DATA SECURITY PRODUCTS LAUNCH TRAINING Q&A

FOR INTERNAL USE ONLY

When is a business required to notify customers that a breach has occurred? **When the breach meets criteria of a given state breach notification law. Notification laws are generally based on where the affected individuals reside, not where the business entity is located.**

If a laptop is stolen, when should an insured report loss and advise possible affected parties? **It should be reported ASAP (policy requires within 60 days of Discovery). Notification will follow as insured will be working with claim adjuster and breach service provider.**

If our insured is a computer programmer/consultant, does the coverage respond to events caused by our insured doing work on other businesses' property? **No. This may be covered under a Tech E&O policy.**

Can coverage be provided for a 3rd party breach? **Yes, if our insured has a direct relationship with the third party in question, and involves a breach of our insured's Personally Identifying Information. If the breach involves data that is being transmitted electronically, the policy requires data must be encrypted.**

Should third parties who provide our insured with services involving personally identifying information be added as named insureds in the policy? **No, not necessary.**

Are the current Data Compromise, Identity Recovery, and CyberOne forms available for BOP only? **Yes. GL forms will be introduced in 2015.**

How is coverage quoted? **For all new business quoted in CIQ, coverage is available as an optional coverage in quote system. For renewals NOT requesting $250,000, $500,000, and $1M limits, quote system is used. For renewals or non CIQ new business requesting $250,000, $500,000, and $1M limits, the agent can download the questionnaire from the e-library and send to insured for completion.**

What is "malware"? **Malware is any software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems.**

Where was the Ponemon Survey taken? **Sampling of small U.S. based businesses.**

If a contractor for our insured causes a data compromise, who is responsible to notify? **If the Personally Identifying Information is in the care, custody, or control of our insured, or with the contractor who has a direct relationship with the insured, our insured is responsible for notification of affected individuals.**

DATA SECURITY PRODUCTS LAUNCH TRAINING Q&A

FOR INTERNAL USE ONLY

How will policyholders be made aware of Data Security Helpline and e-Risk Hub? **All Businessowner policies will include an important notice to policyholders, one for Identity Recovery, and one for Data Compromise/CyberOne. The notices will provide access instructions for the Help Line and the e-Risk Hub along with information on the available insurance products.**

How should an adequate Data Compromise and CyberOne limit be determined? **Refer to Needs Analysis documentation in the agent website for more detail.**

Are there any classes currently not eligible for Data Compromise, Identity Recovery, and CyberOne? **While there are certain classes of business currently ineligible, none of our current BOP portfolio business falls within these categories. Therefore, all BOP accounts today are, in essence, eligible. Any account with a BOP premium greater than $750,000 where Data Compromise is requested to be added must be referred to HSB for review.**

Questions regarding higher Data Compromise limits. Does HSB review the answers to questions on individual accounts? **No. This is a Nationwide underwriting tool to determine access to limit.**

Can an agent manipulate the questionnaire answers to successfully get higher limits for an account? **This is possible, but in our experience not likely. All losses count against agency loss ratios/contingencies, so there is incentive to properly underwrite the risk up front. HSB conducts periodic portfolio reviews with our client companies to measure loss experience and recommend potential adjustments as needed and mutually agreed upon. We would potentially review on an account suffering a loss.**

Is Named Malware sublimit an aggregate sublimit? **No, per Personal Data Compromise. The $50,000 sublimit is subject to the policy annual aggregate limit, however.**

What is policy limitation for Public Relations coverage? **No more than $25 per affected individual, with a sublimit of $5,000.**

Assume a covered Personal Data Compromise to our insured happens, and we notify the affected individuals. What happens if another outside party attempts to pretend to be the insured entity that was compromised and solicits for the same affected individual's personal identifying information? If an individual provides that type of information to the requesting outside party, would our insured be liable? **No. The Personally Identifying Information must be in our insured's care, custody, or control, or with a professional entity the insured has a direct relationship with.**

Is CyberOne coverage an occurrence coverage? **The Computer Attack (1st party) coverage is discovery but the Network Security Liability (3rd party) coverage is a Claims-Made trigger.**

DATA SECURITY PRODUCTS LAUNCH TRAINING Q&A

FOR INTERNAL USE ONLY

Does Data Compromise and CyberOne coverage respond to hardware loss? **No, hardware damage is not covered as part of Systems Restoration Costs. Coverage may exist elsewhere – possibly Equipment Breakdown and/or EDP.**

Are you aware of any large marketing for Cyber Liability in commercials or print? **No.**

Regarding renewals - If the agent wants to add higher limits - is there a supplemental app? **No supplemental application required, but questionnaire must be completed. Available in e-library.**

Regarding sub-limits - if a breach occurs does it reduce the aggregate? In addition is the sub-limit subject to an aggregate (that is, are we subject to the total sub-limit for the entire term, or is it subject just to each occurrence)? **Yes, sublimits are considered to be part of the annual aggregate. The sublimit itself is per occurrence, however.**

Does HSB assist our members with selection of counsel? **Members can select their own counsel, but HSB can assist. e-Risk Hub also has a directory within the e-Risk Resources section.**

How does HSB establish reserves after there is a third party claim for Data Compromise and/or CyberOne coverages? Is there any consideration given to additional suits that could potentially be brought? **The adjuster would only set a reserve based on the claim being presented at the time of loss. If additional suits are brought at a later date, then the file reserves would be changed.**

Can all Cyber endorsements be quoted individually? **Yes. However, when Data Compromise is quoted, Identity Recovery is automatically included as part of the Data Compromise premium.**

Can any of the Cyber Coverages be added mid-term? **Yes, but only if the policy has a renewal effective date of 11/15/14 or later.**

If an existing customer wants higher limits for Data Compromise that requires a completed questionnaire, where would the underwriter obtain the questionnaire? **The Data Compromise Questionnaire is stored in "Supp Forms-Coml" within elibrary. Agents can complete this and send it to their underwriter for approval of the higher limits.**

Is this program specific to Nationwide? **No. However, HSB has tailored this program specifically to Nationwide (i.e. Website, e-Risk Hub segments, communication materials. Pricing is based on Nationwide portfolio specifically.**

What if a rogue 3rd party employee causes a breach of our member's personally identifying information that was given to the 3rd party, would this product cover this breach? **Yes.**

Are there legal services available for policyholders? **E-Risk Hub references.**

Does Data Compromise and/or CyberOne coverage allow for subrogation? **Yes, this is always a possibility.**

If case management services are provided for either affected individuals (Data Compromise), or identity recovery insureds (Identity Recovery), is credit freezing included? **For Data Compromise coverage, this would involve a breach in which the insured offers case management service to an affected individual. If so, the answer is no as the affected individual is not the insured (the business suffering the breach is) and therefore no indemnification is provided to the affected individual. The affected individual would receive access to the case manager at no cost to them. If the insured is offering credit monitoring service, the coverage pays to provide affected individuals with credit monitoring service for up to one year from the date notification is received.**

As respects to Identity Recovery coverage, credit freezes would potentially be covered under the sublimited "Miscellaneous costs" coverage in the Identity Recovery form. That being said, Kroll is often very reluctant to freeze credit and does so only in the most egregious cases. Freezing credit is something that the person needs to carefully consider as it can have implications in their day to day life, e.g. inability to open new credit without first thawing their file – no store cards to take advantage of sales, no buying a car on the weekend without first thawing the file, etc.

Are any/all of these coverages subject to minimum premium in addition to the policy level minimum? **No.**

Is there a coverage summary available in CIQ when coverage is quoted? **Not at this time. Will bring this to attention of product staff for discussion.**

Is our data breach offering under Inland Marine still being offered? **Yes. Once we implement GL, then there will be the opportunity for the accounts that have the IM endorsement, to roll it off and replace the coverage with the Data Compromise endorsement which includes the IM coverages via the response expense portion.**

Does Data Compromise and/or CyberOne coverage cover costs that an insured incurs when using their own internal Legal/IT resources? **No, coverage only applies for costs from outside professional firms.**

Can HSB provide our insureds with contact information for outside legal and IT entities? **Yes.**

How does the Umbrella policy come in over top of these coverages? **Umbrella excludes coverage for these types of events, and would not apply. UMB7010 on Nationwide's Umbrella program should prevent the Cyber coverage from being covered in the Umbrella.**

CyberOne excludes propagation or forward of malware in connection with hardware or software created, produced or modified my insureds for sale, lease or license to third parties. Would an "app" fall under this exclusion? **Yes, an app is considered software.**

Regarding Third Party coverage under CyberOne. Assume that an unintended propagation of malware event affects our insured's client, and the client brings a Network Security Liability Suit against our insured. If that malware continues downstream from that client to another party, and that party brings action, do we respond? **Yes.**

If a questionnaire is filled out and the increased limits are accepted, does that questionnaire need to be filled out annually? Or is it good for any extended period? **The questions need to be answered again if the insured changes limits, e.g. $100k to $250k and then from $250k to $500k.**

If an insured answers too many questions No, and we reject coverage, do we ever reconsider that decision? **Yes we would reconsider.**

Example 1 - insured answers Yes to "suffered a data breach in past 12 months", so we only offer the 50k limit. Now if 2 years go by and they answer that question No (because there hasn't been a data breach in the past 12 months). Are we willing to offer higher limits then? **We would look for 12 months of no breach activity.**

Example 2 - insured answers 3 of 4 questions No for the 250k limit. After 2 years they apply again and answer all of them Yes. Are we willing to offer higher limits then? **So long as the breach question was ok, they could reapply for the higher limits once they take steps to remedy the deficiencies, e.g. they conduct background checks, store information appropriately, etc.**

When a claim is made for coverage and an attorney or computer specialist is needed, does HSB provide or may the insured select an outside resource? **This can be done either way. HSB does have vendors that they contract with, so they will be able to provide service at a contracted rate. The insured will have the ability to use their own resources, but they must be of like kind and quality in their service.**

In the 3 states that do not have state requirements for customer notification of a breach, will insureds in these states want to and be able to purchase coverage? **The insureds are still able to purchase the coverage. While the state may not require a legal notification of a data breach, the potential still exists for an insured to be sued and the need for coverage still exists.**

What will happen to the existing Lifestages & Data Breach coverage through IDT911? **Customers will begin going through HSB instead of IDT911. An important notice is being sent out to customers with renewals to advise them. The IMA911 (data breach expense form) will remain active until the endorsements on the GL are up and running. At that time, the option to convert this endorsement to the BOP or GL will exist.**

How often will the insured be asked the additional underwriting questions that are asked on the higher coverage limits for data compromise coverage? **The insured will be asked when they initially purchase the coverage. They will not be asked these questions again unless they request higher coverage limits in the future.**

Where are the additional underwriting questions located? **For CIQ quoted business, these additional questions will display in CIQ when the higher limits are requested. The system will screen for eligibility. For Acord application business quoted on the mainframe or existing policies with the coverage added, a questionnaire is available in eLibrary > Supp Forms – Coml – IC < Data Compromise Questionnaire. This questionnaire should be added to eFile after it is complete. Underwriters will need to screen for eligibility. For $250,000 limits, question 1 must be answered "no" and at least 2 out of 4 remaining questions must be answered "yes" to be eligible. For $500,000 or $1 million limits, question 1 must be answered "no" and at least 8 out of 9 of the remaining questions must be answered "yes" to be eligible. If eligibility requirements are not met, the highest available limit will be $100,000.**

Where are we in the marketplace with this coverage? **Most agents are not well informed of the coverages. An advantage Nationwide will have is the use of the eRisk Hub as well as a dedicated website that is under development. There will be resources available through these links to calculators and other tools in determining an appropriate limit for the insured. Other carriers do have this available that has to be individually underwritten. Most carriers do not offer as high of limits as we will be extending.**

Are the coverage limits for the cyber coverages on a per location basis? **Coverage is an annual aggregate limit with no per location provisions.**

Can the insured purchase limited first party coverage and full third party coverage under CyberOne? **Only FULL first party can be coupled with third party coverage per filing.**

Are there services available to the insured to assist in claim prevention? **The tools that are available in the eRisk Hub will provide tools to assist in understanding what exposures the insured has, what could happen and how to prepare for the exposures. There will be prerecorded Brainsharks available for viewing on various topics.**

What marketing materials will be available to provide our agents to advertise and educate our insureds? **Links to these will be available in the associate/agent website, in elibrary and on the marketing storefront.**

How do companies discover that they have suffered a data breach? **Many times it is an external organization such as law enforcement or financial institution that notifies the insured of a data breach. Breaches can otherwise go undetected until there is a reason the breach would be otherwise discovered. It may not be until a customer discovers a loss and the transfer of the data are linked back to the insured.**

If a claim is not reported within 60 days, will there be any coverage available? **The claim must be reported within 60 days per policy conditions.**

If an insured knows a breach has occurred, purchases coverage and then reports a loss, will there be a way to know if they were aware of the breach before purchasing the coverage? **Coverage basis is on a discovery trigger. While the ability to research and discover when the breach occurred exists, it may be difficult to prove at what point the insured discovered the breach. The coverage does require that the event occur after the first inception of this or similar coverage. An insured acting in the manner as described above would be committing fraud.**

In the CyberOne coverage under Third Party Network Security Liability, will the "judgment" coverage include fines and penalties assessed to the insured? **No, this coverage is for the judgment itself, but does not include fines or penalties assessed to the insured.**

Is HSB offering these coverages to many other insurance carriers? **Currently, HSB reinsures many carriers for Data Compromise and Identity Recovery. CyberOne coverage is relatively new in the marketplace and HSB reinsures only a small number of carrier programs at this time. However, several carriers are implementing CyberOne programs in the very near future. There is a window of opportunity until other programs are introduced which will give Nationwide a speed to market advantage.**

When an agent advises that their insured already has "fraud" coverage elsewhere, how does this compare to the exposures and coverages provided under the HSB products? **Fraud can be defined for example, where information that was taken in a data breach is then used to re-create an identity so there could possibly be similar coverages. However, because there is not uniformity to the way cyber coverages are provided, the agent would need to review both coverage forms to determine where any coverage overlaps or gaps may exist. They agent will need to review the policy providing fraud coverage to ascertain what type of fraud is covered. For example, fraud could be the use of a computer to impart someone to pay for goods or services never received. This type of fraud may be covered elsewhere but is not covered under Data Compromise or CyberOne. However, someone could "trick" a company into turning over personal information, in which case the Data Compromise coverage would respond to provide notifications and services to those affected.**

How will our agents be trained on these coverages? **There will be training webinars available to our agents in October 2014. Additionally, the eRisk Hub and future website will provide training options to agents.**

How do people find out that they've been hacked? **Often an external organization such as law enforcement or financial institution will notify organizations when a suspected hacking has occurred. Additionally, an insured may learn of a hacking in the event a written demand has been made against them via a third party. Other times, they may simply notice that their computers are not functioning normally.** Does this respond to fines or penalties or legal proceedings? **No**

What is the timing on how long it would take to resolve an IDR vs. DC vs. Cyber claim? **Dependent upon the product or possible combination of product losses. Most IDR claims are closed within 6 months but some more involved claims may take 12 months or longer. Data Compromise claims can take longer than 12 months before the full extent of the loss is known dependent on the services provided to the affected individuals.**

How is malware defined in the policy? What specific virus services are named? **Named Malware definition: Means a "personal data compromise" that is caused, enabled or abetted by a virus or other malicious code that, at the time of the "personal data compromise", Named Virus Services: CERT® Coordination Center, McAfee®, Secunia, Symantec or other comparable third party monitors of malicious code activity.**

Criminal Acts – who would be covered? **Not going to cover any owners involved in criminal acts.**

Can IDR coverage be excluded from Data Compromise? **No.**

Does Data Compromise and/or CyberOne coverage overlap with our Employee Dishonesty coverage? **There shouldn't be any overlap in that the coverages apply to different things. Employee Dishonesty applies to Business Personal Property and Money & Securities. Data Compromise and CyberOne provide coverages that are separate from these items. For example, in the event of a data compromise, we'd provide response expenses that are separate costs from replacing BPP or money & securities.**

Are all data breach services and coverages going to be through HSB now and what we previously had through IDT911 for the BOP going away? **Yes.**

What was the website that agents can access for training and marketing materials? **Nationwide will provide an internal Data Security Products website on your private portal. Details on how to access will be coming in October.**

Is the coverage rated by the system and are there specific eligibility criteria? **CIQ will automatically provide rate. With respects to Nationwide's Businessowners portfolio, no current policies are ineligible.**

What is the minimum premium? How is that calculated? **No minimum premium for the three coverages. Premium is per policy.**

Is it anticipated that these coverages will ultimately be available for Package policies (and not just Businessowners policies)? **Yes.**

Is coverage optionally offered? **Coverage is optional.**

Are there underwriting requirements, or is it similar to EB – i.e. easy, no real underwriting to be done. **No separate application required. For Data Compromise coverage, higher limits require completion of insured questionnaire.**

Will the marketing materials include claim examples like what you provided in this training? Our agents are always asking about claim examples, so that would be great! **Developing loss example content to be made available on the associate/agent website.**

When will rates and endorsements be available in elibrary? **Rules and rates are available now. Forms will show up on the effective date (11/15/14).**

DATA SECURITY PRODUCTS LAUNCH TRAINING Q&A

FOR INTERNAL USE ONLY

If an agent has an HSB contract, can they get a standalone policy to go with our package policy? **HSB offers Data Compromise coverage through independent agents, but only as an endorsement to HSB's monoline Equipment Breakdown policy. Nationwide offers all products and makes it easy to endorse Equipment Breakdown and all three Cyber coverages to BOP.**

How long before we have these coverages available on a non-BOP product? **2015.**

Is it mandatory that these coverages are automatically added when choosing the BOP Product? **No, coverage is optionally selected.**

Will this (and all associated coverages) be available in all states? **Yes.**

Is Third Party Data Compromise coverage not available in New York? **Correct, the NY Department of Insurance has not approved any HSB-sponsored filings for Third Party coverages at this time.**

Can members continue to work with and pay for services (case manager etc) after their limits are exhausted? **Yes.**

Did you say that Cyber One can be purchased stand alone? **Any of the three endorsements can be purchased individually, but these are endorsements that must be attached to an underlying BOP policy. So coverage cannot be written as monoline/standalone. Note that Identity Recovery is automatically included for no cost with the purchase of Data Compromise.**

You mentioned we must offer the 1 year ERP, if the insured declines this should we have a sign off in file? **The ERP for CyberOne wouldn't work any differently for ERPs we have with other coverages (i.e. EPLI, D&O, etc), when it comes to the process.**

What happens if the insured falsely answers these questions? **Any claim would still be honored as long as it meets the policy criteria I would defer to claims on this one. If you become aware of situations involving purposeful deception, you may wish to consult with management as to how to address with an agent and/or member.**

Some of our BOP policies have incidental gaming machines (for example WV).... we consider this exposure incidental to the BOP class. Would this present any coverage or eligibility problems in the event of a loss? **No, all BOPs are eligible for coverage.**

Are mortgage brokers considered financial institutions? **No**.

DATA SECURITY PRODUCTS LAUNCH TRAINING Q&A

FOR INTERNAL USE ONLY

Is information available on how" Kroll" employees are vetted? **The identity theft restoration profession currently has no standard by which to qualify "Restoration Experts." Kroll has chosen the designation of "Licensed Investigator" around which to standardize their restoration experts. This designation is recognized by the law enforcement community.**

Regarding Data Compromise coverage, and independent of a time limitation for triggering a claim, is there a time limitation in terms of how long affected individuals can continue to report losses? **The coverage responses to notices of suits from affected individuals within two years from the date the affected individuals were notified.**

Regarding CyberOne. Although it can sometimes be difficult to determine where malware originates, what evidence must the claimant (3rd party) present to our insured in order to activate a claim? **There is no specific evidence requirement, but do require that a "Network Security Liability Suit" be received by the member to trigger defense and liability coverages. The suit will make allegations which we must then defend and potentially pay settlement/judgment costs. [In order to trigger the Third Party (Network Security Liability) CyberOne coverage, the important thing is the allegation made by the third party. No evidence needs to be presented. The claim made by the third party against the insured, whether it be an actual lawsuit or just an angry letter, has to allege that the claimant was harmed by one of the three kinds of covered events: the breach of third party business information, the transmission of malware or a denial of service attack.**

Are any agency facing materials and highlight sheets going to be available? **Yes. Many communications going out to agents presently. Promotional materials and other agent-oriented content will be available/housed on the Data Security Products Website.**

Does the Cyber Liability offer any coverage for identity theft or credit card fraud by employee? **Identity Recovery Coverage is included with Data Compromise coverage but can also be purchased separately. The coverage provides case management service to help the insured restore their identity to pre-theft status and pays for certain out-of-pocket costs. There is no coverage for the fraudulent charges incurred.**

Data compromise coverage does respond to a rogue employee who acting at their own direction, steals the identity or credit card information of employees or customers of the insured entity.

How about any leaked or lost patient secured information? **Data Compromise coverage does respond to breached patient information. The definition of "Personally Identifying Information" includes health information (definition 8).**