

Posted on January 11, 2017

"The flood of fake news and robot-state-backed attacks in this past year's election are just a sign of things to come, as attackers find new ways to seek faster and wider access to data and exploit sensitive information," he warned.

As governments respond to the threats posed by cyber risks by forming up their online regulatory regimes, businesses may find themselves burdened by the need to interpret 'a fragmented global regulatory landscape' and what that means for their operations, the report indicated.

- **Continued to harness IoT devices as betwixt to breach intelligence.** There will be an increase in compromised IoT devices, harnessed as betwixts and used as launching points for malware propagation, (e.g., distributed denial of service (DDoS) attacks and anonymizing malicious activities).
- **Industry first-movers will embrace pre-NSA cyber security due diligence.** The financial services industry and other regulated sectors will be early adopters of cyber security due diligence as a critical part of the pre-NSA due diligence process, learning from high profile transactions that were derailed in 2016, following the exposure of cyber vulnerabilities.

- **Data integrity attacks to rise.** Data integrity is the need by threat actors to ensure that data is accurate and reliable. "Organizations will seek to solve confusion and doubt over the accuracy and reliability of information, requiring decision-making across the private and public sectors," the report added.

- **Regulatory processes will make "red teaming" the global gold standard with cyber security talent development recognized as a key challenge.** Increased pressure on the security of the supply chain, especially in the automotive sector, is driving the need for a more robust and resilient supply chain. This is leading to a focus on "red teaming" (simulating attacks on the supply chain) and the development of cyber security talent. Regulatory processes will make "red teaming" the global gold standard with cyber security talent development recognized as a key challenge. Increased pressure on the security of the supply chain, especially in the automotive sector, is driving the need for a more robust and resilient supply chain. This is leading to a focus on "red teaming" (simulating attacks on the supply chain) and the development of cyber security talent.

The report also noted that companies, which are not in the cyber business, will face a different challenge: data storage, distribution, optimization and retention. Unlike technical cyber talent in banks,

• **Nation-state cyber espionage and information war to influence global and political policy.** Cyber espionage will continue to influence global politics and remains a major security concern for all nations, particularly the United States, Europe, Japan, and China. Cyber espionage is a major tool for espionage and intelligence gathering, and is used to influence global and political policy.

<sup>10</sup>As government, business, and consumers balance rapid innovation in technology with changing cyber threats, every year sees an identification of existing risks, and a number of

What differs this year is the impetus and mandate to act, because governments worldwide, including the Trump administration, will begin to firm up online regulation and policies

\*With this, businesses in 2017 will be burdened by the need to interpret what a fragmented global regulatory landscape means for its operations," the report said, noting however that the industry is not powerless or obligated to sit by and wait for government directives to manage these risks.

- Optimize company's cyber security posture. Continually assess and prioritize cyber threats and vulnerabilities, and improve incident response (IR) readiness.

- Conduct M&A pre-deal cyber due diligence early. Perform alongside compliance and financial due diligence. Assess, protect and leverage intellectual property, and commercially valuable information.

Photo: <http://www.neurologyjournal.com/news@neurology/2017/05/11/32849.html>

Search

Search

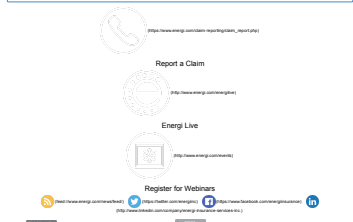
Search

Recent Posts

Amara's TruLens Enterprise Monitoring Technology After Coding Success Milestone (<http://www.energy.com/news/2017/08/america%20trulens%20enterprise%20monitoring%20technology%20after%20coding%20success%20milestone>)

Connecticut Auto Policy Institute on Insurance Profile (<http://www.energy.com/news/2017/08/connecticut%20auto%20policy%20institute%20on%20insurance%20profile>)

Light Foundation Leadership Conference (<http://www.energy.com/news/2017/08/light%20foundation%20leadership%20conference>)



[HOME \(http://www.enr.org/etop/\)](http://www.enr.org/etop/)  
[COMPANY \(http://www.enr.org/etop/contact\)](http://www.enr.org/etop/contact)  
[PROGRAMS \(http://www.enr.org/etop/programs\)](http://www.enr.org/etop/programs)  
[POLICYHOLDER \(http://www.enr.org/etop/etop/etop.html\)](http://www.enr.org/etop/etop/etop.html)  
[PRODUCER \(http://www.enr.org/etop/etop/etop.html\)](http://www.enr.org/etop/etop/etop.html)  
[NEWS \(http://www.enr.org/etop/etop/etop.html\)](http://www.enr.org/etop/etop/etop.html)  
[CONTACT \(http://www.enr.org/etop/etop/etop.html\)](http://www.enr.org/etop/etop/etop.html)  
[REGISTER \(http://www.enr.org/etop/etop/etop.html\)](http://www.enr.org/etop/etop/etop.html)  
[CLAIM REPORT \(http://www.enr.org/etop/etop/etop.html\)](http://www.enr.org/etop/etop/etop.html)  
[ENR'S LIVE \(http://www.enr.org/etop/etop/etop.html\)](http://www.enr.org/etop/etop/etop.html)