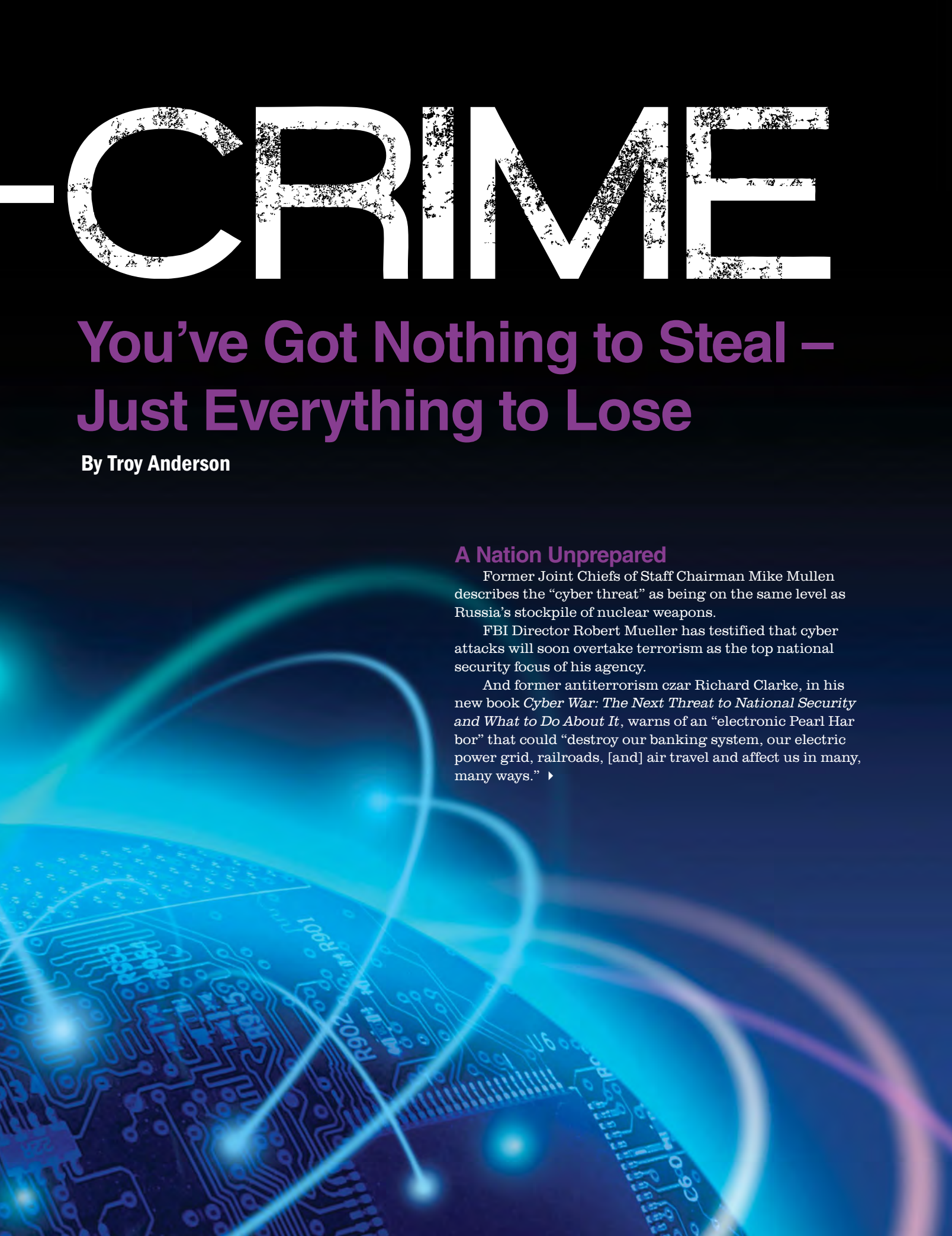

CYBER-

-CRIME

You've Got Nothing to Steal – Just Everything to Lose

By Troy Anderson



A Nation Unprepared

Former Joint Chiefs of Staff Chairman Mike Mullen describes the "cyber threat" as being on the same level as Russia's stockpile of nuclear weapons.

FBI Director Robert Mueller has testified that cyber attacks will soon overtake terrorism as the top national security focus of his agency.

And former antiterrorism czar Richard Clarke, in his new book *Cyber War: The Next Threat to National Security and What to Do About It*, warns of an "electronic Pearl Har bor" that could "destroy our banking system, our electric power grid, railroads, [and] air travel and affect us in many, many ways." ▸

"Cyber threats could be as devastating to this country as the terror strikes that tore apart this country just 10 years ago," Senator Jay Rockefeller (D-W.V.) testified during a recent hearing before the U.S. Senate Homeland Security and Governmental Affairs Committee. "That's why the directors of national intelligence under both President George W. Bush and President Barack Obama have said that the cyber threat is the Number 1 threat to our country."

This hearing, one of several involving cybersecurity in recent months, comes amid growing concerns that the nation's banks, businesses, power grids, telecommunications, and other systems are vulnerable to cyber-attacks that could inflict widespread economic damage and even loss of life.

The nation is not adequately prepared to deal with this emerging threat, much as it wasn't prepared for the September 11, 2001 terrorist attacks, experts say. As the United States increasingly relies on the Internet to conduct business, the nation's most critical infrastructure is vulnerable to cyber-attack by criminals, terrorists, and hostile nation-states halfway across the globe.

CYBER-CRIME BY THE NUMBERS

The Symantec Internet Security Threat Report found more than **286 million** unique variations of malware in 2010, up from **240 million** in 2009.

The FBI received **303,809** Internet-crime complaints in 2010, the second highest total in the decade-long history of the Internet Crime Report.

The Threat Is Real

Cyber-attacks on nuclear power plants, a region's water supply, or a major financial market could have a devastating impact on the nation. Already, the country's digital infrastructure has suffered intrusions that have allowed attackers to steal billions of dollars, intellectual property, and sensitive military information.

"The cyber threat is a very real fact," Rockefeller testified. "This is not alarmism. Here's why: hackers supported by the governments of China and Russia, and also sophisticated criminal syndicates with potential connections to terrorist groups, are now able to crack the codes of our government agencies, our Fortune 500 companies, and everything in between. They are looting our country of our most valuable possessions on an unfathomable scale."

Symantec Corp., which makes Norton antivirus, anti-spyware, and phishing-protection software, estimates the global cost of cybercrime at $114 billion a year. Adding in $274 billion for time lost due to cybercrime, the annual cost soars to $388 billion a year. That's more than the amount involved in the global black market in marijuana, cocaine, and heroin combined.

"The problem is huge," says Vikram Thakur, a principle security-response manager at Symantec. "We are seeing more and more attacks every day. The ones of higher significance involve businesses and organizations losing intellectual property. This is in essence their bread and butter. As this issue has gotten more attention in the last few years, companies are beginning to invest time and resources in protecting their assets."

The magnitude of the problem has caught the attention of a growing segment of the business community, especially following the recent cyber-attacks on Citigroup Inc., Lockheed Martin Corp., and VeriSign, Inc., a company in charge of delivering people safely to more than half the world's websites.

"We're starting to see this getting into very serious areas," says Stan Michaels, the chief technology officer at Web Dynamics, an Internet company based out of Texas. "VeriSign is a company we entrust with verifying that when we visit a website they are who they say they are. Granted, VeriSign isn't the only company that does this. But they are the largest and most well-known. If they are able to be hacked, it's not inconceivable that anybody could be hacked."

In a statement, VeriSign said it does not "believe that the operational integrity of the Domain Name System

(DNS) was compromised."

Bill Woodcock, research director at the Packet Clearing House, a San Francisco-based nonprofit that supports critical Internet infrastructure, says one of the mechanisms that people rely on to ensure the authenticity of websites they visit doesn't "really work anymore." This mechanism is known as a "certificate authority," which helps people know whether they are "talking to their bank or someone pretending to be their bank," Woodcock says.

"The certificate authorities in theory try to verify whether your bank is actually your bank, but that process has been found to be bankrupt," Woodcock says. "That pillar of Internet security has crumbled. So we're in a kind of limbo. This is a really bad time for Internet security."

The New Face of Espionage

The onslaught of cyber-threats comes in a variety of forms—cyber-terrorism, cyber-crime, cyber-espionage, and cyber-activism (the 21st-century equivalent of civil disobedience). Activist groups such as Anonymous have conducted distributed denial-of-service attacks against government and corporate interests they oppose. Meanwhile, well-publicized intrusions into the NASDAQ, International Monetary Fund, Google, and Fortune 500 companies underscore the vulnerability of key sectors of the U.S. and global economy.

"Over the past five years, a highly sophisticated team of operatives has stealthily infiltrated more than 70 U.S. corporations and organizations to steal priceless company secrets," U.S. Commerce Secretary John Bryson wrote in a recent POLITICO op-ed. "This is the new face of corporate espionage. Thieves whose identities are safely obscured by digital tradecraft rather than a ski mask are robbing companies of the ideas that are the source of American ingenuity."

The FBI is currently investigating more than 400 reported cases of corporate account takeovers in which cyber-criminals have initiated unauthorized Automated Clearing House and wire transfers from the bank accounts of U.S. businesses. These cases involve the attempted theft of more than $255 million.

"Often, the attack vector is a targeted phishing email that contains either an infected file or a link to an infected website," FBI Cyber Division Assistant Director Gordon M. Snow testified at a recent House Financial Services Committee Subcommittee on Financial Institutes and Consumer Credit hearing. "The email recipient is generally a person within a targeted company who can initiate fund transfers on behalf of the business or another valid online banking credential account holder. Once the recipient opens the attachment or navigates to the

One of the top cyber-threats today is known as an **"advanced persistent threat,"** a scam where a hacker or a gang of cyber-thieves uses social-engineering techniques to steal intellectual property or state secrets.

website, malware is installed on the user's computer, which often includes a key-logging program that harvests the user's online banking credentials."

Computer and intelligence experts are reporting dramatic increases in both the frequency and sophistication of online attacks. The director of national intelligence reported a significant increase in cyber-activity targeting U.S. computers and systems in 2011, including a more than tripling in the volume of malware since 2009. The Symantec Internet Security Threat Report found more than 286 million unique variations of malware in 2010, up from 240 million in 2009. The FBI received 303,809 Internet-crime complaints in 2010, the second-highest total in the decade-long history of the Internet Crime Report.

A large proportion of these attacks involve cyber-espionage. A recent report by the Office of the National Counterintelligence Executive, "Foreign Spies Stealing U.S. Economic Secrets in Cyberspace," found that many nations, predominantly China and Russia, are stealing U.S. trade and technology secrets to boost their own economies—posing a growing threat to U.S. prosperity and security.

"The proliferation of malicious software, prevalence of cyber-tool sharing, use of hackers as proxies, and routing of operations through third countries make it difficult to attribute responsibility for computer network intrusions," the authors wrote. "Cyber-tools have enhanced the economic espionage threat, and the intelligence community judges [that] the use of such tools is already a larger threat than more traditional espionage methods."

Nation-states, or proxies acting for nation-states, steal technology, research products, and intellectual property from U.S. businesses and government agencies.

"Advanced cyber-criminals have capabilities that approach those of national intelligence agencies, and some criminals have close relationships with their governments," wrote the authors of a recent Center for Strategic & International Studies report, "Cybersecurity: Two Years Later."

"A flourishing black market supports cybercrime. In it, you can buy the latest malware, learn of recently discovered vulnerabilities, or rent 'botnets' (thousands of computers remotely controlled for criminal purposes without the computer owners' knowledge). Credit card numbers, personal information, and bank-account data can be bought in bulk. Some sellers offer guarantees."

One of the top cyber-threats today is known as an "advanced persistent threat," a scam where a hacker or a gang of cyber-thieves uses social-engineering techniques to steal intellectual property or state secrets. This technique involves sending someone a well-crafted email appearing to be from a colleague and dealing with a familiar topic. This is one of the key ways intruders gain access to otherwise secure corporate networks.

"It's not what you see on *Mission Impossible*," says John Kahn, a senior analyst and senior criminal and civil investigator The Arrow Group Inc., a Houston-based company that provides research and security applications for corporations. "It's not like in the movie, where Tom Cruise comes down through the skylight

and breaks into a highly classified computer. Oftentimes, the way they get in is by capturing the credentials of someone in the company. I wish I could say that's a difficult thing to do, but it's not."

One of the greatest concerns among many businesses, Kahn says, is industrial espionage—the theft of a company's proprietary information. This could include sales, accounting, inventory, and gross-revenue records. It can include patent, registration, and licensing information or diagrams for products a company sells. Often, a hacker will resell this information on the black market.

"More and more, company executives are getting in tune with what they need to do to protect their businesses," Kahn says. "But I'm not sure that their Information Technology departments, often a cloistered affair, are as prepared as they might think they are. Otherwise, the hackers wouldn't be having the field day they are having with the amount of theft going on."

In a recent report by McAfee, "In the Crossfire: Critical Infrastructure in the Age of Cyber War," the authors wrote that critical-infrastructure owners report that their IT networks are under constant cyber-attack, often by "high-level adversaries." More than half of the executives surveyed reported that they had experienced large-scale denial-of-service attacks by high-level adversaries like organized crime, terrorists, and nation-states.

U.S. Electrical Infrastructure at High Risk

Of even greater concern, though, is the fact that terrorists and nation-states are targeting the U.S. electrical grid, raising concerns that cyber-attacks could result in devastating power failures in major urban centers. Cyber-spies from China, Russia, and other countries have penetrated the U.S. electrical grid and left software programs that can be used in the future to disrupt the system, experts say.

The U.S. electrical system is composed of several thousand public and private utilities organized into 10 large regional grids. The increased automation, reliance on computer networks, and interconnection within these power grids has left the door open to cyber-attacks, Representative Cliff Stearns (R-Fla.) testified during a recent House Energy and Commerce Subcommittee on Oversight and Investigations hearing.

"We have seen in the past decade what impact both manmade and natural disasters have on our nation's utility systems," Stearns testified. "Imagine the impact of a cyber-attack on the electrical grid. How many days could hospitals operate with on-site electricity generation? How would metro-rail systems operate at all? How would we recharge our smart phones or access the Internet?"

Jim Brazell, a technology forecaster and president of Ventureramp

Inc. in San Antonio, says cyber-attacks could knock out the nation's power grids, having a catastrophic impact on society.

"The real worst-case scenario is not that the lights go out, but that there is panic, a lack of food and water, and no communications," Brazell says. "You'd have to fall back on ham radio operators with big antennae to communicate."

How widespread might these blackouts be, and how long might they last? It depends on whom one talks to, says Greg White, director of the Center for Infrastructure Assurance and Security at the University of Texas, San Antonio.

"If you talk to people in the power industry, they won't want to say they are that vulnerable," White says. "If you talk to people in the security industry, they will say it's wide open. The truth probably lies somewhere in between."

In a recent report, the U.S. Government Accountability Office identified the nation's power grid as a "high-risk area" that could be exploited by cyber-attackers.

"Cybersecurity and industry experts have expressed concern that, if not implemented securely, smart grid systems will be vulnerable to attacks that could result in widespread loss of electrical services essential to maintaining our national economy and security," the GAO authors wrote.

The FBI estimates **108 countries** are developing cyber-warfare capacity. In the future, I don't think you'll ever see any kind of traditional warfare without some cyber-warfare component.

Cyber-Warfare and the U.S. Response

Before the invasion of Georgia in 2008 over disputed territories, Russia launched a massive cyber-attack, paralyzing the nation's websites, email, banking, and communication services. With Georgia's Internet infrastructure in disarray, the Russian military had little trouble with the military invasion. Experts say the Russian-Georgian War is a harbinger of what President Obama describes as "one of the most serious economic and national security challenges we face as a nation."

"The number of countries engaged in cyber-warfare has increased dramatically," says Jon Ramsey, chief technology officer for Dell SecureWorks, a provider of information-security services for Fortune 500 and other companies. "The FBI estimates 108 countries are developing cyber-warfare capacity. In the future, I don't think you'll ever see any kind of traditional warfare without some cyber-warfare component. If you want to go against the U.S. in a conventional war, it doesn't make any sense. You are going to engage in an asymmetric war, and you are going to do it in cyberspace."

This summer, the Obama administration will simulate a cyber-attack on New York City's power supply as part of an effort to boost support for cybersecurity legislation.

In response to the nation's cybersecurity weaknesses, Senator Joe Lieberman, a Connecticut Independent, and other members of Congress have introduced the Cybersecurity Act of 2012. The bill, backed by the Obama administration, is designed to give the federal government and the private sector the tools necessary to protect the nation's infrastructure from growing cyber-threats.

If passed, the bill would require the Secretary of Homeland Security, in consultation with the private sector, the intelligence community, and others, to conduct risk assessments to determine which sectors are subject to the greatest and most immediate cyber-risks. The bill would also authorize the homeland-security secretary, with the private sector, to protect the nation's most critical infrastructure. The bill also calls for improved information sharing while protecting privacy and civil liberties, improving the security of the federal government's networks, and strengthening the cybersecurity workforce.

Internet service providers, including Dallas-based AT&T, have opposed the bill, saying they prefer voluntary sharing of information about cyber-threats.

A group of Republican senators have introduced a competing cybersecurity bill, the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act.

"We are all in agreement that we

need to make our nation's cybersecurity a top priority," Senator Kay Bailey Hutchison (R-Texas) says. "Our bill focuses on giving businesses the tools they need to protect themselves from the looming threat of cybercriminals, and increased requirements for notification of threats to federal agencies."

Johannes Ullrich, chief technology officer at the SANS Internet Storm Center in Jacksonville, Florida, says the legislation should include a national credentialing system for cybersecurity professionals.

"Right now, it's still very much a 'Wild, Wild West' kind of business where everybody is doing network security without having any credentials," Ullrich says. "We need some kind of national system. Cybersecurity professionals would have to get accreditation similar to other professionals. Right now, if you want to build a bridge, you have to be a credentialed engineer. If you want to implement network security, there is no credentialing to prove that you actually know how to do this."

Cybersecurity: Steps to Protecting Your Business

For their part, businesses need to be prepared for cyber-attacks and take steps to improve their cybersecurity, Thakur says.

White says there are a number of things businesses can do. When cybersecurity vendors issue new software patches, install them, White says. It's also important to keep anti-virus and anti-malware software packages up to date. Companies should also provide training to their employees, teaching them not to open suspicious emails and attachments and the proper use of passwords.

"People have a nasty tendency to pick poor passwords and use the same password for all their accounts," White says. "Maybe they are a little more conscious about what they do at the office, making sure they follow the rules by not clicking on links or going to websites they shouldn't go to, but if they use the same password at work as they do on Facebook and are not as careful at home, their work accounts may be compromised too."

Employees should also be made aware of "social engineering" schemes used by master hackers, White says.

"They will call you up, claim to be an individual from IT, say there is a problem and they need to verify that you have the appropriate access," White says. "They will ask, 'What is your user ID and password? We'll check this out for you.' It's surprising how well that works." N

An award-winning journalist at the Los Angeles Daily News, the Press-Enterprise *and other newspapers for 20 years, Troy Anderson writes for Reuters, Newsmax,* Christianity Today, Bankrate Insurance *and many other magazines and online publications. He lives in Southern California. For more information, visit www.troyandersonwriter.com.*