Statement for the Record

Andrew H. Tannenbaum
Cybersecurity Counsel, IBM

Before the
United States House of Representatives
Permanent Select Committee on Intelligence

Regarding
The Growing Cyber Threat and its Impact on American Business

Thursday, March 19, 2015

Chairman Nunes, Ranking Member Schiff, and distinguished Members of the Committee, I am pleased to appear before the Committee today to discuss the impact of the cyber threat on American companies. In my testimony, I will focus in particular on the importance of enacting legislation to provide legal clarity and protection for the voluntary sharing of cyber threat data that companies use to defend their networks.

The Growing Cyber Threat

The cyber threat today is well known. Every day, malicious actors across the globe seek unauthorized access to computer systems to steal the personal data of individuals and the confidential data of businesses and governments. Some are motivated by financial gain, others by political or ideological goals. Valuable intellectual property that took companies years to develop has been stolen in milliseconds. Sensitive personal information such as Social Security numbers and financial account information has been taken and sold on the black market. And we have seen hackers not just steal data, but also disrupt and destroy computer systems, demonstrating that there are greater risks to our critical infrastructure and national security. Privacy, confidentiality, and security are at risk, and no company or entity is immune.

IBM understands the cyber threat from the perspective of a company that is responsible both for securing its own global infrastructure (spanning over 175 countries and more than 375,000 employees) and for providing information technology security services and solutions to virtually every sector of business worldwide. Our clients—many of the largest enterprise companies in the world—are as focused as ever on the need to defend their networks and data against a constant threat of attack. To help safeguard our clients' most critical data and systems, IBM provides a full range of enterprise security solutions, including advanced analytics, security intelligence platforms, intrusion detection and prevention services, anomaly detection, application security, mobile and cloud security, vulnerability management, event and log management, fraud protection, endpoint protection, incident response and forensic services,

identity and access management, and high-end consulting such as security assessment and design.

Risk-Management Approach

Evolving security threats can overwhelm many organizations. Not so long ago, in order to protect its electronic data, a company was mainly concerned with its own employees accessing a few highly controlled applications on a mainframe. Today, companies have potentially millions of users accessing their systems remotely, the amount of data they are responsible for securing has increased exponentially, and the rate of new applications being developed in the world of mobile and cloud is astonishing. This explosion in technology, data, and access has created a sea of new risks and hidden vulnerabilities for hackers to exploit.

The velocity and volume of this threat requires a comprehensive, risk-based approach to cybersecurity. Even the most sophisticated companies know that they cannot eliminate all cybersecurity risk, and they do not have unlimited resources to do so. There is no silver bullet when it comes to cybersecurity—the threats are simply too diverse and dynamic. Instead, companies need to be able to address and manage risk in a systemic and intelligent way across their enterprises. This includes identifying the areas of potential risk relevant to their infrastructure, prioritizing the mitigation of those risks, allocating resources based on that prioritization, and continually setting goals and tracking progress. IBM helps its clients with all stages of risk management, providing companies with advanced and integrated security tools and solutions that map to specific business requirements to address their complex security needs.

IBM has been a strong supporter of the National Institute of Standards and Technology's (NIST's) *Framework for Improving Critical Infrastructure Cybersecurity*,[1] which is aligned with the same risk-management approach. Developed through an exemplary process of public-private collaboration, the NIST Framework appropriately recognizes that lists of specific controls or check-the-box compliance regimes often do not address the actual risks businesses face every day and cannot keep pace with the constant change of cyber threats. Accordingly, the Framework does not instruct companies how to defend their networks. Rather, companies are encouraged to use the Framework voluntarily as a tool to identify and manage risk, and to check their own processes against examples of globally recognized standards and practices. The Framework is designed to be flexible and encourage innovation; companies can adapt and customize the Framework to their own needs, whether that means using it to inform an already established information security program or creating a new one from scratch.

IBM is pleased that the Administration and Congress have both supported the non-regulatory NIST Framework approach. The Administration has made clear that the Framework process should remain collaborative, voluntary, and agile, and that the government should not be in the business of promoting outdated and inflexible rules and procedures.[2] Congress also gave its stamp of approval for the NIST Framework when it passed the Cybersecurity Enhancement Act of 2014 this past December.

---

[1] See www.nist.gov/cyberframework.

[2] See Michael Daniel's May 22 blog, *Assessing Cybersecurity Regulations*, at www.whitehouse.gov/blog/2014/05/22/assessing-cybersecurity-regulations.

Information Sharing

A vital element of any enterprise cybersecurity risk management program is the ability to share and receive information about cyber threats. To manage risk, you need to understand it, but the pace at which cyber risk develops and evolves can seem dizzying to companies big and small. To stay ahead of the hackers, companies need timely and actionable information about specific threats to their infrastructure. And because malicious actors can move through networks at light speed, such threat information needs to be available to potential victims in as close to real time as possible.

IBM understands the importance of cyber threat information first hand. Our business has one of the world's largest cyber threat and vulnerability databases, and we monitor billions of security events for thousands of clients every day. We know from experience that such information provides organizations with visibility and insight into threats that they would not have otherwise. Attacks targeted at specific organizations, for example, may have attributes or patterns of activity that are common across attacks on other entities. When combined with the power of advanced analytics, the sharing of cyber threat indicators can deliver some of the most meaningful insights for protecting potential victims of cyber attacks.

Twenty-first century security is, after all, a data analytics challenge. Because attackers can no longer be fenced out completely with firewalls, the real-time discovery of anomalies and security events within a company's infrastructure is a key element of network defense. Cyber threat data is the fuel that powers the modern security analytic engine.

There are some positive steps that the Administration has taken to improve cyber threat information sharing, but there are limits to what can be done by Executive action alone. Legislation is needed to address key issues and provide companies with appropriate legal protections for the voluntary sharing of threat information. Information sharing legislation should be the immediate priority for Congress in addressing cybersecurity, and IBM strongly urges the passage of such legislation.

IBM would like to emphasize three issues of importance that should be addressed in any information sharing bill: privacy, liability protections, and provisions for sharing information with the government.

<u>Privacy</u>

Privacy is of paramount importance to IBM and our clients. Indeed, IBM has a long history of leadership and trust on privacy issues, from adopting the world's first corporate global privacy code of conduct, to appointing one of the world's first chief privacy officers, to becoming the first major business to establish a genetics privacy policy.

Any cybersecurity information sharing legislation enacted by Congress must be designed to protect the privacy of individuals. It is important to emphasize that the vast majority of cyber threat data does not contain personal information, and companies almost never need to share personal information when alerting others to cyber attacks. Instead, there are categories of technical data that are widely understood to help combat cyber threats, such as the technical markings of a piece of malware, security vulnerabilities in products and the techniques for

exploiting them, and known malicious Internet Protocol addresses that should be blocked from communicating with a company's network. Any information sharing bill should focus on the sharing of these types of technical cyber threat indicators, which rarely implicate privacy concerns. To the extent the sharing of deeper forensic material is required in more limited circumstances, such as an authorized law enforcement investigation into a cyber crime, strong steps must be taken to protect any associated personal information.

Similarly, legislation should recognize that organizations need to monitor their own networks for cyber threats, but Congress should make clear that it is not authorizing any new government surveillance authorities. Rather, there are certain network monitoring activities undertaken by companies that are widely accepted as security best practices, such as the scanning of a company's own networks or devices (or, upon written request, a customer's networks or devices) for indicators of malware, phishing attacks, data loss, unauthorized devices or connections, and software vulnerabilities. The NIST Framework, for example, includes whole categories on "Security Continuous Monitoring" and the detection of "Anomalies and Events."[3] Any monitoring authorization included in a bill should focus on these types of activities conducted by companies as part of accepted best practices.

Ultimately, the goal of information sharing is to protect privacy by helping to better protect the confidential data of potential victims of cyber crimes. Congress can and should help communicate this important message through strong protections for individual privacy and clear, appropriately tailored definitions of the activities authorized and information to be shared.

Liability Protection

The main reason information sharing legislation is needed is to provide legal clarity and protection for companies that seek to better protect their own networks or help other potential victims through the sharing of threat indicators. This is not necessarily because certain types of information sharing or network defense activities are prohibited under current law, but because current law largely consists of a patchwork of older statutes that were not written with the cyber threat in mind. Combined with the rapidly evolving nature of cybersecurity, this has led to an uncertainty among some companies about what they are permitted to do to protect their networks and to assist others in doing the same.

Updating federal law to provide legal clarity and protection against frivolous lawsuits will encourage many more companies to share threat information. Such a result will benefit everyone by helping make American industry more cyber secure. Similar liability protections exist in current privacy statutes for other lawful activities, and the same clarity should be provided for valid cyber defense activities.

In addition to being able to rely on appropriately tailored authorizations for network defense activities and the sharing of threat information, companies need to be assured that information shared voluntarily will be protected from disclosures that are not authorized by the sharing entity. Companies must be able to control when and with whom their information is shared, so that they can protect their proprietary data, preserve legal safeguards such as attorney-client

[3] *See* NIST Framework, Appendix A, at 30-31.

privilege and trade secret protections, and prevent premature public disclosure of security vulnerabilities that could put companies at greater risk.

To encourage companies to share cyber threat indicators that could expose weaknesses in their networks, legislation must preclude government agencies from turning around and using the voluntarily shared information against the companies in a regulatory or other adversarial context. Companies also will be discouraged from participating in information sharing programs and receiving larger volumes of cyber threat information if by doing so they take on additional liability risk in the form of claims that they should have taken specific actions upon receiving the information. Accordingly, reasonable protection against unfair failure to warn or act claims should be provided. Companies should also be given statutory clarity that sharing cyber threat information does not run afoul of antitrust laws.

Sharing with the Government

Finally, special rules need to be put in place for sharing cyber threat indicators with the government itself. Some proposals would establish the Department of Homeland Security (DHS) as the main portal for industry to share with the federal government and provide liability protection only to companies that share with DHS in the first instance. IBM supports the concept of a DHS-led civilian portal. It is important that a civilian, rather than intelligence, agency serves as the primary entry point for information sharing with the private sector.

Any bill also must recognize that there are other legitimate and lawful circumstances in which a company may, for a cybersecurity purpose, voluntarily share threat indicators directly with an agency other than DHS, such as a law enforcement agency in the event of a potential cyber crime investigation, a regulatory agency, or an agency that is a customer under a government contract. The same legal authority and liability protections should be provided for those information sharing situations as well.

In addition, information sharing legislation should appropriately narrow the circumstances in which the government can use threat indicators shared voluntarily by private entities. Strong oversight and Attorney General-approved protections for the privacy and handling of such information within the government should be implemented to make clear that the bill is designed to promote the sharing of technical cyber threat indicators and is not an attempt to expand the government's ability to collect the personal information of individuals. The government must also improve its own ability to provide industry with timely and actionable cyber threat data in a consistent fashion.

Conclusion

Today's enterprises are under constant siege from sophisticated hackers who use rapidly changing techniques to compromise industry's most critical assets and the private information of individuals. The increased sharing of cyber threat indicators among private and public sector organizations represents an opportunity to level the playing field and enable organizations to gain better visibility into the threats facing them. IBM supports bipartisan efforts to enact sensible and effective information sharing legislation as urgently as possible.

Thank you Chairman Nunes, Ranking Member Schiff, and distinguished Members of the Committee for the opportunity to discuss this important topic. I look forward to any questions you may have.