**The Top Security Threats Exposed in the First Half of 2016**

Heading into 2016 there has been an increased awareness of the threat of possible data breaches and IT security threats worldwide. Following a challenging 2015 that was characterized by multiple large retailers experiencing massive data breaches as well as federal security threats, it is thought that more than 16,000 cyber attacks will be attempted in 2016.

The Federal Government recently released the 2016 Data Threat Report which collated data from IT experts and government entities to discuss and ranks the biggest security threats. The study found that 90 percent of those surveyed believed their organizationwas vulnerable to a data breach. Of that 90 percent, 61 percent experienced a data breach including 1 in 5 within the past year. That is a startlingly high assessment for the experts charged with keeping the nation’s data secure.

We took a look at the top security threats exposed early in 2016 to help your company identify arising security challenges, possibly within your own organization. Here is what we found:




# Securing Healthcare Information

In February of 2016 the California Attorney General’s office issued a strong warning to consumers and IT industry leaders alike about the need for increased security around healthcare data. Now that more healthcare providers and insurance companies are relying on a shared network of medical data, there is significant concern about a data breach that would reveal not just social security numbers and other identifying information, but also private information about an individual’s health and well-being.

**$$**

**?**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |

# Flaws in Mobile Apps

In an effort to get the younger generation to buy into traditional savings and investment plans, a number of financial firms have developed mobile-friendly apps that allow people to invest their money on the go with the help of robo-advisors. While the end result has been a positive increase in the number of Millennials getting actively involved in saving and investing, there is also a reason for concern that there are hundreds of thousands of transactions taking place through apps that have not necessarily been tested for security.

In fact, one security report estimates that 25 percent of mobile apps include at least one high-risk security flaw. On average consumers are using mobile apps like these to connect with more than 150 unique servers a day, often using unencrypted data. There will be a boost in awareness as retailers and other service providers continue to integrate mobile

apps with their day to day business operations.

**VS**

**?**

# Internal Threats from Lack of Training

The U.S. Federal Government’s 2016 Data Threat Report noted that the single biggest threat was not outside hackers but a skill shortage among the “wetware” of the system. That is, companies and governments lacked qualified personnel and training regarding proper security protocols. Until these deficiencies are addressed, data breaches will continue to be the norm.

Ironically, the biggest data breaches result not from support staff, but from the privileged manager or executive. These individuals have far greater access to internal systems and data than most employees. One of the most scandalous breaches of 2015, the Sony leak, resulted when several executives handed over their log-in credentials. It’s important to train all staff on proper handling of sensitive data to prevent breaches from occurring from internal sources.

The one bright spot in the report is that 53 percent noted an increase in funding to address data security issues.

# Reduce Points of Access

A study from the Attorney General’s office found that while the majority of data breaches were caused by malware or hacking, approximately 17 percent are caused by errors, such as misdelivery (via email, for example) and inadvertent exposure on the internet.

SYSTRAN is unique among translators because its software operates behind your firewalls. It does not need the cloud to operate which reduces the points of access to your systems. This is critical to address the ongoing skills shortages as SYSTRAN provides secure translations for all of your employees. The fewer opportunities for employees to access unauthorized emails or websites from company computers and exposing them to the external web, the less likely you will experience a data breach.

Learn more about SYSTRAN translation software for customer service and support at: [http://www.systrangroup.com](http://www.systrangroup.com/)

