Cyber Liability Webinar

“Data Breach...The New Wild West”

Cyber Exposures and Insurance

Presented by

John Eubank, CPCU, ARM

Color Commentary by

Bill Wilson, CPCU, ARM

Copyrights and Disclaimers

COPYRIGHT

TRADEMARKS

DISCLAIMER

This material has been designed for use in training programs for insurance industry personnel throughout the United States. It is not intended to be used as a complete reference resource on the programs and coverages outlined herein. Unless indicated otherwise, the coverage discussion herein are based on various editions of "ISO standard" policy forms. Programs, coverages, rules, and coverage interpretations presented in this publication may be different from those used by individual insurance companies writing these programs. Contact individual companies for details about their interpretations of the programs outlined herein and/or their own proprietary programs and contracts. The opinions expressed in this document are just that. No warranties, express or implied, of any kind are made, intended or inferred. The information contained herein is not legal advice, nor should it be taken as such. When such legal issues arise, proper advice should be sought, where applicable and appropriate, from qualified legal counsel.

INDEMNITY

You agree to defend, indemnify, and hold harmless the authors and presenters, together with their respective employees, agents, directors, officers, and shareholders, from and against all the liabilities, claims, damages, and expenses (including reasonable attorney's fees and costs) arising out of your use of this material; your breach or alleged breach of this Agreement; or your breach or alleged breach of the copyright, trademark, proprietary, or other rights the authors, presenters, or third parties.


John Eubank

John O. Eubank, CPCU, ARM is CEO and President of Professional Insurance Education, Inc. in Nashville, Tennessee. He was previously employed by the Insurance Services Office, Inc. and ISO Commercial Risk Services, Inc. as the Regional Operations Manager for the Southern Region. He left ISO in 1987 to form PIE, Inc. and since has logged 14.72 gazillion miles in his insurance-manual-laden Lincoln.

John's professional affiliations include past Regional Vice President of the Society of Chartered Property & Casualty Underwriters (CPCU), PMLG of the Honorable Order of Blue Goose, International (HOBGI), member of the National Fire Protection Association (NFPA), and member of the Society of Fire Protection Engineers (SFPE).

John is recognized as one of the nation's premier insurance education instructors, having served as a National Faculty member of the Society of Certified Insurance Counselors since 1976, and is a recipient of the Professional Leadership Scroll from the American Institute for Property & Liability Underwriters and the Insurance Institute of America.

Since forming Professional Insurance Education, Inc. in 1987, he has served as a speaker and instructor for a wide variety of educational seminars for insurance associations in Alabama, California, Georgia, Illinois, Indiana, Kansas, Kentucky, Louisiana, Ohio, North & South Carolina, and Tennessee; Hoosier Ins. Co.; Society of CIC and the CPCU Society; National Association of Insurance Women (NAIW); and the North American Retail Dealers Association.

John is available for association-sponsored and in-house training programs, though he is usually booked over a year in advance. He can be contacted at 408 Page Road, Nashville, TN 37205, 615-383-5443, insspeak1@bellsouth.net.

Remaining 2015 Countrywide Webinars

August 26
"Beyond the Basics: Emerging Personal Lines Issues"
Presenters: David Thompson, CPCU, AAI and Bill Wilson, CPCU, ARM

September 16
"Certificates of Insurance…2015 Edition"
Presenter: Bill Wilson, CPCU, ARM

October 21
"Contractual Liability Issues and Answers"
Presenter: Craig Stanovich, CPCU, ARM

December TBA
Free webinar?

More info:
http://www.independentagent.com/Education/Webinars/Pages/home.aspx

Check out lots of archived webinars, many of them free!

Cyber Liability (AKA Data Breach)

Presented By
John O. Eubank, CPCU, ARM
Bill Wilson, CPCU, ARM

History

- 1970 – Insurance Service Office formed & the newly formed Intel unveils the Intel 1103, the first Dynamic Access Memory (DRAM) chip.
- 1971: Alan Shugart leads a team of IBM engineers who invent the "floppy disk," allowing data to be shared among computers.
- 1976: Steve Jobs started Apple and on 4/1 roll out the 1st computer with a single-circuit broad
- 1977: Radio Shack's initial production run of the TRS-80 was just 3,000. It sold like crazy. For the first time, non-geeks could write programs and make a computer do what they wished.
- 1985: Microsoft announces Windows, and the **first** dot-com domain name is registered.
- 1986 – ISO introduces the 'simplified' Commercial General Liability form. **Not much reason to address the 'internet' since the World Wide Web didn't come into existence until...**
- 1990 when the Hyper Text Markup Language (HTML) was developed.

History continued

- 2000 – Y2K. Computer insurance problems began. While the array of data processing problems anticipated on January 1, 2000 because of computers' inability to assign the correct value to two-digit-only year designations—**never became a reality**, the possibility of such computer errors remains, both in systems that were never made "Y2K compliant," and with respect to other theoretical problems that may emerge in the future as a result of digitized time-and-date notations. **It is now 15 years later?**
- **But lots more has happened in those 15 years!**

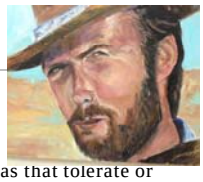
Why This Topic?

- There is probably no one, **at least in the insurance business,** that hasn't heard about the massive data breach epidemic occurring worldwide. **In this seminar we will focus on the insuring 'The Small Guy'.**
- A breach can occur at any company, government agency (school), healthcare provider, law firm or insurance agents office. **As a result, organizations that experience a breach have customers or patients from every walk of life. They may be young, old, educated, wealthy, below poverty level and from any ethnicity. Been watching a new TV CSI Cyber, if hackers can do 10% of what they say—it is scary**

The Wild Wild West

Gene, Roy, Hoppy, Gabby, James, Artemus, Mr. Dillon, Chester, Paladin, Wyatt, Clint, Wild Bill and 'Rooster'. Where have they all gone???

The Wild Wild West



- No Rules
- Cross the border – No pursuit
  The hackers live in the 'Bad Lands' areas that tolerate or encourage their activity
  POSSIBLE RUSSIA, UKRAINE, CHINA, NORTH KOREA
- The data is 'everywhere' – main computers, laptops, tablets, iPads, iPhones, thumb drives (aka USB flash drive), **the new AppleWatch & iPhone to pay your bills & other unencrypted devices**

Smartphones & Tablets

- Smartphones and tablets are quickly replacing computers. **And that's no surprise as they are portable and can do nearly anything your computer can. With this shift toward mobile gadgets, hackers who build viruses for PCs are also setting their sights on this new market. Pick pockets.**
- **That's why** Mobile app infections rose a staggering 600% in 2014.
- **Given that the average smartphone or tablet user downloads more than 100 apps, and that there are millions of apps available online, your odds don't look good. Yet I'm amazed how many people who use their gadgets for banking and other sensitive work still have not taken steps to secure their gear from these very real threats.**

Business is as Vulnerable as its 'Weakest Link'

- **Employees-** ***employees can work from anywhere and they have the data with them HOW MANY OF YOU ARE @ HOME NOW?***
- To find out more about federal laws relating to background reports, visit www.business.ftc.gov, or call the FTC toll-free, 1-877-FTC-HELP (1-877-382-4357)

More Problems

- Vendors – ***Your security may depend on someone else's security (Target)***
- Hackers –NO LONGER THE HIPPIE-VERY SOPHISTICATED

- Kids who download virus onto dad/moms, grandma & granddad's laptop
- Clouds ***– Anything that is connected to the computers***
- USBs ***– Lost & Found***

IoT

THE DATA IS 'EVERYWHERE' ***The Internet of Things (IoT*)***.

It is estimated in 5 years there could be ***80 BILLION*** *connected devices* that can monitor anything from the climate quality in your delivery trucks to whether the plant in your window needs more sun. Everything will be **hackable, trackable and visible.**

How Much Money Do You Have In Your Wallet?

- ***Not a big fan of statistics—could be a result of 25 years with the Insurance Services Office, but*** *these are the latest from NetDiligence:*
  - *The average claim payout was* ***$733,109***
  - *The average cost per-record was* ***$956.21***
  - *The average cost for Crisis Services was* ***$366,484***
  - *The average cost for legal defense was* ***$698,797***

FOLKS HOW MANY INSUREDS CAN PAY THAT---VERY FEW SMALL ONES

PII (personally identifiable information) - 41% of data exposed

PHI (private health information) was second 21%

PCI (payment card information) 19%

Hackers were the most frequent cause of loss 29%

Staff Mistakes were a distant second 13%

Malware/Virus 11%

Rogue Employees 11%. Note that Staff Mistakes and Rogue Employees accounted for 24%.

While Hackers accounted for 29% of claim events, those incidents resulted 74% of records exposed.

Malware/Virus accounted for only 11% of claim events, but 23% of records exposed.

The Top 5---so far!

- **Anthem and the stunning theft of 80 million customer records.** Population of the US is 320M that is **25% of folks in USA**
- **Before Anthem these were the top four.**
  - #4 Home Depot
  - #3 Target Corp.
  - #2 JP Morgan Chase
  - #1 eBay
  - Just Added - On May 26, 2015, the IRS announced that hackers had gained access to tax accounts. July 10 announced this affected 20,000,000 people

Just some of the lessons to be learned from these 'massive' attacks:

- Used to commit identity theft
- Bypass security questions to Lock you out of existing accounts
- And the risk isn't short term, like when a credit card number is stolen. "Just because the attacker stole the data today doesn't mean they'll sell it tomorrow"

More Lessons

They could sit on this information for years

- Victims of insurance company Anthem's breach will have to remain vigilant against fraud for the **rest of their lives**
- **Constant** monitoring of your existing accounts
- The **first thing** you want to watch out for is someone using this info to trick a call center into letting them take over or transfer money out of your existing accounts—more later.

Lessons and more lessons

- Watch for any unauthorized activity or transfers on your current financial accounts, including 401k and brokerage accounts
- File your taxes early. It only takes two pieces of information for a crook to snag your tax refund by filing your taxes early and claiming it for themselves.

Finally "Forever"

No one knows when or where, or if, the stolen identities will be used so affected consumers will simply have to stay mindful...
Forever
Your Social Security number is not going to change

But This Is About The Little Guys---Your Clients

- ***Before we go to the meat of this webinar I have to throw out some 'geekie' terms...***
  - ***"Bots," "zombies," and "botnets"*** *But what exactly are they, how do they work, and what damage can they cause?*

Geek Terms

A **"bot,"** short for "robot," is a type of software application or script that performs tasks on command, allowing an attacker to take complete control remotely of an affected computer. The compromised machine may also be referred to as a **"zombie."** A collection of these infected computers is known as a **"botnet."**

You got all that?????

More Geekie Terms

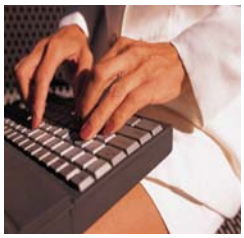
Baiting - Someone gives you a USB drive or other electronic media that is preloaded with malware in the hope you will use the device and enable them to hack your computer.

Do not use any electronic storage device unless you know its origin is legitimate and safe. Scan all electronic media for viruses before use.

Click-jacking - Concealing hyperlinks beneath legitimate clickable content which, when clicked, causes a user to unknowingly perform actions, such as downloading malware, or sending your ID to a site. Numerous click-jacking scams have employed "Like" and "Share" buttons on social network sites.

Need a sign on every computer

Think Before You Click!



You Guessed It, More Geekie Stuff

Cross-Site Scripting (XSS) - Malicious code is injected into a benign or trusted website.

Doxing - Publicly releasing a person's identifying information including full name, date of birth, address, and pictures typically retrieved from social networking site profiles.

Be careful what information you share about yourself, family, and friends (online, in print, and in person). Facebookers beware!!!

Lastly

Elicitation - The strategic use of conversation to extract information from people without giving them the feeling they are being interrogated.

Pharming - Redirecting users from legitimate websites to fraudulent ones for the purpose of extracting confidential data. (E.g.: mimicking bank websites.)

Phishing - Usually an email that looks like it is from a legitimate organization or person, but is not and contains a link or file with malware. Phishing attacks typically try to snag any random victim. Spear phishing attacks target a specific person or organization as their intended victim.

Do not open email or email attachments or click on links sent from people you do not know. If you receive a suspicious email from someone you know, ask them about it before opening it. ***Just got one from E-Z Pass!!!!!!***

Phreaking - Gaining unauthorized access to telecommunication systems.

Scams - Fake deals that trick people into providing money, information, or service in exchange for the deal.

If it sounds too good to be true, it is most likely a scam.

Some new ones, actually old one, revisited

Misappropriating Businesses' Web Addresses

The cyber thief diverts a company's domain name—the very Web address that's critical to the firm's online sales—to such places as China, Eastern Europe and Russia.

The nonprofit Internet Corporation for Assigned Names and Numbers, or ICANN, coordinates how Web addresses are allocated, and it has gotten over 140 complaints about domain-name thefts in the past 20 months.

The thief might hold the domain name for **ransom, resell it or use the information to get access to personal or company data.** Thieves may "also be interested in other means for monetizing the stolen domain name, such as the **display of pay-per-click** advertisements, display of a website that **downloads malware,** or **use of the domain name to send legitimate-looking emails containing spam, viruses and/or phishing correspondence."**

Fake Presidents Fraud

By using a fake identity, this scam consists in convincing the employee of a company to make an emergency bank transfer to a third party. The grifter impersonates a group executive (e.g. the president, CEO, CFO) or a trusted partner (e.g. lawyers, notaries, auditors, accountants etc.) of the company. They contact a specific employee's company by reaching a manager, an accounts payable clerk or any other employee they think useful to achieve their imposture.

The contact may be established by phone calls (imitating the voice) or emails (imitating the email address).

These types of frauds are created by well organized criminal organizations with a complete knowledge regarding the market, structure and customers of the companies they are attacking. This knowledge is used to give them all necessary arguments to convince their victim and act in the wanted direction.

The Dyre Wolf

The attackers target people working in companies by sending spam email with unsafe attachments to get a variant of the malware known as Dyre into as many computers as possible. If installed, the malware waits until it recognizes that the user is navigating to a bank website and instantly creates a fake screen telling the user that the bank's site is having problems and to call a certain number. If users call that number, they get through to an English-speaking operator who already knows what bank the users think they are contacting. The operator then elicits the users' banking details and immediately starts a large wire transfer to take money out of the relevant account. The use of a live phone operator is what makes the scheme unique.

Once the transfer is complete, the money is then quickly moved from bank to bank to evade detection.

Where Is Most Of This Information Being Sold??

"There is the Internet that you and I use. There is the other Internet that we don't. The Surface Web is Google, Facebook, Amazon, eBay and everything else a search site typically shows. Depending on the survey, **Google only catalogs and searches anywhere from 4% to 16% of the Surface Web.**

Below the Surface Web is the **Deep Web**. There, you'll find abandoned websites, paywalled sites (system that prevents Internet users from accessing webpage content without a paid subscription, research firm databases, government databases and other things that aren't meant to be public.

The Dark Web

In the Deep Web, there is a place called the Dark Web.

The Dark Web is where the Internet's illicit activities reside. If you want to buy illegal drugs, guns, counterfeit money, stolen items, fake degrees or passports, cloned debit cards, hacking tools, weapons and more, you can. Dark Web sites also let you hire a hit man or escort, buy someone's identity or swap child pornography. *This is scary stuff.*

Sites for information

www.advisen.com

www.fbi.gov

Lets Talk About Your Clients

1. How about you? Insurance agents—got any records on client information?
2. Law firms?
3. Medical offices? This is now one of the main targets. I just heard they don't need SS #s *except* for Medicare patients

More small clients

4. Day care centers?
5. THOMPSON – SMALL HOTEL in Oregon - wrote down drivers license # and DOB
6. Let your mind wander!!!

Most small to medium sized businesses (SMB) believe they aren't a target for those nefarious cybercriminals. Time to think again. SMBs create 64% of the new jobs in the U.S., account for 54% of all U.S. sales, and about half of all private-sector payrolls. SMBs aren't just targets — they're cybercriminals' top targets.

SMBs are easy targets for cyber criminals for several reasons; one being the lack of security practice. Small business owners are mistaken in believing they don't have what cyber attackers want and thinking that they are immune to attacks targeted at them.

Questions for SMBs

Do you collect credit card information at the point of sale?

Do you run a website that processes credit card transactions?

Are social security numbers, other account numbers, home addresses, email addresses, and phone numbers stored in files on your computers?

Do you use a third party service in the "cloud" for hosting applications or data?

If The Answer is YES

Then they are at risk for a data breach loss!

Lets us digress a minute---**Card Brand Liabilities** may include amounts for alleged failures to maintain certain levels of computer security required by contract (so-called PCI-DSS compliance). The amounts owed for alleged fraudulent charges and replacement of compromised credit cards often dwarfs the amounts of fines. For more read:

http://www.btpolicyholderprotection.com/will-insurance-cover-targets-19-million-mastercard-settlement/

What do the criminals do with this information?

- Use it themselves to send spam, phishing, or other scams to trick consumers into giving up their hard earned money.
- Steal identities, run up loans and purchase charges under the user's name.
- Create denial-of-service (DoS) attacks that flood a legitimate service or network with a crushing volume of traffic.

What do the Criminals do with this information (continued)

- Extortion (pay or have your site taken down) or through payments by groups interested in inflicting damage to a company or network.
- Lease the information to other criminals who want to send spam, scams, phishing, steal identities, and attack legitimate websites, and networks.

Some really scary ones

- Fraudsters use this data to create fake IDs ***to buy medical equipment or drugs that can be resold, or they combine a patient number with a false provider number and file made-up claims with insurers.***
- Fraudulently bill. ***Consumers sometimes discover their credentials have been stolen only after fraudsters use their personal medical ID to impersonate them and obtain health services. When the unpaid bills are sent on to debt collectors, they track down the fraud victims and seek payment.***
- ***Last year in which one patient learned that his records at a major hospital chain were compromised after he started receiving bills related to a heart procedure he had not undergone. The man's credentials were also used to buy a mobility scooter and several pieces of medical equipment, racking up tens of thousands of dollars in total fraud.***

Young & Old(er)

- Children have a 51 percent higher chance of becoming a victim of identity theft than adults.
- CHILD STILL ALIVE
- Older, less suspecting adults *what about your parents that are less suspecting, and open items just to see what it says? They may give out email and passwords to hackers and never realize what they have done until too late.* ***WARN THEM!***
- Never let your kids *(in my case Grandkids)* use your computer!

Risk Management 101 The short list

Educate employees about how their own online behavior could impact the company.

Do not store any information you want to protect on any device that connects to the Internet

Always use high security settings on social networking sites, and be very limited in the personal information you share.

Change your important passwords periodically

Do not post anything that might embarrass you later, or that you don't want strangers to know. **Duh!**

More RM

Verify those you correspond with.

Do not automatically download, or respond to content on a website or in an email.

Do not click on links in email messages claiming to be from a social networking site.

Only install applications or software that come from trusted, well-known sites. "Free" software may come with malware.

Avoid accessing your personal accounts from public computers or through public Wi-Fi spots.

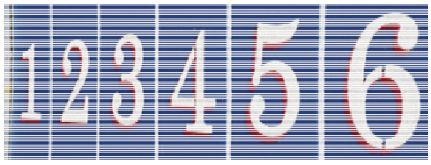
Hotel scam----Ask for credit card information over phone.

A Word About 'Passwords'

- 75% of people use the same password for all accounts, INCLUDING "Facebook" account.
- But for many accounts---*Who Cares!!!!!!!*
- Don't use dictionary words. Computer systems can cycle thru all potential passwords.
- Add a period or lower/upper case letters:
  - Example pk9^2chi = 3 hours to hack
  - pk9^2.hi = 24 hours to hack
  - pK9^2.hi = 20 DAYS to hack
  - ***pK9^2.hi. = 5 YEARS to hack***
  - ***pK9^2.hI> = a really long time to hack***

Is your password weak or strong?

http://www.passwordmeter.com



Password recommendations

Here is a review of tactics to use when choosing a password:

Don't use passwords that are based on personal information that can be easily accessed or guessed.

Don't use words that can be found in any dictionary of any language.

Develop a mnemonic for remembering complex passwords.

Use both lowercase and capital letters.

Use a combination of letters, numbers, and special characters.

Use passphrases when you can.

Use different passwords on different systems---no one really cares what your password is at Krogers, unless it the same for your banking

Cost of a breach

Cost of a data breach, which consistently hovers around **$217** per record
Health records have cost on average of $398 each
Retail records have an average cost of $189 each.
Here's a more complete breakdown of the kinds of costs associated with a data breach:

- **Investigation**
- **Notification. See the state laws later for more on this subject.**
- **Identity-theft repair and credit monitoring**
- **Regulatory fines (more in a minute)**
- **Disruptions in normal business operations**
- **Plus loss of brand name (see more later).**
- **Lost business**
- **Class-action lawsuits**

A DATA BREACH CALCULATOR

Great sales tool for you to sell coverage.

https://databreachcalculator.com

First Party Cyber Risk

- Viruses
- Website hacking and defacement
- Denial of service
- Financial fraud - Outside losses & Inside losses
- Computer extortion
- Extra expenses associated with remediation 56% IS BI/EE COST
- Physical damage to host computer equipment and network equipment
- Breaches of security by employees, former employees or contract professionals
- Breaches of security by outsiders (hackers)
- Destruction of information technology assets by employees, former employees or contract employees
- Destruction of information technology assets by outsiders (hackers)
- ***Much more***

Third Party Cyber Risk

- Breach of confidentiality
- Advertising liability
- Credit injury
- Software development/performance E&O
- Liability (including fines and penalties) for theft/loss of customer information
- Wrongful access by hackers to credit card numbers or credit history information of a website's customers

Pesky Fines –Federal Laws SOME INSURER POLICIES MAY COVER SOME OF THIS

If you want to read up on these go to DOJ report
http://www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf

- Health Insurance and Accountability Act (HIPAA)
- Health Information Technology for Economic and Clinical Health (HITECH)
- Fair Credit Reporting Act (FCRA)
- Gramm-Leach Bliley Act (GLBA)
- Consumer Fraud and Abuse Act (CFAA)
- Electronic Communications Privacy Act (ECPA)
- Store Communications Act (SCA)
- Children's Online Privacy Protection Act (COPPA)
- USA Patriot Act
- Drivers Privacy Protection Act
- Cyberspace Electronic Security Act
- Cyber Security Enhancement Act
- Fair and Accurate Credit Transaction Act (FACTA)
- FTC Red Flag Rules

New Law - Public Law 113-282

National Cybersecurity Protection Act of 2014 –

Amends the Homeland Security Act of 2002 to establish a national cybersecurity and communications integration center in the Department of Homeland Security (DHS) to carry out the responsibilities of the DHS Under Secretary responsible for overseeing critical infrastructure protection, cybersecurity, and related DHS programs.

The Real Problem

Congress has still not addressed the real problem - The current regulatory framework in the United States does not provide for a national uniform data breach notification standard. Instead, businesses are guided by a patchwork of existing laws in 47 states, the District of Colombia, Puerto Rico and the Virgin Islands. In fact, only three states do not have such laws. They are Alabama, New Mexico and South Dakota.

State Laws – Go To Sites TAKE A SCREEN SHOT OF PAGE IF YOU CAN

- http://www.perkinscoie.com/statebreachchart/

  OR
- http://www.clausen.com/dir_docs/ind_pubs/bbdee664-5581-4268-9de5-29af9eeb7eb7_pdfdocument.pdf

  OR
- http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

Most state laws include:

What is a data breach?
Who does this law apply to?
Who must be notified?
When must they be notified?
What must be included in the notification?
How must they be notified?
Do any exceptions or exemptions apply?
What are the legal consequences for violating the law?

A quick word about Insurance Services Office forms

Not all ISO forms and endorsements are used verbatim. The insured may change the language if they so desire.

How do you tell if the form you are reviewing is an "unedited" edition? Well look at the very bottom of a form page and if it says © ISO Properties, Inc., or Insurance Services Office, Inc.© or for some of the older editions it might say Copyright, Insurance Services, Inc.

However, if it says Used With Permission Of Insurance Services Office, Inc. then something has been changed and you need to look very closely to determine what has been altered.

ISO Form numbering

The numbering of ISO forms and endorsements have a very specific meaning. A 10-digit format is used. For example CG 00 01 04 13

The first two places are letters indicating the line of insurance, such as CG for commercial general liability.

The next two places indicate the category of insurance, 00 is a Coverage form

The next two are the item or form number within the category. 01 is the first of the category 00.

The next two are the month of that form's edition date. In this case April

The final two are the year of that form's edition date. 2013

Finally not all companies will adopt the most current form edition, nor does every state approve the revisions on the countrywide Effective Date (which doesn't always match up to the Edition Date). So we must be careful in our forms review. I'll be covering the most current ISO forms unless stated otherwise.

ISO MOST CURRENT EDITION MAY NOT BE APPROVED IN ALL STATES OR USED BY ALL INSURERS

Property policies only cover damages arising from ***direct physical loss.***

CP 00 10 Building & Personal Property Coverage Form – The 1985 (effective 1-1-86) thru the current form (Effective in most states April 1, 2013) says:

"We will pay for direct physical loss of or damage to Covered Property…"

Some courts have ruled that covered property included 'Electronic Data' thus the 2002 & later Coverage Forms ISO added Electronic Data as 'Property Not Covered' and defined it as follows.

NOTE THIS DEFINITION AMENDED IN THE 2012 (APPROVED 2013) FORM TO BROADEN COVERAGE BOLD LANGUAGE

2. Property Not Covered

Covered Property does not include:

n. "Electronic data means information, facts or computer programs stored as or on, created or used on, or transmitted to or from computer software (including systems and applications software), on hard or floppy disks, CD-ROMS, tapes, drives, cells, data processing devices or any other repositories of computer software which are used with electronically controlled equipment. The term computer programs, referred to in the foregoing description of electronic data, means a set of related electronic instruction which direct the operations and functions of a computer or device connected to it, which enable the computer or device to receive, process, store, retrieve or send data. This paragraph, n. does not apply to your 'stock' or prepackaged software **or to electronic data which is integrated in and operates or controls the building's elevator, lighting, heating, ventilation, air conditioning or security system." (10 12 form added the 'bold' language)**

Very limited Electronic Data Coverage (MINT ON THE PILLOW TRICK)

Under the Additional Coverage section of the CP 00 10 ISO added a little Electronic Data Coverage:

(4) The most we will pay under this Additional Coverage, Electronic Data, is **$2,500** *(unless a higher limit is shown in the Declarations)* for all loss or damage sustained in any one policy year, regardless of the number of occurrences of loss or damage or the number of premises, locations or computer systems involved.

NOTE **Added to the 2012 Edition**

Business Income CP 00 30 AT LEAST 50% OF LOSS FROM BI – REALLY BAD PR

a. Coverage for Business Income does not apply when a "suspension" of "operations" is caused by destruction or corruption of electronic data, or any loss or damage to electronic data, **except as provided under the Additional Coverage – Interruption Of Computer Operations.**

d. Interruption Of Computer Operations – Only partially reproduced

(4) The most we will pay under this Additional Coverage – Interruption of Computer Operations is **$2,500** for all loss sustained and expense incurred in any one policy year, regardless of the number of interruptions or the number of premises, locations or computer systems involved. ...

Note – No option to increase

CG 00 01 General Liability

Coverage A covers "Property Damage"

The "property damage" definition is:

- "Physical injury to tangible property, including all resulting loss of use of that property."
- "Loss of use of tangible property that is not physically injured."

"For the purpose of this insurance, ***electronic data*** *is* ***not*** *tangible property*." CLEVER - ADDED AN EXCLUSION IN A DEFINITION-BET ~~MOST~~ NO INSUREDS WOULD CATCH THAT- TRICKIE

Belt and Suspenders

Exclusion p. is in case the exclusion in the Definition doesn't work. **It was added in the 2004 ISO Revision**

p. Electronic Data

Damages arising out of the loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data.

However, this exclusion does not apply to liability for damages because of "bodily injury". (added in 04 13 Edition)

As used in this exclusion, electronic data means information, facts or programs stored as or on, created or used on, or transmitted to or from computer software, including systems and applications software, hard or floppy disks, CD-ROMs, tapes, drives, cells, data processing devices or any other media which are used with electronically controlled equipment.

Translation Please

- Damage to intangible property (data, reputation, etc.) **is not covered**
- Loss of use of intangible property **is not covered**
- Third party liability for negligent damage to or use of intangible property **is not covered**
- First party legal costs to protect intangible property **is not covered**

Belt, Suspenders & Jethro Bodine's Rope BEVERLY HILLBILLYS

Mandatory (Eff. 5/1/2014) endorsement **CG 21 06 05 14 added this to Exclusion p.**

Damages arising out of:

(1) Any access to or disclosure of any person's or organization's confidential or personal information, including patents, trade secrets, processing methods, customer lists, financial information, credit card information, health information or any other type of nonpublic information; or

(2) …

This exclusion applies even if damages are claimed for notification costs, credit monitoring expenses, forensic expenses, public relations expenses or any other loss, cost or expense incurred by you or others arising out of that which is described in Paragraph (1) or (2) above.

New Coverage B Exclusion W/O ENDORSEMENT NO EXCLUSION COV. B

B. The following is added to Paragraph 2. Exclusions of Section I - Coverage B - Personal And Advertising Injury Liability:

2. Exclusions

This insurance does not apply to:

Access Or Disclosure Of Confidential Or Personal Information

"Personal and advertising injury" arising out of any access to or disclosure of any person's or organization's confidential or personal information, including patents, trade secrets, processing methods, customer lists, financial information, credit card information, health information or any other type of nonpublic information.

This exclusion applies even if damages are claimed for notification costs, credit monitoring expenses, forensic expenses, public relations expenses or any other loss, cost or expense incurred by you or others arising out of any access to or disclosure of any person's or organization's confidential or personal information.

CG 21 06 is a mandatory endorsement--- UNLESS!

ISO's Rule says:

> *When Endorsement CG 21 07 or Endorsement CG 21 08 is attached to the policy, do not attach Endorsement CG 21 06 or Endorsement CG 04 37.*

SAY WHAT? 21 07 HAS NO BI COVERAGE; 21 08 MODIFIES ONLY COVERAGE B

Crime Coverage ---None cover "electronic data". THIS IS THE ISO CRIME FORM

Crime Coverage - These Exclusions apply to all Insuring Agreements.

d. Confidential Or Personal Information

Loss resulting from:

(1) The disclosure of your or another person's or organization's confidential or personal information including, but not limited to, patents, trade secrets, processing methods, customer lists, financial information, credit card information, health information or any other type of nonpublic information; or

(2) The use of another person's or organization's confidential or personal information including, but not limited to, patents, trade secrets, processing methods, customer lists, financial information, credit card information, health information or any other type of nonpublic information.

Crime exclusion continued

e. Data Security Breach

Fees, costs, fines, penalties and other expenses incurred by you which are related to the access to or disclosure of another person's or organization's confidential or personal information including, but not limited to, patents, trade secrets, processing methods, customer lists, financial information, credit card information, health information or any other type of nonpublic information.

Limited ISO Coverages

- **CG 00 65 (other's data) + CG 04 30 (your data) = Poor man's cyber insurance**
- **ISO BP 05 95** Electronic Data Liability – Limited Coverage comparable to **CG 04 37**
- **ISO BP 05 96** Electronic Data Liability – Broad Coverage comparable to **CG 00 65**
- **BP 14 01 – Identity Fraud Expense Coverage**

New ISO BOP 3-1-2015

BP 15 07 – Information Security Protection Endorsement

This endorsement can be used to provide three tiers of coverage: (1) Tier 1 first-party electronic data restoration, public relations, and security breach notification, (2) Tier 2 third-party liability coverage, and (3) Tier 3 first-party extortion and business income/extra expense and Tier 3 liability coverage for web site publishing. Tier 2 requires prerequisite Tier 1 coverage and Tier 3 requires both Tier 1 and Tier 2 coverage.

BP 15 08 – Payment Card Industry (PCI) – Provide Coverage For Defense Expenses And Fines Or Penalties Endorsement

This endorsement provides coverage for defense, fines or penalties assessed by card companies that allege noncompliance with PCI data Security Standards involving wrongful acts covered under insuring agreement d.(1) for security breach liability.

BP 15 10 – Provide Coverage For Dishonest, Malicious Or Fraudulent Acts Committed By Employees Endorsement

This endorsement replaces exclusion r. in endorsement BP 15 07 in order to provide coverage for employee acts under all insurance agreements.

Where Is Information Available?

- "2014 Cyber/Privacy Insurance Market Survey"
  - Over 160 pages
- Free 18-page summary: **http://betterley.com/samples/cpims14_nt.pdf**
  - Product comparisons include: Ace, Admiral, Allied World, Arch, Argo Pro, Axis, Beazley, Berkley, Brit, CFC, Chartis, Chubb, CNA, Crum & Forster, Digital Risk, The Hartford, Hiscox, Ironshore, Liberty International, Markel, NAS, Navigators, OneBeacon, Philadelphia, RLI, RSUI, Safeonline, ThinkRisk, Travelers, XL, Zurich

Epilogue

As you have now realized this is a tough subject to speak on especially if the audience (that's you'll) is looking for solutions.

There are such a variety of problems and products to cover them in the marketplace, each with their own strengths and weaknesses, we could spend hours or days or weeks on each.

Then we would find that someone has devised a new way to steal the data or something else has temporarily emerged as a superior alternative for a particular customer's exposures.

Back to goals of this webinar------
Trying to make you, and ultimately your customers aware of the exposures.
Making sure everyone is aware of the problem and its magnitude.
Explaining why traditional P&C products, for the most part, are inadequate
Rather than trying to summarize or compare the dozens of marketplace products, I have tried to make you aware of resources such as the Betterley Report

First Question At E & O Trial

DOES YOUR AGENCY HAVE CYBER COVERAGE?

Thank You!

John Eubank
insspeak1@bellsouth.net
Bill Wilson
Bill.Wilson@iiaba.net