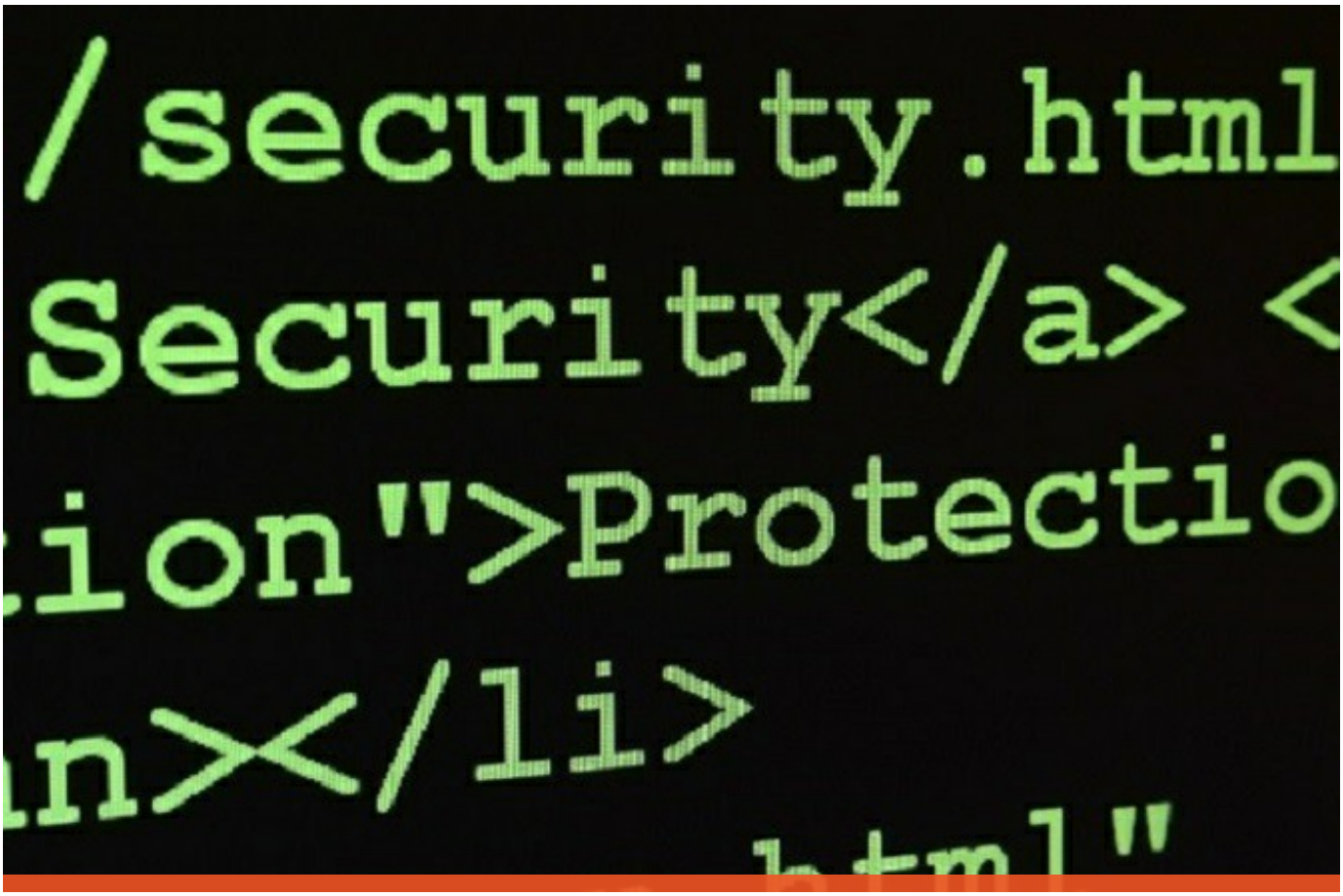
"What will the data breach landscape look like in 2017?"



Dominic A. Paluzzi | Wednesday, November 30, 2016

While many companies have data breach preparedness on their radar, it takes constant vigilance to stay ahead of emerging threats and increasingly sophisticated cybercriminals. To learn more about what risks may lie ahead, Experian Data Breach Resolution releases its fourth annual Data Breach Industry Forecast white paper.

The industry predictions in the report are rooted in Experian's history helping companies navigate more than 17,000 breaches over the last decade and almost 4,000 breaches in 2016 alone. The anticipated issues include nation-state cyberattacks possibly moving from espionage to full-scale cyber conflicts and new attacks targeting the healthcare industry.

"Preparing for a data breach has become much more complex over the last few years," said Michael Bruemmer, vice president at Experian Data Breach Resolution. "Organizations must keep an eye on the many new and constantly evolving threats and address these threats in their incident response plans. Our report sheds a light on a few areas that could be troublesome in 2017 and beyond."

"Experian's annual Data Breach Forecast has proven to be great insight for cyber and risk management professionals, particularly in the healthcare sector as the industry adopts emerging technology at a record pace, creating an ever wider cyber-attack surface, adds Ann Patterson, senior vice president, Medical Identity Fraud Alliance (MIFA). "The consequences of a medical data breach are wide-ranging, with devastating effects across the board - from the breached entity to consumers who may experience medical ID fraud to the healthcare industry as a whole. There is no silver bullet for cybersecurity, however, making good use of trends and analysis to keep evolving our cyber protections along with forecasted threats is vital."

To read the five industry predictions, access the complimentary white paper at http://bit.ly/2fcDeUA. The content also addresses issues such as ransomware and international breach notice laws.

"The 72 hour notice requirement to EU authorities under the GDPR is going to put U.S.-based organizations in a difficult situation, said **Dominic Paluzzi**, co-chair of the **Data Privacy & Cybersecurity Practice** at McDonald Hopkins. "The upcoming EU law may just have the effect of expediting breach notification globally, although 72 hour notice from discovery will be extremely difficult to comply with in many breaches. Organizations' incident response plans should certainly be updated to account for these new laws set to go in effect in 2017."

Omer Tene, Vice President of Research and Education for International Association of Privacy Professionals, added "Clearly, the biggest challenge for businesses in 2017 will be preparing for the entry into force of the GDPR, a massive regulatory framework with implications for budget and staff, carrying stiff fines and penalties in an unprecedented amount. Against a backdrop of escalating cyber events, such as the recent attack on Internet backbone orchestrated through IoT devices,

companies will need to train, educate and certify their staff to mitigate personal data risks."

Click here to read Experian's original press release, available at experianplc.com

Dominic A. Paluzzi