CYBERRISKS+LIABILITIES

IN THIS ISSUE

JRG ADVISORS

Cyber Tips for Small Businesses

According to a recent internet security threat report, small businesses have increasingly become targets for cyber criminals. With over 40 percent of cyber attacks targeting small businesses, it is important to not only lower the risk of an attack but also be prepared if one occurs. The following simple, economical steps can help reduce your risk of falling victim to a costly cyber attack:

1. Equip each of your business's computers with anti-virus software and anti-spyware, and update it regularly.
2. Use a firewall and encrypting information to safeguard your internet connection. Password-protect access to your router.
3. Establish policies outlining how employees should handle and protect personally identifiable information and other sensitive data.
4. Educate employees about cyber threats and hold them accountable to the business's internet security policies and procedures.
5. Require employees to choose strong passwords and to change them often.
6. Make sure your banks and card processors utilize trusted anti-fraud services. Isolate payment systems from other, less secure programs.
7. Regularly back up data on all company computers, and store copies either off-site or in the cloud.
8. Control physical access to computers and network components. Require individual user accounts for each employee.
9. Create a mobile device action plan for lost or stolen equipment.
10. Protect every page of public-facing websites, not just the login page.

Contact JRG Advisors, LLC for tools to ensure you have the proper coverage to protect your company against losses from cyber attacks.

Fast-food Chain Arby's Hacked

Over 355,000 credit and debit cards could be compromised after malware was installed on hundreds of Arby's point-of-sale (POS) systems in the United States. No franchises were affected by the breach—only the corporate-owned locations. Approximately one-third of Arby's stores are corporate owned.

An Arby's spokesperson notified law enforcement after learning of the security breach and contacted several computer security firms to assist. The fast-food chain has since eliminated the malware that infected its POS systems and led to the breach.

The Arby's spokesperson said that its customers should check their credit card statements for any unauthorized payments and report any suspicious activity to their banks.

Turkish Hacker Sentenced to U.S. Prison Term

For masterminding three cyber heists that allowed $55 million to be stolen from ATMs around the world, a Turkish hacker was sentenced to eight years in a U.S. prison after stealing information from prepaid debit cards. That information was used to create new cards, which were used to conduct thousands of fraudulent ATM withdrawals worldwide. After completing the U.S. sentence, he will be deported to Turkey to serve the remainder of a sentence from a prior conviction.

Trial Begins for Software Developer and Pastor Charged in Illegal Bitcoin Exchange

A Florida software engineer and a New Jersey pastor are being tried for their involvement in an illegal bitcoin exchange. The pastor is accused of accepting bribes and church donations from the software engineer in exchange for relinquishing control of a small credit union housed in the pastor's church. Both individuals pleaded not guilty and are among nine people charged following an investigation connected to a 2014 JPMorgan breach that exposed more than 83 million accounts.

Fraud on the Rise

A recent global fraud and risk report by Kroll, Inc. gives insight into the state of fraud and risk incidents in 2016, during which 82 percent of respondents experienced a fraud incident—up from 75 percent in 2015 and 61 percent in 2012.

Fraud concerns affect not only a company's bottom line, but also its ability to expand overseas. Over two-thirds of executives say their companies have been deterred from operating in a particular country or region due to fraud concerns.

The Most Common Perpetrators Come From Within

Contrary to the popular belief that security breaches come from external sources, the most common perpetrators of fraud, cyber incidents and security incidents were internal.

- Fraud—Sixty percent of respondents who experienced fraud identified a combination of current employees, former employees and third parties as perpetrators.
- Cyber Incidents—Overall, 44 percent of respondents reported that insiders were to blame for cyber incidents, with 20 percent of the source of risk attributed to former employees.
- Security Incidents—Insiders were the main perpetrators of security incidents at 56 percent, with former employees accounting for 23 percent of security incidents.

Increasingly Complex Threats for Businesses

The evolving nature of incidents reflects a growing challenge for businesses. While every fraud category has seen an increase in incidents between 2015 and 2016, market collusion and misappropriation of company funds realized the greatest increases, at 15 percent and 11 percent, respectively.

Mitigating Fraud

While insiders are cited as the main perpetrators of fraud, they are also the most likely to discover it, with 44 percent of respondents reporting that it had been discovered through a whistleblowing program, and 39 percent reporting that it was detected through an internal audit. In fact, over 75 percent of respondents indicated that their companies have adopted employee-focused anti-fraud measures, technical countermeasures and physical security measures.

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