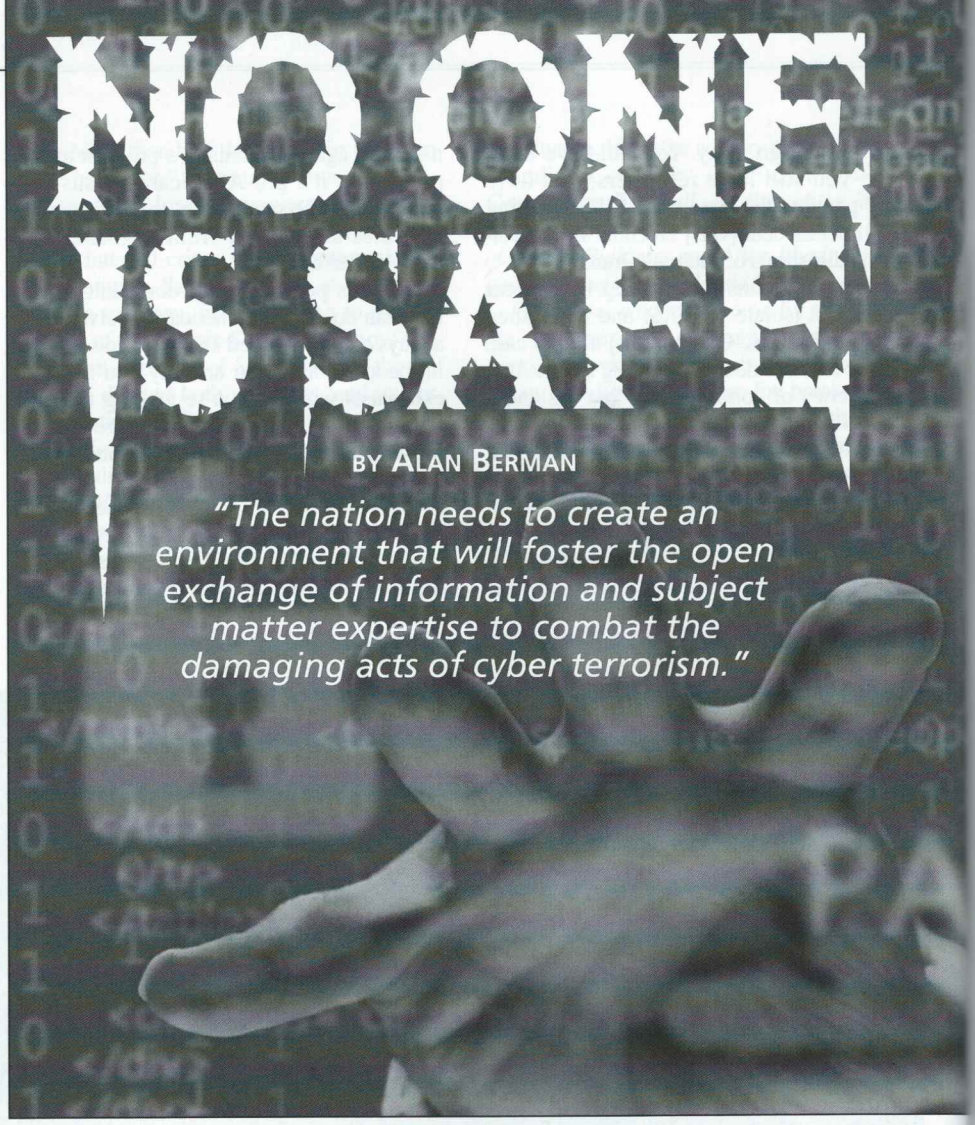
NO ONE IS SAFE

BY ALAN BERMAN



"The nation needs to create an environment that will foster the open exchange of information and subject matter expertise to combat the damaging acts of cyber terrorism."

IT IS HARD not to be aware of the threat of cyber terrorism. Media in all of its forms has assaulted us with the risks of hacking on a daily basis. No industry, government, or media outlet source is safe: Twitter, Target, Home Depot, SONY, J.P. Morgan, the Internal Revenue Service, U.S. Office of Personnel Management, and Ashleymadison.com's adulterers' site, with its 37,000,000 members, all have been hit. There is no doubt that cyber terrorism has made us question the safety of using any cyber site or resource.

Despite the best efforts of cyber security professionals armed with a variety of intercept, detection, and deterrent software, successful attacks still are taking place at an alarming rate. The apparent ease of penetration and inability to identify threats until after an incident occurs has made it possible to create a new industry of thieves that have found back doors and other intrusion means through which they can extort, compromise, sell, and destroy information while being any place in the world.

In support of these invaders is a collection of software tools: password and wireless crackers, sniffers, spanners, vulnerability scanners, e-mail flooders, and other instruments of intrusion and disruption. While cyber security breaches have been a present threat for decades, much of the hacking performed in the past was done for the sheer sport of showing off prowess and gaining bragging rights. Those days are gone. The new breed of hackers is not the benevolent hackers of old, but a new group interested in the profits that can be derived from its efforts. Hacking has turned into an industry—and a very financially rewarding one.

Credit card hacking and the sale of information is a big business. Like all well-defined industries, hacking has a distribution system worthy of any major information network. Credit card data stolen from retailers, for instance, is sold in an underground hacker market (forums). The information containing customers' card numbers, names, and addresses are put up for sale and priced to match the value of the product. One such website, registered in Latvia, lists the credit card information (name, credit card number, expiration date, authentication code, etc.) along with zip codes, security codes, and e-mail addresses from the information stolen from the hacked site—in this particular case, Target. Like any good merchant, the seller enhances the product's effectiveness by making it easier for the buyer to use the cards for purchasing goods online or withdrawing money from bank accounts. The value of the card directly is proportionate to how new the information is. The information on a credit card that recently has been stolen, and whose theft has yet to be discovered, may have a value of upwards of $100 per card. The value decreases dramatically as the time from the theft increases.

To stymie the efforts of law enforcement personnel attempting to infiltrate hacker marketplaces, the most sophisticated criminals hide their "carder forums" on the "Dark Web," which conceals the location of the computer servers hosting the websites. Secrecy is ensured by routing computer messages randomly through several places on the Internet, wrapped in encrypted code, so no single point can link the source to the destination, making the sites nearly impossible to trace.

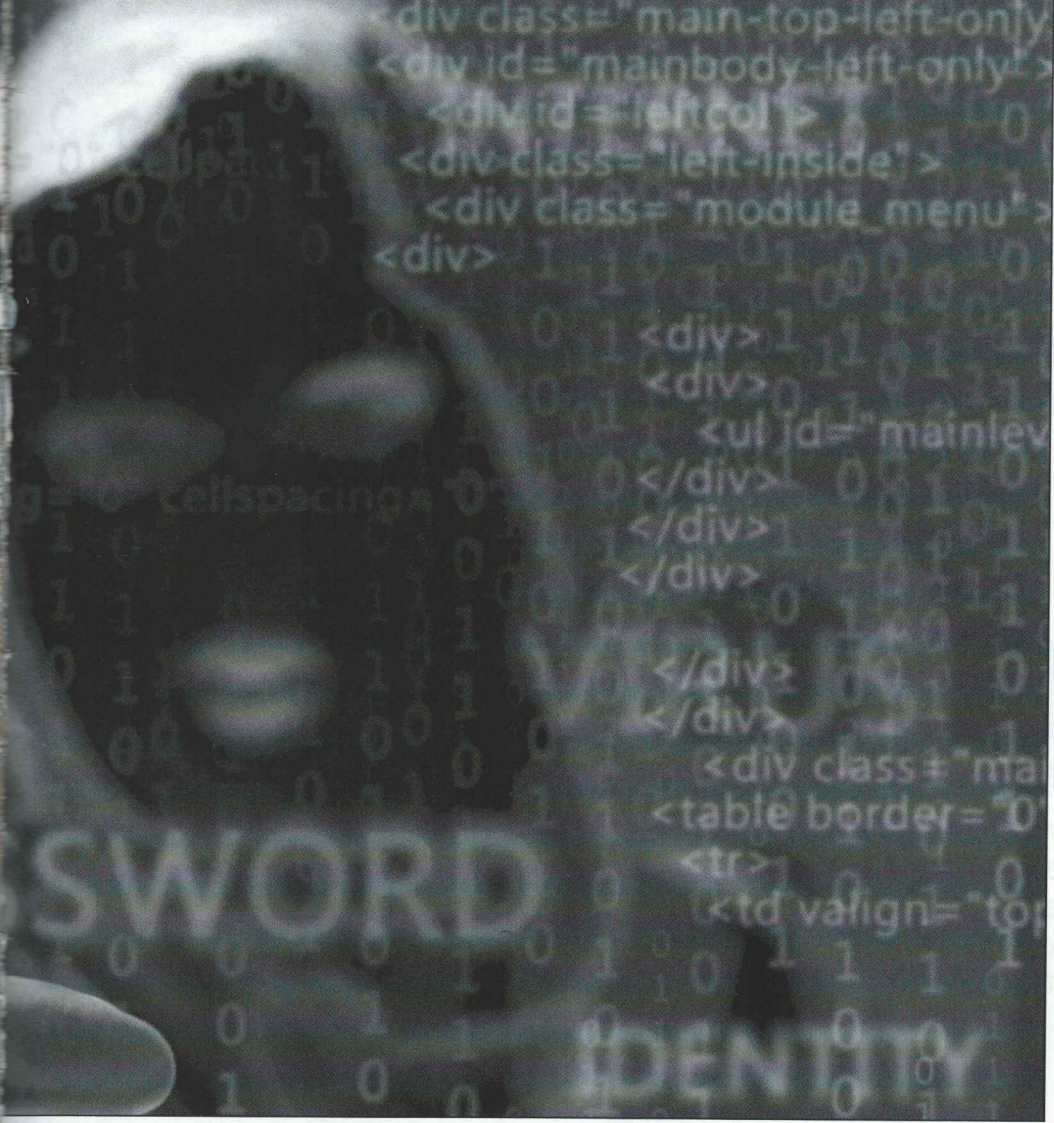
While hacking of credit card and other information that might lead to identity theft may garner much of the headlines, hackers bent upon destruction create even more dangerous situations. Damage to critical infrastructures components can cause immeasurable harm. A report by the University of Cambridge Centre for Risk Studies and Lloyd's of London Insurance put together a scenario of a cyber attack blacking out New York and Washington, D.C. It estimated the impact upon the U.S. economy of upwards of one trillion dollars.

The hacking of airplane systems in mid flight can destroy a pilot's ability to control a jetliner with hundreds of people aboard. The recently disclosed act of hackers being able to penetrate the networks that operate key components of an automobile identifies an issue that affects millions of car owners. What started out as a means to unlock car doors remotely became more intrusive and dangerous, as the hackers took control of a Jeep's audio system, wiper controls, and finally, steering mechanism. In a demonstration, the Jeep then was driven off the road.

The pervasive nature of hacking has given rise to a feeling of cyber paranoia. So, it is understandable why a simple software glitch at the New York Stock Exchange portended thoughts of the ultimate hack that could halt trading around the world. In response, stock prices fell. The issue ultimately was identified as a relatively simple computer program malfunction and not a cyber attack.

If the problem seems overwhelming, then you are starting to grasp the magnitude and complexity of what is facing those who are vested with the responsibility of guarding those resources that define the very essence of our daily lives. With the magnitude of the problem being so clear, it would seem that there should be few obstacles to a consensus approach to address the situation. However, while there are a great number of private sector initiatives and a strengthening of the regulatory environment to ensure greater diligence in the testing of institutions, there is no coordinated holistic approach to dealing with cyber terrorism.

The private sector has addressed the problem with proactive measures centered around the sharing of information, which has proven to be more effective than the sharing of information between the private and public sector, most notably the Federal government. A common bond tends to exist among private entity groups as part of a co-dependency that is a re-



sult of years of sharing information at industry conferences and round-tables, through career movement, and even on a social level. So, moving to a more formal, yet unregulated, structure is an outgrowth of the mutual respect and trust that has grown out of positive experiences with other members of the industry group. The result of this cooperation has been the emergence of information-sharing membership organizations.

Since private sector industries vary so greatly, measures taken by one industry may not meet the needs of another one. This created a need for industry groups to be formed so that members of that group could share information and take specific actions that help protect members of that industry sector. To address the issue of cyber threats and other security risks, the private sector relies on the ability to obtain information (while maintaining anonymity) from like organizations. These ISACs (Information Sharing and Analysis Centers) are created by industry groups, whose goal is to advance the physical and cyber security of the critical infrastructure of North America.

An example of this can be found within the Automotive ISACs, which have been working together to address this issue and create a more secure network for vehicles—to counter the Jeep hacking disclosure. Their sharing of information is an attempt to create some uniformity in approach to create more secure networks.

While there is some interface between private sector organizations and the Federal government, most notably industry councils, the overall lack of clear-cut policy and an inherent lack of confidence in the ability of the government to protect private information has limited any meaningful coordinated efforts. Congress, in fact, has failed to address this serious and growing problem that surely affects critical infrastructure and, as such, national security.

Indeed, the Senate has failed to pass any meaningful cyber security legislation. Its failure to act upon the cyber-terrorism legislation attached to the National Defense Authorization Act, which was passed by the House on April 23 clearly is a sign of the lack of urgency concerning the risk of cyber terrorism. The issue is that private sector entities want "safe harbor"—a provision of a statute or a regulation that specifies that certain conduct will be deemed not to violate a given rule—protection when sharing information with the government and others. The extent of the limited liability is the basis for lack of an agreement on the provision.

As Tom Carper (D.-Del.), who chairs the Senate Homeland Security and Governmental Affairs Committee, said during a March 26 hearing he called on cyber-threat information sharing between the Federal government and the private sector: "If we can solve this one, I think we'll move a long way to where we need to go in this arena."

The lack of trust that exists between the private and public sectors is hindering the efforts to create the very important cyber-terrorism policy. The fundamental distrust probably was summed up best by the ranking Republican member of the committee, Tom Coburn of Oklahoma, who said there is an assumption in government that businesspeople are going to do something wrong, not right. Sen. Coburn envisions a situation where two Internet service providers are sharing cyber-threat information when the Justice Department antitrust division lawyers insist: "Hey, wait a minute: you have to prove that was necessary for cyber security rather than you guys colluding to keep somebody out."

In fact, the Internet Service Providers never have demonstrated that they were not willing to share information among themselves if they felt it was in the best interest of national security, but the divide will continue to impede any meaningful policies to counter cyber terrorism. If the hack of the more than 20,000,000 accounts at the Office of Personnel Management and the numerous retail, financial, manufacturing, utility, health care, tech, transportation, military, and other municipal, state and Federal government agencies cannot prompt action, it is doubtful that anything short of an unthinkable event will be able to do so.

Now we see the Senate proposing legislation for Automobile Cyber Security Standards. While this may be a headline-grabbing event, and certainly is an important issue, it will not replace an overall strategy for protecting our cyber infrastructure. By embarking upon another piece of legislation, the Senate is failing to deal with the bigger issue of Internet security. While hacking of automobile systems is a problem, it is not as important as overall cyber legislation. Consider the protection of the financial systems or, even more basic, the power grids and the damage that would be caused by a cyber-terrorist attack.

The nation needs to create an environment that will foster the open exchange of information and subject matter expertise to combat the damaging acts of cyber terrorism. Without such a program, hackers will continue to have a major advantage over disorganized and uncoordinated tactics to prevent and limit damage from their assaults. This leaves the consumer and insurers to bear the brunt of the incursions into their private information to commit fraudulent acts upon their well-being and their digital identification. ★

***Alan Berman**, former member of the New York City Partnership for Security and Risk Management, is executive director of Disaster Recovery Institute International, New York; cochair of the Alfred P. Sloan Foundation committee to create a new standard for the U.S. Private Sector Preparedness Act; and author of* Down but not Out: A Guide to Your Disaster Recovery and Contingency Plan.