# Client Alert: National Cybersecurity Awareness Month and Board Considerations

October is National Cybersecurity Awareness Month, and cybersecurity continues to be a board-level concern for companies across multiple sizes and industries. In recognition of National Cybersecurity Awareness Month, we are sharing excerpts from Aon's *October 2018 Cyber Predictions: Reality Check* report.

In January, Aon's Cyber Solutions made predictions with regard to cybersecurity trends; in this October 2018 update, we review past predictions, as well as our findings with regard to how those predictions have transpired. A full copy of the report, along with our recommendation for each of these topics can be found here: https://content.strozfriedberg.com/updated-2018-cybersecurity-trends-predictions-report

1. **Prediction:** Businesses adopt standalone cyber insurance policies as boards and executives wake up to cyber liability.

   **Reality:** Businesses continue to adopt cyber insurance policies, as Aon has seen cyber insurance sales grow in excess of 25% year over year.

   Three factors have driven this growth. First, as we predicted, boards and executives have become acutely aware of the potential for financial loss arising out of a cyber attack. The major ransomware attacks from 2017 were a wake-up call. Throughout 2018, for example, businesses have still been reporting losses from the NotPetya attack. Enterprises have seen financial losses and additional expenses estimated starting at USD 2.2 billion per public filings.

   Second, some of these financial losses stemmed from business' inability to operate as a result of the attack. As a result, executives are looking for insurance solutions to help solve cyber-driven business continuity risk.

   Third, insurance carriers have been reviewing cyber coverage extensions under property and casualty policies with increased scrutiny, just as executives have begun to want affirmative protections for damages caused by cyber attacks. Executives have been looking for insurance solutions that address cyber risks, whether under a property or casualty policy, or a standalone cyber insurance policy.

2. **Prediction** As the physical and cyber worlds collide, chief risk officers take center stage to manage cyber as an enterprise risk.

   **Reality:** Stakeholders across organizations are becoming better aligned to address cyber risk as an enterprise risk. One result is a new level of attention on cyber risk quantification.

   As cyber risk becomes treated more like an enterprise risk, traditional risk management practices such as quantification are being applied. Cyber risk quantification helps organizations understand the maximum financial impact of cyber-related financial loss, and then prioritize and plan risk reduction and transfer strategies appropriately.

## We're here to empower results

If you have any questions about your specific coverage or are interested in obtaining coverage, please contact your Aon broker.

aon.com

AON
Empower Results®

3. **Prediction:** Regulatory spotlight widens and becomes more complex, provoking calls for harmonization. The European Union holds global companies to account over the General Data Protection Regulation ("GDPR") violations; big data aggregators come under scrutiny in the US.

   **Reality:** No global company has been held accountable (yet) for GDPR violations, but data privacy and cybersecurity regulations are an increasing challenge for most organizations, as they become more numerous and complex. The GDPR has encouraged U.S. states such as California to pass similar privacy regulations, raising the question if other U.S. states will follow suit. Recently Vermont passed the United States' first law regulating data brokers. At the federal level, the Social Media Privacy Act of 2018 was introduced to the Senate. In February 2018, the Securities and Exchange Commission issued guidance to public companies for disclosing cybersecurity risks and incidents, emphasizing the breadth of corporate liability. Following this guidance, the SEC fined a major internet company millions of dollars for failing to disclose a breach.

## Conclusion

As companies continue to rely on technology, and as the Internet of Things grows, cybersecurity oversight will become a more critical board function. Corporate boards will need to be proactive in engaging industry thought leaders to review insurance programs, quantify the exposure, and utilize such leaders to help mitigate this risk.

### About Aon's Financial Services Group

Aon's Financial Services Group ("FSG") is the premier team of executive liability brokerage professionals, with extensive experience in representing buyers of complex insurance products including directors' and officers' liability, employment practices liability, fiduciary liability, fidelity, and professional liability insurance. FSG's global platform assists clients in addressing their executive liability exposures across their worldwide operations. Aon's Financial Services Group manages more than $2.2 billion in annual premiums, assists with annual claim settlements in excess of $1 billion, and uses its unmatched data to support the diverse business goals of its clients