Marc Weber Tobias Contributor

I am an investigative attorney and physical security specialist.

Opinions expressed by Forbes Contributors are their own.

Internet Security: Whom Should You Trust?

Participants at the annual Chaos Computer Club hackers' congress on Dec. 28 in Hamburg, Germany. (Image credit: Getty Images via @daylife)

Internet security is all about trust at a distance. That is because you are dealing with everyone remotely and not able to confirm identity or authenticity in the traditional sense. Even with secure connections, encryption, and the various other authentication schemes there is always a way to spoof identity, provide forged documents or credentials, hold

computers and servers hostage to “ransomware” or allow cyber-criminals to be whoever they want to be.

I was just in New York and attended one of a series of Town Hall Meetings presented by the Online Trust Alliance based in Seattle, Wash. This is a group that is headed by Craig Spiezle, a former Microsoftexecutive and Director of Security and Privacy Product management for Internet Explorer. If you are a business or government entity you should know about what the OTA is working to accomplish because it might help protect your digital environment from a variety of threats and the potential for a costly data breach.

Last week, the speakers at the OTA meeting included the FBI, the Attorney General’s office of New York, the Federal Trade Commission, and representatives of the commercial sector. They discussed how criminals worldwide have seized upon the Internet as a treasure trove to breach, steal, scam, extort, phish, stalk, track and victimize any individual or entity that has a connection to the worldwide web. For the OTA, it is all about enhancing online trust while promoting innovation and the vitality of the Internet. For business, it translates into security, privacy, reputation and liability and money.

The Online Trust Alliance and its Mission

Listen to my interview with Craig Speizle about their mission. The OTA represents more than one hundred organizations and companies that reflect the broad internet ecosystem. It has major players in the industry including software vendors such as Microsoft, security and anti-virus developers such as Symantec, social media that includes Twitter, Facebook and eHarmony, and online payment systems such as Paypal and VeriSign.

The organization is deeply involved in seven areas that are highly relevant to business and how companies can safely interact with customers, clients and anyone that uses the Internet, while protecting internal confidential information. They have developed educational materials and are actively engaged in a variety of programs to target and address the following issues:

- **Anti-Malvertising:** to help protect consumers and sites from malicious advertising;

- **Email Security and Authentication:** They are part of a group that is tasked with addressing deceptive email and spear phishing. They are working to promote standards for email authentication best practices for interactive marketers, ISPs, enterprise and government agencies;
- **Data Protection and Breach Readiness Planning:** This is one of OTA's critical missions because of the negative impact and liability such occurrences can cause. They have developed a comprehensive guide to enhance data protection practices, and preparation for incidents before they occur;
- **International Issues:** The Internet is global which means that users, regardless of geographical boundaries must be able to trust sessions and interactions with others across the web. OTA is promoting partnerships with major stakeholders throughout the world;
- **Privacy:** Especially in the European Union, there is a greater focus on the control, collection, use and sharing of consumer data. The Online Trust Alliance is working to protect consumers in this regard;
- **Education:** The organization is developing programs to provide relevant and actionable advice and training to assist in protecting online brands, intellectual property, and those using the Internet;
- **Public Policy:** The OTA interfaces with industry, business, consumer groups and government to develop self-regulation, legislation, and best practices.

No organization is immune to the loss or compromise of confidential and sensitive data. Consumer information, employee records, proprietary and trade secret information, and intellectual property are all available for the taking if infrastructures are not properly protected and contingency plans developed should a breach occur. While many businesses may understand the potential threat they are often not prepared to deal with an incident, or they naively believe it will never happen to them. Many have a misguided sense of security and believe that it is IT's problem, purely technical in nature. The reality is that every department must be involved in readiness planning. It is not simply a technical issue and can impact customers, employees business associates and the public perception of the entity.

One of their most important documents that are offered by the OTA is the *2013 Data Protection & Breach Readiness Guide*. Every company should read it. This document points out the resilience and inventiveness of criminals to attack your infrastructure and the data it contains, and measures that can be taken to protect against such attacks.

Well worth reading is the article in the New York Times last week that described how the paper was the subject of an intensive attack by hackers from China for an extended duration. It is not alone. One of my colleagues has been working on a federal investigation into the systematic compromise of computer infrastructures of law firms that specialize in patents and intellectual property. These incursions appear to have been government-sponsored, aimed at securing information and highly sensitive intellectual property years in advance of when the technology becomes public.

Even the most cyber-savvy organization can and have been compromised in both the commercial and government sectors. Most are ill-prepared to deal with the operational, legal, financial, regulatory, and public relations ramifications of such incidents. The OTA is working with regulators, law enforcement, the FCC, and carriers to enhance consumer online trust and confidence and protect companies, their brands and reputations from abuse and cybercrime. In short, they can provide significant assistance to protect and enhance the Internet. I came away from the meeting in New York with a better understanding of the threats and that every organization should at least review the work done by the Online Trust Alliance to reduce their potential for often the inevitable.

http://www.forbes.com/sites/marcwebertobias/2013/02/10/internet-security-whom-should-you-trust/