
2/13/2019

- Eight risk areas underscore how the shift to digital is bringing great opportunity and more risk

LONDON, Feb. 13, 2019 /PRNewswire/ -- Aon plc (NYSE:AON), the leading global professional services firm providing a broad range of risk, retirement and health solutions, released its 2019 Cyber Security Risk Report today. The report, which details the greatest cyber security threats and challenges organizations are currently facing, discusses that as companies continue to use technology to speed up the transfer of information, game-changing business opportunities are created, as well as increased cyber risk.

"In 2018 we witnessed that a proactive approach to cyber preparation and planning paid off for the companies that invested in it, and in 2019, we anticipate the need for advanced planning will only further accelerate," said J. Hogg, CEO of Cyber Solutions at Aon. "Leaders must work to better insulate their companies and their processes, while simultaneously identifying the ways they can benefit from the opportunities offered through technology and digital transformation."

Hogg continued: "Our 2019 report also shows that organizations must recognize the need to share threat intelligence across not only their own network but with others as well. While it may seem counterintuitive when thinking about cyber security, collaboration within and across enterprises and industries can keep private data of companies and individuals alike safer. Working together can result in improved efforts to hunt bad actors, while also raising the bar and making all parties more prepared for the inevitable day when a disruption does happen."

The "What's Now and What's Next" report focuses on eight specific risk areas that companies may face in 2019. The risks illustrate how, as organizations transition to a digital-first approach across all transactions, the attack surface of global business expands rapidly and sometimes in unexpected ways. In other words, thanks to the rapid enhancements and constant changes in technology, the number of touch points that cyber criminals can access within a business is growing exponentially.
Highlights from the report include:

**Technology** – While technology has revolutionized the way organizations today conduct business, broader and wider-spread use of technology also brings vulnerabilities. From publishing to automotive, industries are facing new, evolving services and business models. These new opportunities however, bring with them a radically different set of risks, which organizations will need to anticipate and manage as they continue the digital transformation process.

**Supply Chain** – Two prevailing supply chain trends will heighten cyber risks dramatically in the coming year: one is the rapid expansion of operational data exposed to cyber adversaries, from mobile and edge devices like the Internet of Things (IoT); and the other trend is companies' growing reliance on third-party—and even fourth-party—vendors and service providers. Both trends present attackers with new openings into supply chains, and require board-level, forward-looking risk management in order to sustain reliable and viable business operations.

**IoT** – IoT devices are everywhere, and every device in a workplace now presents a potential security risk. Many companies don't securely manage or even inventory all IoT devices that touch their business, which is already resulting in breaches. As time goes on, the number of IoT endpoints will increase dramatically, facilitated by the current worldwide rollouts of cellular IoT and the forthcoming transition to 5G. Effective organizational inventory and monitoring process implementation will be critical for companies in the coming year and beyond.

**Business Operations** – Connectivity to the Internet improves operational tasks dramatically, but increased connectivity also leads to new security vulnerabilities. The attack surface expands greatly as connectivity increases, making it easier for attackers to move laterally across an entire network. Further, operational shortcuts or ineffective backup processes can make the impact of an attack on business operations even more significant. Organizations need to be better aware of, and prepared for, the cyber impact of increased connectivity.

**Employees** – Employees remain one of the most common causes of breaches. Yet employees likely do not even realize the true threat they pose to an entire organization's cyber security. As technology continues to impact every job function, from the CEO to the entry-level intern, it is imperative for organizations to establish a comprehensive approach to mitigate insider risks, including strong data governance, communicating cyber security policies throughout the organization, and implementing effective access and data-protection controls.

**Mergers & Acquisitions (M&A)** – Projections anticipate that M&A deal value will top $4 trillion in 2018, which would be the highest in four years [1]. The conundrum this poses to companies acquiring other businesses is that while they may have a flawless approach to cyber security enterprise risk, there is no guarantee that their M&A target has the same approach in place. Dealmakers must weave specific cyber security strategies into their larger M&A plans if they want to ensure seamless transitions in the future.

**Regulatory** – Increased regulation, laws, rules and standards related to cyber are designed to protect and insulate businesses and their customers. The pace of cyber regulation enforcement increased in 2018, setting the stage for heightened compliance risk in 2019. Regulation and compliance, however, cannot become the sole focus. Firms must balance both new regulations and evolving cyber threats, which will require vigilance on all sides.

**Board of Directors** – Cyber security oversight continues to be a point of emphasis for board directors and
officers, but recent history has seen an expanding personal risk raising the stakes. Boards must continue to expand their focus and set a strong tone across the company, not only for actions taken after a cyber incident, but also proactive preparation and planning.

Learn more about the risks included in Aon’s 2019 Cyber Security Risk Report. To learn more about the solutions offered by Aon, please also visit Aon.com.


About Aon
Aon plc (NYSE:AON) 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.

Follow Aon on Twitter and LinkedIn
Stay up to date by visiting the Aon Newsroom and hear from our expert advisors in The One Brief.

Media Contact:
Nicole Baudouin, 415-271-1978, Nicole.Baudouin1@aon.com


SOURCE Aon plc