Pipeline
Your OSS/BSS Information Source.
www.pipelinepub.com Volume 7, Issue 3

Multi-Disciplined Partnerships are Central to Country's Cybersecurity

By Greg Oslan

Recently, attacks on our government and corporate infrastructure have been occurring with more regularity, compromising corporate, personal, and classified information. No longer is the task of cybersecurity relegated to IT offices and CIOs in the private sector, nor to a select number of government agencies. Instead, a call to action has been put forth to all entities—especially the government—to make cybersecurity a top priority. It is now recognized as one of the most important national security challenges of our time.

> "Government computers are attacked 1.8 billion times a month; U.S. companies have lost billions in intellectual property."

The U.S. government is taking notice, albeit after large-scale attacks in recent years. For example, in August 2007 the United States suffered a wave of cyber attacks, inflicting damage to U.S. national and economic security. The Center for Strategic and International Studies (CSIS) reported that the Departments of Defense, State, Homeland Security and Commerce; NASA; and National Defense University all suffered major intrusions by unknown foreign entities .

More recently, Senate Sergeant-at-Arms Terrance Gainer remarked in March 2010 that government computers are attacked an average of 1.8 billion times a month, and the Senate Security Operations Center alone receives 13.9 million cyber attacks a day. Add to this that senior representatives from the intelligence community have conclusive evidence that U.S. companies have lost billions in intellectual property , and one can safely conclude that ineffective cybersecurity undermines our nation's strength and puts the United States at risk.

Undoubtedly, the United States' power, status, and security in the world depend largely on its economic strength; yet, not prioritizing cybersecurity could put this position in jeopardy.

The United States must ask itself some difficult questions:

- Are we prepared to risk an economic disaster because individual hackers, organized crime, or nation states have infiltrated our virtual infrastructure?
- Are we prepared to risk our national security if military secrets fall into the wrong hands or are rendered unusable as a result of a coordinated cyber attack?
- Is the United States ready to face the consequences of not having airtight cybersecurity?

Clearly the issue of cybersecurity must be viewed as a multi-dimensional problem. We are taking our first steps, as exemplified by the launch of the new U.S. Cyber Command under General Keith Alexander, to supplement those activities conducted by the Department of Homeland Security and the intelligence communities. As a nation, we must continue to take specific steps to address this mounting problem. Specifically:

- Leverage the technology expertise of government organizations along with the private sector, and encourage open information sharing between the two.
- Build international relations to help curtail cyber threats
- Have private citizens assist in cybersecurity
- Encourage and support robust private-sector investments in research and development of key

technologies that support the war against malicious cyber activity

Cyber Concerns Hit Washington: Public and Private Sectors as a Coalition

Last May, as he reviewed the nation's cybersecurity policies, President Obama called upon the government to collaborate closely with the private sector to protect the nation's information infrastructure. And, at the March 2010 RSA security conference, cybersecurity czar Howard Schmidt reiterated the president's call to action, stating that the government should "continue to seek out innovative new partnerships—not only within government, but also among industry, government, and the American public."

A lack of information-sharing between the public and private sectors has impeded partnerships necessary to properly address cyber threats. Conversely, cyber criminals, terrorists, and even nation-states freely share information to devise and execute cyber attacks. We, however, need a multi-faceted focus to conquer the problem—and we are seeing a start.

The technology industry is starting to gel and focus its efforts on improving defenses in cybersecurity. There is now a clear perspective that signature-based solutions, purpose-built appliances, manually searching large data stores, and other methods alone are not adequate to protect our computer systems and our infrastructure. Consequently, we are seeing a heightened awareness that events must be correlated and end-to-end, and multi-faceted approaches must be implemented to protect and manage IP networks. To put it simply, "you can't protect or manage what you can't see."

> "Enabling Services are tied tightly to the network and provide CSPs with an opportunity to differentiate themselves from other carriers."

Even with this awareness, we have to question whether we, in the United States, have sufficient knowledge resources to focus on cybersecurity. Not only must we recognize the problem, we must align and train our current resources to find solutions. And since we expect cyber threats to increase in breadth and the sheer number of attempted attacks, we need a call to action in our grade schools, colleges,

> “A lack of information-sharing between the public and private sectors has impeded crucial threat-prevention partnerships.”

and universities for more education before these graduates enter the workforce.

I have seen the rudiments of “eco-systems” being formed to battle cyberthreats. We are participating with partners and systems integrators to provide a holistic and multi-layered approach to cybersecurity. As the recognition of the need for complete solutions grows, I see additional acquisitions, partnerships, and alliances being formed over time because our customers and clients are now understanding the threat and feel the need to address that threat on a holistic basis.

We must be able to share information among various groups that have a common purpose to stamp out cyber threats. One area that needs greater emphasis is that of information-sharing between the public and the private sectors. A lack of information-sharing between the public and private sectors has impeded partnerships necessary to properly address cyber threats. Conversely, cyber criminals, terrorists, and even nation states freely share information to devise and execute attacks. This not only requires a change to the way private industry and government work together, in many cases it will require changes to our laws to allow information to be shared. Awareness and support from our legislators in Congress, the Senate, and the courts is needed now, not in our traditional multi-year, political process of changing laws. The problem is now and it is only getting worse. If we don’t take real actions today, then our ability to control it later will be severely compromised.

We might benefit by looking at this issue within a historical framework. Specifically, let’s consider the airline industry around the 1930s, during which international travel began in earnest, and the beginning of World War II demanded the separation of private and military air space. Multiple policies, procedures, international treaties, and firm military consequences were put in place to ensure that we could freely protect our airspace, while simultaneously enabling the commercial airline industry to successfully create a business. In the same way that the government established landing rights for commercial flights, so too should the

> "Not only must we recognize the problem, we must align and train our current resources to find solutions."

government work closely with the private sector to ensure that all cyber traffic is "good traffic."

Second, we must continue to encourage the best and brightest minds in government, industry, and universities to tackle these problems. I have seen progress in this area through some systems integrators developing and implementing cyber labs for the industry. That is a good start and should be expanded to every university. At Narus, we fund a program in which we work closely with universities to develop methods and algorithms to understand traffic as it moves across networks and to counter cyber threats. We are beginning to see some of the fruits of our efforts as we leverage the NarusInsight system's visibility into traffic and apply our latest analytics to identify anomalies as they traverse networks.

International Relations a Critical Piece to the Puzzle

Another area of cooperation entails the support among the international community to solve the problem. We must realize that cyber threats, in essence, can be a pandemic. Given the interconnectedness of the Internet, everyone on our RSA panel agreed—as does the industry as a whole—that the problem of cybersecurity is one that our government must engage in at an international level. To this point, former presidential advisor Richard Clarke argues in his new book that international agreements are crucial to prevent cyber warfare. Not surprisingly, he also states that international cooperation is necessary in identifying the source of attacks that violate these agreements.

Of course, the United States is often the victim in this cybersecurity challenge as other countries seek to explore how they might achieve an advance in cyberspace. In March 2009, two separate reports implicated China in a major cyber espionage operation that compromised nearly 1,300 computers in more than 100 countries. The computers, which include machines at NATO, governments, and embassies, were infected with software that allows attackers to gain complete control of them, according to the reports .

One potentially encouraging sign about our ability to negotiate cyber agreements came at a Russian-sponsored conference on Internet security held in April in Garmisch, Germany. A New York Times article stated that, at the conference, "the Russians were optimistic that progress was being made in bridging more of the cultural divide that has hindered international cooperation." More materially, the story noted that, according to Russian officials, Russia and the United States "have agreed to renew bilateral discussions that began last November in Washington."

The Role of Private Citizens in Cybersecurity

Engagement with foreign governments and private industry by our administration, ultimately, may not be enough: until the American public looks at the threats of cyber intrusions as passionately as issues such as healthcare and the economy, significant change may only be incremental. We must recognize that computers and the Internet are the bedrock for our economy. The electric grid, the water supply, the air traffic systems, most financial transactions, and the very essence of our communications via texting, e-mailing, and voice all rely on the Internet. A sustained, well-coordinated attack or set of attacks in close time frame to one another on one or more of these valued assets would be an unfortunate wake-up call. But we must not wait until then to act. Cybersecurity must no longer be regarded as a mere "insurance policy;" but rather, it must become an issue that we deal with collectively as a world population, seriously and urgently.

Certainly, these are complex problems, and ones that won't be solved by technology alone. Ultimately, they are issues that we'll need to address with a combination of technology, people in our workforce trained in this unique skill set, smart legislation, foreign policy, and partnerships between the public and private sectors.