

THE NEWSLETTER OF THE BDO INSURANCE PRACTICE

INSURANCE **ADVISOR**



EFFECTIVE CYBERSECURITY POLICIES: MEETING THE GROWING THREAT THAT FACES THE INSURANCE INDUSTRY

By John Green

During a recent meeting with a prospective client, a sizable mutual insurance company, we asked the CEO what challenges currently face his company. The CEO quickly responded that his primary concern – the issue that keeps him up at night – is protecting the company's network and especially the personal data amassed as part of everyday operations. While he was comfortable with the policies and procedures currently in place, he questioned if such infrastructure was sufficient to stand up to the future threat that will exist in the new world of "the Internet of things."

While the insurance industry is not exclusive in its vulnerability to cybercrime, the volume of personal data and proprietary

information gathered and maintained by property and casualty (P&C), life and health insurers exceeds most other business entities. This personal data includes Social Security numbers, dates of birth, credit card information, home addresses, financial information, health information, etc. Insurance companies of all sizes must adopt sound cybersecurity policies and must continually upgrade their systems and software to meet the ever increasing threats from viruses, malware, intrusions and unauthorized access to systems.

The first step to protecting such information is to conduct an information technology (IT) system review. BDO's audit methodology requires a thorough review of our client's

► DID YOU KNOW...

Life insurance policies sold in the life settlement market reached \$2.57 billion in 2013, up from \$2.13 billion in 2012, according to *InsuranceNews.net*.

According to a survey by *Verisk Analytics' ISO unit and the Property Casualty Insurers Association of America*, the U.S. property and casualty insurance industry's net income for the first quarter of 2014 fell 4 percent from that of the same period a year earlier to \$13.75 billion.

The World Bank issued a \$30 million catastrophe bond through its newly created Capital-at-Risk Notes Program to cover earthquake and tropical cyclone risk in 16 Caribbean countries, according to *Business Insurance*.

According to a report published by insurance broker *Willis Group Holdings*, the largest ever volume of non-life catastrophe bonds was issued in Q2 2014 with \$4.5 billion of non-life catastrophe bond capacity issued in 17 deals, compared to \$3.3 billion issued in 17 deals in the same quarter of last year.

According to *SNL Financial*, the insurance industry's M&A market is up 20 percent in deal volume year-to-date through June 20, compared to the same time period in 2013.

On June 30, the U.S. Supreme Court denied the former head of American International Group (AIG) Maurice "Hank" Greenberg's appeal on his charge that the federal bailout of American International Group (AIG) was illegal, according to *CBS News*.

►CONTINUED FROM PAGE 1

EFFECTIVE CYBERSECURITY POLICIES:

IT systems, which includes matching our client's policies and procedures against the current standards and protocols adopted by IT professionals. The IT review often results in findings that we report to management and the board of directors. Some of the more common and repeated cybersecurity mistakes insurance companies are susceptible to include:

- **Permitting the existence of "super users," one or two individuals in an organization that have access to all programs without any oversight** – Sometimes these super users also have authority to make changes to operating systems.
- **The lack of change controls** – Due to changes in laws or company policies, insurance companies routinely make changes to programs. In some companies, primarily smaller carriers, the controls over changes to systems lack the proper documentation and authorization.
- **Physical security vulnerabilities** – For example, server rooms that are accessible to any employee. We recently came across a server room that also functioned as a storage closet.
- **The lack of password control** – On several occasions we noted that passwords were not required to be changed regularly and passwords for terminated employees were still active in the system.
- **The lack of encryption** – Unintentionally permitting unauthorized people access to company information hosted on the web – a particularly important issue when dealing with remote access.

Obviously, insurance companies must balance the need for security and access control with efficient day-to-day operations. If security measures are too strict, employees may lose the ability to perform their tasks promptly which could lead to a loss of business or other operational issues. Conversely, policies that are too loose result in compromised systems that are susceptible to cyberattacks.

Over the past several months and years there have been a number of well-publicized

UPDATES FROM THE NAIC SPRING 2014 MEETING

By Barb Woltjer

Significant regulatory updates were announced and adopted during the Spring 2014 National Association of Insurance Commissioners (NAIC) meeting, which took place in Orlando, Fla., this past March.

During the meeting, the NAIC's Corporate Governance Committee adopted changes to the Annual Financial Reporting Model Regulation, which will require large insurers to incorporate an internal audit function into their overall corporate governance structure.

The Committee also agreed upon amendments and a re-exposure of the draft Corporate Governance Annual Disclosure (CGAD) Model Act. It is expected that the CGAD Model Act will be effective Jan. 1, 2016, and will require disclosures about the insurer or insurance group's corporate governance structure, policies and practices.

For more information, please contact Barb Woltjer at bwoltjer@bdo.com.

The NAIC Emerging Issues Task Force issued Interpretation 2013-04, "Accounting for the Risk Sharing Provisions of the Affordable Care Act (ACA)," to prescribe appropriate statutory accounting treatment for the risk adjustment, reinsurance and risk corridor sections of the ACA. The task force also requested the Statutory Accounting Principles Working Group to consider issuing formal guidance in a Statement of Standard Accounting Practice (SSAP) on accounting for ACA risk-sharing provisions, including non-admittance considerations. On March 29, 2014, the NAIC adopted "balance" disclosures pertaining to the risk-sharing provisions of the ACA programs (risk adjustment, reinsurance and risk corridors). Reporting entities are to include disclosures quarterly, beginning with the first quarter of 2014. Additionally, on June 12, 2014 the NAIC adopted SSAP No. 106 "Affordable Care Act Assessments" to move the ACA Section 9010 fee guidance from SSAP No. 35R to a new SSAP.

security breaches at major U.S. companies and government organizations. These security breaches all had one common theme: a seemingly minor security weakness was exploited either by outside parties or employees leading to compromised personal information or theft of proprietary information. It's important to note that these are the breaches that are known. A common saying among BDO's IT auditors is "there are two types of companies: those that have been hacked and know it and those that have been hacked and don't know it."

While each IT system is different and each company has different needs, the standard policies that most companies should comply with include the following:

- **Adopt heightened physical security measures**
 - Consider banning all flash drives, personal hard drives and disk drives. Instead, set up a secured file sharing service to transfer large data files.
 - Encrypt all computers with the highest level of encryption. This is especially important for laptop users. Also consider physical locking devices to prevent laptops from being stolen.
 - Consider restricting remote access to encrypted devices only. Home computers are notorious for all sorts of viruses that can migrate to a network through a remote connection.
 - Establish procedures for mobile devices such as smartphones and tablets. Allowing

►CONTINUED FROM PAGE 2

EFFECTIVE CYBERSECURITY POLICIES:

access to sensitive information through mobile devices, especially those that connect through public Wi-Fi can be risky.

• Enforce password controls and access controls

- Passwords of at least six to eight characters that include requirements for alpha and numeric characters with upper case and/or symbols provide a much greater level of security than less complex password protocols.
- Require passwords to be changed regularly.
- Immediately delete user accounts of terminated employees.
- Ensure that each employee's access to systems is appropriate and remove access that is not required.
- Never allow personal data or proprietary data to be stored on a laptop, portable drive, flash drive, disk or other medium that is portable.
- Institute policies that allow all mobile devices to be wiped clean in the event of loss or theft.
- Block access to websites that are not necessary or appropriate for business operations.

• Ensure network security

- Constantly update anti-virus, spam filters and encryption software and devices.
- Monitor network access and analyze for unusual activity.
- Test backup systems regularly.
- Ensure that appropriate intrusion detection software and devices are installed and perform regular tests to detect weak points.
- Consider co-sourcing servers at secure data locations that operate in the most current security environment.
- Encrypt all personal data transmitted. Consider adopting the Massachusetts standard for transmittal of personal data via email or electronic means.
- Establish a protocol to ensure any breaches or potential breaches are

PErspective in Insurance

After a relatively slow 2013, merger and acquisition (M&A) activity in the insurance industry has grown dramatically. According to *SNL Financial*, the insurance M&A market has seen a roughly 20 percent increase in deal volume year-to-date through June 20, compared to the same time period in 2013.

Within the insurance industry, three subsectors are driving M&A activity, which include underwriting, property and casualty (P&C) and life insurance. While only 34 of the total 160 deals are in the underwriting subsector, according to *SNL Financial*, deals in this subsector alone have a combined value of \$10.65 billion – a nearly 140 percent increase in total value – leaving insurance professionals and industry dealmakers optimistic for the future.

In addition to robust deal volume, private equity activity in the P&C and life subsectors is also expected to increase. *Mergermarket's* recently published Global Insurance M&A Outlook Report, which surveyed the opinions of 75 insurers and reinsurers in the life and/or P&C subsectors as well as bankers and private equity practitioners, found that 93 percent of industry professionals anticipate that private equity activity will rise in the P&C subsector and 88 percent believe it will rise in the life subsector. Furthermore, the

promptly and properly communicated to third parties as required.

- Never allow sensitive data to be sent via unsecured email services (i.e., Gmail).

We routinely see that cybersecurity is not a high priority for many insurance companies and consequently IT systems are vulnerable. For small and medium-sized carriers it may make more economical sense to outsource some or all of the IT security to established firms that provide cost-effective solutions.

Today, insurance companies face a real challenge of providing easily accessible

majority of survey respondents believe that private equity buyouts will be the most common deal type over the next six months for both the P&C (60 percent) and life (55 percent) subsectors.

While 68 percent of survey respondents cite the improving economy as the main cause for the uptick in deal flow, it is important to note that 25 percent of survey respondents indicated that private equity firms are particularly interested in life insurance companies because of their expertise and capability when it comes to lessening the risk of current low interest rates and improving spreads for these portfolio companies.

Private equity investors are driving not only strong deal activity in the insurance industry but talent as well. *Business Insurance* recently reported that during the What's Ahead for Insurance M&A and Corporate Finance Conference in April 2014, Patrick G. Ryan, chairman and CEO of independent insurance brokerage Ryan Specialty Group LLC, stated that he has never seen anywhere near the movement of talent that he sees happening today. He also observed that underwriting is a particularly valuable skill in today's marketplace due to the number of people willing to invest in that talent.

PErspective in Insurance is a feature examining the role of private equity in the insurance industry.

and current information to customers and employees alike while at the same time ensuring that appropriate security measures are in place to prevent security breaches. Undoubtedly we have not heard the last about security breaches and expect the imposing of regulatory fines and/or litigation in the future. Making cybersecurity a top priority is the first line of defense for insurance companies to mitigate the possible repercussions associated with IT security.

For more information, please contact John Green at jgreen@bdo.com.

MARK YOUR CALENDAR...

SEPTEMBER

Sept. 10-12

NALC Spring Meeting

Grove Park Inn Resort and Spa
Asheville, N.C.

Sept. 14-16

PCI Investment Seminar

Wigwam Resort
Phoenix, Ariz.

Sept. 14-17

Society of Insurance Financial Management Annual Conference

Borgata Hotel, Casino and Spa
Atlantic City, N.J.

Sept. 20-23

CPCU Society Annual Meeting

Anaheim, Calif.

Sept. 21-22

Executive Edge

Chicago, Ill.

OCTOBER

Oct. 20-23

ACLI Annual Conference

J.W. Marriott
Washington, D.C.

BDO INSURANCE PRACTICE

BDO's Insurance practice understands the complexities of the industry and the implications for your business. Whether you're looking to tap our extensive SEC experience in order to enter the public market, discuss the latest insurance accounting and reporting requirements from the NAIC, or comply with state regulatory agencies, BDO's Insurance practice provides proactive guidance to our clients. We know that no two insurers are alike, and we tailor our services accordingly. We're proud of our industry focus and experience, and our commitment to delivering the right team with relevant industry experience, both as we begin our relationship and for the long term.

ABOUT BDO

BDO is the brand name for BDO USA, LLP, a U.S. professional services firm providing assurance, tax, financial advisory and consulting services to a wide range of publicly traded and privately held companies. For more than 100 years, BDO has provided quality service through the active involvement of experienced and committed professionals. The firm serves clients through 52 offices and over 400 independent alliance firm locations nationwide. As an independent Member Firm of BDO International Limited, BDO serves multinational clients through a global network of 1,264 offices in 144 countries.

BDO USA, LLP, a Delaware limited liability partnership, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. BDO is the brand name for the BDO network and for each of the BDO Member Firms. For more information, please visit www.bdo.com.

To ensure compliance with Treasury Department regulations, we wish to inform you that any tax advice that may be contained in this communication (including any attachments) is not intended or written to be used, and cannot be used, for the purpose of (i) avoiding tax-related penalties under the Internal Revenue Code or applicable state or local tax or (ii) promoting, marketing or recommending to another party any tax-related matters addressed herein.

Material discussed is meant to provide general information and should not be acted on without professional advice tailored to your firm's individual needs.

CONTACT:

RICHARD BERTUGLIA

Assurance Partner / New York
212-885-8342 / rbertuglia@bdo.com

DOUG BEKKER

Tax Partner / Grand Rapids
616-776-3685 / dbekker@bdo.com

PHIL FORRET

Assurance Partner / Dallas
214-665-0769 / pforret@bdo.com

CARLA FREEMAN

Assurance Partner / Los Angeles
310-557-0300 / cfreeman@bdo.com

JAY GOLDMAN

Assurance Partner / Atlanta
404-979-7237 / jgoldman@bdo.com

JOHN GREEN

Assurance Partner / New York
212-885-8174 / jgreen@bdo.com

THOMAS HILLER

Partner and Insurance Practice Leader
/ Grand Rapids
616-774-7000 / thiller@bdo.com

BRENT HORAK

Assurance Partner / Dallas
214-665-0661 / bhorak@bdo.com

TIMOTHY KOVEL

Sr. Tax Director / New York
631-501-9600 / tkovel@bdo.com

ALBERT LOPEZ

Partner and Regional Business Line
Leader / Miami
305-420-8008 / alopez@bdo.com

IMRAN MAKDA

Assurance Partner / New York
212-885-8461 / imakda@bdo.com

BARB WOLTJER

Assurance Partner / Grand Rapids
616-802-3368 / bwoltjer@bdo.com