# Cybercrime, Data Breach Crises on the Rise.... Are You Prepared to Communicate with Stakeholders?

*By Deb Hileman*, ICM

For its 2016 Annual Crisis Report, the Institute for Crisis Management expanded its news tracking research database, tracking more than six hundred thousand crisis stories in the news world-wide. We broadened our review of the news in 2016 with more media outlets and adjusted to account for some extraordinary occurrences in highly-charged environments across the globe. Some crisis trends remained consistent year over year, while others grew from spikes in some categories in election-year politically charged climates such as the United States and Europe.

Cybercrime and data breaches continued to make headlines in 2016, with a reported breach increase of 25% in the U.S. alone. Cybercrime stories creeped up slightly to just under 5% of stories tracked by ICM in 2016. The Identity Theft Resource Center tracked 980 reported U.S. breaches comprising more than 35 million records, an increase of 25% over the ITRC's 2015 results.

SO FAR IN 2017 ITRC HAS LOGGED 617 BREACHES, NOT INCLUDING THE MASSIVE RANSOMWARE ATTACKS THAT BEGAN MAY 12, 2017!

Healthcare accounted for 36% of breaches and an alarming 44% of records, while Government comprised 6.7% of breaches for 37% of records hacked. In their annual study, Ponemon Institute and IBM reported the average cost of a data breach at $4 million, a 29% average cost increase since 2013. The study noted an average per-record-breached cost of $158 USD.

Among the notable breaches reported were industry stalwarts like retailer Eddie Bauer, Verizon Enterprise Solutions, Capital One and Charles Schwab, Habitat for Humanity and the Florida Bar Association, Omni Hotels and Wyndham Vacation Resorts, Chicago Public Schools, Dropbox, Tumblr and Google, even Krispy Kreme Donuts.

More alarming were well-planned attacks that knocked out electric utilities in Ukraine and the summertime hack of the U.S. Democratic National Committee's network. Officials in several countries have raised concerns about the security of critical infrastructure such as power and water utilities. Three years ago, at least four American electric utility companies were hacked, threatening to destabilize large areas of the power grid. A variety of malware programs were used, including BlackEnergy, KillDisk and others. Ransomware attacks ramped up in 2016, as well, with disturbing attacks on large healthcare systems, including against Washington, D.C.-area hospital chain MedStar Health.