GROWING OPPORTUNITIES IN THE CYBERSECURITY ECONOMY

CYBER CRIMINALS INCREASINGLY TARGET MIDSIZE BUSINESSES.

>> As worldwide development and growth of the Internet has exploded over the past two decades, it's driven tremendous business opportunities and accelerated globalization while becoming deeply ingrained into everyday life. Unfortunately, that expansion has also been accompanied by an increase in the volume and sophistication of electronic attacks, fraud and espionage, especially against aerospace and defense firms, energy companies and financial institutions.

Although estimates vary as to exactly how much malicious cyber activity is costing U.S. companies, private individuals and the government, the economic impacts range from at least a few billion dollars to possibly hundreds of billions, according to a recent joint study from the Center for Strategic and International Studies and McAfee.

The National Security Agency (NSA) secrets leaked by Eric Snowden earlier this year have certainly stirred up controversy, but they've also brought attention to the broader efforts to bolster cybersecurity around the country. Areas strong in high-tech, defense and IT sectors and experienced in supporting academic collaborations and spinoffs, will especially benefit as private investment and government spending in the sector continue to grow.

TALENT AND PARTNERSHIPS DRIVE SUCCESS

"Cybersecurity is probably going to be one of the largest threats that we face as a nation and it's not going to go away," says Dr. Rick Raines, cyber portfolio manager of the global security directorate at Oak Ridge National Laboratory. "Companies are developing new technical capabilities and applications that make our lives easier and more convenient, but unfortunately, there are various actors out there — whether organized crime, terrorists, nation-states or individuals — who will try to exploit the vulnerabilities that may exist in new systems."

When looking at cybersecurity issues, there are no one-size-fits all solutions. This has created a challenge and opportunity in the area of human capital, Raines suggests. There are roughly 165 schools across the country educating people in this

area, but even if all of these institutions were operating at full capacity, they still would probably not meet the need for different types of specialists in the field. That's where building partnerships and leveraging talent is key, he says.

"Besides threats at the national level, we're seeing a shift in the way cybercrime is going," says Gary Warner, chief technologist at Malcovery Security and director of research in computer forensics at the University of Alabama at Birmingham (UAB). "Where in the past we saw mostly individuals and then very large banks being attacked, the sweet spot for today's criminals has turned out to be midsized businesses.

"From an industry standpoint, we're seeing that not only are the large existing security companies beginning to diversify their offerings to address this space, but also many new companies are starting up and quite often being acquired," Warner continues. "The concept of threat intelligence as a company model is really taking off."

To drive innovation and support emerging businesses in the sector, Warner urges more commercialization of fundamental research that's going to help protect businesses from electronic crime. "The main thing you need is an academic base," he says. "There's no point in saying you're going to become a 'Silicon Alley' if you don't have a strong university with an understanding of economic development and the ability to create strong local talent and produce in this area. Having a community come together and create something like what we have at the UAB Innovation Depot to help young companies in the industry survive is a major advantage."

In addition to industrial crimes, the theft of military technology data — which also affects export markets for defense technologies and products — has become more common as well. To counter such threats, the U.S. Department of Defense (DoD) intends to spend $23 billion on cybersecurity over the next five years, seeking more than $4.6 billion for cybersecurity in fiscal 2014 — an 18 percent increase from 2013. The U.S. Cyber Command's headquarters alone is projected to receive $405 million in 2015 and as much as $1.28 billion through 2018, according to Bloomberg News.

EXISTING STRENGTHS COUNTER NEW THREATS

Much of the nation's best-developed cybersecurity infrastructure is centered around the Mid-Atlantic region, especially throughout Virginia and Maryland — home to the Army's Aberdeen Proving Ground (APV) and a large ecosystem of federal agencies, defense contractors and science and technology organizations.

"Two main components to our success are a highly-educated, specialized workforce and a location that's close to Washington, D.C., yet provides a high quality of life," says Jim Richardson, director, Harford County (Md.) Office of Economic Development. "Among the biggest players in cybersecurity in Harford County are SafeNet, the Communications and Electronics

Command at APV, Johns Hopkins University and the Cybersecurity Center at the University of Maryland, all of which attract lots of research and engineering talent."

Other resources fueling local growth in cybersecurity and defense security applications, Richardson says, include the Harford Business Innovation Center and the state's $3 million Cybersecurity Investment Incentive Tax Credit, which uniquely targets industry-specific investments from both either in-state or out-of-state investors.

In Arizona, a strong foundation in aerospace, aviation, financial services and information technology is contributing to a significant and growing cluster of cybersecurity activity.

"Over the last 10 years, we've done a much better job of getting Silicon Valley-based companies to invest in this market thanks to our combination of data service, data management, coding and software development capabilities," says Barry Broome, president and CEO, Greater Phoenix Economic Council. "When you're storing or servicing your data here, it also makes a lot of sense to manage, analyze and protect it here too. A lot of the emerging cybersecurity businesses are a great market for us."

The region features a high-tech talent base attracted by the presence of large companies like eBay, PayPal, Yelp, Honeywell, Charles Schwab, American Express and JDA Software, as well as cyberwarfare research groups such as ARTIS and boutique firms like Bishop Fox and Securosis, which protect much of the *Fortune* 100, Broome notes.

Arizona's cluster also benefits from a communications infrastructure of more than 60 fiber, telecommunications, broadband and wireless providers. Greater Phoenix alone has one of the top 10 regional fiber optic deployments in the United States, with more than 156,000 route miles of fiber-optic network capacity. Academic resources include Arizona State University's new Information Assurance Center and the University of Advancing Technology in Tempe that produce recruits for cybersecurity firms and clandestine agencies of the U.S. government.

Another up-and-coming area leveraging its existing strengths to develop a thriving cybersecurity presence is over in the state of Michigan where new leadership is hosting targeted industry initiatives such as the "*2013 Michigan Cyber Summit*."

"Southeast Michigan and the metro Detroit region in particular are hotspots right now for everything related to IT and software, including cybersecurity," says Michael Finney, president and CEO, Michigan Economic Development Corp. "We expect it to be a growing sector in our state and intend on investing in it pretty aggressively here in the coming years."

Michigan's longtime auto industry has spawned many technologies that cross over to aerospace and defense, Finney continues. "We look at cybersecurity the same way — as a lead for innovations that can be applied in other industries, with the potential for related spinoff opportunities being very significant."

Among the state's cybersecurity assets Finney points to is the state's

leadership in information technology transfer and R&D, with five colleges and universities designated by the NSA as "National Centers of Academic Excellence in Information Assurance."

Since 2003, Michigan has been a member of the Multi-State Information Sharing and Analysis Center, a partnership between state governments and federal agencies, such as the National Cybersecurity and Communications Integration Center at the Department of Homeland Security. To address Michigan's cybersecurity readiness and coordinate the combined efforts of its cyber emergency responders, the state established the Michigan Information Sharing and Analysis Center and is creating the Michigan Cyber Command Center.

SECURING THE FUTURE

Computer and information technology will continue to evolve and so will the threats. As public and private-sector leaders work to protect our security and economic interests, the high demand for firms and professionals in the sector is likely to position cybersecurity as a job creator for years, perhaps decades, to come.

"The threats are becoming more and more prominent and the criminals are working 24/7," Warner cautions. "There's a major shortage of qualified candidates which makes the industry a very good career choice for our young students. But it's also an opportunity for people with existing computer skills to come back and retool themselves to work in the computer forensics and security management space."

"Between hacking, international attacks and other computer threats, I think we're going to see cybersecurity just explode and possibly rival health care as the biggest industry in the United States," Broome says. "Our reputation globally is on the rise in this tech sector and the "all-things-Internet" initiatives we keep developing in the Greater Phoenix area are really going to feed off this digital space. I think we could be the most dynamic market in the country in the next five years."

Mark Kleszczewski is president and CEO of GoBusiness Group LLC and a freelance writer on critical business topics. He can be reached at mark@gobusinessgroup.net.

MORE DETAILS

Greater Phoenix Economic Council
www.gpec.org

Harford County (Md.) Office of Economic Development
www.harfordbusiness.org

Malcovery Security
www.malcovery.com

Michigan Economic Development Corp.
www.michiganbusiness.org

Oak Ridge National Laboratory
www.ornl.gov

University of Alabama at Birmingham
http://thecenter.uab.edu