HAPPY HOLIDAYS

T@GS

The Independent Insurance Agents' Association of Montana

Independent Insurance Agent®
The Trusted Choice®

December 2016

Find us on Facebook

Tips, infographics, & articles for you to share with your customers.
Association notices. Education info.
like the Independent Insurance Agents of Montana on Facebook for these and more!

Return to table of contents

IMPORTANT MESSAGE FROM BOB BISKUPIAK

With mixed emotions, I am announcing that I have decided to leave the association to become the next Deputy Insurance Commissioner.

It has been my absolute pleasure to serve the association, company partners and member agents for the last 9 years. Joining a new leadership team at the Insurance Department is an excellent opportunity for me to continue my dedication to the insurance industry and consumers.

The Montana Big "I" is in good hands with a dedicated staff and strong board of directors.

I have complete confidence the association will continue to flourish and be an important part of your success. My last day is December 29th.

Thanks for allowing me to serve as the Executive Director of the Montana Big I!

Bob Biskupiak

Return to table of contents

WHERE ARE THEY NOW?

Many of you will recognize the gentleman on the left as Roger McGlenn, retired Executive Director of the IIA of Montana. You might—or might not! - recognize the young man standing to his right.

That's Ryan McGlenn, Roger's son and decorated Marine. Most of us remember him as a little boy following his dad at convention time.

Roger will be returning to the trenches on your behalf as our contracted lobbyist for the 2017 Legislative Session. We're excited to have his knowledge and expertise when the session starts on January 2nd.

Sign up to receive our bi-weekly legislative bulletin.

Return to table of contents

CHECK YOUR AGENCY’S CYBER-HYGIENE

by Steve Anderson

The Center for Internet Security (CIS) is a nonprofit organization funded by the Department of Homeland Security, focused on enhancing the cyber-security readiness and response of public and private sector entities.

Starting this past summer, the CIS has been working with the ACT Security Issues Work Group to review the existing CIS tools to make them as useful as possible for insurance agencies.

The CIS toolkits help agents count, configure, control, and patch their hardware and software resources so they are as secure as possible. The free program is called "Cyber Hygiene."

Ryan Spelman, program executive at the Center for Internet Security, presented at the November 1, 2016, ACT Meeting and did an excellent job of highlighting some of the security issues agencies face. The following notes are from Ryan's session at the ACT Meeting.

No Let-Up from Hackers and Thieves

Criminals are targeting your organization. They want data. Why? Data is money. Credit card apps are worth $2 each. A black card is $10. A medical record can garner as much as $100.

There are two kinds of companies — those that have had a data breach and those that don't yet know they have. (Note that the average time from data breach to detection is 229 days, according to FireEye.)

Anyone can take down a network. Hackers used to be kids in the basement hacking into the federal government. Not anymore. The number of cyber criminals is growing fast. It's easy to rent some servers, hire guys for thousands of dollars a week, and rent an old aircraft hangar. It's a less risky crime than bank robbery, and you don't get shot at. Cyber-crime may be larger than the drug trade in its financial impact on society.

Kids in basements have become "hacktivists," where many are doing harmless things. However, other times it can be vicious. Hackers can use your servers to attack governments.

Interestingly, not all breaches are from outside hackers — one-third of malicious attacks are caused by human error.

Your company computers may be loaded with vulnerable software as well: Microsoft, Java, Adobe, and Firefox are all at risk. Hacking is common across all systems.

Moreover, industrial control systems can be breached fairly easier. For example, hackers can use a patch for an HVAC system, making that a great jumping-off point for a cyber invasion.

There are multiple types of cyber incidents, the most common of which are phishing, browser attacks, ransomware, and lost/stolen devices or data. These comprise 90% of cyber events.

Preparedness is Lacking

Agencies need to ask themselves some critical questions, such as what their readiness level is. Seventy-five percent of organizations are not prepared to respond to attacks, and 55% lack sufficient risk awareness.

(Continued on page 4)

(Continued from page 3)

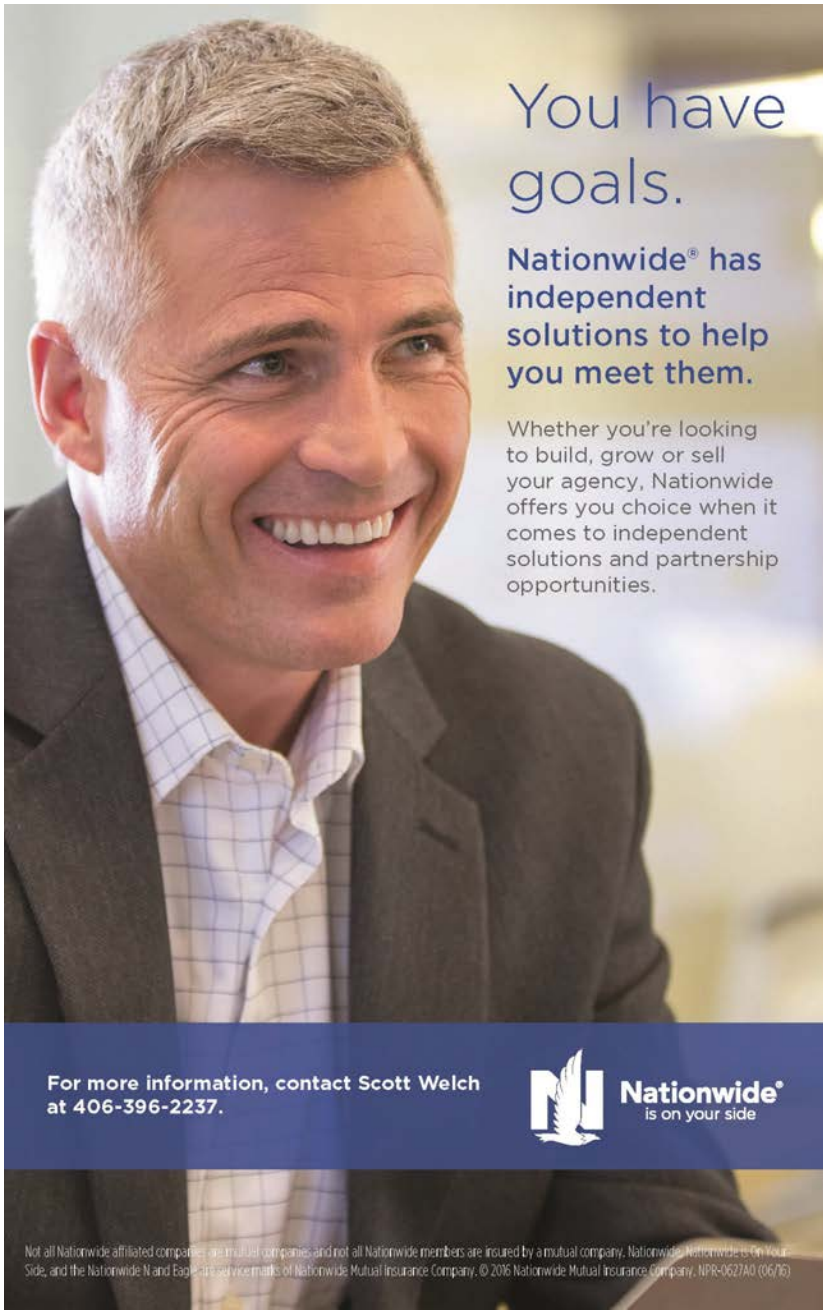
It's possible to prevent attacks by upgrading software, but one-third of people who are notified to update software (browsers, operating systems) don't do it. That is foolhardy when you consider the magnitude of the threat: the cost of each record in a data breach is more than $200. The average total cost of a data breach across large corporations is $5.5 million.

Compliance costs money, but so do violations, so make sure your agency knows and complies with all state and federal laws regarding data privacy and protections.

National Campaign for Cyber Hygiene

The CIS is working with ACT on a free "Cyber Hygiene" program for the distribution channel. There are five basic steps:

1. **Count:** Know what's connected to and running on your network. If you have five employees, it's easy. If you have 500, it's tough. Include all personal devices, even a smart watch.
2. **Configure:** Implement key security settings to protect your systems.
3. **Patch:** Regularly update all apps, software, and operating systems.
4. **Control:** Limit and manage admin privileges and security settings.
5. **Repeat:** Regularize the top priorities to form a solid foundation of cyber security. Cyber security is not a destination, it's a journey, and you want to keep as far ahead as you can. Hackers will move forward.


You have goals.
Nationwide® has independent solutions to help you meet them.
Whether you're looking to build, grow or sell your agency, Nationwide offers you choice when it comes to independent solutions and partnership opportunities.
For more information, contact Scott Welch at 406-396-2237.
Nationwide® is on your side
Not all Nationwide affiliated companies are mutual companies and not all Nationwide members are insured by a mutual company. Nationwide, Nationwide is On Your Side, and the Nationwide N and Eagle are service marks of Nationwide Mutual Insurance Company. © 2016 Nationwide Mutual Insurance Company. NPR-0627A0 (06/16)

Other aspects of a solid program include maintaining, monitoring and analyzing audit logs, and installing protections for email and web browsers, such as black/white listing. Email attachments are one of the primary methods by which attackers seek access to your network. Both black and white listings can limit your exposure.

(Continued on page 5)

Return to table of contents

(Continued from page 4)

Proxies can reduce your vulnerability. Have technologies (e.g., web filtering) in place that limit your users' access to risky and malicious sites.

You need firewalls, a technology that controls incoming and outgoing traffic on your network. But remember, people say that they limit only 20% of hacks or breaches.

Run and update anti-virus software. Ransomware is a fast-growing crime. Hackers get into your system and encrypt your data, holding it hostage for a price. A hospital in Hollywood initially was asked for $2 million to get back its data. It eventually paid $17,000. The average for individuals can be $500 or more.

Encrypt mobile devices. If the device is lost or stolen but you encrypted the data, the theft might not result in a breach. To reduce your chances of a data breach, you need a written information-security policy that is shared with people.

Security awareness training should be conducted on the basics of cyber hygiene, including the dangers of phishing, email attachments, etc. And you should insist on secure coding, a set of clearly defined controls that must be in place when developing an application.

Resources

I encourage you to access the Cyber Hygiene toolkits. ACT and the CIS are also working to create and release a free Small Business Guide to Cyber Security. They estimate this will be available in early 2017, so be on the lookout for it. Cyber Security is a top issue for everyone in the insurance industry. The CIS toolkit is an excellent resource for any size agency.

Return to table of contents

THE POWER OF 30 SECONDS™

The first 30 seconds of any inbound sales call set the tone for the entire customer experience. In that short time agencies can either earn valuable new business or develop an unfavorable view among potential clients.

Trusted Choice is aiming to help members make those seconds count with The Power of 30 Seconds.

The Power of 30 Seconds is a free online training tool designed to help Trusted Choice agents convert inbound sales calls into clients. The training program coaches agents on creating and managing an inbound sales process for their agencies.

Through The Power of 30 Seconds, you will learn how to:

- establish an effective call workflow,
- provide a positive customer experience and
- manage phone system automation.

SET THE TONE TO SELL.
THE POWER OF 30 SECONDS™
If a customer likes you and continues to like you, they will do business with you. If they don't, they won't.
— Paul Greenberg
45%
of customers share negative reviews on social media.
63%
of consumers read negative reviews on social media.
65%
are likely to speak negatively about their customer service experience.**
Trusted Choice®
After a positive customer experience,
69%
of Americans would recommend that company to others.*
IndependentAgent.com/30Seconds

You can also earn a certificate of completion by testing your knowledge of the principles of handling inbound sales calls through the post-training quiz. Boost profit, experience growth and cement your reputation by visiting the Power of 30 Seconds.

Return to table of contents

CRACKING THE CONDOMINIUM CONUNDRUM

Join us January 18, 2017, to crack the condominium conundrum, or just to figure out how to properly write coverage for the unit owner AND/OR the association.

In this webinar we show you how to answer three key questions when analyzing and placing coverage for either a unit owner OR a condominium association, while at the same time revealing:

- Three levels of associational responsibility (and, thus, the unit owner's responsibility);
- Four "real property" definitions unique to condominiums;
- How to properly extend real property coverage for the unit owner;
- How an NFIP policy muddies the water (so to speak); and
- Various valuation methods potentially applicable to associations.

Whether you write the association or the unit owner, you can learn a lot from this webinar. REGISTER

CE will not be offered.

Return to table of contents