# CYBERRISKS+LIABILITIES

## IN THIS ISSUE



JRG ADVISORS

## Report Predicts Escalation of Cyber Attacks in 2017

According to a recent report from Experian, a global information services group, businesses can expect to see an increase in the number and severity of cyber attacks in 2017. The report also predicts that a large number of politically-motivated cyber attacks near the end of 2016 will escalate into a larger cyber attack conflict, and that businesses in the financial, security and health care industries will be the most frequently targeted.

### Major Predictions

As a part of the report, Experian made five major predictions for cyber attacks in 2017:

- **Password breaches will contribute to the abandonment of the password as a security measure.** Although the theft of login IDs and passwords constitutes a short-term threat, the report states that cyber criminals continue to sell passwords long after they are stolen. And, as businesses and consumers are lured into a false sense of security after their password is unknowingly stolen, passwords alone will begin to fall out of favor. Instead, the report emphasizes that two-factor identification—where two separate pieces of authentication evidence are required—should be used by businesses to defend against cyber attacks.

- **New, sophisticated attacks will continue to target the health care industry.** Because medical identities and information remains relatively easy to access and profitable for hackers, the health care industry will continue to be a target in 2017. The report also states that large establishments, such as hospital networks, will continue to face threats like ransomware, a type of attack where an organization is "locked out" until a financial ransom is payed.

*(Continued on next page)*

### Research Shows that Overcompensation for Cyber Attacks Can Backfire

Research conducted by the Sam M. Walton College of Business and the Billingsley Chair of Information Systems has shown that consumers are often suspicious when they are given too much compensation following a cyber attack.

The research noted that because it can be difficult to ascertain the exact costs of a cyber attack, offering appropriate compensation to consumers can be just as challenging.

For example, in 2013, a cyber attack against Target affected 110 million customers. After the attack had been resolved, Target offered customers a 10 percent discount on purchases—an offer that was met favorably. However, the research found that customers grew suspicious when the company also offered free credit monitoring as reimbursement.

### Authorities Shut Down Cyber Crime Ring

Authorities in the United States and EU recently shut down a network of hackers known as the Avalanche network. The group had operated since at least 2010 and targeted more than 500,000 computers with a variety of cyber attacks.

The Avalanche network was also used as a platform to distribute and purchase malware for a variety of purposes—though the network was mostly used to steal online banking information or to install ransomware on various computer systems.

It was recently revealed that a state prosecutor's office in Pennsylvania was targeted by one of the Avalanche network's ransomware attacks and was forced to pay $1,400 in bitcoin to release its infected computer network. However, it's unknown if the cyber crime ring targeted additional government agencies. Five known members of the group are currently facing charges in numerous countries.

*(Continued from previous page)*

- **Politically-motivated and state-sponsored attacks will become more common.** The large number of high-profile cyber attacks at the end of 2016, along with the accusation that many of the attacks were state-sponsored, may lead to businesses being affected by the collateral damage of these attacks. Additionally, the report predicts that such attacks will only grow as politically-motivated hackers seek retaliation against others.

- **Hackers will focus on payment-based attacks, despite new credit card security measures.** Although the switch to EMV chip cards and the PIN liability shift were expected to protect against payment breaches, uneven adoption could lead to additional cyber exposures in 2017. Additionally, criminals are beginning to use sophisticated skimming machines to steal card data at physical retail and ATM locations.

- **International data breaches will cause major problems for multinational businesses.** The loss of consumers' data is a large problem if it occurs in just one country, but multinational businesses must also deal with ever-changing regulations in all of their markets. The United States, EU, Australia and Canada have all passed new regulations that will force businesses to re-evaluate their cyber security plans.

## New Malware Campaign Affects 1 Million Google Accounts

A malware campaign called Googlian has breached over 1 million Android devices, and continues to affect approximately 13,000 devices every day. The malware is capable of stealing a user's authentication, which allows it to gain access to personal data from Google Play, Gmail, Google Photos and other platforms.

Googlian uses a Trojan horse attack, in which the malware poses as a legitimate app that is downloaded onto a user's device. However, Googlian uses the data on a user's phone effectively as a marketing scheme, and surreptitiously downloads additional apps onto the device. And, although Googlian has not yet targeted personal information for profit, advertisements located in the apps generate revenue for the hackers.

Google has stated that the Googlian apps come from third-party app stores, and not the company's official Google Play store. As a result, Android users should delete any third-party apps from their devices and only download apps from the official store.

**JRG Advisors, LLC**
7000 Stonewood Drive, Suite 251
Wexford, PA 15090
412-456-7000
http://www.jrgadvisors.net/