MICHAEL T. McCAUL, TEXAS
CHAIRMAN

BENNIE G. THOMPSON, MISSISSIPPI
RANKING MEMBER

One Hundred Fourteenth Congress
U.S. House of Representatives
Committee on Homeland Security
Washington, DC 20515

May 24, 2016

U.S. Department of Homeland Security
National Protection and Programs Directorate
Attn: Matt Shabat
Director, Performance Management, Office of Cybersecurity and Communications
cyber.security.insurance@hq.dhs.gov

Re: Docket No. DHS-2015-0068

Dear Mr. Shabat:

Cyberinsurance is a product used to protect businesses from Internet-based risks, and more generally from risks relating to information technology infrastructure and activities. Risks of this nature are typically excluded from traditional commercial general liability policies. If a company chooses to store and maintain a database of any type of personal information, such as names, addresses, Social Security numbers, or payment card details, they are responsible for protecting that data, and a company's reputation depends on its ability to do so.

While it is widely recognized that the first-party cybersecurity insurance market is a embryonic one, particularly when it comes to coverage for cyber-related critical infrastructure loss, issuers have cited several reasons for their limited offerings in this area, chief among them being: a lack of actuarial data; aggregation concerns; and the unknowable nature of all potential cyber threat vectors. Additionally, I have concerns about how these limited offerings affect small and medium sized businesses.

Many companies have become increasingly aware of cyber risk as a result of highly publicized data breaches and their costs. This increased awareness will likely help insurance brokers and underwriters make the case for including cyber risk within 'Enterprise Risk Management' (ERM) programs in the future.

In recent years, the Department of Homeland Security's (DHS) National Protection and Programs Directorate (NPPD) has brought together insurance stakeholders in a public-private forum to discuss the benefits and impediments to cybersecurity insurance. The group convened under the name Cyber Incident Data and Analysis Working Group, or

CIDAWG (c-dog), and included groups of private and public sector stakeholders – including insurance carriers, risk managers, IT/cyber experts, critical infrastructure owners, and social scientists – to examine the current state of the cybersecurity insurance market and how to best advance the industry's capacity to encourage and reward better cyber risk management for companies at large.

Challenges for Small and Medium sized Businesses

As small and medium sized businesses continue to leverage broadband technology, including smartphones, mobile payments, and the cloud, they must increase their information security and follow best practices to continue to run efficiently. Small businesses face unique challenges in addressing cyber insurance to help them mitigate interruptions to business and financial loss from cyber-attacks.

According to a 2012 Verizon Data Breach Report, 71 percent of commercial cyberattacks occur at businesses with fewer than 100 employees,[1] and the average cost of a data breach for those small businesses is $36,000. Other reports indicate that up to 83 percent don't have a formal cybersecurity plan to protect against cyber threats.[2] As larger companies improve cyber defenses, American small businesses are becoming more vulnerable targets. According to Symantec, a large American cyber security, mid-size and small businesses were subject to hundreds of millions of cyber threats in just the first few months of 2012.[3] A typical cyber-attack that infiltrates a medium-sized business can cost, on average, close to $200,000 – enough to put many of them out of business.[4]

.

Many mid-size and small businesses are struggling with their cyber and information security efforts, and are particularly ripe targets for cyber-attacks. Often these businesses are the weakest link in the supply chain for larger corporations. They lack the resources, time, and expertise, and consequently will have a more difficult time qualifying for comprehensive cyber insurance. Large corporations realize their dependence on mid-size and small businesses, and that the corporation's greatest vulnerabilities may arise from them. (Example: a HVAC vendor was a key attack link of the Target breach).

As important as the needs of the insurance carriers are in establishing a first-party cybersecurity market, it will be necessary for owners of American companies and critical infrastructure to implement an effective cyber risk *culture* that insurance carriers have identified as particularly attractive from an underwriting perspective:

- Engaged executive leadership;
- Targeted cyber risk education and awareness;

---

[1] http://www.wired.com/images_blogs/threatlevel/2012/03/Verizon-Data-Breach-Report-2012.pdf

[2] 2012 NCSA/Symantec Small Business Study, Oct. 2012: http://www.staysafeonline.org/stay-safe-online/resources/. 87 percent of SMBs do not have a formal written Internet security policy for employees, while 69 percent do not even have an informal Internet security policy.

[3] Symantec Press Release, Oct. 15, 2012. Almost 40 percent of the over 1 billion cyberattacks Symantec prevented in the first three months of 2012 targeted companies with less than 500 employees.

[4] Symantec Global SMB Information Protection Survey, Jun. 2010: http://www.symantec.com/about/news/release/article.jsp?prid=20100621_01.

- Cost-effective technology investments; and
- Relevant information sharing.

Also, collaboration among large, mid-size and small companies is essential to address these challenges, and larger companies can help create an ecosystem of cybersecurity excellence by extending their Enterprise Risk Management (ERMs) practices to mid-size and small businesses that provide supplies and services to their corporate partners.

The development of a mature cyber and information insurance market is generally viewed as a valuable tool to increase and incentivize business cyber-security by encouraging the adoption of best practices. Insurers will require a level of security as a precondition of coverage, and companies adopting better security practices often receive lower insurance rates. The security requirements used by cyber-insurers are likely to become de facto standards, and since insurers will be required to pay out cyber-losses, they have a strong interest in greater information security.

DHS's Cyber Incident Data and Analysis Working Group was a good start to bring large insurance industry stakeholders and large company participation together to focus on their needs. I would assert that now is the time to address the insurance procedures and insurance industry structures needed to support cybersecurity by mid-size and small companies.

Sincerely,

Bennie G. Thompson
Ranking Member
Committee on Homeland Security