



Online Trust Alliance Finds Consumer Data Breaches Level Off While Other Cyberattacks Skyrocket

OTA documents 82,000 “cyber incidents” in 2016 negatively impacted businesses and organizations; admits there could have been more than 250,000 when accounting for unreported incidents

Bellevue, Wash. – Jan. 25, 2017 – Today the [Online Trust Alliance \(OTA\)](#), the non-profit with the mission to enhance online trust, released its [2017 Cyber Incident & Breach Response Guide](#). The ninth annual guide, which is being released in recognition of [Data Privacy & Protection Day](#), provides organizations with tools to enhance data protection, adopt responsible privacy practices and help to detect, mitigate and effectively respond to a cyber incident.

OTA’s 2017 Guide has broadened to include the wider impact of what OTA calls “cyber incidents.” These incidents include more than the compromise of consumer data. They involve business interruption from ransomware, stealing of funds via business email compromise (BEC), distributed denial of service attacks (DDoS), and takeover of critical infrastructure and physical systems. Examples include attacks on the Democratic National Committee which focused on unearthing political data and campaign intelligence for reputational harm, the breaching of the World Anti-Doping Agency database which resulted in the public disclosure of confidential medical data of world-class athletes, ransomware which resulted in the Hollywood Presbyterian Medical Center being taken offline for weeks and business email compromises which successfully extracted millions of dollars in unauthorized bank transfers.

In the report, OTA concludes that there were approximately 82,000 cyber incidents in 2016 impacting about 225 organizations worldwide every day. Since the majority of cyber incidents are never reported, OTA believes the actual number in 2016 could exceed 250,000. The 82,000 confirmed cyber incidents is more than twenty times that of the estimated number of consumer data breaches reported for 2016.

“The high profile cyber incidents of 2016 have taught us that financial loss is only one of many other potential dangers of cybercrime,” said Craig Spiegle, Executive Director and President of OTA. “Organizations are susceptible to security threats, reputation damage and much more. It is essential for all organizations to plan ahead and secure technologies, processes and procedures to help prevent, detect, remediate and respond to the impact of a cyber incident.”

more

OTA came to its conclusions by tracking and analyzing threat intelligence data from multiple sources. These sources include but are not limited to the Anti-Phishing Working Group (APWG), the FBI, the Global Cyber Alliance, Infoblox, Interpol, Malwarebytes, Microsoft, Risk Based Security, Security Scorecard, Symantec, the U.S. Secret Service and Verisign.

How Organizations Can Help Protect Their Customers, Data and the Internet at Large

OTA determined that more than 90 percent of all cyber incidents in 2016 could have been easily prevented. In the guide, OTA provides a series of checklists to help organizations prevent, detect, remediate and respond to data loss incidents. This end-to-end readiness plan, which recognizes one size does not fit all, enables organizations to control and manage the fall-out of an incident. As outlined in OTA's Guide, the best defense is a three-step strategy:

1. Implement a broad set of operational and technical best practices that help maximize the protection of customer and company data
2. Be prepared with an incident response plan that allows the company to respond with immediacy, while ensuring maximal business continuity
3. Understand that human factors play a critical role in how strong or weak an organization's security defenses are, how they respond and most importantly how their actions are judged

"Establishing safeguards upfront and being prepared to react strategically to cyber incidents are critical components of any healthy and sustainable enterprise," said Johan Roets, CEO of Identity Guard. "Following OTA's advice, as outlined in this guide, is an essential first step in protecting data and helping to decrease data loss incidents."

"With so many personal records breached in the last few years, many consumers are facing the reality that their personal information has likely already been stolen, and that they could be vulnerable to identity theft," said Neil Daswani, Chief Information Security Officer at LifeLock. "The Online Trust Alliance, for the ninth year in a row, has given the information security community a valuable resource to help protect customer data as well as respond to cyber incidents, and LifeLock is proud to support that effort."

"While one cannot stop cybercrime, one can control and manage the fall-out of an incident," said Dena Graziano, Director of Government Affairs at Symantec. "Having security processes in place and being prepared to manage the impact of an incident, is the responsibility of every organization. As ransomware, spear phishing, and DDoS threats continue to grow, OTA's incident response guidance should be a part of every organization's data security and privacy practices."

OTA will present its findings during a congressional briefing cohosted by the [Congressional Cybersecurity Caucus](#) on Tuesday, Jan. 31 at 11:30 am EST in Washington, DC at the [Rayburn House Office Building](#), Room 2044. Congressional staff and press can register [here](#). In addition, OTA will hold a webinar on Feb 7 at 10am PST/1pm EST to review the data and Guide. To register go [here](#). To download the guide, go to <https://otalliance.org/incident>.

About OTA

The Online Trust Alliance (OTA) is a non-profit think tank with the mission to enhance online trust and user empowerment while promoting innovation and the vitality of the Internet. Its goal is to help educate businesses, policy makers and stakeholders while developing and advancing best practices and tools to enhance the protection of users' security, privacy and identity. OTA supports collaborative public-private partnerships, benchmark reporting, and meaningful self-regulation and data stewardship. Its members and supporters include leaders spanning the public policy, technology, ecommerce, social networking, mobile, email and interactive marketing, financial, service provider, government agency and industry organization sectors. <https://otalliance.org>

Contact:

Andrew Goss

Voxus PR (for OTA)

253.444.5446

agoss@voxuspr.com