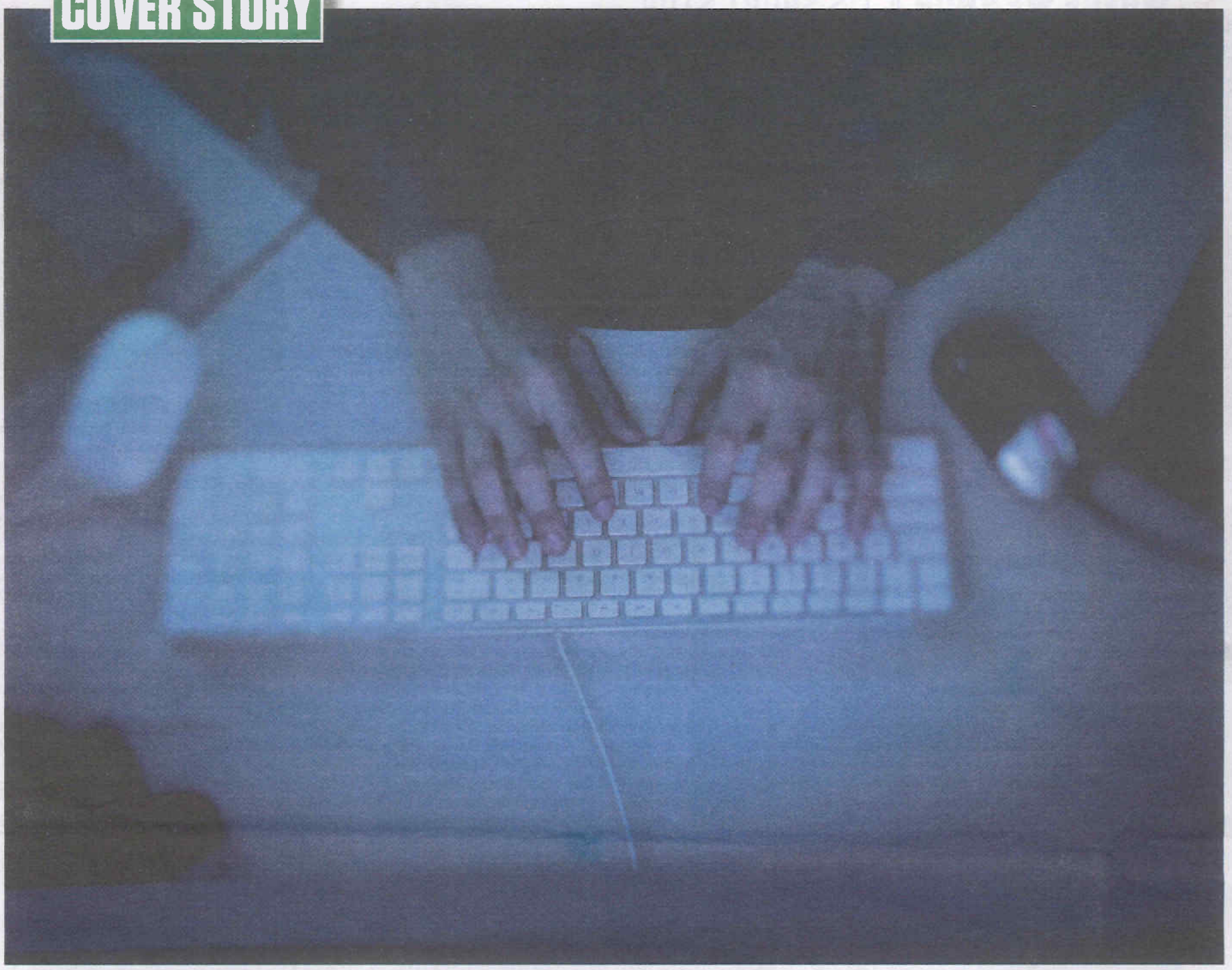
COVER STORY



Photos by Jeffrey MacMillan for Capital Business

THE CYBERSECURITY BOOM

AS THE GOVERNMENT DEEPENS ITS FOCUS ON THREATS, COMPANIES GEAR UP TO PLAY ROLE

By **MARJORIE CENSER**
and **TOM TEMIN**

When cybersecurity firm Triumfant was founded in late 2002, it developed software meant to assist help desks in managing information technology problems. The company soon found a more valuable use for its software: detecting malicious acts on networks of computers and making automatic fixes.

Earlier this year, the small Rockville-based firm, which has fewer than 20 employees, announced it is partnering with Fairfax-based SRA International, a major government contractor, to beef up SRA's cybersecurity product.

The company — which today works exclusively in the cybersecurity field — is just one of the beneficiaries of what analysts say is a growing boom in cybersecurity work. From small, recently-established firms all the way up to the well-known defense contracting giants, local companies are building up their cyber credentials.

There's plenty of reason for the surge. The increasing number and intensity of cyberattacks has attracted the attention of the Obama administration and Congress, which have begun steering new dollars to the problem. And much of that new spending is focused on the Washington region, as the federal government consolidates many of its cybersecurity-focused agencies in the area.

With the National Security Agency, the soon-to-be-relocated Defense Information Systems Agency and the newly-founded U.S. Cyber Command at Fort Meade; the Department of Homeland Security set to move to Anacostia; and the Pentagon just across the river, a region known for information technology is fast becoming a cybersecurity capital.

"There's this gravitational pull in Washington," said Philip Eliot, a principal at the D.C. private equity firm Paladin Capital Group.

David Z. Bodenheimer, a partner at law firm Crowell & Moring in Washington who leads the firm's homeland security practice and specializes in government contracts, said the unclassified portion of the federal government's cybersecurity work is estimated at $6 to $7 billion annually. The classified portion is likely just as large — and potentially bigger, he said.

"I think it is a real growth opportunity in coming years," Bodenheimer said. "The market is still rather fragmented and in flux, but is developing with a speed that it is attracting both the major defense and homeland security contractors who are establishing independent business units to pursue these opportunities, and it is also a real opportunity for the smaller players who have niche products."

$6-7 billion

government's annual spending on unclassified cybersecurity contracts

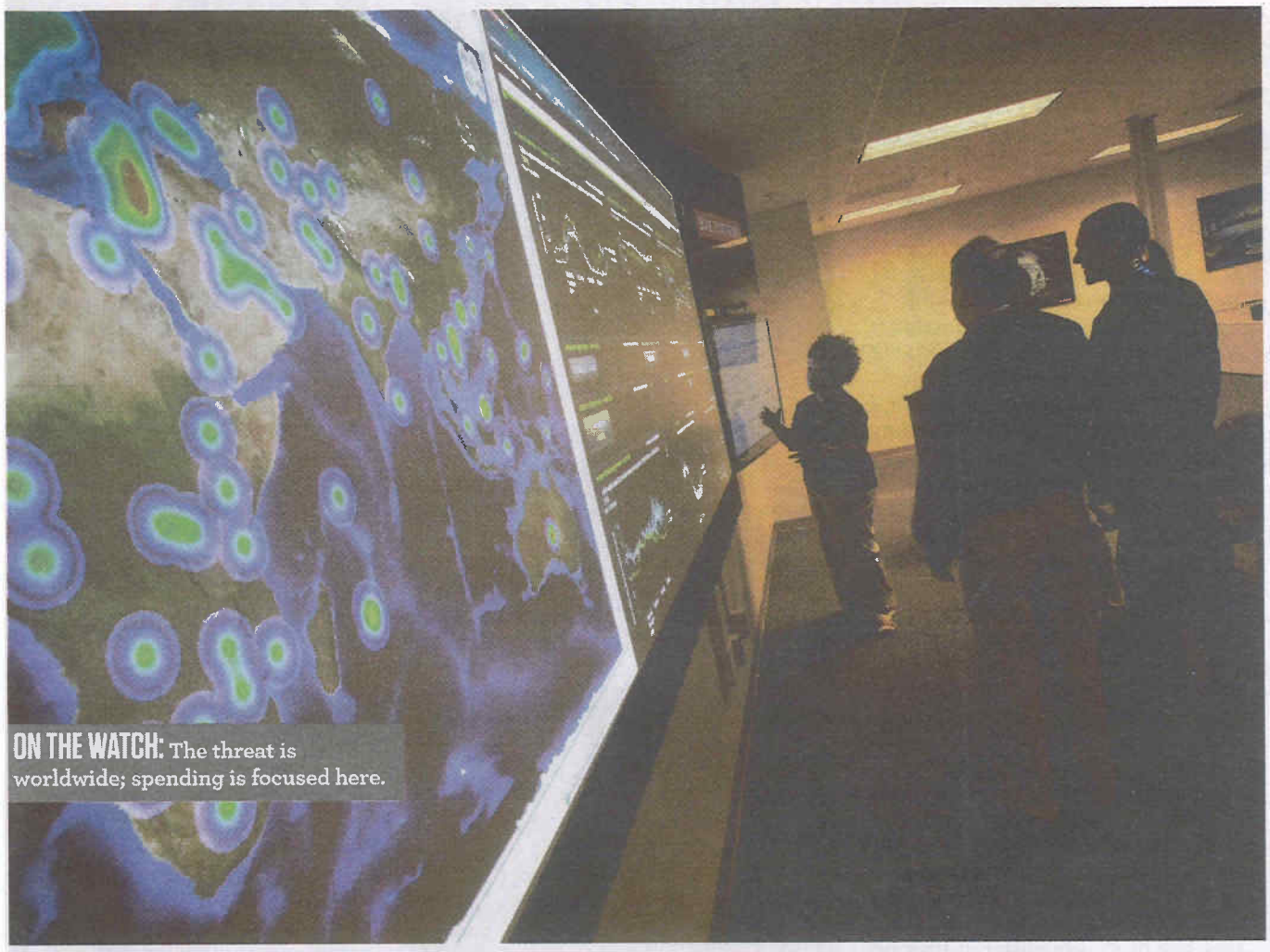
As start-ups and others rush to stake claims, some wonder if a bubble of sorts is beginning to inflate. Roger Novak, founder of Novak Biddle Venture Partners, recalled that many venture firms in the early 2000s chased similar prospects.

"A lot of the early people made significant money, but there were a lot of 'me too' companies," he said. "So a lot of people in the investment community probably absorbed losses in the space and began to move on."

But now, he said, the administration's focus is once again piquing venture interest and spurring larger companies to pursue acquisitions of companies that already have cybersecurity footholds. Novak is bullish on the sector; after all, his firm invested in Triumfant in 2006.

Eliot said key opportunities right now are in securing mobile devices, protecting against Web-based attacks that come from reputable Web sites,

» *Continued on following page*



ON THE WATCH: The threat is worldwide; spending is focused here.

David Z. Bodenheimer: "The market is still rather fragmented and in flux, but is developing with a speed that is attracting both the major defense and homeland security contractors."

» *Continued from previous page*

and fending off internal threats.

Those are problems "that to date don't have good solutions," he said.

One reason the field is attracting so many companies is that the barriers to entry are low — at least relative to other defense industries.

"The strictly defense markets largely have strictly defense suppliers," said David L. Rockwell, a senior analyst at the Teal Group. "In cybersecurity — so far you [have] had a lot more variety in who's able to get contracts, and I think we can expect that to continue."

The big defense contractors are moving quickly to protect their turf. Lockheed Martin in late 2009 opened what it calls the NexGen Cyber Innovation and Technology Center, a research and development center, in Gaithersburg.

The center brings together 14 companies — including Hewlett-Packard, Intel, McAfee, Microsoft and Symantec — that make up a cybersecurity technology alliance formed at the same time.

BAE Systems opened in January a new cyber facility in Columbia intended to give BAE a "world-class analytical capability," said John Osterholz, the company's vice president for cyberwarfare and cybersecurity. Staffed by 20 to 25 people, the office helps BAE quickly understand and characterize threats.

And Chantilly-based TASC, divested from Northrop Grumman last year, has named a new lead executive for its cyber business, said TASC's president and chief executive, Wood Parker.

"I'm sure that every company says that they are interested or they have a cyber business," he acknowledged. "I can tell you that TASC has a robust cyber business today."

The largest IT and defense contractors are keenly interested in helping the government manage its computer networks. Lockheed Martin, Boeing, General Dynamics, ManTech International, Northrop Grumman and SAIC (which recently acquired CloudShield Technologies) are all competing in the space.

Smaller companies see more opportunity in creating products that can protect networks or help the government keep tabs on threats — especially if that gear and software can be deployed across agencies and departments.

A key player in shaping future business is likely to be the Commerce Department, chiefly via the National Institute of Standards and Technology in Gaithersburg. NIST has been systematically revising its extensive collection of guidance documents for network security. It is including industry and military experts in these revisions in an attempt to unify approaches taken by the federal government broadly.

NIST figures prominently in legislation making its way through Congress. A major bill, reported out in late March by the Senate Commerce, Science and Transportation Committee, chaired by John D. Rockefeller IV (D-W.Va.) would create a cybersecurity advisory panel with the White House, designate the Commerce Department as the clearinghouse for cyberthreat information, and strengthen NIST's authority to set cybersecurity standards for federal contractors and grant recipients. The bill, S 773, would also give the National Science Foundation new authority to establish what it calls a Federal Cyber Service: Scholarship for Service program.

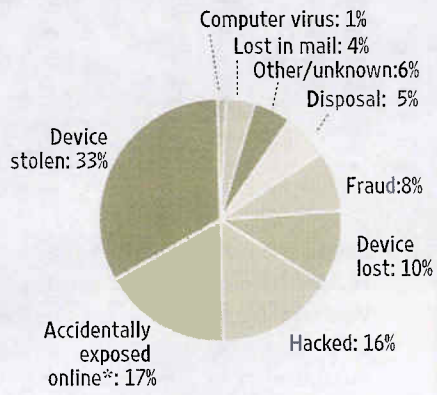
On the House side, the Homeland Security, Science and Technology Authorization Act would double the money available to DHS for cybersecurity research and development.

censerm@washpost.com

Censer is a Capital Business staff writer. Tom Temin has followed federal information technology for nearly 20 years. He is co-host of "The Federal Drive" on Federal News Radio (1500 AM), weekdays at 6-10 a.m. He has also launched a new technology blog, Temin on Tech.

Losing it

No matter how many companies engage in protecting data in cyberspace, there will always be a risk of human error. A breakdown of the causes of reported data breaches over the past 10 years:



*Includes e-mailing and posting on a public site

SOURCE: Open Source Foundation *Capital Business*

244

federal records compromised in April, when documents from the Naval Facilities Engineering Service Center were accidentally e-mailed to three suspended employees, according to the Open Source Foundation, which monitors reported cybersecurity breaches.

THE CYBERSECURITY CORRIDOR

Government's line of defense runs from Fort Meade to D.C. Can companies be far behind?

By MARJORIE CENSER

Telecommunications companies and government contractors dominate the Dulles Toll Road corridor in Virginia, and biotechnology firms line the corridor along Interstate 270 in Maryland.

What's next? Walter P. Havenstein, chief executive of SAIC, predicts it could be a cybersecurity corridor along the Interstate 95 corridor between Washington and Baltimore.

The government is doing its part by relocating the Defense Information Systems Agency from Falls Church to Fort Meade, Md. and establishing U.S. Cyber Command and the Navy's U.S. Fleet Cyber Command at Fort Meade. The base, just south of Baltimore-Washington International Marshall Airport, is already home to the National Security Agency.

The southern anchor could be the new Department of Homeland Security headquarters going up in Southeast Washington. In between, sits NASA's Goddard Space Flight Center, off the Baltimore-Washington Parkway, and the University of Maryland's College Park campus.

Will industry follow suit? More than a dozen companies with locations near Fort Meade have indicated they are expanding cyber practices, according to the Anne Arundel Economic Development Corp.

Robert Hannon, president of the economic development office, said the county is also seeing real estate respond to anticipated demand.

"If you look at the major business areas around Fort Meade, you'll see five, six, seven major real estate projects that are doing the groundwork for making the land available and starting building," he said. "There clearly is a spike here."

Hannon argued a corridor — albeit one focused on signals intelligence and information technologies — is already in place. Cybersecurity, he said, will simply be an added initiative.

"It's already here," Hannon said. "There already is a concentration, and that concentration is growing as we speak."

George Vradenburg, a former AOL Time Warner executive, is one of the founders of the Chesapeake Crescent Initiative, an organization chaired by the governors of Maryland and Virginia and the D.C. mayor to promote innovation within the region.

He said the demand for cybersecurity reaches far beyond the military into areas like health care and financial infrastructure, so creating a true cybersecurity cluster will mean drawing companies that work in other sectors.

"Every business in America and virtually every person in America who communicates via the Internet needs the benefit of stronger cybersecurity techniques," he said.

Attracting major companies to the corridor will depend on the investment Maryland makes and the readiness of the military to assist, according to Vradenburg.

"This depends in part on the willingness of the military to spend some time on thinking about what it is they really need to hold close . . . [and] what it is that can be developed and released to the private sector," he said.

censerm@washpost.com