STATEMENT ON BEHALF OF WILLIS TOWERS WATSON

BEFORE THE
UNITED STATES HOUSE OF REPRESENTATIVES
COMMITTEE ON SMALL BUSINESS
HEARING ENTITLED, "PROTECTING SMALL BUSINESSES FROM CYBER ATTACKS: THE CYBERSECURITY INSURANCE OPTION"
JULY 26, 2017

On behalf of Willis Towers Watson, we submit the following statement in response to the above-referenced hearing.

Small businesses (SBs) tend to be less concerned about their technology/cyber risks than their publicly traded counterparts. This view may be due primarily to a limited understanding of the scope of risks these organizations face. According to the Verizon Data Breach Report, approximately 61% of data breach victims are businesses with less than 1,000 employees. With this in mind, here are some of the common misconceptions we found among SBs:

a. ***We're not a target for attackers because we don't have valuable data*:** Any business that processes data and is connected to the internet has cyber risk. While SBs often do not have large 'troves' of data, they still have data. Attackers view access to SB networks as a 'path of least resistance.' Compared to large publicly traded companies, SBs may not have significant resources invested and dedicated to protecting their critical assets. As such, it is easier for a hacker to infiltrate a high volume of SBs than one large organization with stronger controls.
b. ***We outsource the storage/processing of data:*** Most SBs think outsourcing data storage and processing will completely transfer their risk and potential liability to the outsource provider. However, the organization that owns the data ultimately has responsibility for it. While there may be some shared liability with outsource providers, most have limit of liability provisions in their contracts. Further, determining liability is a lengthy process and something an organization will be challenged to devote time to while responding to a breach.
c. ***We have adequate technology security controls:*** While technology controls are important and part of the solution, cyber risk at its core is a people risk. Willis Towers Watson claims data reveals that 69% of cyber breaches can be attributed to an organization's employees and can stem from a lost laptop, a disgruntled employee, inadequate cyber awareness training or hiring of non-qualified employees. Therefore, to address these vulnerabilities, it is important organizations to also devote attention and resources to people solutions, such as employee engagement, awareness and hiring the appropriate IT talent.

Both Business to Business (B2B) and Business to Consumer (B2C) organizations should understand their cyber risk and consider cyber insurance as a method of risk transfer. For B2B organizations, it's easier to understand why cyber insurance is important. When dealing with other businesses, there may be contractual requirements that require organizations to carry cyber insurance or technology professional services coverage.

If an organization is providing technology professional services, it is important for them to put together technology professional services coverage with cyber liability insurance, as there is an overlap in coverage. Even if an organization is not providing a technology professional service, cyber insurance should be considered as it can provide balance sheet protection for both first-party coverage (out of pocket expenses – i.e., business interruption, data restoration, and cyber extortion) and third-party liabilities (lawsuits alleging financial harm as a result of an organization's errors or omissions).

For B2C organizations, historical buyers of cyber insurance were industries that held a lot of records (i.e., retail, healthcare and education); however, the more recent cyber claims have affected other industries such as manufacturing, nonprofits and critical infrastructure.

One of the best practices for SBs seeking to understand their cyber exposures is to review cyber claims and losses scenarios, such as the following:

Retail
An online retailer noticed unusual activity on its server, which prompted an investigation. They discovered that hackers had stolen an employee's credentials and used them to access the names, billing addresses and credit card numbers of approximately 50,000 customers during checkout.
Outcome: The insurer retained the appropriate vendors and notified the necessary individuals and agencies. The retailer incurred approximately $1M in first-party costs.

Healthcare
A hospital office employee stole medical profiles, histories and detailed personal information on approximately 125,000 patients.
Outcome: The insurer provided the client hospital with crisis support team, made up of outside vendors, to help resolve the breach and reimbursed the hospital approximately **$800,000** for the crisis team's expenses.

Manufacturing
A consumer products company underwent a software system upgrade performed by a vendor. The system upgrade failed, which caused all of the manufacturer's systems to malfunction on the same day. This caused an unintentional and unplanned outage, which resulted in the suspension of the manufacturer's operations.
Outcome: $2M was paid by the insurer for extra expenses associated with the business interruption, including expenses to continue normal business operations.

Technology Professional Services
A technology services provider of software applications, implementation services and support contracted with a social welfare organization to consolidate and update its legacy IT systems. The social welfare organization filed suit against insured, claiming it failed to meet contractual deadlines, delivered a poorly performing system and failed to properly staff the project.
Outcome: The social welfare organization sought damages in excess of $15M.

Cyber Extortion
A client's computer server was maliciously attacked by a virus that encrypted their data and demanded a $5,000 ransom to unencrypt. The insured reported the matter to the FBI and local authorities, and refused to pay the ransom.

Outcome: The insurer engaged an expert to perform a forensic analysis of the client's system. The expert found the impacted server didn't contain any confidential information. They removed the virus and strengthened the client's data security protections. The insurer reimbursed the insured $45,000 for **forensic costs** incurred.

Handling cyber breaches can be complex and expensive, and costs can easily amount to thousands of dollars or millions if an organization is not proactive. SBs need to take advantage of cyber insurance, as it provides a risk transfer, as well as a partnership with the various experts (such as forensics, attorneys and public relations) that need to be involved in the event of a breach. Most cyber insurers offer their policyholders a choice of breach response services, typically from a list of pre-approved vendors. Many allow the policyholders' own choice of vendor. Most insurers also grant policyholders access to a complimentary cyber risk management portal that includes the most updated information on emerging cyber threats and the latest reports on risk mitigation measures and practices. Moreover, premiums and other terms and conditions are extremely competitive as market conditions are relatively soft with slight rate decreases. This is likely due to additional capacity in the market and underwriters being able to better quantify exposure.

In sum, SBs need to be as proactive as their larger counterparts by: (1) conducting proper risk assessment and quantification; (2) investing in a cyber-savvy culture; (3) insuring cyber threats they can't mitigate and; (4) allocating enough capital to technological cyber defenses.

Willis Towers Watson (NASDAQ: WLTW) is a leading global advisory, broking and solutions company that helps clients around the world turn risk into a path for growth. With roots dating to 1828, Willis Towers Watson has 39,000 employees in more than 120 countries. We design and deliver solutions that manage risk, optimize benefits, cultivate talent, and expand the power of capital to protect and strengthen institutions and individuals. Our unique perspective allows us to see the critical intersections between talent, assets and ideas — the dynamic formula that drives business performance. Together, we unlock potential. Learn more at willistowerswatson.com.