News From Aon

Aon's Cybersecurity 2018 Predictions: Companies Will Make Major Enterprise-Wide Changes to Address Cyber Risk

Companies to take out more standalone cyber insurance policies; chief risk officer steps boldly into cybersecurity spotlight; greater regulatory pressure globally; increasing importance of multi-factor authentication; full extent of insider risk goes unreported

TORONTO (January 8, 2018) – As cyber attacks increasingly threaten every aspect of business and grow in volume and scale, companies will be forced to take new measures to address cybersecurity risk holistically, integrating it more aggressively into their enterprise risk management, according to Aon's Cyber Solutions industry specialists in the 2018 Cybersecurity Predictions report. The report outlines a number of specific actions that Aon believes companies will take in 2018 to address cyber threats, as well as other cyber trends that it anticipates in the New Year.

"In 2017, cyber attackers created havoc through a range of levers, from phishing attacks that influenced political campaigns to ransomware cryptoworms that infiltrated operating systems on a global scale. With the growth of Internet of Things (IoT), we have also witnessed a proliferation of distributed denial-of-service (DDoS) attacks on IoT devices, crippling the device's functionality" said Jason J. Hogg, CEO, Aon Cyber Solutions. "In 2018, we anticipate heightened cyber exposure due to a convergence of three trends: first, companies' increasing reliance on technology; second, regulators' intensified focus on protecting consumer data; and third, the rising value of non-physical assets. Heightened exposure will require an integrated cybersecurity approach to both business culture and risk management frameworks. Leaders must adopt a coordinated, C-suite driven approach to cyber risk management, enabling them to better assess and mitigate risk across all enterprise functions."

The 2018 Predictions look at the ways in which the increasing scale and impact of cyber attacks, coupled with companies having to accept more liability and accountability over cyber attacks, will lead to significant changes in the corporate landscape. The report predicts an expanding role for the chief risk officer (CRO), the importance of implementing multi-factor authentication, the increased threats from insiders, and an expansion of bug bounty programs in new sectors.

Highlights of the predictions report include:

- **Businesses adopt standalone cyber insurance policies as boards and executives wake up to cyber liability.** As boards and executives experience and witness the impact of cyber attacks, including reduced earnings, operational disruption, and claims brought against directors and officers, businesses will turn to tailored enterprise cyber insurance policies, rather than relying on "silent" components in other policies. Adoption will spread beyond traditional buyers of cyber insurance, such as retail, financial, and healthcare sectors, to others vulnerable to cyber-related business disruption, including manufacturing, transportation, utility, oil, and gas.

- **As the physical and cyber worlds collide, chief risk officers take center stage to manage cyber as an enterprise risk.** As sophisticated cyber attacks generate real-world consequences that impact business operations at increasing scale, C-suites will wake up to the enterprise nature of cyber risk. In 2018, expect CROs to have a seat at the cyber table, working closely with chief information security officers (CISOs) to help organizations understand the holistic impact of cyber risk on the business.

- **Regulatory spotlight widens and becomes more complex, provoking calls for harmonization. EU holds global companies to account over GDPR violation; big data aggregators come under scrutiny in the United States.** In 2018, regulators at the international, national, and local levels will more strictly enforce existing cybersecurity regulations and increase compliance pressures on companies by introducing new ones. Expect to see the EU Commission holding major U.S. and global companies to account for GDPR violations. Across the Atlantic, big data organizations (aggregators and resellers) will come under scrutiny on how they are collecting, using, and securing data. Under the burden of significant and ever increasing regulatory pressures, industry organizations will push back on regulators, calling for alignment of cyber regulations.

- **Criminals look to attack businesses embracing the Internet of Things, in particular targeting small to mid-sized businesses providing services to global organizations.** In 2018, global organizations will need to consider the increased complexities when it comes to how businesses are using the IoT in relation to third-party risk management. However, the report predicts this will not happen, and as a result, expects a large company will be brought down by an attack on a small vendor or contractor that targets the IoT, using it as a way into their network. This will serve as a wake-up call for large organizations to update their approach to third-party risk management, and for Small and Midsized Business (SMBs) to implement better security measures or risk losing business.

- **As passwords continue to be hacked, and attackers circumvent physical biometrics, multi-factor authentication becomes more important than ever before.** Beyond passwords, companies are implementing new methods of authentication – from facial recognition to fingerprints. However, these technologies are still vulnerable and as such, the report anticipates that a new wave of companies will embrace multi-factor authentication to combat the assault on passwords and attacks targeting biometrics. This will require individuals to present several pieces of evidence to an authentication instrument. With the new need for multi-factor authentication, and consumer demand for unobtrusive layers of security, expect to see the implementation of behavioral biometrics.

- **Criminals will target transactions that use points as currency, spurring mainstream adoption of bug bounty programs:** Companies beyond the technology, government, automotive, and financial services sectors will introduce bug bounty platforms into their security programs. Businesses with loyalty, gift, and rewards programs, such as airlines, retailers, and hospitality providers, will be the next wave of adopters, as criminals target transactions that use points as currency. As more organizations adopt the programs, they will require support from external experts to avoid introducing new risks with improperly configured programs.

- **Ransomware attackers get targeted; cryptocurrencies help ransomware industry flourish.** In 2018, ransomware criminals will evolve their tactics. The report predicts that attackers utilizing forms of benign malware—such as software designed to cause DDoS attacks or launch display ads on thousands of systems— will launch huge outbreaks of ransomware. While attackers will continue to launch scatter-gun-style attacks to disrupt as many systems as possible, the report predicts an increase in instances of attacks targeting specific companies and demanding ransomware payments proportional to the value of the encrypted assets. Cryptocurrencies will continue to support the flourishing ransomware industry overall, despite law enforcement becoming more advanced in their ability to trace attacks, for example through bitcoin wallets.

- **Insider risks plague organizations as they underestimate their severe vulnerability and liability, as major attacks fly under the radar.** In 2017, businesses underinvested in proactive insider risk mitigation strategies, and 2018 will be no different. According to the report, with a continued lack of security training and technical controls, coupled with the changing dynamics of the modern workforce, the full extent of cyber attacks and incidents caused by insiders will not become fully public. Many companies will continue to reactively respond to incidents behind closed doors and remain unaware of the true cost and impact of insider risk on the organization.

For Canada, Aon's industry experts see five major trends playing out next year:

- **New breed of IT professional**: In order to better manage potential cyber risks, C-suites, Risk Management, Legal and other enterprise stakeholders will need to speak and understand IT language and concepts. Look for the rise of IT professionals dedicated to enhancing the quality of communications between the departments around cyber-risk.
- **Ransomware beyond money or value:** Cyber-attacks will target brands, not just payoffs, and will look for ways to force companies to change behaviours or simply stop operations.
- **More emphasis on IT employees' engagement:** IT employees are key to protecting companies from major attacks. Ensuring they're engaged will be a major focus to avoid breaches.
- **Canada's mandatory data breach notification law is likely to come into force in 2018:** There will be a renewed emphasis on organizations to establish appropriate breach notification protocols and procedures in line with the requirements of the new regulations.

- **New technologies:** Expect the debut and adoption of alternative identification-authentication methods to make it more difficult for hackers to circumvent ID checks.
- **The Canadian insurance industry starts to deal with the complexities of transferring modern cyber risks.**

“Until recently, Corporate Canada had a lot of uncertainty – and therefore angst – over cyber coverage relating to property and personal injury losses as a result of cyber incident, but times are changing,” says Brian Rosenbaum, Senior Vice President, Financial Services Group, National Director, Legal and Research Practice, ARS Canada. “Coverage is now being restricted in base wordings of traditional policies, but it’s also being offered through enhancements to those policies for an additional premium. We’re also seeing the creation of all-in-one cyber policies that address not only traditional risks such as failure to protect confidential information, but also personal injury and property damage exposures for when cyber attacks become a catalyst for the loss. These moves were long overdue, and we expect them to come into even greater focus in 2018.”

To download the full report, click here.

About Aon
Aon plc (NYSE:AON) is a leading global professional services firm providing a broad range of risk, retirement and health solutions. Our 50,000 colleagues in 120 countries empower results for clients by using proprietary data and analytics to deliver insights that reduce volatility and improve performance.

About Stroz Friedberg, an Aon Company
Stroz Friedberg, an Aon company, is a specialized risk management firm built to help clients solve the complex challenges prevalent in today's digital, connected, and regulated business world. A global leader in the fields of cybersecurity, with leading experts in digital forensics, incident response, and security science; investigation; eDiscovery; and due diligence, Stroz Friedberg works to maximize the health of an organization, ensuring its longevity, protection, and resilience. Founded in 2000 and acquired by Aon in 2016, Stroz Friedberg has thirteen offices across nine U.S. cities, London, Zurich, Dubai, and Hong Kong, Stroz Friedberg serves Fortune 100 companies, 80% of the AmLaw 100, and the Top 20 UK law firms. Learn more at https://www.strozfriedberg.com/.

Follow Aon on Twitter: @AonCanada
Follow Aon on LinkedIn @Aon_Canada

Twitter: @StrozFriedberg
LinkedIn: https://www.linkedin.com/company/stroz-friedberg-llc

Media contacts
For further information please contact Alexandre Daudelin (+1.514.982.4910)

Empower Results®