WHAT IS CYBER SECURITY?

CYBERBULLYING

CYBERTHREAT

ARE YOU AT RISK FOR
IDENTITY THEFT?

POTHOLEs IN THE
INFORMATION HIGHWAY
Comprehensive integrated claims services, business process outsourcing and consulting services for major product lines including:

- Property and casualty claims management,
- Workers compensation claims and medical management, and
- Legal settlement administration

Based in Atlanta, Georgia, Crawford & Company is the world’s largest independent provider of claims management solutions to the risk management and insurance industry as well as self-insured entities, with an expansive global network serving clients in more than 70 countries. The Company’s shares are traded on the NYSE under the symbols CRDA and CRDB. EOE
What's Inside...

28 Cyber Threats
Janet Smith

30 What is Cybersecurity?
Mindi McDowell & Allen Householder

31 Dealing with Cyberbullies
Mindi McDowell

32 Cyber Coverages: Understanding Policy Trends and Opportunities
Bryan Acohido & Edward Iwata

36 Realistically, How Bad is a Data Breach for Business
Deena Coffman

MANAGEMENT PERSPECTIVES

8 Are You at Risk for Identity Theft?
The Identity Theft Resource Center

9 Debunking Some Common Myths
Mindi McDowell

10 Cyber Security Questions for CEOs
Department of Homeland Security

NEW PERSPECTIVES

14 Good Security Habits
Mindi McDowell & Allen Householder

15 Overcoming the Emotional Impact of Identity Theft
Eva Velasquez

16 Cybersecurity Insurance Selling Tips
Nick Carozza

18 How Do You Keep Your Child Safe from Being a Victim of Cyber Crimes?
Pamela M. Holt

TECHNOLOGY TRENDS

20 Cyber Progress in the Insurance Industry
Mary Hauri

23 Beware of Potholes in the Information Superhighway
Sue C. Quimby

25 New Laws Increase Value of Cyber Insurance for Small Businesses
Mindy Pollack

ASSOCIATION NEWS

39 Thank You Legacy Foundation Donors

40 Welcome New Members

41 Congratulations New Designation Recipients

42 Meet the Candidate
Editor’s Note

The terms “Cybersecurity” and “cyber security” are often confused and incorrectly used; so much that they are becoming increasingly ambiguous. While there isn’t any official authority on the subject, there are at least some credible sources providing guidance that can help us understand when, why and how to use the term correctly.

Cybersecurity is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access.

Cybertechnology is defined as a field of technology that deals with the development of artificial devices or machines that can be surgically implanted into a humanoid form to improve or otherwise augment their physical or mental abilities.

Sometimes referred to as computer security, Information Technology Security is information security applied to technology (most often some form of computer system).

There is so much confusion in the market over how the terms should be used, technology analysts Andrew Walls, Earl Perkins and Juergen Weiss wrote that “use of the term ‘cybersecurity’ as a synonym for information security or IT security confuses customers and security practitioners, and obscures critical differences between these disciplines.” To help set the record straight, the team defined the term:

“Cybersecurity encompasses a broad range of practices, tools and concepts related closely to those of information and operational technology security. Cybersecurity is distinctive in its inclusion of the offensive use of information technology to attack adversaries.” This is one definition and recommendation, but certainly not the only one in circulation. Here are just some of the many definitions I found currently in circulation:

“Cybersecurity is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access. In a computing context, the term security implies cybersecurity.” –TechTarget

“A comprehensive cybersecurity program leverages industry standards and best practices to protect systems and detect potential problems, along with processes to be informed of current, threats and enable timely response and recovery.” –DoHS

“Cybersecurity refers to preventative methods to protect information from being stolen, compromised or attacked in some other way. It requires an understanding of potential information threats, such as viruses and other malicious code. Cybersecurity strategies include identity management, risk management and incident management.”

–Techopedia

The spring issue of Today’s Insurance Professionals covers multiple facets of the Cybersecurity discussion, including but not limited to: Cyber Threat, Cyber Coverages, Cyberbullying, Identity Theft, Cybersecurity Insurance Selling Tips, Cyber progress in the insurance industry, and Potholes in the Information Superhighway.

Share your opinions on Cybersecurity on our social media sites LinkedIn, Facebook and Twitter, so that we may continue to enjoy the process of...

...Connecting Members... Building Careers.

Betsey Blimline
Editor, Today’s Insurance Professionals Magazine

*Cybersecurity or Cyber Security?
Joe Franscella www.infosecisland.com
President’s Message

The Plague of Cybercrime

I’m sure that many of you, or at least someone you know, have received this phone call. “Did you mean to send me an email offering free prescription drugs and relationship assistance? And do you really need bail money to get out of jail in Africa?”

You probably didn’t mean to offer your friends and colleagues either and you’ve never been to Africa, so your email account has probably been hacked. That problem is on the minor end of the severity scale; some of you may even have been the victim of identity theft, meaning you’ve spent hours, days, months or even years trying to reclaim your assets and set the record straight. Unfortunately, these problems are a reality for many of us in 2016!

When the world was first introduced to the Internet, few of us considered the impact Cybercrime would have on every aspect of our lives. These crimes can include stalking and child solicitation, in addition to hacking and identity theft, and reported numbers seem to increase all the time. Estimates suggest there are in excess of 4,000 cyber-attacks daily, translating to approximately 170 attacks an hour, or nearly three attacks each minute of each day! These strike individuals, businesses and even world governments. The current issue of Today’s Insurance Professional will assist you in understanding the far-reaching impact of these crimes, while suggesting ideas and strategies on protecting ourselves and our clients.

…Connecting Members… Building Careers.

Debra C. Kuhne
AAI, AIC, AIS, CIIP, DAE, CELS
IAIP President 2015-2016
The 75th Annual International Association of Insurance Professionals Convention will feature:

- Education sessions and workshops
- Networking and socializing with fellow industry experts
- Celebration of award recipients

Educational workshops are structured around three different Learning Tracks to boost all aspects of your career including:

- Insurance industry topics and trends with CE approved courses
- Career development to enhance your leadership and professional skills
- Association management training for leaders at all levels with information that is transferable to job responsibilities

The following International award winners will be announced at the 2016 Convention:

- Claims Professional of the Year
- Client Service Professional of the Year
- Confidence While Communicating (CWC) Speak-Off
- Insurance Professional of the Year
- Professional Underwriter of the Year
- Risk Management Professional of the Year
- Rookie of the Year
- Young New Professional of the Year

Find us on:

Facebook | Twitter | LinkedIn
Are You at Risk for Identity THEFT?

Take this short quiz to determine the level of risk associated with your own possible identity theft.

**INFORMATION HANDLING:**
- I use a locked, secured mailbox or P.O. Box to receive mail. (+5pts)
- I never leave mail for pickup in an unlocked location at home or at work. (+5pts)
- I always watch my surroundings for people who might be listening when giving out SSN or financial information. (+5pts)
- I keep personal identifying information in a locked or protected area of my home; one that visitors can’t access. (+5pts)
- I have ordered a copy of my free annual credit reports during the last year. (+8pts)

**SCAMS:**
- I keep an eye on my credit cards when they leave my hands to avoid skimming. (+5pts)
- I do not respond to Internet scams and I also hang up on telephone solicitors. (+5pts)
- Whenever I am asked to provide my SSN, I always ask how that information will be safeguarded and why it is necessary for them to have it in the first place. (+6pts)
- I always use firewall(s) and current anti-virus software for any connection to the Internet. (+7pts)

**DOCUMENT DISPOSAL:**
- I own a cross-cut shredder and use it regularly. (+8pts)
- My shredder is near the trash can or in the office where most of my mail is sorted. (+5pts)
- I shred all pre-approved credit offers I receive before putting them in the trash. (+5pts)
- I shred all “convenience checks” or “balance forward checks” I receive from credit card companies before putting them in the trash. (+5pts)
- I understand that thieves root around in my trash looking for credit/financial info. (+5pts)

**SOCIAL SECURITY NUMBER PROTECTION:**
- I never carry my Social Security card in my wallet or purse. (+5pts)
- I make sure that I have no other cards in my wallet or purse with my SSN on it. (+5pts)
- I have a card with my SSN on it in my wallet or purse, but it is a copy and part of the SSN has been cut off. (+6pts)
- I have my SSN or driver’s license number printed on my personal checks. (-7pts)
- My SSN is my driver’s license number - I have made no effort to change that. (-8pts)
- I make sure that my SSN is never publicly displayed or used at work or school, i.e. timecards, test scores, receipts, badges. (+5pts)

**RESULTS:**
Each one of these questions represents a possible risk factor or protection against ID theft.

Your score: ________________ [Range: -15 to +100.]

- **If you scored 85 – 100** consider yourself savvy about identity theft risks; continue your proactive steps.
- **If you scored 45 – 84** you need to consider your identity theft risk factors more closely and take some corrective actions.
- **If you scored below 45**, you are at high risk of becoming this crime’s next victim! Please make the effort to become more informed about identity theft and the simple steps you can take to minimize your risk.

*This fact sheet should not be used in lieu of legal advice. Any requests to reproduce this material, other than by individual victims for their own use, should be directed to ITRC. The Identity Theft Resource Center® (ITRC) is a non-profit organization established to support victims of identity theft in resolving their cases, and to broaden public education and awareness in the understanding of identity theft. Visit www.idtheftcenter.org. Victims may contact the ITRC at 888-400-5530.*
DEBUNKING Some COMMON MYTHS

by: Mindi McDowell, US Homeland Security

How are these myths established?
There is no one cause for these myths. They may have been formed because of a lack of information, an assumption, knowledge of a specific case that was then generalized, or some other source. As with any myth, they are passed from one individual to another, usually because they seem legitimate enough to be true.

What are some common myths, and what is the truth behind them?

Myth: Anti-virus software and firewalls are 100% effective.
Truth: Anti-virus software and firewalls are important elements to protecting your information. However, neither of these elements are guaranteed to protect you from an attack. Combining these technologies with good security habits is the best way to reduce your risk.

Myth: Once software is installed on your computer, you do not have to worry about it anymore.
Truth: Vendors may release updated versions of software to address problems or fix vulnerabilities. You should install the updates as soon as possible; some software even offers the option to obtain updates automatically. Making sure that you have the latest virus definitions for your anti-virus software is especially important.

Myth: There is nothing important on your machine, so you do not need to protect it.
Truth: Your opinion about what is important may differ from an attacker’s opinion. If you have personal or financial data on your computer, attackers may be able to collect it and use it for their own financial gain. Even if you do not store that kind of information on your computer, an attacker who can gain control of your computer may be able to use it in attacks against other people.

Myth: Attackers only target people with money.
Truth: Anyone can become a victim of identity theft. Attackers look for the biggest reward for the least amount of effort, so they typically target databases that store information about many people. If your information happens to be in the database, it could be collected and used for malicious purposes. It is important to pay attention to your credit information so that you can minimize any potential damage.

Myth: When computers slow down, it means that they are old and should be replaced.
Truth: It is possible that running newer or larger software programs on an older computer could lead to slow performance, but you may just need to replace or upgrade a particular component (memory, operating system, CD or DVD drive, etc.). Another possibility is that there are other processes or programs running in the background. If your computer has suddenly become slower, it may be compromised by malware or spyware, or you may be experiencing a denial-of-service attack.

Why is it important to know the truth?
While believing these myths may not present a direct threat, they may cause you to be more lax about your security habits. If you are not diligent about protecting yourself, you may be more likely to become a victim of an attack.
Cyber Security Questions for CEOs

Cyber threats constantly evolve with increasing intensity and complexity. The ability to achieve mission objectives and deliver business functions is increasingly reliant on information systems and the Internet, resulting in increased cyber risks that could cause severe disruption to a company’s business functions or operational supply chain, impact reputation, or compromise sensitive customer data and intellectual property.

Organizations will face a host of cyber threats, some with severe impacts that will require security measures that go beyond compliance. For example, according to a 2011 Ponemon Institute study, the average cost of a compromised record in the U.S. was $194 per record and the loss of customer business due to a cyber breach was estimated at $3 million.

This document provides key questions to guide leadership discussions about cybersecurity risk management for your company, along with key cyber risk management concepts.

5 Questions CEOs Should Ask About Cyber Risks

How Is Our Executive Leadership Informed About the Current Level and Business Impact of Cyber Risks to Our Company?

What Is the Current Level and Business Impact of Cyber Risks to Our Company? What Is Our Plan to Address Identified Risks?

How Does Our Cybersecurity Program Apply Industry Standards and Best Practices?

How Many and What Types of Cyber Incidents Do We Detect In a Normal Week? What is the Threshold for Notifying Our Executive Leadership?

How Comprehensive Is Our Cyber Incident Response Plan? How Often Is It Tested?

Key Cyber Risk Management Concepts

Incorporate cyber risks into existing risk management and governance processes.

Cybersecurity is NOT implementing a checklist of requirements; rather it is managing cyber risks to an acceptable level. Managing cybersecurity risk as part of an organization’s governance, risk management, and business continuity frameworks provides the strategic framework for managing cybersecurity risk throughout the enterprise.

Elevate cyber risk management discussions to the CEO.

CEO engagement in defining the risk strategy and levels of acceptable risk enables more cost effective management of cyber risks that is aligned with the business needs of the organization. Regular communication between the CEO and those held accountable for managing cyber risks provides awareness of current risks affecting their organization and associated business impact.

Implement industry standards and best practices, don’t rely on compliance.

A comprehensive cybersecurity program leverages industry standards and best practices to protect systems and detect potential problems, along with processes to be informed of current
Develop and test incident response plans and procedures.

Even a well-defended organization will experience a cyber incident at some point. When network defenses are penetrated, a CEO should be prepared to answer, “What is our Plan B?” Documented cyber incident response plans that are exercised regularly help to enable timely response and minimize impacts.

Coordinate cyber incident response planning across the enterprise.

Early response actions can limit or even prevent possible damage. A key component of cyber incident response preparation is planning in conjunction with the Chief Information Officer/Chief Information Security Officer, business leaders, continuity planners, system operators, general counsel, and public affairs. This includes integrating cyber incident response policies and procedures with existing disaster recovery and business continuity plans.

Maintain situational awareness of cyber threats.

Situational awareness of an organization’s cyber risk environment involves timely detection of cyber incidents, along with the awareness of current threats and vulnerabilities specific to that organization and associated business impacts. Analyzing, aggregating, and integrating risk data from various sources and participating in threat information sharing with partners helps organizations identify and respond to incidents quickly and ensure protective efforts are commensurate with risk.

A network operations center can provide real-time and trend data on cyber events. Business-line managers can help identify strategic risks, such as risks to the supply chain created through third-party vendors or cyber interdependencies. Sector Information-Sharing and Analysis Centers, government and intelligence agencies, academic institutions, and research firms also serve as valuable sources of threat and vulnerability information that can be used to enhance situational awareness.

The Department of Homeland Security (DHS) is responsible for safeguarding our Nation’s critical infrastructure from physical and cyber threats that can affect our national security, public safety, and economic prosperity. For more information, please visit: www.dhs.gov/cyber.
The McGowan Companies (TMC) is built on three generations of dedication to the insurance and financial services industry. TMC consists of the following:

**McGowan Program Administrators (MPA)** is a Managing General Underwriter and Program Manager for highly-specialized programs of insurance.
Fairview Park, OH • mcgowanprograms.com • 440.333.6300

**McGowan Excess & Casualty (MEC)** is a Managing General Underwriter that specializes in Umbrella and Excess Liability products for a broad range of types and sizes.
Eatontown, NJ • mcgowanexcess.com • 732.335.8470

**McGowan, Donnelly & Oberheu, LLC (MDO)** is a Wholesale Insurance Broker specializing in the placement of Professional and Management Liability risks.
Austin, TX • mdoinsurance.com • 512.600.2280

mcgowancompanies.com • 800.545.1538 • Think McGowan.
What will your customers drive if their car is in an accident?

The average length of a collision repair is 13 days. Are your customers prepared to borrow a car from the family for that long?

Research shows that Rental Reimbursement coverage drives both satisfaction and retention.

Find out more and share the news at my13days.com.
Good Security Habits

How can you minimize the access other people have to your information?

You may be able to easily identify people who could, legitimately or not, gain physical access to your computer—family members, roommates, co-workers, members of a cleaning crew, and maybe others. Identifying the people who could gain remote access to your computer becomes much more difficult. As long as you have a computer and connect it to a network, you are vulnerable to someone or something else accessing or corrupting your information; however, you can develop habits that make it more difficult.

Lock your computer when you are away from it. Even if you only step away from your computer for a few minutes, it’s enough time for someone else to destroy or corrupt your information. Locking your computer prevents another person from being able to simply sit down at your computer and access all of your information.

Disconnect your computer from the Internet when you aren’t using it. The development of technologies such as DSL and cable modems have made it possible for users to be online all the time, but this convenience comes with risks. The likelihood that attackers or viruses scanning the network for available computers will target your computer becomes much higher if your computer is always connected. Depending on what method you use to connect to the Internet, disconnecting may mean disabling a wireless connection, turning off your computer or modem, or disconnecting cables. When you are connected, make sure that you have a firewall enabled.

Evaluate your security settings. Most software, including browsers and email programs, offers a variety of features that you can tailor to meet your needs and requirements. Enabling certain features to increase convenience or functionality may leave you more vulnerable to being attacked. It is important to examine the settings, particularly the security settings, and select options that meet your needs without putting you at increased risk. If you install a patch or a new version of the software, or if you hear of something that might affect your settings, reevaluate your settings to make sure they are still appropriate.

What other steps can you take?

Sometimes the threats to your information aren’t from other people but from natural or technological causes. Although there is no way to control or prevent these problems, you can prepare for them and try to minimize the damage.

Protect your computer against power surges and brief outages. Aside from providing outlets to plug in your computer and all of its peripherals, some power strips protect your computer against power surges. Many power strips now advertise compensation if they do not effectively protect your computer. Power strips alone will not protect you from power outages, but there are products that do offer an uninterruptible power supply when there are power surges or outages. During a lightning storm or construction work that increases the odds of power surges, consider shutting your computer down and unplugging it from all power sources.

Back up all of your data. Whether or not you take steps to protect yourself, there will always be a possibility that something will happen to destroy your data. You have probably already experienced this at least once—losing one or more files due to an accident, a virus or worm, a natural event, or a problem with your equipment. Regularly backing up your data on a CD or network reduces the stress and other negative consequences that result from losing important information. Determining how often to back up your data is a personal decision. If you are constantly adding or changing data, you may find weekly backups to be the best alternative; if your content rarely changes, you may decide that your backups do not need to be as frequent. You don’t need to back up software that you own on CD-ROM or DVD-ROM—you can reinstall the software from the original media if necessary.

Both the National Cyber Security Alliance and US-CERT have identified this topic as one of the top tips for home users.
Overcoming the Emotional Impact of Identity Theft

Identity theft is a crime that impacts millions of people a year; it can be unsettling and upsetting, to say the least. The process of cleaning up the aftermath of identity theft can lead to feelings of powerlessness, embarrassment, and frustration, feelings that no one should have to endure. If your identity has been compromised in some way, it’s important that you understand what steps you can take in order to relinquish those feelings and move forward.

There was a time when identity theft was often a “victim blaming” type of crime, when authorities, your financial institutions, and even your family or friends would ask what you had done to allow someone to infiltrate your information. The early days of internet scams and the so-called Nigerian Prince scams only furthered this notion, as many of the early victims of these types of crimes were seen as greedy or gullible, and therefore deserving of the consequences.

Now, however, with a record high number of data breaches in 2014 alone, the public is more aware that there may be steps you can take to minimize your risk, but that there is still the possibility of a hacker accessing your data through no fault of your own. Here are some important points to ponder for moving past the negative feelings associated with identity theft so you can adopt a healthier, happier outlook and feel safe again:

Security
It’s perfectly natural to feel like you’re in danger following an identity theft, and do not let anyone try to downplay your feelings about it. Some faceless criminal has access to your entire persona, and could be committing a wide variety of crimes with it. This person may have gained access not just to your name or Social Security number, but also to your phone number, your address, even the name of the business where you work. While it’s not likely that this person stole your information in order to cause you physical harm, it’s still upsetting to not know how far this could go.

Embarrassment
Even if you were somehow at fault for your own identity theft—such as by clicking on a phishing email or handing over your information to a scammer—what’s done is done. More important, just because you fell for it does not make you deserving of whatever the thief has planned. The crime and the wrongdoing are his, not yours, and you have nothing to be embarrassed about.

Frustration
While the process of clearing up an identity theft is getting more and more streamlined thanks to the high rates of this crime, it’s still a time consuming, frustrating process. You’ll spend more time on the phone—quite possibly sitting on hold, listening to canned music—than you ever thought you would. There may also be time lost from work while you resolve the matter, which can cause additional stress and can result in having to work overtime to make up for it. But just because millions of other people each year can find themselves in the same boat does not mean you don’t have a right to feel irritated by it.

Violation
Face it, even if it wasn’t your physical boundaries that were compromised, your personal security and the safety you thought you once enjoyed have been violated. That can be frightening, can cause anger issues, and can manifest itself in a wide variety of ways.

While you work to restore your good name after identity theft, remember to take some time for your emotional health. Care for your needs and the needs of your family, and consider professional help if you find that the overwhelming feelings are more than you can handle on your own.

About the Author
Eva Velasquez is the President/CEO at the Identity Theft Resource Center, a non-profit organization which serves victims of identity theft. Velasquez previously served as the Vice President of Operations for the San Diego Better Business Bureau and spent 21 years at the San Diego District Attorney’s Office.

The Identity Theft Resource Center® (ITRC) is a non-profit organization established to support victims of identity theft in resolving their cases, and to broaden public education and awareness in the understanding of identity theft. Visit www.idtheftcenter.org. Victims may contact ITRC at 888-400-5530.
In the past few years, large companies such as Target, Home Depot and most recently, Anthem, have gone through massive data breaches affecting millions of customers. These companies are large enough to afford the most sophisticated IT security firms to ensure that their data is protected. However, even with the funds to protect themselves, each of these companies suffered data breaches, and ultimately paid millions of dollars in notification, public relations and computer forensic costs, as well as the subsequent fines, penalties and legal costs associated with any privacy breach.
But what about the small to medium-sized businesses that cannot afford their own top IT security team? The “it won’t happen to me” attitude is slowly fading as businesses are forced to close their doors due to the costs associated with a data breach.

According to the 2015 Net Diligence Cyber Claims Study, it was reported that businesses earning less than $50m in revenue suffered the majority of breaches. If billion dollar companies can’t protect themselves, how will the average-sized business protect themselves when, inevitably, a data breach occurs? The answer to this question is simple: by purchasing a comprehensive Cyber Insurance Policy. This cost affective option will pay many returns if redeemed. It is our job as Insurance Professionals to make our clients aware of their exposures, and how purchasing a Cyber Liability policy will help their business.

Here are six tips to help your client better understand Cyber and help you sell your next policy.

1. Make your client aware of exclusions in their current policies.

In standard GL and Property forms, there are exclusions that prevent coverage when a breach occurs. There are exclusions for claims of copyright and trademark infringement. Property coverage will protect your physical computers, but not the data that is stored on them – (lost data can be costlier than the computer itself!)

2. Ask your client – “Do you have an incident response plan in place for a Data Breach?”

Most businesses do not have a response plan. Purchasing a Cyber Policy from RPS Technology & Cyber can be the first step in starting this response plan – it gives each client a toll-free “hotline” to call when a breach occurs and immediately starts the process of determining the extent of the breach, along with subsequent steps to help your client when they most need it.

3. Educate your client on how a Cyber policy works and what it covers.

Most business owners have no idea what a Cyber Liability policy covers. As licensed agents, our job is to make sure their business is properly insured, and help educate owners on what each part of their insurance coverage is protecting. For example, First Party coverages include things like notification expenses, credit card and identity monitoring, IT forensics and business interruption. Third Party coverages protect against potential lawsuits by clients or various regulatory entities. Does your client know that a cyber policy also covers paper/hard copies of PII (Personally Identifiable Information)? The more the client understands how the policy works and the costs associated with NOT purchasing the policy, the greater the chance you will receive a bind order.

4. Make your client aware of the fines and penalties in your state if they don’t protect their customer’s personal information.

Depending on the type of data that was breached (names, credit card numbers, passwords, health care information, etc.) there are different governing bodies that assess fines and penalties if a customer’s PII is released. For example, if credit card information is taken, the Payment Card Industry Council can assess fines for “Non-compliance with their security standards.” In addition, each state has laws regarding when and how to notify customers when their personal information has been breached. Without a Cyber Liability policy and a knowledgeable breach team to assist them, each business owner is left to try and navigate the state laws and notify their clients in a timely fashion.

5. Even though they store their data in “The Cloud”, they are still responsible for notification costs and fines and penalties in the event of a data breach.

Most businesses believe that because they are outsourcing services such as electronic data storage or payment processing that they are passing off the liability. This is not the case – the majority of contracts put the liability back on the data owner (your client). As mentioned above, state law makes it the businesses’ duty to notify their customers, not the vendors.

6. Show them why buying a Cyber Liability policy is essential for their business.

According to studies conducted by IBM and the Ponemon Institute, the average cost to a business that has been breached is $3.8 Million. When discussing this important coverage with your client, it is a good idea to discuss the costs of a breach without cyber coverage. There are a number of tools available that can assist with this discussion: websites that let you search for specific types of breaches, the states they occurred in and the classes of business that were affected; as well as online calculators that allow you to break down the costs associated with a data breach, i.e., notification, IT Forensics, credit monitoring, legal costs, public relations and marketing. For many businesses that have experienced a data breach, the tremendous costs, both from a monetary and a public relations standpoint, may be too overwhelming for them to continue doing business.

Now that you have some additional ammo for selling a cyber policy, what is next? At RPS Technology and Cyber we invest a great deal of time into putting together resources to assist our clients with their cyber needs. Whether helping with marketing materials, joining in on conference calls, or holding quarterly webinars – we strive to be an extension of your team.

About the Author

Nick Carozza is a National Sales Executive at RPS Technology and Cyber. For more information on Cyber Liability, contact Nick at nick_carozza@rpsins.com or 410-901-0732. If you have additional questions on cyber or how partnering with RPS Technology and Cyber can benefit you and your agency please feel free to contact him.

Learn more from Nick Carozza in the IAIP pre-recorded Wednesday Webinar series: Cyber Insurance.

In this webinar you will learn current trends in the market place, review coverages and discuss claims and common misconceptions of cyber insurance. The webinar qualifies for IAIP education hours for DAE and CIIP designations; it was recorded on Wednesday, November 18, 2015 and presented by Steven Robinson and Nick Carozza. https://naiw.site-ym.com/store/ViewProduct.aspx?id=4697352
How Do You Keep Your Child Safe from Being a Victim of Cyber Crimes?

Today children have access to the internet 24/7, not only from their desk top computers but from laptops, tablets, and smartphones. How much harder does this make it for you as a parent to keep your child safe? And what can you do as a parent to insure the safety of your children? Here are a few tips to help you:

1. Use parental control software. This software will record your child’s internet activity and blocks inappropriate material. Make sure your child is aware that activity is being monitored. A review of the software available can be found at parental-software-review.toptenreviews.com

2. Make sure the location of the home computer is in a high trafficked area. Don’t let your child keep the computer in their room. This way you can see what actually your child is doing.

3. Teach your child how to save their favorite websites so the chances are lowered for the child to avoid spam or sites that are inappropriate. Spend time with them and have them show you their favorite websites.

4. Teach your child to always ask permission before downloading anything from the websites.

5. Limit the time your child can use the computer especially late at night. Late night is when the sexual predators target children.

6. Make sure you set rules for internet use, making sure they are posted in clear sight. Take control as the parent don’t let your child be in control.

7. Stay up-to-date on the changing trends and technology. Today children know how to use the computer and smartphones before they are old enough to go to school. It is your responsibility as a parent to make sure the child knows the dangers associated with the internet.

8. Always maintain access to your child’s online account and randomly check their email.

9. Instruct your child not to ever arrange a face-to-face meeting with anyone they meet online. Never to upload pictures of themselves to people they do not know. Never give out identifying information such as name, address, telephone number, or school name. Never download pictures from a source they don’t know.

There are dangers everywhere in society that can affect your child. The most important way you can protect them is by educating them to the various dangers around and do what you have to do to protect your child.


About the Author
Pamela M. Holt, AIS, AINS, DAE, CLP, CIIP is from the Insurance Professionals of Greater Knoxville.
EXPERIENCE HAS ITS PRIVILEGES!
Put your insurance expertise to good use.
Earn income from home as you phase into retirement.

YOUR TIME.
YOUR TERMS.

WAHVE’s innovative remote staffing solution matches your skills, training, and work parameters with insurance firms that need professionals like you. Our full-service support team takes care of placing you on an assignment of your choice; plus our relationship manager is your personal assurance that WAHVE is always there for you.

Enjoy rewarding work and continued income with the flexibility of working remotely from home with our one-of-a-kind approach that is creating a “wahve” of change in the insurance industry.

Are you ready to phase into retirement?

Visit WAHVE.com
or call us at (646) 807-4372

“WAHVE is the best thing that happened to me; it changed my life. When people see how happy I am, they want to know all about WAHVE.”

– Judy Bush
Russian Hackers Steal 1.2 Billion Internet User Names and Passwords
A Milwaukee security firm reported a discovery that a group of Russian hackers used common SQL injection attacks to successfully steal 1.2 billion user names and passwords, as well as more than 500 million email addresses, from hundreds of thousands of websites. Although many security experts believe that the stolen email addresses will be used for spam email distribution (and to potentially distribute malware), the stolen log-in credentials are concerning – particularly because many users routinely re-use the same log-in credentials for multiple websites and services, including online banking, investments, and other important accounts. The bottom line: 1) Change your passwords (using strong passwords), 2) Don’t re-use passwords for multiple sites or services, 3) Stay alert for unusual account activity, 4) Change your passwords on a regular basis, and 5) THINK before you click, open, or download.

Company that was a Victim of Cybercrime loses $350,000
TRC Operating Co. Inc., a California oil production company, had $3.5 million stolen from its business bank account in a 2011 cyber theft involving multiple fraudulent wire transfers to accounts in the Ukraine. TRC’s bank was able to stop or reverse several transfers, recovering all but $299,000. TRC later sued its bank to recover the remaining losses, and recently received a pre-trial settlement for $350,000, with neither side admitting fault.

Cyber ID Theft Hits Local Business
A six year old computer services business discovered it was being impersonated by scammers operating a website nearly identical to its own. The real business discovered the impersonation when it began receiving calls from people all over the country who had been contacted by the scammers. Claiming to be from the real business, the scammers threatened that without immediate payment, their computer would be confiscated by the FBI. The victimized business owner successfully had the impostor website taken down twice, only to have it re-appear at new hosting companies.

Document Shredding Company Employee Eyed in Multi-State ID Theft Ring
An employee who drove a document shredding truck for shredding company Cintas may have shared sensitive documents with identity thieves, rather than destroying them. According to law enforcement and court documents, the ring spanned multiple states and there are potentially thousands of victims, including businesses. The resulting fraud losses reportedly may be in the millions.

Cyber PROGRESS in the INSURANCE INDUSTRY
by: Mary Hauri

When I started in the software industry 25 years ago, none of our group could have imagined the far reaching effect that computers would have on us today. And, believe me, we imagined a lot of things that were considered way out there, at the time. Sometimes people looked at me like I had two heads. But as we learned how to develop and innovate this new and exciting way of doing things with computers, we didn’t realize we were also contributing to the foundation of our future way of thinking. Our focus was all about how could we help people see the benefits of what the computer could do, and how could we make the programs and applications better, faster, and more helpful. And now, these headlines are appearing every day in our news…
Today, all of us have customers that want things done better, faster, and easier. But back then, security was not even in the picture, and did not come along until much later when the internet became a “can’t live without” commodity. The “better, faster” train of thinking with computers has permeated our culture, and indeed, our daily lives. Many of us have dual or triple monitors at our work stations, we multi-task like there is no tomorrow, and many cannot get through an hour without checking email or social media. And as we do this, we are always thinking about how great it would be if we just had “that” ability, or how much we could get done if we could just do “this”.

And we know that, if we can think it, we can probably do it. So a new program develops, and a new app is born, and our thing is created. And unfortunately, security is not always in the forefront of design or creativity. As these “better, faster” programs are delivered to us, we only find out about the security issues later on, when criminals have figured out a way to exploit our programs and information. We were pretty innocent back then, and many are still today.

In the insurance industry, we collect a lot of information about our customers in order to give them a quote, write their policies, and administer their changes. And we have found great ways to do this more efficiently and improve productivity with the storage and transmittal of electronic records. What we have been slow to do, however, is implement the back-end processes and procedures with security as a major focus. It’s not that the information has been unavailable to us; it’s just that we want the benefit first of the “better, faster” train, and then realize we need to clean up the internal process to accommodate the workflow more safely.

As we conduct more and more business electronically, the risks to us increase exponentially and the target to criminals becomes bigger. When we say electronic record, we mean a record created, generated, sent, communicated, received, or stored by electronic means. When we say electronic signature, we mean an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record.

Just understanding these definitions can make some people long for the days of paper and pen. And as I speak and train about security issues, I used to find that eyes would glaze over and people would nod their head as if understanding but continue risky behaviors. It did not take long to realize that I needed to take the “KISS” approach to this. By Keeping It Simple, I was much more effective at getting through and developing “security awareness” for my customers. First we understand the laws, we then look at the big security picture, and then bring it down to the users and behaviors that increase risk.

So, let’s look at some of the laws first that apply to us in protecting our clients information in the insurance industry. We have the Federal Laws such as (ESIGN)- Electronic Signatures in Global and National Commerce Act, (UETA) Uniform Electronic Transactions Act, Gramm-Leech-Bliley, Identity Theft and Assumption Deterrence Act of 1998, HPPA- The Health Insurance Portability and Accountability Act, Federal Fair Credit Reporting Act. Many of these laws require that the paper or electronic transactions process (taking applications, delivery of the insurance policy package, policyholder services transactions and other transactions involving sensitive information) be conducted securely, where, for example, sensitive health information, social security numbers and other sensitive data is transmitted through only secure channels.

Now let’s further define what these laws mean when they say we must protect our clients’ personal information from an insurance perspective. Generally, personal information is described as an individual’s last name and first name or first initial, in combination with a Social security number, driver’s license number or state identification number, financial account number including a credit or debit card account number, or any security code, access code or password that would permit access to the individual’s financial account, or DNA profile or any unique biometric data including fingerprint, voiceprint, retina or iris image, or any other unique physical representation.

We know that some documents cannot be done electronically such as wills, codicils or testamentary trusts. These exception could be relevant in some estate planning techniques involving life insurance and testamentary trusts. The second possibly relevant exception is that notices of termination of health insurance or benefits of life insurance (excluding annuities) may not be given solely via e-delivery.

So what are some of the most important things that we can do in our everyday life that can help our business reduce our exposure to cybercrime and protect ourselves? We need to start out by recognizing that young people who grew up with computers don’t always understand the security issues that we face in the insurance industry. When we bring on young people to our business, we need to spend more time training on the laws that apply to us, policies and procedures in all workflows, and what not to do with the computer. In addition, all employees should be required to take an annual update on new laws and office rules and policies. Technology is always changing, and if an employee is not given guidance, they will find their own way of doing things, right or wrong. With all of our employees, we need to make sure that we openly address emerging technology issues and take time to educate them on safe computer behavior. In addition, consider using a six layer approach:

2. Physical Security - Keep the building secure with servers and equipment, and make sure you have a security system for the building. Customers should not be allowed to wander throughout the office. Do not leave passwords in easy reach.
3. Data Security - Restrict your data on a “need to know” basis. Make sure portals and gateways to data are secure. Use SSL and limit web-site access to users.
4. Application Security - This includes anti-virus/malware and spyware, intrusion prevention software, and personal firewalls. Passwords should never be written down and stored at the desk. Change passwords immediately when employees leave. Use monitoring software to detect recent activity.
5. Network Security - Use VPNs, routers, hard and soft firewalls, web content filtering, and HTTPS. Use a more complex password system, i.e. alpha caps and non-caps, numeric and symbol. Daily back-ups are a must. Mirror drives off-site, use the cloud, or tapes off-site in a safe. Random files should be restored once each quarter to make sure data is valid.

6. Management Awareness - Stay current on all applications, patches and updates. Monitor all layers for compliance and vulnerabilities. Stay on top of emerging threats and remediation requirements. Have a plan in place for the prevention, and for the cure, including cyber liability policies.

As we become more mobile and we begin to carry around pocket size computers, we have additional concerns with mobile devices cusk as laptops, tablets, smartphones, CDs, DVDs and flash drives. Here are some security tips for mobile devices:

1. Encrypt your hard drives and sensitive emails.
2. Install BIOS (the first program to run when the machine is turned on) password and get recovery software
3. Use thin client (all capability is on protected server or cloud) if possible
4. Allow only limited client information on laptop- name, phone, notes (not addresses, policy info, etc.)
5. For users - Password, Password, Password! Don't share them, don't store near machine, and use four4-tier-alpha/lowercase, alpha uppercase, numeric and symbol.
6. BWW (Be Wary of Wireless). Use SSL (the url should start with HTTPS).
7. Use a “remote wipe” feature that allows the business to erase the hard drive of a stolen or misplaced computer remotely when it is turned on.
8. Never open attachments that are not from a trusted source.
9. Use additional multi-layered defenses such as those six items listed above.
10. Use anti-virus software, firewalls anti-spyware/malware, and a SPAM filter.

Use Tamper Seals- Your software vendor should include an audit trail in their process and deploy a technology to apply a “Tamper Seal to Electronic Records” Although audit trails and tamper seals are not required by law, they will improve the likelihood of Electronic Records with Electronic Signatures being admitted into court as evidence. Talk to your vendor on what type of tamper seals are in place for your system.

Remember that as diligent as we are, there is no 100 percent guarantee that something won’t happen. Keeping everyone in your office aware of security concerns, along with consistent education on new technology, will be one of the most effective tools you have in your arsenal. It is when employees accidentally leave their laptops at an airport or coffee shop that you will have the highest security risk. Or when they open up the one email that they can’t resist, or download a program from the internet that seems very innocent.

Things that seem clearly risky to me don’t always resonate security risk to my clients. Something as simple as when they make a copy of a check for a customer and store it on their local hard drive, and then take a tape back home to a drawer in the kitchen, or better yet, leave it in their car while they shop and run errands. When I hear this, my security radar goes red. That type of risky behavior and many others will keep me doing seminars and training well into the future. And may continue to give me a few sleepless nights here and there.

About the Author
Mary is President of Insurance Concepts In Motion, Inc. and has worked with Independent insurance agents and companies in the Midwest with their E&O, technology, security, and procedures and processes. You may contact her at maryhauri@icmotion.net.

Some data courtesy of businessidtheft.org/ News
Beware of Potholes in the Information Superhighway

Rapid advances in technology have brought our world together, and in many ways, made our lives easier. But this progress is not without its drawbacks. As technology and internet usage evolve, and we become more dependent on them, companies may inadvertently leave themselves exposed and often extremely vulnerable to the gray zone of cyberspace. Standard insurance policies do not address all of these exposures. Cyberspace, or the information superhighway does not have a specific address - it is everywhere. This creates a unique challenge for insurers and their agents. It’s essential for agents and insurers to understand and address these issues with their clients.

Most coverage forms define coverage territories as tangible places, such as the United States and its possessions or territories. However, cyberspace encompasses so much more than geographical places and airspace. Electromagnetic waves are transmitted from one side of the world to another within milliseconds, containing things that cannot be seen or touched: intangible things. Unlike loss exposures that can be seen, such as a hurricane or tsunami, cyber loss exposures are most often unfathomable, yet have the potential for similar financial impact. A local business selling products on their website opens their company to worldwide products liability, as well as attacks by hackers. The hackers seem to evolve with more aggression and ingenuity, determined to overcome any security measures that may be in place.

Common cyber loss exposures include:

**Denial of Service Attacks:** The insured’s website is inundated with volumes of communications, which in turn, cripple the operating system until it comes to almost a complete standstill. Although there is no direct physical loss or damage to tangible property, the amount of income lost could be substantial, and this does not include the cost of marketing to restore lost good will and customer confidence.

**Flaws in the Intelligence of a System:** A malfunction interaction with another system component or components impairs the performance of the operating system. For example, if cryptographic hardware is used for passwords, malfunctioning hardware can potentially mismatch private information, thereby creating a security breach.

**Security Breach or Privacy Loss:** This involves an improper disclosure of personal information, whether intentional or unintentional. Examples include the disgruntled employee who steals social security lists to sell the information, or hackers who can “sniff” ATM passwords from across the street, or pick up keystrokes from the electromagnetic signals that are being emitted. Almost every state has a Security Breach Regulation. Companies must understand and be in compliance with the laws of each state where the breach occurred, as well as those states where the affected individuals reside. This can be very time-consuming, however the penalties and fines for noncompliance can be substantial.

It is estimated that the cost to notify a person that a security breach has taken place is somewhere in the range of $200 per compromised customer. If 10,000 policyholders are affected, that would equate to approximately two million dollars just in notification costs. This does not include the cost to repair the actual problem.

**Copyright and Trademark Infringement:** Just because the Internet is “free”, it does not mean that everything found is “free” for the taking. Copyright and trademark infringement claims may result from people downloading picture, or music, or printing information. This is true for personal lines customers as well as commercial.

In the beginning of his first term, President Obama said:

“It’s long been said that the revolutions in communications and information technology have given birth to a virtual world. But make no mistake: This world -- cyberspace -- is a world that we depend on every single day. It’s our hardware and our software, our desktops and laptops and cell phones… that have become woven into every aspect of our lives.”

Recently, there have been a number of high profile cyber-attacks, including companies such as SONY, Target, and Staples. The SONY attack led to cancellation of the release of the movie The Interview, Target paid $10 million to settle a lawsuit ensuing from a breach of debit and credit card information of 40 million people and personal information of 70 million. Some of the attacks may not be as publicized. A USA TODAY report stated that U.S. Department of Energy computer systems were compromised more than 150 times between 2010 and 2014. Tax records of more than 300,000 individuals were accessed in May 2015.

The Federal Government continues to work to protect information on the worldwide web. Most recently, the Cyber Security Information and Protection Act was passed by the Senate. It would allow sharing of information between federal agencies and manufacturing and technology companies. Detractors fear that there are not enough privacy safeguards in the bill.

As more and more businesses and individuals turn to the Internet to conduct business, they are entrusting their personal and confidential data to cyberspace. Social media sites Facebook, Instagram, LinkedIn, Twitter and activities such as blogging create potential worldwide exposures. Information and photos that are published cannot be taken back. Even worse, these items can be edited and republished.

It is essential for insurance agents to address cyber exposures with their clients before claims happen. There are insurance programs available that address cyber property and liability exposures. The well-informed agent is an asset to his insureds.

About the Author

Sue C. Quimby, CPCU, AU, CIC, CPIW, DAE Assistant Vice President/Media Editor Client Services and Training; Senior Product Development Analyst MSO, Inc.

Insurance Professionals of Central NJ; NJ Council Director-Elect
The value of Cyber Insurance took a big leap forward on October 1, 2015, at least in Connecticut. My state’s expanded data security law now requires that businesses offer appropriate identity theft prevention and mitigation services after a breach of personal information. Connecticut will surely not be the last state to enact this type of law.
Currently 47 states have enacted data breach laws with a variety of requirements, and many federal laws apply to certain risks and activities. Every year a handful of legislatures expand the definitions or tighten the notification standards, as Connecticut did. The good news is that Cyber insurance is designed to help businesses comply with the laws, as they are today and as they evolve.

**Breach Law Trends**

The core of any data breach statute is notification, namely if, when and how the business must report the breach to potentially affected customers and regulators. Small businesses are no less accountable than large corporations when it comes to compliance. Most of these components are addressed in state laws:

- Definition of Personally Identifiable Information
- Type of Breach – Paper or Electronic Only
- Safe Harbor for Encryption
- Risk of Harm Analysis
- Timing of Notification
- Notification to State Attorney General
- Private Right of Action

In 2015, Connecticut added the required offer of identity theft and loss mitigation services to its law. If a small business discovers a breach of electronic data after October 1, 2015 affecting Connecticut residents, it must offer “appropriate” identity theft prevention services and ID theft mitigation services, at no cost for at least 12 months. California is the only other state with a similar requirement, but it only applies to the loss of Social Security, driver’s license or state ID numbers. Connecticut’s mandate also kicks in when the breach involves health information, credit/debit card numbers and bank account numbers.

Seven more states revised their data breach laws in 2015. Montana, North Dakota, Oregon, Rhode Island and Washington now require that breaches be reported to the state’s Attorney General, depending on the number of affected residents. Nevada, as well as Montana, Oregon and Rhode Island, expanded the definition of PII so that more types of information trigger the breach law. Washington and a few of the states adopted strict time deadlines for notifications after discovery, to replace the “as soon as practicable” standard still prevalent in state laws.

**Marketplace Expectations**

The reality is that consumers are demanding notifications and services with or without state laws. Recent surveys found that, after a breach:

- 84% of customers say notification and communication are critical to regaining trust
- 63% expect ID theft protection
- 58% expect credit monitoring

Regulatory and consumer expectations create an enormous challenge for a small business. With 30 or 45 days to notify under many state laws, there is little time to investigate the breach, determine who was affected, send out the notice and arrange for loss mitigation services. How does the business owner find these services after a breach, or determine which providers have the necessary expertise?

**Cyber Insurance Products and Services**

As state laws and consumer expectations grow, so does the demand for Cyber insurance. The typical Cyber policy includes the provision of services essential to satisfying both constituents. It will likely embed Forensic investigation to determine the cause and scope of breach, Legal assistance for determining notice requirements, notification services, public relations support, and finally the offer of credit monitoring and ID restoration required in Connecticut. Upon reporting the suspected breach to the insurer, these services are triggered and the business owner is protected.

Not all Cyber insurance policies and services are alike. The expertise of the insurer and breach service provider is the first area of differentiation. At a minimum any insurer or provider needs to stay current with changing breach laws and trends. Does the insurer manage the breach response or does a third-party vendor take over? How many and what types of breaches have they handled? Have they delivered the services in time for the business to meet statutory deadlines? These are important questions any business or agent can ask when comparing product offerings.

The coverage structure can also vary. Some policies provide a single limit that can be used for any combination of the services, while others sublimit certain items, most likely Legal and Forensic costs. The amount of the policy limit can range from $25,000 on up to many millions, with most small business policies at $50,000 or $100,000. Based on the median cost of a small business breach – roughly $33,000 per one recent study – these limits will be adequate for most losses. Many carriers offer higher amounts should more protection be desired.

Most of the Cyber policies include third-party liability defense, indemnity, government fines and additional elements. But the core of the coverage has always been the breach response services designed to help businesses comply with state laws and consumer expectations. That is what is driving the growth of the Cyber insurance market in the small business marketplace.


**About the Author**

Mindy Pollack is an attorney and business development specialist for Gen Re’s Cyber and EPLI insurance business. In that role, she supports turnkey insurance products and helps insurers establish and grow their Cyber and EPLI books of business. She has over 30 years of experience with insurance law, regulation, claims, coverage and product development. You can contact Mindy at 203 328 6153 or mpollac@genre.com.
At State Auto we focus on our only means of distribution... the independent agent!

PaceSetter Program—exceptional training for your producers

Inner Circle—recognizing agency profitability and growth

Agency and CSR incentives—rewarding our best performers

Proud partner of the IAIP—If you’re interested in partnering with State Auto, please contact Terra Boroff at 614-917-5128 or email Terra.Boroff@StateAuto.com
Are you an insurance professional looking to advance your career?

INsure your future.
Join IAIP today.
GoAllInWithIAIP.org
Cyber threats are reported almost daily in the news. From the federal government to small businesses, cybersecurity is a challenge to manage. Understanding those exposures, mitigating the risk, and insuring potential damages can be difficult for insurance industry professionals. The following are all areas of concern when reviewing your client’s cyber exposure. Addressing these concerns will ensure their trust in you.

Serious consideration must be given to the amount of Personally Identifiable Information (PII) the client has and how well they protect that information. These questions will be at the top of underwriter’s concerns when reviewing the application.

- What information does the client collect in their operations?
- How is that information stored?
- Who has access to it?

The “what, how, and who” of your client’s data will determine their potential exposure to loss. Additional questions will be:

- Do they receive credit card payments, and no other PII?
- Do they collect full credit reporting information, including social security numbers?
- Do they collect or store personal health information?

by: Janet Smith
Should your client experience a breach, it will be a scary time for them. But with solid insurance coverage in place, that process can be much less traumatic. A claims response team is immediately available to assist with determining the extent of the breach, the legal notification requirements, and the proper public relations announcements. This will make the entire experience much smoother and dramatically cut the costs and negative publicity of a breach.

Finding comprehensive coverage for your client can be challenging. Understanding these issues is the first step. There are policies out there available to address these concerns. Many policies include Risk Management Services to help your clients understand and mitigate their exposures to prevent a breach. The best policies also include a dedicated claims response team that will help guide your client through the forensic, compliance, and media requirements. Looking for a carrier that has established relationships with experts is critical.

The answers to these questions will make a difference in the type of coverage needed. The rules for addressing a breach of each type of information vary. Personal health information is subject to even stricter regulation than PII with specific laws, such as HIPAA and Hi-Tech. Forty seven states have privacy laws regulating how your clients must respond in the event of a breach. And each state’s law may be different. Additionally, your client must respond to the breach based on the laws of the states where the breached individuals live, not where your client maintains an office.

The type and volume of information that they have and hold will determine whether they will be legally required to comply with the breach laws. When reviewing PII held by your clients, be sure to consider all sources of the information and not just that stored on their servers. Paper files, mobile devices, and the often-overlooked hard drives of copiers can all store data.

Don’t forget to discuss whether third parties have access to the client’s confidential information. A major concern for small businesses are the IT professionals they use. Should the IT vendors suffer a breach and compromise your client’s data, things get tricky. The facts are, your client required the PII and that makes them responsible for protecting it. As such, they must comply with all the privacy laws and regulations, despite the fact that they contracted with an IT vendor to protect it.

Another area of concern is with those clients that accept credit and debit card purchases. To accept credit and debit payments, your clients must sign a merchant service agreement with the credit card companies. This relationship is regulated by the Payment Card Industry (PCI) – Data Security Standard Council. The requirements and mandatory compliance standards in these agreements can be overwhelming and confusing. Additionally, experiencing a cyber breach can trigger PCI fines and penalties. Some insurance policies exclude these fines and penalties - leaving your clients alone in addressing these issues and handling the costs.

During the initial discussions with your clients it is important to identify the costs they should expect to face should they experience a breach. These include:

- Forensic and legal costs
  - to determine the size and scope of the breach
  - to determine if notification of affected individuals is required

* These costs can soar as experts are expensive. Forensic costs can start at $25,000 and may top out upward of $500,000.

- Notification costs often range up to $30 per record for each individual identity breached.

- Your client may have to establish a call center, offer credit monitoring to those affected, and make public relations statements to the press. These costs come fast and add up significantly.

- On top of the costs to handle the breach, your client may face regulatory fines and penalties which could exceed $1,000,000.

About the Author

Janet Smith is the president of Bailey Special Risks, Inc. BSR is a professional lines wholesale/broker and has been in business since 1989. BSR focuses on professional liability, cyber liability, employment practices liability, and directors & officers’ liability, sold exclusively to independent insurance agents for their commercial clients. Additional information is available at www.bsrins.com.
What Is Cybersecurity?

by: Mindi McDowell & Allen Householder, US Homeland Security

It seems that everything relies on computers and the internet now – communication (email, cell phones), entertainment (digital cable, mp3s), transportation (car engine systems, airplane navigation), shopping (online stores, credit cards), medicine (equipment, medical records), and the list goes on. How much of your daily life relies on computers? How much of your personal information is stored either on your own computer or on someone else’s system? Cybersecurity involves protecting that information by preventing, detecting, and responding to attacks.

What are the risks?

There are many risks, some more serious than others. Among these dangers are viruses erasing your entire system, someone breaking into your system and altering files, someone using your computer to attack others, or someone stealing your credit card information and making unauthorized purchases. Unfortunately, there’s no 100% guarantee that even with the best precautions some of these things won’t happen to you, but there are steps you can take to minimize the chances.

What can you do?

The first step in protecting yourself is to recognize the risks and become familiar with some of the terminology associated with them.

Hacker, attacker, or intruder - These terms are applied to the people who seek to exploit weaknesses in software and computer systems for their own gain. Although their intentions are sometimes fairly benign and motivated solely by curiosity, their actions are typically in violation of the intended use of the systems they are exploiting. The results can range from mere mischief (creating a virus with no intentionally negative impact) to malicious activity (stealing or altering information).

Malicious code - Malicious code, sometimes called malware, is a broad category that includes any code that could be used to attack your computer. Malicious code can have the following characteristics:

• It might require you to actually do something before it infects your computer. This action could be opening an email attachment or going to a particular web page.

• Some forms propagate without user intervention and typically start by exploiting a software vulnerability. Once the victim computer has been infected, the malicious code will attempt to find and infect other computers. This code can also propagate via email, websites, or network-based software.

• Some malicious code claims to be one thing while in fact doing something different behind the scenes. For example, a program that claims it will speed up your computer may actually be sending confidential information to a remote intruder.

Viruses and worms are examples of malicious code.

Vulnerability - In most cases, vulnerabilities are caused by programming errors in software. Attackers might be able to take advantage of these errors to infect your computer, so it is important to apply updates or patches that address known vulnerabilities.

This series of cybersecurity tips will give you more information about how to recognize and protect yourself from attacks.
DEALING WITH CYBERBULLIES

by: Mindi McDowell
US Homeland Security

Bullies are taking advantage of technology to intimidate and harass their victims. Dealing with cyberbullying can be difficult, but there are steps you can take.

What is cyberbullying?

Cyberbullying refers to practice of using technology to harass, or bully, someone else. Bullies used to be restricted to methods such as physical intimidation, postal mail, or the telephone. Now, developments in electronic media offer forums such as email, instant messaging, web pages, and digital photos to add to the arsenal. Computers, cell phones, and PDAs are current tools that are being used to conduct an old practice.

Forms of cyberbullying can range in severity from cruel or embarrassing rumors to threats, harassment, or stalking. It can affect any age group; however, teenagers and young adults are common victims, and cyberbullying is a growing problem in schools.

Why has cyberbullying become such a problem?

The relative anonymity of the internet is appealing for bullies because it enhances the intimidation and makes tracing the activity more difficult. Some bullies also find it easier to be more vicious because there is no personal contact. Unfortunately, the internet and email can also increase the visibility of the activity. Information or pictures posted online or forwarded in mass emails can reach a larger audience faster than more traditional methods, causing more damage to the victims. And because of the amount of personal information available online, bullies may be able to arbitrarily choose their victims.

Cyberbullying may also indicate a tendency toward more serious behavior. While bullying has always been an unfortunate reality, most bullies grow out of it. Cyberbullying has not existed long enough to have solid research, but there is evidence that it may be an early warning for more violent behavior.

How can you protect yourself or your children?

• Teach your children good online habits - Explain the risks of technology, and teach children how to be responsible online. Reduce their risk of becoming cyberbullies by setting guidelines for and monitoring their use of the internet and other electronic media (cell phones, PDAs, etc.).

• Keep lines of communication open - Regularly talk to your children about their online activities so that they feel comfortable telling you if they are being victimized.

• Watch for warning signs - If you notice changes in your child’s behavior, try to identify the cause as soon as possible. If cyberbullying is involved, acting early can limit the damage.

• Limit availability of personal information - Limiting the number of people who have access to contact information or details about interests, habits, or employment reduces exposure to bullies that you or your child do not know. This may limit the risk of becoming a victim and may make it easier to identify the bully if you or your child are victimized.

• Avoid escalating the situation - Responding with hostility is likely to provoke a bully and escalate the situation. Depending on the circumstances, consider ignoring the issue. Often, bullies thrive on the reaction of their victims. Other options include subtle actions. For example, you may be able to block the messages on social networking sites or stop unwanted emails by changing the email address. If you continue to get messages at the new email address, you may have a stronger case for legal action.

• Document the activity - Keep a record of any online activity (emails, web pages, instant messages, etc.), including relevant dates and times. In addition to archiving an electronic version, consider printing a copy.

• Report cyberbullying to the appropriate authorities - If you or your child are being harassed or threatened, report the activity. Many schools have instituted bullying programs, so school officials may have established policies for dealing with activity that involves students. If necessary, contact your local law enforcement. Law enforcement agencies have different policies, but your local police department or FBI branch are good starting points. Unfortunately, there is a distinction between free speech and punishable offenses, but the legal implications should be decided by the law enforcement officials and the prosecutors.

Additional information

The following organizations offer additional information about this topic:


StopBullying.gov - http://www.stopbullying.gov/
CYBER COVERAGES:

Understanding Policy Trends and Opportunities

by: Byron Acohido & Edward Iwata
1. Cyber Coverage - Insurance coverage that focuses on services and systems related to technology and their use in business. Risks addressed include website and software design, network equipment, damage caused by service interruptions and computer viruses, and much of the work performed by technology vendors and consultants. Insureds are also commonly covered for damages if they inadvertently transfer a virus to a network owned or operated by someone else.

2. Data Breach Coverage - Often used interchangeably with Privacy Breach Coverage and/or Security Breach Coverage. Coverage that protects businesses in the event sensitive, protected data is compromised or exposed. Many policies also cover costs associated with first-party response and third-party liability exposures.

Misconceptions and myths about data breach, privacy, and cyber coverages abound. Insurers, brokers, and agents may be as confused as their clients, potentially putting businesses at risk if they believe they don't need crucial coverage, or if they think they have coverage when in reality they do not. By developing a more in-depth understanding of the latest insurance solutions, agents and clients alike will be in a better position to assess the options.

HISTORY OF CYBER AND PRIVACY BREACH COVERAGES

The first cyber coverage solutions appeared in the early 1990s, as technology began to play a larger role in daily life and the Internet was emerging as a viable business tool. Service interruption and website-liability coverages were popular early options as businesses discovered the need for risk management and mitigation in a world that was increasingly reliant on technology. Websites evolved into active business platforms rather than just online placeholders, or the digital equivalent of billboards. With this evolution in the late 90s, the increase in the connections to consumers and other businesses grew exponentially. Coverages that spoke to network liability soon followed and became prominent, at least for larger companies and specialized online businesses.

In 2003, the first privacy breach notification legislation was passed in California, prompting a major leap into what we recognize today as privacy data breach coverage. More businesses recognized the need for first- and third-party coverages as they grappled with a wide range of new data protection issues and the risks associated with them. Breach notification obligations were being mandated at the state level. In addition, industry standards in the payment card sector and federal regulations in the form of HIPAA and HITECH brought more stringent compliance requirements as well.

The expanding scope of risks businesses face today has prompted carriers to create a broader array of coverage solutions. These new options are designed to more fully address not only the conventional issues of doing business online, but also the dangers surrounding consumer data breaches and cyber business interruption as well as emerging threats such as data ransom and cyber extortion.

Unfortunately, while there may be more variety in the coverage options available for cyber coverage, this must remain the number one priority for producers.

With big breaches dominating headlines, more business owners are looking for ways to move from fear to action. They are increasingly acknowledging the need for cyber coverage and want help determining their needs, but many don't know where to turn, especially if their broker isn't familiar with or doesn't offer cyber policies. The need is there. How can the industry better drive demand? The answer: Education. Today's environment has created a prime opportunity for insurance companies to market and sell cyber risk programs much more effectively by creating a solid foundation of knowledge for producers and clients.

Education and awareness of risks and mitigation best practices are key to proactive protection. Policyholders have the tools available to significantly improve their security posture and reduce their risk of a breach, but identifying and implementing effective measures requires they have a better understanding of today's cyber threat environment. Insurers also must have top-tier knowledge available to help guide clients toward the right solution.

The evolution from narrowly focused coverage to coverage that addresses multiple risks in interrelated areas is one reason behind the confusion felt by businesses and producers. Knowing which risks a particular company faces and how best to mitigate them isn't nearly as straightforward as it was even five years ago. Current thought leadership...
and insight into the evolving world of best practices from experts in the cyber coverage realm is crucial to marrying risks with appropriate mitigation strategies.

UNDERSTANDING POLICY TYPES AND COVERAGE

The terms “cyber” and “privacy breach” are often used interchangeably when referring to the policies available, but there are significant differences between them.

BIG FIRMS ARE AT HIGHER RISK FOR CYBEREXPOSURE

Cyber coverage typically focuses on services and systems related to technology, and their use in business. Risks addressed include website and software design, network equipment, damage caused by service interruptions and computer viruses, and much of the work performed by technology vendors and consultants. Insureds are also commonly covered for damages if they inadvertently transfer a virus to a network owned or operated by someone else. Privacy breach coverage protects businesses in the event customer, consumer or patient data is compromised or exposed. Also covered under many policies are costs associated with first-party response costs and third-party liability exposures.

First-party coverage provides for legal expenses associated with regulatory compliance, such as state breach notification regulations, federal healthcare mandates including HIPAA and HITECH, and financial industry regulations including contractual agreements surrounding PCI compliance. It also covers expenditures incurred as part of any forensic investigations into the duration and extent of exposures to determine specifically what data was compromised and who was impacted. The costs to respond to a breach, to notify affected parties and any applicable regulatory agencies, and to provide victims (and potential victims) with credit monitoring tools and identity theft remediation services are further benefits of first-party coverage.

Third-party coverage focuses on liability costs related to defending against consumer-based litigation or regulatory actions that arise as a result of a breach. The majority of these risks are significantly reduced—if not eliminated—by appropriate use of first-party coverage.

The way policies are currently being offered and written is also notable. Only 57 percent of companies that write cyber risk write dedicated policies. More often, cyber is bundled with existing policies, notably general liability, property and business interruption, and E&O. This general reluctance to participate in the cyber market is dominated by insurers’ concerns about a lack of data surrounding cyber policies and claims. Launching in 2015, ISO’s data breach policy and claim data sharing program—part of the organization’s cyber risk platform—will begin to address much of the existing data scarcity.

MARKET PROFILE: LARGE COMPANIES

The nature of a big company and its way of doing business means that they commonly need strong privacy breach and cyber coverage. A vast number of them gather, process and store large amounts of information, and they also typically have complex technology and network infrastructures supporting their operations. These companies often deploy and manage much of the underpinnings that drive wider activities, such as the processing of financial transactions and the compilation and analysis of large databases.

Systems within the infrastructures of Fortune 1000 and similar companies usually have many connections to outside partners, such as suppliers and client organizations. Cloud computing is also heavily leveraged for core computing functions, and the extensive use of external vendors also leads many big businesses to allow network access to companies and people outside their own workforce.

These factors put the typical large company at risk for cyber exposure. Privacy breach risks, on the other hand, are often managed through the proactive policy making and robust security measures available to big firms that have sufficient funding and ample internal resources.

MARKET PROFILE: SMBS

In contrast to large organizations, the majority of small and midsized businesses don’t often run the same levels of risk when it comes to cyber exposure. They may have their own internal systems while only occasionally providing services to other companies or using their networks for extensive connected activities. And they may rely on cloud technology regularly, but its use within the organization is typically limited.

SMBs do, however, often have higher privacy breach risk. Most don’t employ data protection experts or large technology teams, making the information they collect and manage potentially more vulnerable to exposure. They’re also less likely to implement strict data retention policies, they may not be familiar with the safest ways to store and dispose of information, and in some instances they may be unaware that they’re subject to state, federal, or industry compliance regulations.

In addition, non-digital breach causes remain a top-tier risk among small and midsized businesses (SMB). Mailing hardcopy invoices and patient statements to the wrong address, for example, or improperly disposing of obsolete paper files, may pose as great a breach risk as any electronic network intrusion.

Breach impacts in the SMB sector have the potential to inflict significant damage. Ongoing customer concerns about data privacy and exposure was shown to have a measurable impact on the bottom line in the case of the Target breach. Couple that lost revenue with the costs necessary to respond to a security incident—from investigative services that determine the extent of an exposure, to litigation brought by affected parties—and a breach has the very real potential to threaten a small company’s financial health. In stark contrast to the big business sector, an SMB breach and resulting costs typically aren’t as easily absorbed as they might be with companies like Target and Home Depot. Business continuity and long-term viability are of serious concern.

SPECIFIC NEEDS

A subset of firms both large and small have risk profiles shaped by more than just their size. Companies that operate in specific industries—healthcare, legal, and financial to name a few—often require more robust privacy breach coverage. These businesses are responsible for managing the most sensitive information types, and exposure of that data could lead those impacted to suffer significant harm. Whether it’s a large hospital organization or an individual doctor’s office, a nationwide law firm or a small-town attorney, these companies have valuable and highly confidential information that is actively sought by hackers and that the businesses must vigorously strive to protect.

MARKET STRATEGIES

The market needs for both cyber and privacy breach coverage solutions are specific to the size of the business being considered as well as industry or other risk factors that may be present.

Big companies generally have a number of other insurance products in their portfolios, and cyber risk coverage will often naturally dovetail with existing initiatives overseen by the organization’s
risk management group. It’s likely that these internal teams already have identified where potential liabilities lurk and what can be done to mitigate them. And while large firms regularly absorb significant levels of risk internally for financial reasons, most have also accepted sizable insurance premiums as a normal cost of doing business.

Contrast that to the small company sector, which has been largely overlooked in the past as a segment of the marketplace that was either uninterested or unable to secure robust coverage. But many SMBs, and particularly those in the high-risk categories related to the healthcare, financial, and legal industries, often benefit from highly targeted and carefully underwritten policies. Keep in mind that, regardless of their risk profile, most SMBs are likely to be much more price-sensitive than larger firms, as they often have far less budget available to cover high premiums. However, small companies are often receptive to the concept of add-on coverages to the commercial package or business owners’ policies they already have.

In all business sectors, increased awareness of the need for cyber and data breach coverage drives greater demand for these types of policies. However, there is still a significant lack of awareness among potential clients that cyber coverage is something they should have. In fact, companies that don’t believe they need cyber insurance is cited as the greatest selling challenge by 40 percent of producers in a recent study conducted by Hanover Research. Opportunities for increased revenue will follow when businesses understand the critical need for breach coverage and how accessible effective coverage options are to organizations of any size.

In addition SMBs rarely have internal legal or risk management resources that can help them navigate through their firm’s specific areas of risk. Small business operators may not be familiar with their existing insurance products or they may misunderstand what the various coverage solutions offers. Producers who present cyber- and privacy breach coverage options to smaller firms must have a thorough understanding of the coverages and be able to provide guidance on where liabilities exist or where their present policies may have gaps.

SUMMARY
Though technology touches nearly every aspect of business in today’s environment, cyber and privacy breach coverage solutions extend far beyond hacking incidents. Even low-tech businesses and non-digital data face breach risks, such as when a small construction firm loses its personnel files in an office break-in. The need for breach coverage is becoming a far more crucial offering for clients as well as the producers and carriers who serve them.

Education has become a critical tool for agents and brokers, with a number of support options available to ensure that the advantages of the various coverage solutions are clear. With a good understanding of the coverages available, producers can build a profitable risk-averse breach coverage that properly supports their insureds and provides increased revenue opportunities.

About the Authors
By Byron Acohido and Edward Iwata, ThirdCertainty
ThirdCertainty’s mission is to deliver actionable intelligence accessible to our target audience of non-technical company decision makers. We want to help them better understand emerging security and privacy exposures. We have established ThirdCertainty as a mobile-optimized venue where thought leaders can engage in intelligent discussions to help make things better. Our stories are adding to discussions that crop up in social media over an extended period of time. You can follow the latest developments at ThirdCertainty by signing up for our free weekly newsletter.
REALISTICALLY, How Bad is a Data Breach for Business?

by: Deena Coffman

Many executives express doubt that a data breach will have a long-term or even impactful effect on business. They feel it would, at worst, be a news story that can be outlived if it even occurs. The "It can't happen to me" view is prevalent. The experiences from companies that have had the misfortune of public data breach event show us that real risks clearly exist, ranging from lost revenue to lawsuits to executive-level terminations. The impacts seen from a data breach event occur in the areas of risk that every CEO is ultimately responsible for managing – revenue, expenses, productivity, and brand equity.
Revenue

The first risk a business faces in the aftermath of a public breach event is to revenue. Skeptical CEOs are reluctant to believe that customers really leave because of a data breach, choosing instead to believe that even if customers initially leave, they will return. In reality, the number of customers that leave is dependent upon “switching costs”; in other words, how painful it is for the customer to move their business elsewhere? For retail stores, switching costs are typically very low, so retail businesses face a greater risk of revenue loss due to a data breach. Target’s SEC filings showed both traffic and transaction volume decreased year over year for the retailer during the year after their breach. Because this was not the case for Target’s competitors, it supports a position that argues that Target’s customer confidence indeed took a hit in the wake of the breach and that it had an impact on revenue from sales.

Public polls offer limited insight as some polls show that 60% of people are inclined to change buying behavior while other polls show only 40% stating that buying behavior would change. Regardless of what people say in a poll, the concern is what customers will actually do, and statements made in the hypothetical may be very different from what occurs in reality. For medical practices and retail banks, switching costs are typically higher as many people are not willing to find a new doctor or complete the paperwork required for new bank accounts or go through the trouble of setting up all new online bill payments.

Another important factor is the amount of trust that forms the basis of the relationship with your customer and how much damage the breach does to that trust. Here is where banks stand to fare worse, despite higher switching costs. Even if customers eventually come back, an initial loss of revenue may cause a strain on cash flow in the short term, which, for companies without sufficient cash reserves, may create a financial situation is difficult to overcome. Smaller organizations tend to have less of a cushion, especially in low margin businesses. A publicly traded company must also consider the impact of news on the opinions of analysts and investors, as a drop in stock price may trigger loan covenants and other barriers to obtaining financing.

Expenses

The tremendous cost of cleaning up after a data breach will exacerbate the financial pain because as revenue is declining, expenses are rising. Together the profitability squeeze may not be sustainable. The Ponemon 2015 Cost of Data Breach Study surveyed 350 companies to calculate the mean average cost of a lost or stolen information record and found it to be just over $154 each. Another organization, NetDiligence, reported on 160 breach events large enough to result in an insurance claim and found the per record cost to be $964. Large variation exists in breach events which makes calculating a mean average extremely difficult and can render the estimate of limited use. Nevertheless, it is helpful to have visibility into the potential impact, especially given the growth in both probability and impact of a data breach event both domestically and globally.

The largest and most immediate expenses faced by a company after a data breach are those associated with legal and technical investigations and system recovery. Not as immediate, but not far delayed, are expenses for legal defense and, if the breach is for payment card data, card replacement costs, contractual obligations and payment card information (PCI) fines and penalties. Finally, smaller, but still notable near term costs may need to be borne for PR, victim notification and resolution as well as additional advertising and incentives to entice customers to return.

Longer term, millions of dollars in expenses may accumulate from legal fees, fines and penalties. Heartland Payment Systems paid over $140 million in costs, fines and penalties following a data breach. TJ Maxx had a data breach tab of $162 million. Target’s cost is $252 million and counting. The list of companies with double and triple-digit million dollar costs related to data breach events is already long and still growing. The vast majority of data exposures are not reported and are small and of little financial impact to the companies experiencing or causing them, however, it is unwise to discount the less likely, but still entirely possible. There is just too much at stake.

Productivity

In some circumstances, employees, managers and even executives may be terminated as was the case with Sony’s Co-Chairman, Target’s CIO and CEO, Ashley Madison’s CEO and many others. A change in leadership, especially amidst a crisis, can be distracting and unnerving to the employee population, impacting productivity, even if the transition happens quickly. But, most transitions are not quick. Finding, recruiting and on-boarding a new employee at any level takes time and interrupts productivity. In addition, companies often face additional, subsequent turnover of employees who are not happy with the departure of someone they liked or their replacement. It may take a year or more for that to settle.

In cases where a data breach exposes the employee population’s personal and/or financial information, it would be naive to think that employees are able to focus fully on work even in the face of questions from the public, friends and family as well as tremendous personal financial exposure. The larger the number of employees impacted, the longer the conversation will continue to exist and distract. In these instances, it is even more important for management to communicate clearly, accurately and proactively and to offer support for the individual employees at risk for identity theft.

Brand Equity

Given the difficulty of assessing the actual value of a brand, it is even more challenging to quantify the negative impact that a data breach can have on a previously strong brand. Brands can motivate buying behavior and support premium pricing, which translates to real revenue and profitability. Companies buy and sell brands like physical assets, and brands are carefully managed and, when threatened, defended vigorously through expensive litigation. No one would suggest that a breach can boost brand valuation just as no one would say that all breach events would have an equal impact. But, context, timing, size, announcement and other factors may yield a decline, whether large or small, to a company’s brand strength. YouGov, which publishes a brand strength index, compared the impact of Target’s data breach announcement to that of Home Depot. Target has been publicly criticized repeatedly for the many mistakes made in handling their data breach, while Home Depot executed according to advice published by many experts as best practice. Both brands showed damage, but Target’s brand suffered more and the impact lasted longer. Companies who take care to prepare, prevent and properly respond can be in a better position than those that leave their corporate image to chance.

About the Author

Deena Coffman, CEO IDT911 Consulting
IAIP Corporate Partners

Platinum Level Corporate Partner

![Crawford](image)

Gold Level Corporate Partners

![Enterprise](image)  ![Imperial PFS](image)  ![Liberty Mutual](image)

Silver Level Corporate Partners

![Paul Davis](image)  ![Wahve](image)

Bronze Level Corporate Partners

![Cincinnati Insurance Companies](image)  ![West Bend](image)  ![Wright Flood](image)

Companies can partner with IAIP to promote the insurance industry through providing education, networking and industry alliance, as well as providing insurance products to the general population. Several levels of corporate partnership are available to meet your business's needs.

Contact the Director of Marketing at 800-766-6249, extension 4, or email marketing@iaip-ins.org today to find out how your company can benefit from partnering with IAIP.
Legacy Foundation Donors

The NAIW International Legacy Foundation wishes to recognize our supporters for their generosity and commitment to help transform the insurance industry through the development of educational programs for insurance professionals.

The Legacy Foundation was formed in 2006 as the philanthropic arm of the International Association of Insurance Professionals, an association of insurance and risk management professionals dedicated to the perpetuation of those industries through education, networking and industry alliances.

Donations will be used to:

• Develop education courses
• Fund educational seminars and workshops
• Fund keynote speakers

All financial contributions to the Legacy Foundation are tax-deductible as a charitable contribution.

Thank you to our generous donors from December 2, 2015 through March 1, 2016:

**Trendsetters ($100 - $999)**
- Mary Corvaia - Nationwide United Way Campaign, Matching Donation
- Betty Curry - FL Council Meeting
- Charlotte Association of Insurance Professionals - In honor of Robin Bennington & Geraldine Plott, Convention Grand Prize Donation
- Florida Council - FL Council Meeting
- Insurance Professionals of Acadiana
- Piedmont Association of Insurance Professionals - Convention Grand Prize Donation
- Geraldine Plott - Convention Grand Prize Donation
- Tennessee Council of Insurance Professionals
- Linda Wilson

**Pacesetters ($25 - $99)**
- Sharon Clark - Convention Grand Prize Donation
- Contra Costa Chapter of IAIP
- Durham Association of Insurance Professionals - Convention Grand Prize Donation
- Greensboro Insurance Professionals - Convention Grand Prize Donation
- Brenda Hornyak
- Linda Luka - In memory of past Region V RVP Carol Draba
- Randolph Insurance Professionals Association - Convention Grand Prize Donation
- Maribeth Rizzardi
- Billie Sleet - Convention Grand Prize Donation
- Valley of the Sun Insurance Professionals - In honor of Cindy Martin’s father
- Brenda Webster - Convention Grand Prize Donation
- Margaret & Mary Wildi - In memory of rox Horton’s brother
- John Donnell, Convention Grand Prize Donation
- Wilmington Insurance Professionals - Convention Grand Prize Donation

**Advocates ($1 - $24)**
- Gracellen Donnelley
- Cherri Harris

A NOTE TO OUR SUPPORTERS:
We appreciate your generous donations to the Legacy Foundation, and we want to recognize everyone accordingly with 100% accuracy. If we have inadvertently made an error, please contact the Legacy Foundation at 800-766-6249 ext. 1 with concerns or corrections.
WELCOME
New IAIP Members!

Welcome our new members from December 2, 2015 through March 1, 2016

REGION I
Kelly Alderfer
Christy Ann Berard
Tiffany Corpuz
Martine Finney
Bernardine Kane
Sylvia S. Kennedy
Shannon Latham
Robina M. Lods
Stephen Mansi, CFP
Dawn Norton
Katy O’Brien
Laura Pabellon
Antonia Schachter
Susan S. Smith, AIC, CPIW
Lynne Tomasello
Mallory Tomczyk
Michele Turgeon

REGION II
Melissa Berry
Shannon Hauser
Alexis LaPorte
Debbie McDuffie, AAI AIS CPIS
Diane J. Sudderth, CPCU, AU, CIC, CPIW

REGION III
Candy Campbell
Saundra Etchison, CIC, CISR
Kally Flytzanis
Christina Gay
Susan Guenther
Michele Harris
John Huttner
Paula Keyes, CPCU, ARE, CPIW, AIR
Carla A. Lopez
Emily McDaniel
Libba McKinney
Becky McMillan
Jessica Mizenko, CPA, CGMA
Melody Norris
Chris Nuedecker
Teresa Pietrzak, CIC
Tish Pollard, CISR
Melissa Ruzicka, AAI
Alicia Saunders
Marianne Barish
Stephanie F. Glickauf, Esq.
R. Tyler Bryant, Esq.
Rachel E. Hudgins, Esq.

REGION IV
Nichole Bacovin
Linsey Bibler
Sheila Eskue, CIC, CPIW, AAI, AINS, CMIB, CLCS
Bruce Ford
Molly McClellan, CPCU, FLMI, AU, API, AIT
Nan M. Mierzwiak
Rose Thorsby
Chalise Ann Underwood

REGION V
Julie Andrew
Delanna Collins, AIS, API, AINS, ACS
Dennis Gruetzmacher, AIC AIS
Emily Stevens, CISR, CLCS

REGION VI
Susie Current
Lyndsey M. Graham
Beverly Jenkins
Jane Kersh
Dolores Rodriguez
Michelle Villarreal, AIC

REGION VII
Tammy Eischen
Wanda Roehl

REGION VIII
Tiffany Ackley
Katie Beyerle
Samantha Castillo
Rocky Duran
Alexander S. Gareeb
Pat Geier
Greg Kinninger
J. Michael Krill
Nichole McClellan
Teresa Peterson

REGION IX
Krista Alexander
Mishalla Green, CIC, CRIS
Kyle Silk-Eglit, Esq.

International Association of Insurance Professionals is a professional association open to individuals in the insurance and risk management industries, and provides insurance education, skills enhancement and leadership development. Membership provides you the opportunity to increase your business productivity and profitability by participating in educational offerings and making business connections with other industry professionals. More than 70% of our members have advanced their careers through belonging to IAIP.

To join, contact Amanda Hammerli, Director of Membership, at 800-766-6249 extension 2, or email membership@iaip-ins.org.
Advance Your Career

IAIP offers the following prestigious industry designations:

Certified Insurance Industry Professional (CIIP)

Diversified Advanced Education (DAE)

Certified Leadership Professional (CLP)

CONGRATULATIONS!

NEW CLPs

Tammy Lawrey, CPIW, CLP - Region I
Vikki Angelo, AIC, ITP, CLP - Region IV
Jennifer Thompson, AIS, FLMI, CLP - Region IV
Pam Haakenson, CIIP, DAE, AIS, CLP - Region V
Kim Woods, AINS, API, AIS, ACS, CLP - Region V
Gina Thomas Patterson, CISR, CPIW, DAE, CLP - Region VIII

NEW DAEs

Tracy A. Carfora, CISR, CPIW, DAE - Region I
Debra Chong, MBA, CIIP, DAE - Region VIII

NEW CIIPs

Jennifer V. Modica, CIIP - Region I
Emily Mauney, CISR, CIIP - Region III
Angela Falcone, CISR, CIIP - Region VI

To learn more about these designations, including how to qualify, visit insuranceprofessionals.org and click on Designations under the Education tab. Contact Rebecca Clusserath, Director of Education at 800-766-6249 extension 3 for more information.
Meet the Candidate for the Office of 

International Secretary

Cindy J. Prud’homme
AINS, CPIA, CIIP, CLP

Candidate Question:
During the past two years, the Board of Directors along with our staff at Meeting Expectations, have provided members with many new resources; toolkits, best practices library, streamlined applications, business skills webinars, etc. How do you see these resources and the use by the local associations assisting us with growing and retaining our membership? What additional resources would you recommend to continue on the path of Association Revitalization?
Our leaders have made enormous progress in making IAIP an organization that is easy to work with, providing resources to help us achieve our goals, and offering training to help us rise to the next level. But these are tools; it's what we do with them that make the difference.

I believe our success or failure in growing our association is a choice. Our results stem from the choices we make, starting with the priority and effort we give the goal. For many it can be as simple as making the choice to invite a colleague to the next IAIP meeting.

To retain members we must deliver value. This means quality education, relevant industry-related programs, plentiful networking opportunities, and using the networks we build. To attract new members we must do these things and more. We must market ourselves in a positive manner, mindful of the message we send when we speak candidly, we must enthusiastically share the message as to why membership is valuable, and we must be welcoming and inclusive.

The choice is ours whether we will succeed in meeting our goals. It’s up to us to make use of the tools available to us, put best practices into place, share ideas and find creative solutions to challenges, and devote time and energy into building membership. Any of us can do it; all of us can do it. The question becomes, will we CHOOSE to do it?

If there are additional tools needed, I would say that we should try to help with voice & video conferencing resources and execute an aggressive marketing campaign. A critical resource would be a central database of insurance organizations with key contact information, to help us reach potential members and supporters.

But all these things are simply the next generation of tools that will serve us. At the end of the day it still comes down to each of us and whether we will make the choice to use them and to push forward to achieve the goals we’ve set for ourselves.

About Cindy J. Prud’homme, AINS, CPIA, CIIP, CLP

Board Leadership
- Served on IAIP Board of Directors 2012-2014 as Region IV RVP
- Served on NAIW Legacy Foundation Board of Directors 2012-2014
- Served on NetVU (AMS Users’ Group) Board of Directors 2008-2010
- IAIP Budget & Finance Committee 2012-2014
- IAIP Nominating Committee (3 times)
- NetVU Nominating Committee
- Served on Underground Railroad (domestic violence shelter/agency) Board of Directors 1994-1997

Project & Change Leadership
- Conference Recommendations Task Force Co-Chair, instituted 3-track education strategy at IAIP convention, implemented new cost containment controls, proposed comprehensive recommendations to increase value and decrease costs.
- Chair of IAIP Education Task Force: currently implementing 6 new IAIP classes, new Sales Essentials series, and implementing Confidence While Communicating for online delivery

- Chair of NetVU Sagitta Education Committee, planning & organizing 56 classes at annual convention each year
- Reputation for adding value; track record for delivering results.
- Professional Project Manager and Business Analyst for Meadowbrook Insurance Group
- Specialized in Business Process Improvement

Team Building & Engagement
- Created & Presented Bridging the Membership Gap IAIP Workshop (exploring diversity of membership)
- Increased average Confidence While Communicating class size from 2 to 20 within one year.
- Ability to communicate and share a leadership vision, and recruit support and engagement toward that vision.
- Charter member and President of Mid-Michigan Association of Insurance Professionals
- Charter member and President of Midwest Sagitta Users Group – Grew local chapter to 7 states within 2 years
- Delegates effectively
- Implemented cross-training initiative at Michigan Council

Strong Communicator
- Completed Confidence While Communicating
- Competed in Region IV Confidence While Communicating Speak Off 3 Times
- Published in Today’s Insurance Professionals, 2013

Skills
- Exceptional Computer Skills
- Experienced Trainer & Presenter
- Leads Effective Meetings & Teams
- Project Delivery & Implementations
- Supervisory Management
- Budget & Financial Experience
- Conference Planning
- Develop Business Plans & Strategy

IAIP Leadership History
- RVP - IAIP Region IV - 2012-2014
- Local Association President - Insurance Association of Metropolitan Detroit
- Local Association President - Mid-Michigan Association of Insurance Professionals 1998
- Committee work, chairmanship, or oversight appropriate to, and leading up to each of these positions.

Designations
AINS, CPIA, CIIP, CLP
The Legacy Foundation was formed in 2006 as the philanthropic arm of the International Association of Insurance Professionals, best known for providing insurance education, skills enhancement and leadership development to its members. Make a contribution by mail or online at:

Legacy Foundation

c/o IAIP

3525 Piedmont Road
Building Five, Suite 300
Atlanta, GA 30305

or visit www.insuranceprofessionals.org

The NAIW (International) Legacy Foundation is an IRS approved 501(c)3 foundation.

Contributions to the NAIW (International) Legacy Foundation are tax deductible as a charitable contribution.