By Adam Hamm, North Dakota Insurance Commissioner and NAIC Cybersecurity (EX) Task Force Chair

I recall the times when I thought it was a nuisance having to shred documents containing personal information so somebody wouldn’t steal my identity by going through my trash each week. Now, I wish that was my only identity theft concern. With the proliferation of electronic communication, social media, emails and massive databases housing personal financial and health information, it’s enough to make anyone lose sleep at night. It makes all of us wonder what can be done to protect ourselves.

In this article, I will discuss some steps being taken by state insurance regulators to proactively address cybersecurity issues.

**Defining the Problem**

As people become more reliant on electronic communication, and as businesses collect and maintain ever more granular pieces of information on their customers, the opportunity for bad actors to cause difficulties for businesses and the public is exploding. Identity theft is a growing problem for consumers.

The statistics collected by the U.S. Bureau of Justice Statistics (BJS) confirm our fears related to identity theft. The BJS periodically collects information through a survey called the National Crime Victimization Survey. For purposes of the survey, the definition of identity theft includes three general types of incidents:

1. Unauthorized use or attempted use of an existing account.
2. Unauthorized use or attempted use of personal information to open a new account.
3. Misuse of personal information for a fraudulent purpose.

The BJS report called *Victims of Identity Theft, 2012* (the most recent year available) shows:

- About 7% of persons age 16 or older were victims of identity theft in 2012.
- The majority of identity theft incidents (85%) involved the fraudulent use of existing account information, such as credit card or bank account information.
- Victims who had personal information used to open a new account or for other fraudulent purposes were more likely than victims of existing account fraud to experience financial, credit, and relationship problems and severe emotional distress.
- About 14% of identity theft victims experienced out-of-pocket losses of $1 or more. Of these victims, about half suffered losses of less than $100.
- More than half of identity theft victims who were able to resolve any associated problems did so in a day or less; among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems.

The BJS also collects information on cybercrime. However, the most recent data available from them is for 2005. There is another vehicle for gathering information about cybersecurity threats to the financial sector. Perhaps the best way for insurers to share information on cyber activity is through the Financial Services Information Sharing and Analysis Center (FS-ISAC). The FS-ISAC is a resource for the financial sector on cyber and physical threat intelligence analysis and information-sharing. The FS-ISAC is a member-owned non-profit entity providing an anonymous information-sharing capability across the entire financial services industry. For more information on the FS-ISAC visit www.fsisac.com.

Identity theft for individuals and cybercrimes for business are closely interrelated. There are a number of reasons why a business might be hacked. Some of these reasons are more critical than others for guarding against identity theft. One type of cybercrime is hacking by an individual just to show he or she can successfully perpetrate the act. The motivation is simply the challenge of being able to break through the firewall of a business and cause some form of disruption.

This type of hacking often shows itself as a denial-of-service attack. The intent of the hacker is to disrupt or degrade the Internet connectivity or email system of a business. This is accomplished by “ping” attacks, port-canning probes and by causing excessive amounts of data to arrive in a short period of time with the intent of disrupting service. From an identity theft perspective, this type of attack is relatively

(Continued on page 3)

benign. The intent of the hacker is not to steal and sell or use identities, but rather to be a nuisance to the business.

Other hackers, sometimes known as “hacktivists,” are intent on using technology to deliver an ideological, political or religious message. Cyberterrorists are included in this category, as they use denial-of-service or Web defacement to damage a firm that fails to live up to the hacker’s ideological expectations. Others hack to expose perceived wrong-doing or to make confidential information available to the public.

Another source of hacking is the nation state. We know some nations support hacking activities for various reasons. A rogue nation state might be interested in cyber warfare as a way to disrupt the economy of another nation or to do harm to its people. Other nations might simply be interested in spying on businesses in another nation or gaining information and insight from government websites. Sometimes, nation states target businesses to hack where access to trade secrets and business processes is the desired goal.

It is hacking for profit that is the cause of greatest concern. It could be an individual or an organized criminal gang who is engaged in hacking, with the goal to obtain personal financial and health information to exploit people and business for ill-gotten financial gain.

The bottom line is if you own a computer or a smart phone or other electronic equipment using the Internet, you are at risk. State insurance regulators are not going to be able to solve this broad public policy issue. However, state insurance regulators are in a position to help protect the public—policyholders, beneficiaries and claimants—by making sure that insurers implement the best practices for data security available.

From a state insurance regulator’s perspective, the problem can be defined in four ways:

- Regulators know consumer information is at risk and want to do whatever is within their regulatory power to assist insurance consumers when consumer information is compromised by a breach from an insurer, an insurance producer or the regulator.
- Regulators have authority to monitor the market activities of insurers and insurance producers and are actively overseeing the cybersecurity capabilities of insurers and insurance producers.
- Regulators need to work together to make sure state computer networks and the computer network at the NAIC are state-of-the-art when it comes to cybersecurity measures.
- Regulators need to exercise authority over the insurers involved in selling cybersecurity insurance products to individuals and businesses in the U.S.

**The NAIC Cybersecurity (EX) Task Force**

The NAIC Executive (EX) Committee recently appointed the Cybersecurity (EX) Task Force and asked it to serve as the central focus for insurance regulatory activities related to cybersecurity. I am honored to serve as chair of this new Task Force. The Task Force has a fairly aggressive work plan, which involves coordination with various NAIC groups working on certain aspects of cybersecurity.

The first project for the Task Force was establishing a set of guiding principles to plant a “flag in the ground” on cybersecurity. An initial draft set of eighteen guiding principles was released for public comment in March. After receiving and considering feedback from interested parties, the Task Force revised and combined some of the principles. The Task Force then adopted a final set of twelve guiding principles on April 16. These principles will serve as the foundation for protecting consumers personally identifiable information held by insurers as well as insurance producers and will guide state insurance regulators who oversee the insurance industry. A copy of the guiding principles can be found on the NAIC website.

The Task Force will be working with the Property and Casualty Insurance (C) Committee on a proposal to add a cybersecurity supplement to the P&C Annual Statement. The purpose of this would be to get a clear picture of the size and breakdown of the cyber insurance market. The Committee recently adopted a motion to release the Annual Statement Supplement for public comment and asked for written comments to be submitted March 23. The Committee discussed the comments received during its March 29 meeting in Phoenix at the Spring National Meeting. Several states and interested parties made suggestions for im-

(Continued on page 4)
proving the draft Annual Statement Supplement. Commissioner Mike Chaney (MS), who chairs this Committee, convened a conference call to discuss the comments and suggested changes. The proposed supplement was then adopted during the call.

Additionally, the Task Force will be working with the IT Examination (E) Working Group. The Working Group plans to review existing guidance in the Financial Condition Examiners Handbook (Handbook) and will be working with the Task Force on improvements to the examination protocols for state financial examiners to check on the cybersecurity capabilities of insurers. Patrick McNaughton (WA) leads this Working Group.

Currently, every state is required to use specialists at companies when reviewing their data-security controls. These specialists generally have specialized training enabling them to successfully review insurer data security controls. These specialists typically have obtained the certified information systems auditor (CISA) designation, as well as the automated examination specialist certification from the Society of Financial Examiners (SOFE). Using these specialists is an accreditation requirement on all multi-state financial examinations.

The NAIC maintains the Handbook to provide guidance to financial examiners. The Handbook has an extensive section regarding the review of automated controls and uses the COBIT 5 standards, which are recommended and promoted by the Information Systems Audit and Control Association (ISACA). The standards are strict and robust with respect to evaluating and determining whether the general information technology controls at a company are operating as they should.

The difference between what a state financial examiner with data security skills and what a cybersecurity firm does is that the financial examiner ensures an insurer is evaluating its risks and hiring the necessary firms to examine its data and systems. A cybersecurity firm does actual penetration testing, monitoring, and ongoing reviews on behalf of the insurer.

The IT Examination (E) Working Group regularly revises its guidelines and standards. The Working Group has used the draft principles assembled by the Task Force to determine the Working Groups next steps to ensure the Handbook guidance includes a more robust look at cybersecurity. The Working Group is going to compare the National Institute of Standard Technology (NIST) framework to its existing framework to be sure there are no gaps between the two frameworks.

When financial regulators conduct a risk-focused examination of an insurer, they look at how the insurer identifies and defines its risks, as well as the steps taken to mitigate identified risks. The financial examiner will also weigh what the CEO and board members have to say regarding these risks. Often, the financial examiner finds data security and cybersecurity are not high enough on the list of risks identified by insurer management. The Cybersecurity (EX) Task Force, working together with the IT Examination (E) Working Group, plans to change that dynamic in the future.

The Task Force will also be looking to create a survey of the states to assess state cyber vulnerabilities. Work on this project is expected to occur over the summer. The Task Force plans to be able to discuss results of the survey during the Fall National Meeting.

Another important project for the Task Force is the creation of a Consumer Bill of Rights. I expect it will cover existing regulations and statutes regarding the security breach notification. It will also outline state insurance regulators’ expectations of insurers if they experience a cybersecurity issue. Consumers deserve to know insurers are protecting their sensitive financial and health information. They also deserve to know when a breach occurs so they can take steps to safeguard themselves from identity theft or other fraud. Now that the guiding principles have been adopted, plans call for work on the Consumer Bill of Rights to begin.

The Task Force also plans to stay abreast of what is happening in the Financial and Banking Information Infrastructure Committee (FBIIIC), the Cybersecurity Forum for Independent and Executive Branch Regulators and the FS-ISAC. Plans call for the Task Force to host a webinar to receive information from the FS-ISAC. The webinar will cover the benefits of information sharing through the FS-ISAC.

The NAIC maintains numerous model laws, regulations and guidelines. Some of them deal with issues related to cybersecurity. The Task Force will review several model laws and regulations to update them with regard to privacy and cybersecurity. Among the models under consideration are: the NAIC Insurance Information and Privacy Protection Model Act (#670); the Privacy of Consumer Financial and Health
The Task Force may also take a look at the Insurance Fraud Prevention Model Act (#680). No definite timeframe has been set for this work. It is important to note the Model #670 and Model #672 were created in response to the federal Gramm-Leach-Bliley Act. They provide the basis of the annual privacy notifications for the insurance sector. Careful attention must be paid to these important models.

**CONCLUSION**

These days, everyone who owns a computer is at risk. Hackers with a variety of motivations spend their days trying to stay one step ahead of the firms who sell cybersecurity tools. Sound firewalls and robust network security are able to turn away most hacking attempts, but we know no system is perfect. As such, I am proud to say state insurance regulators are stepping up to do their part to attempt to make the electronic world safer.
The National Association of Insurance Commissioners (NAIC) is the U.S. standard-setting and regulatory support organization created and governed by the chief insurance regulators from the 50 states, the District of Columbia and five U.S. territories. Through the NAIC, state insurance regulators establish standards and best practices, conduct peer review, and coordinate their regulatory oversight. NAIC staff supports these efforts and represents the collective views of state regulators domestically and internationally. NAIC members, together with the central resources of the NAIC, form the national system of state-based insurance regulation in the U.S. For more information, visit www.naic.org.

The views expressed in this publication do not necessarily represent the views of NAIC, its officers or members. All information contained in this document is obtained from sources believed by the NAIC to be accurate and reliable. Because of the possibility of human or mechanical error as well as other factors, however, such information is provided “as is” without warranty of any kind. NO WARRANTY IS MADE, EXPRESS OR IMPLIED, AS TO THE ACCURACY, TIMELINESS, COMPLETENESS, MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OF ANY OPINION OR INFORMATION GIVEN OR MADE IN THIS PUBLICATION.

This publication is provided solely to subscribers and then solely in connection with and in furtherance of the regulatory purposes and objectives of the NAIC and state insurance regulation. Data or information discussed or shown may be confidential and or proprietary. Further distribution of this publication by the recipient to anyone is strictly prohibited. Anyone desiring to become a subscriber should contact the Center for Insurance Policy and Research Department directly.