



Testimony

Bolstering US Cybersecurity

Robert Holleyman, President and CEO, BSA | The Software Alliance

Testimony before the US House of Representatives, Committee on the Judiciary, Subcommittee on Crime, Terrorism, Homeland Security, and Investigations

Hearing: Investigating and Prosecuting 21st Century Cyber Threats

March 13, 2013

Mr. Chairman, Ranking Member Scott and distinguished members of the Subcommittee, thank you for convening this hearing and for drawing attention to the issue of cybersecurity.

My name is Robert Holleyman. I am president and CEO of BSA | The Software Alliance, an association of the world's leading software companies. They operate on the front lines of the digital economy, investing heavily in research and development to provide software solutions and security tools to consumers and enterprises in all sectors of the economy. BSA member companies understand better than anyone the nature of the cybersecurity threats America faces today — and what we can do to confront them.

The Growing Threat Landscape

BSA member company Symantec publishes an annual *Internet Security Threat Report*. The most recent edition found more than 400 million unique variants of malicious computer code present in the global IT ecosystem. And only a few years ago, BSA member company McAfee identified a new piece of malware every 15 minutes. Today it's one per second, and McAfee's Fort Detrick-like vault of dangerous digital viruses contains more than 100 million specimens. Moreover, hack attacks on mobile devices are up over 700 percent in one year.

Cybercrimes and attacks carry enormous economic costs and security risks. For example, Symantec has calculated that cybercrimes perpetrated on consumers alone account for \$110 billion in damages. This does not take into account harm done to government computers or the value of intellectual property stolen from businesses.

There are increasing numbers and varieties of advanced, determined, and persistent threats targeting businesses and government. Recent attacks on major US Banks were one

alarming example. Another was the attack on Saudi Aramco, the world's largest oil producer. Its entire computer network — at least 30,000 computers — were shut down. Employees were forced to run oil production processes with telephones and fax machines.

The important lesson we should take from these attacks is that cybersecurity threats are becoming bigger and more sophisticated. We need to respond by bolstering America's cybersecurity posture for what will be an ongoing fight.

BSA Recommendations

➤ Promote real-time sharing of cyber-threat information.

Legislation is needed to promote increased sharing of cyber-threat information. First and foremost, we need to ensure that government shares a greater quantity of actionable information with the private sector. Information should be categorized according to its actual level of sensitivity, not deemed "Top Secret" by default. This will ensure that frontline IT professionals have access to essential cyber threat information. BSA also believes that applications for security clearances for cybersecurity professionals should be expedited.

There should also be more sharing among and between private companies and the government. Legislation can help by eliminate unnecessary legal barriers that serve to deter the timely sharing of threat information with those who are actually positioned to act on it. The legal changes should include safeguarding of trade secrets and ensuring that there are adequate liability protections, while also carefully balancing privacy and civil-liberties concerns. This includes ensuring that any new liability-protected channel for information sharing by industry with the government is run by a civilian agency.

➤ Strengthen law enforcement tools and resources.

Despite concerted efforts by authorities at all levels, budget constraints and gaps in existing law make it harder than it should be to effectively investigate and prosecute of cybercrime. If we reach a point where criminals can act with virtual impunity, it would threaten online consumer confidence in the security of ecommerce. To ensure this doesn't happen, Congress should close loopholes in criminal statutes and stiffen penalties and sanctions to provide more effective deterrence. It also should provide more resources to law-enforcement authorities so they can keep pace with evolving threats. FBI Director Robert Mueller previously testified that cybercrime is a top priority for the FBI. This is as it should be. However, we must make sure he has the resources to back that commitment up.

It is important for laws and law enforcement to be strengthened in appropriate proportions — so that innocent and minor infractions are not over-penalized, but serious crimes are effectively deterred.

Finally, legislation should strengthen and support federal authorities' ability to coordinate and collaborate with their counterparts internationally. BSA member Microsoft has studied infection rates of computers around the world. The company found that countries with the lowest malware infection rates were significantly more likely to have signed one or more international treaties on cybercrime. For this reason, BSA believes that giving the federal government greater authority to improve the quality of legal frameworks around the world would be a positive step.

➤ **Support cybersecurity research and development.**

Technological innovation is our best tool against cyber-criminals. Comprehensive cyber-legislation should contain a robust R&D plan and give researchers more resources to develop new technologies and practices that will improve the country's cybersecurity posture.

➤ **Reform FISMA.**

There is overwhelming agreement that the Federal Information Security Management Act of 2002 (FISMA) needs to be reformed. The Act was an important step in improving our nation's cybersecurity, but its effectiveness in today's world is questionable. FISMA serves as a reminder that legislation should be written with the understanding that the future is unpredictable and that the cyber-landscape will undoubtedly change faster legislation can be updated. To make FISMA more "future-proof" — and to support important work being done by the Administration to move toward more dynamic models of risk management — the law should be reformed to encourage agencies to engage in continuous, real-time monitoring instead of conducting rigid, "check-the-box" exercises. This shift in tactics will make federal IT systems more adaptive and reliable.

➤ **Pass a uniform data-breach notification law.**

A separate, but related cybersecurity issue is how and when to notify people when a data breach has compromised their personal information.

First, BSA believes organizations should adopt security measures that are appropriate for the level of sensitivity of the data and information they are holding. If, despite those security measures, a breach occurs that poses significant risk of serious harm, then there should be consistent national policies to ensure that customers and consumers are notified in an appropriate manner.

Today, 47 states have data-breach notification laws. And while we have managed to adapt to these various laws, a properly defined data-breach notification standard would go a long way to guide organizations on how to address cyber threats in their risk management policies. It also would help prevent breaches and give guidance on how best to respond if

an organization should fall victim to a breach caused by an attack. It would be particularly helpful for smaller businesses. Because of the Internet, they are able to do business in every state, but many cannot afford teams of lawyers to navigate 47 data breach standards should something bad actually happen.

National data-breach legislation should be carefully crafted, and in particular be technology-neutral, to help organizations prevent and respond to security incidents while avoiding costly, burdensome rules that would not provide any real protection to consumers and freeze security innovation. Such legislation will provide much-needed regulatory relief to companies facing conflicting legal obligations under today's patchwork of state laws.

Effectively Implementing the Executive Order on Critical Infrastructure

While Congress works on cybersecurity legislation, the Administration has begun implementing the President's recent Executive Order on protecting critical infrastructure. Implementing the Administration's policy effectively should be one of our biggest priorities. The Executive Order attempts to:

1. Improve the coordination of cybersecurity policy within the federal government;
2. Increase and accelerate "government-to-industry" information sharing efforts while at the same time protecting privacy and civil liberties;
3. Establish a "framework" to reduce cyber threats to critical infrastructure through a voluntary program with industry; and
4. Use of market-based incentives to encourage adoption of industry-led standards and widely accepted business practices beyond just critical infrastructure.
5. Make the preservation of innovation a central principle of our country's efforts to strengthen cybersecurity.

BSA welcomes the Order's emphasis on innovation and applauds the measures to improve coordination and increase information sharing. But we believe it will be important to develop the framework on critical infrastructure protection in careful partnership with industry. Even more important is ensuring that this work continues to be led by NIST, which has an admirable track record of working with industry to identify and foster the development of consensus-based guidance that leverages globally recognized standards and widely accepted business practices. Done well, there is an opportunity for it to serve as a model for best practices beyond just infrastructure that is deemed critical. It also can serve as a formula for other countries that tend to favor strict, command-and-control regulations that are ill-suited to the modern cybersecurity environment because of their inflexibility.

Conclusion

There will be no silver bullet to effectively combat cybercrimes and attacks. Instead, the public and private sectors need to have a variety of tools at their disposal. I appreciate the opportunity to testify today. BSA looks forward to working with Congress to bring these urgently needed policy solutions to fruition.