Internet trust at all time low; not enough being done to protect data, says Internet Society report

Five step approach identified to address data breaches and increase online trust

[London, UK – 23 November 2016] – The Internet Society has today released the findings from its 2016 Global Internet Report in which 59 percent of users admit they would likely not do business with a company which had suffered a data breach[i]. Highlighting the extent of the data breach problem, the report makes key recommendations for building user trust in the online environment, stating that more needs to be done to protect online personal information.

"One of the key questions raised by this report is why are organisations doing so little to protect their customers' data?" said Michael Kende, Economist and Internet Society Fellow who authoured the report. "Everyone knows that data security is a major issue for both consumers and businesses, yet companies are not doing everything they could to prevent breaches."

"According to the Online Trust Alliance, 93 percent of breaches are preventable. And steps to mitigate the cost of breaches that do occur are not taken – attackers cannot steal data that is not stored, and cannot use data that is encrypted. This status-quo isn't good enough anymore. As more and more of our lives migrate online, the cost and risk of a data breach is greatly increased, and will lead to lost revenues and a lack of trust."

The average cost of a data breach is now $4 million, up 29 percent since 2013.[ii] With a reported 1,673 breaches and 707 million exposed records occurring in 2015[iii], the Internet Society is urging organisations to change their stance and follow five recommendations to reduce the number and impact of data breaches globally:

1. Put users -who are the ultimate victims of data breaches- at the centre of solutions. When assessing the costs of data breaches, include the costs to both users and organisations.
2. Increase transparency about the risk, incidence and impact of data breaches globally. Sharing information responsibly helps organisations improve data security, helps policymakers improve policies and regulators pursue attackers, and helps the data security industry create better solutions.
3. Data security must be a priority – organisations should be held to best practice standards when it comes to data security.
4. Increase accountability – organisations should be held accountable for their breaches. Rules regarding liability and remediation must be established up front.
5. Increase incentives to invest in security – create a market for trusted, independent assessment of data security measures so that organisations can credibly signal their level of data security. Security signals help organisations indicate that that they are less vulnerable than competitors.

The IoT security black hole
The report also draws parallels with threats posed by the Internet of Things (IoT). Forecast to grow to tens of billions of devices by 2020, interconnected components and sensors that can track locations, health and other daily habits are opening gateways into user's personal lives, leaving data exposed.

"We are at a turning point in the level of trust users are placing in the Internet," said Internet Society's Olaf Kolkman, Chief Internet Technology Officer. "With more of the devices in our pockets now having Internet connectivity, the opportunities for us to lose personal data is extremely high. Direct attacks on websites such as Ashley Madison and the recent IoT-based attack on Internet performance management company Dyn that rendered some of the world's most famous websites including Reddit, Twitter and The New York Times temporarily inaccessible, are incredibly damaging both in terms of profits and reputation, but also to the levels of trust users have in the Internet."

"Up-to-date security systems, usable security, and awareness on how to deal with threats and social engineering are needed for reducing the opportunities for data breaches and device compromise. The report shows that as much as 93 percent of all breaches could have been avoided if the correct measures were put in place. In a day and age where having a positive online presence really is a case of sink or swim for businesses, gambling with online security, really isn't an option. This is why we are urging people to take action and follow our 5 recommendations to protect themselves both now and in the future," added Kolkman.

Other report highlights include:

- The average cost per lost record is $158, up 15 percent since 2013[iv]
- Within business, the retail sector represents 13 percent of all breaches and six percent of all records stolen, while financial institutions represent 15 percent of breaches, but just 0.1 percent of records stolen, indicating these businesses might have greater resilience built in to protect their users[v]

The 2016 Global Internet Report can be download here: https://www.internetsociety.org/globalinternetreport/2016/.

About the Internet Society
Founded by Internet pioneers, the Internet Society (ISOC) is a non-profit organization dedicated to ensuring the open development, evolution, and use of the Internet. Working through a global community of chapters and members, the Internet Society collaborates with a broad range of groups to promote the technologies that keep the Internet safe and secure, and advocate for policies that enable universal access. The Internet Society is also the organizational home of the Internet Engineering Task Force (IETF).

Media Contact:
Allesandra de Santillana - desantillana@isoc.org

---

[i] http://www2.gemalto.com/email/2014/dp/GlobalCustomerSentiment/index.html#631

[ii] http://www-03.ibm.com/security/infographics/data-breach/

[iii] http://www.gemalto.com/press/Pages/Gemalto-releases-findings-of-2015-Breach-Level-Index.aspx

[iv] http://www-03.ibm.com/security/infographics/data-breach/

[v] http://breachlevelindex.com