

FORTUNE



© 2003 Time Inc. Printed in U.S.A.

safeguarding *the* nation

featuring
VeriSign[®]
The Value of Trust[™]

The fight against terrorism takes on a new intensity.





The largest blackout in North American history began innocently enough. Shortly after 2 P.M. on Thursday, Aug. 14, a power-generating plant in northern Ohio was taken out of service and an overheated transmission line in the southern part of the state sagged and brushed against a tree. Nothing unusual so far, but then the trouble started. To provide the Cleveland area with lost power, plants in other parts of Ohio stepped up their output. At about the same time, Canadian power companies, also attempting to help Ohio make up its

shortfall, began pouring electricity into the area.

As the Midwest was flooded with more power than it could handle, transmission lines overloaded and plants shut down to protect themselves from burnout. The electricity from Canada, with no place to go, boomeranged via power lines across the New York border. There the fail-safes built into the complex North American electrical grid gave way, causing power plants and transmission facilities from Detroit to New York City to shut down. The electricity that fuels lights, air conditioners, computers, and other necessities we take for granted flickered and went out.

A terrorist attack—the first thought that came to many minds—was ruled out within an hour. There were no signs of bombs, break-ins, or the cyber-footprints hackers invariably leave in their wake. But that was scarce comfort. If something as benign as an unexpected surge in power can close airports, bring New York City's subways to a halt, and throw 50 million people into darkness, it's hard not to wonder what might happen if terrorists purposely set out to bring the system down.

Two days before the blackout, a British arms dealer named Hekmat Lakhani was arrested in New Jersey after picking up a crate at a port near Baltimore. The crate, labeled MEDICAL SUPPLIES, contained a Russian-made surface-to-air missile system, and Lakhani told the buyer, an undercover FBI agent, that he could deliver another 50 of the shoulder-launched systems. According to the BBC, Lakhani, who was taped saying he hoped the missile would be used to bring down a passenger airliner, also allegedly called the Sept. 11 attacks a "good thing."

While all that was going on, a string of worms and viruses—computer programs that replicate themselves by stealing e-mail addresses from unsuspecting hard drives and then e-mailing messages to all of them—was

busy clogging computer networks around the world, forcing airlines, trains, department stores, and other businesses to temporarily shut down. "Blaster" was eventually quarantined, but not before it infected more than a million computers, costing North American companies \$1.3 billion in lost business. An anticipated attack from "Sobig.F," a potentially more dangerous virus that infected 100,000 computers, was thwarted at the last minute when the FBI shut down 20 Internet servers that were poised to launch a fresh barrage of mass mailings.

Just the Beginning

What does it all mean? The atrocities of Sept. 11, 2001, were just the beginning. Terrorism, once a fuzzy concept that involved nasty events in faraway places, is now part of the fabric of everyday American life. Everyone is concerned about it. Thousands of people in both the public and private sectors are actively seeking ways to secure the country from attack, with billions of dollars going into the effort. President Bush's fiscal-year 2004 budget includes \$36.2 billion for the Department of Homeland Security (DHS), up 7.4% from the money spent on these activities in 2003. Other government departments are expected to add another \$5 billion or so to the 2004 total.

The DHS, the federal agency established in early 2003 to lead the country's fight against

Since the atrocities of Sept. 11, homeland security has been hoisted to the top of the administration's to-do list.

terrorism, has taken flak about the color-coded approach it created to alert the country to danger. (As we all know by now, red indicates that a terrorist attack has occurred or is imminent, green indicates a low degree of risk, and orange, yellow, and blue fill in the missing pieces in the middle.) The department's suggestion that Americans defend themselves against chemical or biological attacks with duct tape and plastic sheeting was seen as another sign of naiveté. There is also dismay over the snail's pace at which the agency is working.

In its defense, the DHS started from scratch. "Before Sept. 11, the federal response to terrorism was in thousands of pieces," says Larry Holloran, a staff member of Congressman Christopher Shays (R-Connecticut), a member of the House Committee on Government Reform and Oversight Subcommittee on Human Resources and Intergovernmental Relations.



"Three national commissions were looking into terrorism issues at that point, and they all agreed we didn't have a sound intelligence base or assessment capability. They also concluded that there was a vulnerability du jour we were reacting to, and that we didn't have a strategy to address it or an organizational structure that could implement one." Holloran continues, "At the federal level, we were a Cold War organization in terms of intelligence, and at the local level we were relying for protection on an outdated concept called civil defense."

The National Defense Industrial Association (NDIA) has pitched in to help. "To date," says Gen. Lawrence P. Farrell Jr., president and CEO, "the NDIA's homeland security division has focused its efforts on the internal reorganization needed to meet its expanded charter. This involved monitoring the buildup and maturation of the DHS to identify key linkages between the new department and the defense industrial base." It sponsored conferences focused on national homeland security policies and the equipment needs of first responders. The NDIA, with the U.S. Coast Guard and the Transportation Security Administration, has co-sponsored national conferences and exhibitions designed to enhance government-industry communication, encourage collaborative efforts to develop technology solutions for pressing security needs, and promote the vital role that industry must play in securing the homeland, Farrell explains.

Part of the DHS's problem is money, which has been slow coming out of Congress. A bigger part involves to the immensity of the task the department inherited. In being asked to merge 22 separate federal agencies into a lean, mean fighting machine, Tom Ridge and his associates are attempting to pull off the largest government reorganization since Harry Truman combined the various branches of the military

into a single Defense Department at the end of World War II. Equally significant, while the Hart-Rudman report of 2001 and several others not only were critical of U.S. vulnerability to a terrorist attack but also predicted one would occur, the mindset of the vast majority of Americans had little room for anything as weird and off the charts as a homeland-defense effort.

Until, Sept. 11, 2001, that is. Since then, the administration has hoisted homeland security and antiterrorism to the top of its to-do list. Congress and the bulk of the country are on-board. And while the Department of Homeland Security will always be open to criticism, it's stepping up to the plate and beginning to make things happen. Example: *Get Ready Now*, an 11-page booklet available in hard copy or by downloading from the department's website, may not stop an Osama bin Laden in his tracks, but it contains a clear and sensible analysis of the various threats the country faces and sound advice on ways the public and industry can prepare for and deal with them.

Working with the FBI

For those who scoff at booklets, the DHS has established a series of operating divisions, the newest being the National Cyber Security Division (NCSD), which opened for business on June 6, 2003. Its job: to provide 24/7 cyberspace analysis, issue alerts and warnings, improve information sharing, respond to major cyber-incidents, and aid in national recovery efforts. "Cyber-security cuts across all aspects of infrastructure protection," Ridge said at the time, adding that most companies aren't able to separate the cyber parts of their operations from the physical parts because they operate interdependently. That was abundantly clear this summer, when Blaster and Sobig.F were wreaking havoc on U.S. industry. The new



NCSA didn't play a lead role in the counter attack, but it teamed well with the FBI and other federal agencies that were on the case.

The private sector was on the case too. They may not all be household names, but F-Secure, Truesecure, MessageLabs, Sophos Anti-Virus, Trend Micro, Central Command, Network Associates, McAfee, and Symantec are among the many companies that spend much of their time developing defenses against malicious new computer codes. Gartner Inc., a market-research firm, says computer security software is now a \$3.8 billion business, and demand for the industry's products and services is certain to grow. "We don't have any technical reason to expect a follow-on of Sobig," says Brian King, an Internet-security expert at the Computer Emergency Response Team Coordination Center at Carnegie Mellon University, "but given past history, it is reasonable to assume there will be more."

Cyber-security is just one of the problems in need of solutions. Since Sept. 11, progress has been made in beefing up security at our airports, seaports, trains, and subways, but they remain potential targets with many vulnerabilities. The same goes for nuclear power plants and other key parts of the country's infrastructure. Our 7,500 miles of borders and 95,000 miles of shoreline remain conspicuously porous, and the scattered anthrax attacks we suffered were a wake-up call. Public-health officials and industry experts have since gone in search of ways to upgrade the country's defenses against bioterrorism and weapons of mass destruction. Yet the hard work has only begun.

But if there's anything U.S. industry loves, it's a challenge. And companies large and small are responding in encouraging—and in some cases dramatic—ways. Example: InVision Technologies—a small (2002 sales: \$571 million), obscure company based in Newark, Calif.—which vaulted to the top of FORTUNE's 2003 list of the country's fastest-growing companies. Since Sept. 11, InVision has installed more than 750 of its high-tech explosives-detection systems at airports across the country, and it is in the process of pushing into new markets. "The need for advanced security technology goes well beyond airports," says a company spokesperson, which is looking to place its anti-terrorism equipment in government buildings, border crossings, sports arenas, post offices, and schools.

At the other end of the size spectrum, Northrop Grumman Corp., a \$25 billion global defense company based in Los Angeles, is involved in hundreds of projects related to homeland security, including a scanning system to detect biological agents for post-office use; an infrared countermeasure device to protect commercial aircraft from shoulder-launched missiles; and a program called Deepwater, designed to modernize the Coast Guard's aging fleet.

More than Nuts and Bolts

Northrop is also helping the Department of Homeland Security get its feet on the ground. "Bringing 22 agencies with 100,000-plus people, separate databases, and all sorts of different systems together into an organization that works is a huge, complicated job," says Steve Carrier, the lead executive for Northrop's homeland-security effort. And it's more than just nuts and bolts. "The chief information officer says he wants unified e-mail, phone, and videoconferencing systems.

Pretty basic stuff, but once you get past the technical problems you've then got to convince people who are used to doing things their own way that they've got to share information and start working together. It's an enormous challenge," says Carrier, "but we'll get there."

On another front, Northrop is creating smart ID cards, which hold everything from finger and palm prints to iris,

voice, and fullfacial information. Part of the company's InfoShield™ suite of information assurance tools is a software package designed to protect desktops, servers, and networks from cyber-attacks. In August, the company released CommandPoint, a software suite designed to provide law-enforcement, fire, and medical agencies and other first responders with better tools to coordinate the command-and-control aspects of emergency situations. And Northrop's Firescut—a cousin to the Global Hawk, the unmanned vehicle that was cited for its part in the war in Iraq—is being configured to peer down on nuclear power plants here at home and be used for border security.

Lockheed Martin, another heavyweight in the defense business, is partnering with Northrop on Deepwater, the \$11 billion program designed to modernize the Coast Guard. Boeing, Raytheon, and General Dynamics have large homeland-defense operations. L-3 Communications, a six-year-old company, now does \$400 million a year in that end of the business, using technology

Responding to the call, U.S. companies are developing technologies and services to protect the nation's infrastructure.



originally developed to process military surveillance and reconnaissance photos. Another line of L-3 scanners, designed to reveal concealed weapons, is based on technology the company developed to help the military locate Taliban fighters hiding in Afghan caves.

A New Ballgame

Honeywell, a \$22 billion company, has turned its leadership in aerospace, safety, and security technologies and in engineered materials into a large and expanding lineup of homeland-security products and services. "Antiterrorism protection is a new ballgame," says David Willett, who leads Honeywell's homeland-security efforts. "The current threats are not answerable using traditional forms of security. They require new types of assessments, solutions, and integration that haven't previously been explored."

David M. Cote, chairman and CEO of Honeywell, discusses the technologies and systems integration capabilities that drive the company's broad perspective on safety and security: "With traditional security, individual discreet components produce streams of raw data, but one rarely talks to the other. They operate in a vacuum. Honeywell designs fully integrated systems and technologies that integrate raw data into actionable information. The result is real-time intelligence that is critical to meet terrorist threats. Research and development expertise—particularly in sensing and control, aerospace, and engineered materials—combined with decades of experience protecting and managing major public and private facilities, creates state-of-the-art, sophisticated security solutions for any enterprise, anywhere in the world."

Honeywell has a long-established, global presence in the aerospace industry and in airports. Honeywell security, building control, and life-safety systems are in operation today at more than 200 airports around the world, including those in Miami, Dubai, Sydney, and Munich. Closed circuit TV cameras provide airport security staffs with a view of what's happening in all parts of the facility, from the parking lot to the boarding gate. Honeywell researchers are also busy developing technologies, including

biometric identification systems, for managing access to security-sensitive areas.

In the air, the company is the leading provider of aircraft safety, communications, and guidance control systems and products. That includes secure communications systems that enable federal air marshals to communicate with other marshals on the plane, the flight deck, and the command-and-control center on the ground. And the company's Spectra Shield®, ultra-lightweight, ballistic-resistant product, which is ten times stronger than steel, is used to reinforce cockpit doors on commercial airliners. It is also used extensively in body armor worn by the armed forces and government agency personnel.

In seaport operations, Honeywell sensor technologies can be used in tracking, processing, and verifying freight to enable safer commerce while maintaining operational efficiency. To help the U.S. government with the daunting task of securing the border with Mexico, high-capacity Honeywell video systems manage feeds from hundreds of low-light cameras, sending images to appropriate monitors and recording key movements along the border. At the northern border, Honeywell access control solutions help protect and automate remote border-crossing points.

In addition to airports, seaports, and borders, Honeywell technology is at work securing many of the country's critical nuclear power and research facilities, gas and electric providers, and petroleum pipelines. To protect people, facilities, assets, and data in other areas, Honeywell produces, installs, and maintains safety and security systems integrated with building control systems for hospitals, airports, schools, manufacturing plants, retail centers, and commercial properties. The company's safety protection and fire and gas detection systems, which are digitally monitored over telephone lines, through wireless technology, or via the Internet, employ integrated control systems and sensors to detect intrusion in buildings and other high-security locations.

Breathing Life into Buildings

EMCOR Group, a \$4.5 billion construction and facilities services company headquartered





tackling digital predators

Bugs have always been an unwelcome yet commonplace occurrence in the IT scene, but the damages they inflict have suddenly ratcheted into the serious-money realm. The ironically named Love Bug, which wormed its way into millions of computers in 2000, cost more than \$8 billion to clean up. This year's crop—Slammer, Blaster, and the Sobig family of worms—threatens to cost even more: something in the neighborhood of \$12 billion to \$13 billion.

Although the 2003 attacks look more like vandalism than terrorism, they are cause for major concern. Blaster hammered Air Canada, shutting down big chunks of its reservation and airport check-in facilities. Sobig infected CSX Corp.'s operations, causing traffic delays along its freight lines and snafus throughout other parts of the rail giant's system.

Each worm and virus has its own *modus operandi*, but most turn innocent computers into drones that send out millions of e-mails, clogging systems and, at times, shutting them down. That's a problem, but the real fear is that a virus-armed terrorist might go a step further and wipe out the data on millions of hard drives, destroying vital information and bringing a country that relies on IT to a halt.

That's where VeriSign, a \$1 billion leading provider of critical infrastructure services that make Internet and telecommunications networks reliable and secure, comes in. In the early 1990s, when PCs became common and the commercialization of the Internet created an explosion of e-mail, websites, and browsers, VeriSign won a contract to act as the sole registry for domain names ending in .com or .net.

That role has given VeriSign a unique view of Internet patterns and activity, plus the ability to quickly detect threats and take steps to head them off. The company—which handles nine billion domain-name

lookups each day and processes 30% of all U.S. online commerce—withstands an average of 1,000 website attacks a day on behalf of its 90,000 merchants and 4,000 enterprise customers.

This type of protection is particularly vital to the banking industry, in which more and more transactions are being done electronically. "Customers and clients who conduct their business online need to know that their personal information and funds will not be compromised," says Stratton Sclavos, president and CEO of VeriSign. "By taking an offensive approach to security, the financial industry can anticipate malicious behavior and stop it before it happens."

A real-time example of how this relates to homeland security is the Pennsylvania Justice Network (JNET). "JNET links federal, state, and local law-enforcement agencies to one another on the network," says Linda Rosenberg, executive director of JNET. "Data integrity and data security are essential to all aspects of homeland security. If criminal activities and the resulting data are not shared it could have an adverse impact on critical decisions, and ultimately on public safety."

"Access to the most accurate, timely, and dependable justice information on the justice network is the essence of the JNET vision and represents one of the greatest needs of the justice system and homeland security," Rosenberg continues. "This information that has historically lied dormant in legacy systems, is key to all aspects of criminal investigation, apprehension, and crime prevention. Using the JNET Public Key Infrastructure (PKI) and VeriSign technology, authorized agencies throughout Pennsylvania are able to query and exchange sensitive and protected information. This has dramatically changed the nature of the justice system and has provided technology solutions to age-old information barriers."



The National Defense Industrial Association

The National Defense Industrial Association (NDIA)—headquartered in Arlington, Va.—and its affiliates serve as a key link between government and industry, providing a forum for the exchange of ideas and information. The NDIA has 50 chapters across the U.S., 1,100 corporate members, and more than 28,000 individual members. Its main goal is to represent the interests of the defense industry—fostering technological growth and weapons-system excellence.

The NDIA's primary areas of focus are the business and technical aspects of the government-industry relationship, including the acquisition process, research and development, procurement, logistics support, and many technical areas.

With the establishment of the Department of Homeland Security, early in 2003, the NDIA reconfigured some functions of several of its divisions into a new unit—the homeland-security division. This division mirrors the applicable functions of the DHS, The Defense Department force-protection efforts, and security-systems research and development. The areas the new division focuses on include information analysis and infrastructure protection, border and transportation security, security science and technology, emergency preparedness and response, Coast Guard programs, force protection, information and cyber-security, and industrial security.

in Norwalk, Conn., services more than 850 million square feet of high-end commercial and industrial property. "Our job," says CEO Frank MacInnis, "is to manage all systems that breathe life into a building and make it run. A big part of that job involves solving the security problems of our clients."

The solutions, MacInnis says, range from the basic to the esoteric. On the basic side, it can be as simple as moving the location of air intakes from the ground level to a higher location on a building, or moving the water handling equipment from the roof to a secure room within the building—in each case making it difficult for someone to introduce a noxious substance into the system. On the more esoteric side, a one-button shutdown system that EMCOR installed at its Washington, D.C., command center, which enables emergency shutdown of ventilation in over 140 buildings, was put through its paces recently when adjacent buildings were threatened by contamination from a gas leak at nearby Ronald Reagan Washington National Airport. "The one-button shutdown capability is sort of a fail-safe mechanism that can be used when even a momentary delay in the complete shutdown of an entire system would render your personnel that much more vulnerable," says MacInnis. "It's a user-friendly system that gives people charged with the protection of a

group of people or a facility the ability to put their decisions into effect as quickly as they make them."

EMCOR, whose command-and-control system in Washington was used as a communications backup when the city's commercial circuits were overloaded on Sept. 11, is currently working closely with government agencies to bring the mission-critical systems in the hospitals, fire departments, schools, and government buildings of its clients into 21st-century condition, including making them more secure. EMCOR helps a number of government agencies manage their facilities, including those of the new Homeland Security Department, for which it is currently building an office for the Secretary.

Future Algorithms

Looking ahead, even more sophisticated equipment is in the works. DynPort has a fast-acting anthrax vaccine in Phase I clinical trials. Anacor Pharmaceuticals is conducting animal tests on antibiotics to treat anthrax and other bioterrorism agents. L-3 Communications will soon be demonstrating a screening device that can spot soft explosives hidden on the body. InVision, using X-ray defraction technology, is working on scanners that can zoom in on a suspicious object in a closed suitcase and determine its chemical composition. Varian Medical Systems has developed an X-ray machine that can penetrate 17 inches of steel—giving customs inspectors the chance to see what's behind the thick walls of the seven million cargo containers that enter the country each year.

All all this suggests that homeland defense is here to stay and that the price of security will be a permanent addition to the cost of living, not only on a federal, state, and local level but on a personal level as well. Homeowners are already spending millions each year on basic alarm systems. Millions more are certain to go for super-high-tech add-ons like keyless door locks, infrared cameras that see in the dark, robots that are programmed to startle intruders, laser fences and, of course, backup generators that spring into action when the electricity shuts down.

But while homeland security is a big, costly, and serious business, a sense of humor is probably the key ingredient we'll need to make it work. Larry Holloran, the staffer in Representative Shays's office, tells a story that makes the point: "We've been working with a company called Community Research Associates, which runs simulated tests for cities and states. We tried to set up a meeting recently, but one of the principals said they couldn't do it on the day we suggested because that was the day they were bombing Worcester." ■