APPLICATION FOR INFORMATION SECURITY AND PRIVACY LIABILITY COVERAGE

THE POLICY FOR WHICH THIS APPLICATION IS MADE IS A CLAIMS MADE AND REPORTED POLICY SUBJECT TO ITS TERMS. THIS POLICY APPLIES ONLY TO ANY CLAIMS FIRST MADE AGAINST THE INSUREDS AND REPORTED IN WRITING TO THE UNDERWRITERS DURING THE POLICY PERIOD OR OPTIONAL EXTENSION PERIOD, IF APPLICABLE. AMOUNTS INCURRED AS CLAIMS EXPENSES SHALL REDUCE AND MAY EXHAUST THE LIMIT OF LIABILITY AND ARE SUBJECT TO THE DEDUCTIBLE. THE UNDERWRITERS ARE NOT OBLIGATED TO PAY SETTLEMENTS, JUDGMENTS OR CLAIMS EXPENSES ONCE THE LIMIT OF LIABILITY IS EXHAUSTED. PLEASE READ THE POLICY CAREFULLY.

Please fully answer all questions and submit all requested information and supplemental forms. Terms appearing in bold face in this **Application** are defined in the Policy and have the same meaning in this **Application** as in the Policy. If you do not have a copy of the Policy, please request it from your agent or broker. This **Application**, including all materials submitted herewith, shall be held in confidence.

I. APPLICANT DETAILS

Applicant Name:				
Address:				
State:	Zip:	Phone:	Website:	Year Established:

Does the applicant engage in any operations other than insurance agent/broker ☐ Yes ☐ No
If yes, please describe:

Current Year Gross Annual Revenue ($)net of premium paid to carriers ($): _____

What percentage of total revenues is derived from the sale or administration of Group Benefit Plans? _____

Breach Response Contact: (Provide the contact details for the person in your office that will be designated to manage a breach response including consumer notification.)

Name: _____

E-mail: _____

Phone: _____

II. MANAGEMENT OF PRIVACY EXPOSURE

1. Does the Applicant accept credit cards for goods sold or services rendered? ☐ Yes ☐ No
   If Yes:
   A. Is the Applicant compliant with applicable data security standards issued by financial institutions the Applicant transacts business with (e.g. PCI standards) ☐ Yes ☐ No
   B. If the Applicant is not compliant with applicable data security standards, please describe the current status of any compliance work and the estimated date of completion:
2. Does the Applicant use a third party to process credit card transactions? ☐ Yes ☐ No
   If yes:
   A. Does the Applicant require third parties to be compliant with applicable data security standards issued by financial institutions? ☐ Yes ☐ No
   B. Do you have a Merchant Services Agreement? ☐ Yes ☐ No
3. Please check the computer security controls that are currently in place:
   Anti-virus software ☐ Written information security policy ☐
   Firewall ☐ Formal software updating process ☐
4. Does the applicant encrypt data stored on laptops, back-up tapes, or other portable media? ☐ Yes ☐ No

III. REGULATORY ISSUES

1. Has the Applicant ever been investigated in respect of the safeguards for personally identifiable information? ☐ Yes ☐ No
   If yes, please explain:
2. Has the Applicant ever received complaints about how someone's personally identifiable information is handled? ☐ Yes ☐ No

IV. PRIOR CLAIMS AND CIRCUMSTANCES

1. Has the Applicant ever received, or is there currently pending, any claims or complaints with respect to allegations of or injury to privacy, identify theft, theft of information, breach of information security, software copyright infringement or content infringement or been required to provide notification to individuals due to an actual or suspected disclosure of personal information? ☐ Yes ☐ No

   If Yes, provide details of such claim, allegation or incident, including costs, losses or damages incurred or paid, and any amounts paid as a loss under any insurance policy:

2. Is any Applicant, director, officer or other proposed Insured have knowledge or information of any fact, circumstance, situation, event or transaction which may give rise to a Claim under the proposed insurance? ☐ Yes ☐ No
   If Yes, provide details:

3. Is the Applicant aware of any release, loss or disclosure of personally identifiable information in its care, custody or control or anyone holding such information on behalf of the Applicant in the most recent three year time period from the date of this Application? ☐ Yes ☐ No
   If yes, please describe:

V. PRIOR INSURANCE

1. Does the Applicant currently have insurance in place covering media, privacy or network security exposures? ☐ Yes ☐ No

The undersigned declares that the statements set forth herein are true. For New Hampshire Applicants, the foregoing statement is limited to the best of the undersigned's knowledge, after reasonable inquiry. The signing of this Application does not bind the undersigned or the Insurer to complete the insurance. It is represented that the statements contained in this Application and the materials submitted herewith are the basis of the contract should a policy be issued and have been relied upon by the Insurer in issuing any policy. The Insurer is authorized to make any investigation and inquiry in connection with this Application as it deems necessary. Nothing contained herein or incorporated herein by reference shall constitute notice of a claim or potential claim so as to trigger coverage under any contract of insurance.

This Application and materials submitted with it shall be retained on file with the Insurer and shall be deemed attached to and become part of the policy if issued. For Utah and Wisconsin Applicants, such Application and materials are part of the policy, if issued, only if attached at issuance. It is agreed in the event there is any material change in the answers to the questions contained in this Application prior to the effective date of the policy, the Applicant will immediately notify the Insurer in writing and any outstanding quotations may be modified or withdrawn at the Insurer's discretion.

FRAUD WARNINGS

ANY PERSON WHO, WITH INTENT TO DEFRAUD OR KNOWING THAT S(HE) IS FACILITATING A FRAUD AGAINST THE UNDERWRITER, SUBMITS AN APPLICATION OR FILES A CLAIM CONTAINING A FALSE OR DECEPTIVE STATEMENT MAY BE GUILTY OF INSURANCE FRAUD.

NOTICE TO COLORADO APPLICANTS: IT IS UNLAWFUL TO KNOWINGLY PROVIDE FALSE, INCOMPLETE, OR MISLEADING FACTS OR INFORMATION TO AN INSURANCE COMPANY FOR THE PURPOSE OF DEFRAUDING OR ATTEMPTING TO DEFRAUD THE COMPANY. PENALTIES MAY INCLUDE IMPRISONMENT, FINES, DENIAL OF INSURANCE, AND CIVIL DAMAGES. ANY INSURANCE COMPANY OR AGENT OF AN INSURANCE COMPANY WHO

KNOWINGLY PROVIDES FALSE, INCOMPLETE, OR MISLEADING FACTS OR INFORMATION TO A POLICYHOLDER OR CLAIMANT FOR THE PURPOSE OF DEFRAUDING OR ATTEMPTING TO DEFRAUD THE POLICYHOLDER OR CLAIMANT WITH REGARD TO A SETTLEMENT OR AWARD PAYABLE FROM INSURANCE PROCEEDS SHALL BE REPORTED TO THE COLORADO DIVISION OF INSURANCE WITHIN THE DEPARTMENT OF REGULATORY AGENCIES.

NOTICE TO DISTRICT OF COLUMBIA APPLICANTS: WARNING: IT IS A CRIME TO PROVIDE FALSE OR MISLEADING INFORMATION TO AN INSURER FOR THE PURPOSE OF DEFRAUDING THE INSURER OR ANY OTHER PERSON. PENALTIES INCLUDE IMPRISONMENT AND/OR FINES. IN ADDITION, AN INSURER MAY DENY INSURANCE BENEFITS IF FALSE INFORMATION MATERIALLY RELATED TO A CLAIM WAS PROVIDED BY THE APPLICANT.

NOTICE TO FLORIDA APPLICANTS: ANY PERSON WHO KNOWINGLY AND WITH INTENT TO INJURE, DEFRAUD, OR DECEIVE ANY INSURER FILES A STATEMENT OF CLAIM OR AN APPLICATION, INCLUDING ANY ATTACHED SUPPLEMENTAL QUESTIONNAIRE, CONTAINING ANY FALSE, INCOMPLETE OR MISLEADING INFORMATION IS GUILTY OF A FELONY IN THE THIRD DEGREE.

NOTICE TO LOUISIANA AND MARYLAND APPLICANTS: ANY PERSON WHO KNOWINGLY AND WILLFULLY PRESENTS A FALSE OR FRAUDULENT CLAIM FOR PAYMENT OF A LOSS OR BENEFIT OR WHO KNOWINGLY AND WILLFULLY PRESENTS FALSE INFORMATION IN AN APPLICATION FOR INSURANCE IS GUILTY OF A CRIME AND MAY BE SUBJECT TO FINES AND CONFINEMENT IN PRISON.

NOTICE TO MAINE, TENNESSEE, VIRGINIA AND WASHINGTON APPLICANTS: IT IS A CRIME TO KNOWINGLY PROVIDE FALSE, INCOMPLETE OR MISLEADING INFORMATION TO AN INSURANCE COMPANY FOR THE PURPOSE OF DEFRAUDING THE COMPANY. PENALTIES MAY INCLUDE IMPRISONMENT, FINES OR A DENIAL OF INSURANCE BENEFITS.

NOTICE TO OKLAHOMA APPLICANTS: ANY PERSON WHO KNOWINGLY, AND WITH INTENT TO INJURE, DEFRAUD OR DECEIVE ANY INSURER, MAKES ANY CLAIM FOR THE PROCEEDS OF AN INSURANCE POLICY CONTAINING ANY FALSE, INCOMPLETE OR MISLEADING INFORMATION IS GUILTY OF A FELONY.

NOTICE TO PENNSYLVANIA APPLICANTS: ANY PERSON WHO KNOWINGLY AND WITH INTENT TO DEFRAUD ANY INSURANCE COMPANY OR OTHER PERSON FILES AN APPLICATION FOR INSURANCE OR STATEMENT OF CLAIM CONTAINING ANY MATERIALLY FALSE INFORMATION OR CONCEALS FOR THE PURPOSE OF MISLEADING, INFORMATION CONCERNING ANY FACT MATERIAL THERETO COMMITS A FRAUDULENT INSURANCE ACT, WHICH IS A CRIME AND SUBJECTS SUCH PERSON TO CRIMINAL AND CIVIL PENALTIES.

NOTICE TO NEW YORK AND KENTUCKY APPLICANTS: ANY PERSON WHO KNOWINGLY AND WITH INTENT TO DEFRAUD ANY INSURANCE COMPANY OR OTHER PERSON FILES AN APPLICATION FOR INSURANCE OR STATEMENT OF CLAIMS CONTAINING ANY MATERIALLY FALSE INFORMATION, OR CONCEALS FOR THE PURPOSE OF MISLEADING, INFORMATION CONCERNING ANY FACT MATERIAL THERETO, COMMITS A FRAUDULENT INSURANCE ACT, WHICH IS A CRIME, AND SHALL ALSO BE SUBJECT TO A CIVIL PENALTY NOT TO EXCEED FIVE THOUSAND DOLLARS AND THE STATED VALUE OF THE CLAIM FOR EACH SUCH VIOLATION.

Signed:

_____

Must be signed by corporate officer with authority to sign on Applicant's behalf

Printed Name: _____

Title: _____

Date: _____

For more information, please contact:

IIANC Member Services
Sharon A Koches CPCU, RPLU, AAI, AU, ITP
Asst VP Insurance Operations
Phone: 888.275.8912
skoches@iianc.com

ADDENDUM TO BEAZLEY CYBER LIABILITY APPLICATION

1. We will need the following to bind a Cyber Liability Policy:

   Completed, signed and dated application.
   Check attached to application for the first year premium.
   (Mail check and application to: IIANC Member Services, Inc.
   P.O. Box 1165 Cary, NC 27512)
   Information completed below and returned with application.

2. What Limit option are you requesting? _____

3. What effective date would you like? _____

4. Provide current year revenues (commission income) for your total book of business. $_____

5. What percentage of total revenues is derived from benefits? (Life, Accident & Health Insurance Product Sale): %_____

6. If you have current Cyber Liability coverage with a retro date, provide a copy of current declaration page showing this date.

7. If you have full prior acts coverage on the Cyber policy advise the date the agency was established: _____

8. Provide full contact name, full contact email address and contact phone number of the person in your office that will be designated to manage a breach response, including consumer notification:

   Name: _____

   Email: _____

   Phone #: _____

Beazley Data Breach Program
Explanation of Insuring Agreements

Limit of Liability

The Limit of Liability is the aggregate amount that will be paid by the carrier for defense and damages. This aggregate will include the following sublimits that are part of this limit; Information Security & Privacy Liability, Regulatory Defense and Penalties, Website Media Content Liability, Public Relations, PCI Fines and Costs.

Notification Limit

This limit is the amount of records that the carrier will provide for notification, call center services and credit monitoring. This limit is separate from and in addition to the policy limit of liability aggregate. The Legal & Forensics and the Foreign Notification costs are sublimits that are part of the Notification Limit. The notification limit does not have a deductible, however it does have a threshold. This threshold only pertains to the call center and credit monitoring services. If the breach affects over 100 records, these services are activated. If it does not, all notification will be provided except the call center and credit monitoring services.

Information Security & Privacy Liability

This is inuring agreement A. This will pay on behalf of the insured damages and claims expenses for;

1. Failure to protect private information
2. Transmission of a virus from your system to another
3. Failure to notify individuals of a breach
4. Failure to comply with a Privacy Policy

Regulatory Defense & Penalties

This will pay on behalf of the insured claims expenses and penalties assessed by regulatory agencies.

PCI Fines & Penalties

This will indemnify the insured for Payment Card Industry fines and costs.

Website Media Content

This will pay on behalf of the insured damages and claims expenses for allegations of copyright infringement and defamation arising from their website.

Cyber Extortion

This will indemnify the insured for loss paid as a result of an extortion threat to protect private information.

Legal & Forensics

This will provide the insured with a computer security expert to determine the extent and cause of a breach. It will then provide for an attorney to determine which notification laws the insured will need to comply.

Public Relations

This will pay for a Public Relations Consultant to help the insured introduce the breach to the public.

Fraud Resolution

This will provide services to the affected individuals in restoring their identity.

If you have any questions, please contact:

Sharon Koches
IIANC Member Services
PO Box 1165
Cary, NC 27512
(888) 275-8912

beazley

PE Data Breach

Could your insurance agency weather a data security breach?

A full 80 percent of businesses that experience one don't.[1] The right insurance can keep your agency from becoming part of this startling statistic. If that is not enough reason to consider purchasing data breach protection for your business, here are six more:

1 **Data breaches are common among smaller businesses like yours.** Some 55 percent of small businesses responding to a recent survey have experienced a data breach and 53 percent have reported multiple incidents.[2] If you collect sensitive information from policyholders, you are at high risk.

Data held by small businesses is low hanging fruit... hackers know these enterprises lack the security resources of their larger counterparts. Only 38 percent of breaches in the latest Verizon study impacted larger organizations.[3]

2 **Responding to a breach is not only costly – running an estimated $200,000 – it's complex.** Experts from multiple disciplines – from forensic investigators, to public relations firms, to privacy counsel -- may be needed to mount a coordinated response to even a small incident. Botch the response and your reputation can be irreparably damaged. There is also the specter of regulatory fines and penalties and legal liability.

A single laptop left on a commuter train or stolen at an airport can cost an agent nearly $50,000 – most of that being expenses to respond to data breached – or potentially breached.[4]

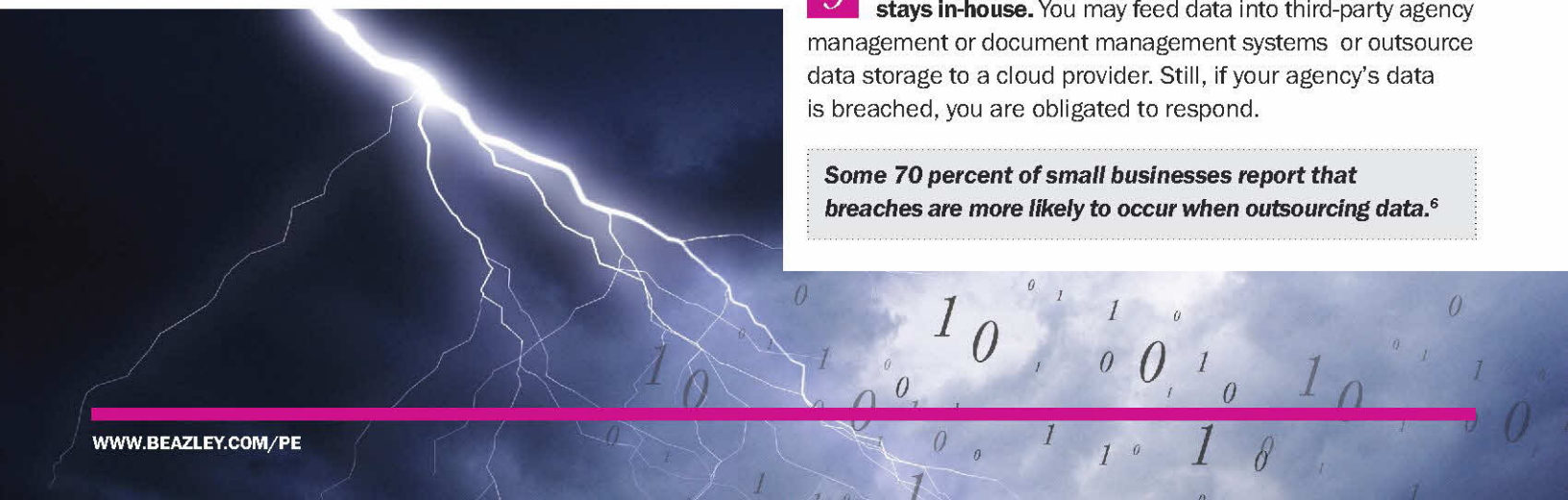
3 **Package policies are not up for the task.** Your commercial package policy may have a cyber liability extension, but take a hard look at the coverage it provides. Endorsements typically carry low limits and few options. If first-party coverage is provided, limits may be inadequate for the exposure. For third-party liability, coverage may fall short in key areas, such as responding to acts of rogue employees. Does it address regulatory fines and penalties? Does the insurer have the duty to defend?

4 **You are obligated to protect data you collect.** This might include everything from personal information, such as addresses, Social Security and driver's license numbers of employees, policyholders or prospects, as well as corporate information -- including sensitive financial information on commercial clients. If you handle employee benefits, you may have personal health information in your care.

State and federal regulations dictate proper handling of private information. If this information is breached, agents must navigate the different laws in 46 states that mandate how victims must be notified. [5]

5 **Even if you outsource data handling, your exposure stays in-house.** You may feed data into third-party agency management or document management systems or outsource data storage to a cloud provider. Still, if your agency's data is breached, you are obligated to respond.

Some 70 percent of small businesses report that breaches are more likely to occur when outsourcing data.[6]

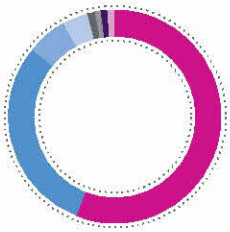


beazley

PE Data Breach

6 **The exposure is not just from hackers intruding on electronic systems.** Breaches are caused by everything from lost, discarded, or stolen laptops, PDAs, smartphones, and portable memory devices, to innocent procedural errors and acts of disgruntled employees.

Records breached



Total
563.9 million
Since 2005

Source: Privacy Rights Clearinghouse, 10/18/2012

Hacking or malware – Electronic entry by an outside party	56%
Portable device – Lost, discarded or stolen laptop, PDA, smartphone, portable memory device, CD, hard drive, data tape, etc	30%
Insider – Someone with legitimate access intentionally breaches information – such as an employee or contractor	6%
Unintended disclosure – Sensitive information posted publicly on a website, mishandled or sent to the wrong party via email, fax or mail	4%
Stationary device – Lost, discarded or stolen stationary electronic device such as a computer or server not designed for mobility	1%
Payment card fraud – Fraud involving debit and credit cards that is not accomplished via hacking. For example, skimming devices	1%
Physical loss – Lost, discarded or stolen non-electronic records, such as paper documents	1%
Unknown or other	1%

What amps up an insurance agency's exposure?

Answering yes to any of the following questions:

Do you have employees?

Do you keep employee records?

Do your client records include third party corporate information (such as company financials)?

Do you handle personal lines?

Do you offer premium financing?

Do you have computers, back-up tapes, a copier, a fax machine?

What can happen

A computer network used by insurance agents was breached by cybercriminals. While the attack was discovered and contained quickly, the personal information -- including Social Security and driver's license numbers of one million policyholder and non-policyholders was comprised.[7]

How it adds up

Every data breach is different. Generally speaking, however, in considering the cost of a response you can expect to pay from $10,000 to $100,000 just for a forensics expert to get to the root of a breach and contain it. Creating and mailing notification letters to victims is in itself costly. Once you do that, you typically must also set up a call center to respond to inquiries from victims, and offer credit monitoring to victims to help mitigate damages. Smaller businesses are less likely than larger ones to have the internal resources and expertise to handle a breach response, so they are more likely to have to pay outside experts – including specialized privacy counsel, consultants, crisis management and public relations professionals – to assist. Then there is the cost of any regulatory actions, penalties, or lawsuits that could arise from the incident.

Being protected = Being prepared to respond

It could be a lost flash drive, or a persistent attack by hackers a world away. Every breach is different -- and every one requires a smart, strategic response.

With Beazley Breach Response, your agency can secure comprehensive coverage for the expenses incurred to respond to a breach – and have experts standing ready to deliver the well-coordinated response you need to mitigate financial damages and protect your reputation. It encompasses everything from forensic investigation, legal, compliance and public relations services, to breach notifications, call center servicing, and on-going credit and data monitoring.

To learn more, contact your Beazley territory manager or underwriter or go to www.beazley.com/pe.

1. Privacy Rights Clearinghouse: Chronology of Data Breaches
2. Ponemon Institute. (Also citation 6)
3. Verizon2013 Data Breach Investigation Report, p. 5
4. California Attorney General/Privacyrights.org (Also citation 7)
5. http://www.ncsl.org/issues-research/telecom/security-breach-notification-laws.aspx

POLICYHOLDER SERVICES

NEW SERVICES INCLUDE

- Training and Awareness Programs
- Animated Staff Training Programs
- Expanded HIPAA Compliance Tools

DATA SECURITY RISK MANAGEMENT

NoDataBreach.com provides risk management policies, procedures, training, and other tools to help insureds prevent a breach of confidential data.

As a Beazley Breach Response® policyholder, you have unlimited access to:

ON-LINE COMPLIANCE MATERIALS

Federal and state compliance materials regarding data security, data breaches, and data privacy, including:

- Quick Tips on many subjects; Summaries of federal/state laws
- Links to statutes & regulations; Sample policies & procedures
- Continuing updates and electronic notification of significant changes to the on-line materials

QUARTERLY NEWSLETTER & "INSTANT ALERTS"

Sent by email, learn about changes in federal and state laws regarding data security, data breach, and data privacy issues; Instant Alerts sent by email for events require immediate attention.

EXPERT SUPPORT ON-LINE

Experts support from consultants/attorneys on data security issues; including:

- Health care & HIPAA compliance issues
- Data breach prevention issues
- Data Security best practices
- Computer forensic issues

STEP-BY-STEP PROCEDURES TO LOWER RISK

Procedures and on-line forms help you:

- Understand the scope of "personal information" ("PI")
- Determine where PI is stored
- Collect and/or retain the minimum amount of PI as required for business needs
- Properly destroy PI that is no longer needed
- Implement an Incident Response Plan

TRAINING MODULES

- Comic Strip training
- Online training programs; Employee training bulletins
- Webinars for privacy compliance and IT staff
- Audio and PodCast training for managers and/or employees

HANDLING DATA BREACHES

Guidance provided to:

- Help prevent data security incidents
- Respond to a data breach

NoDataBreach.com

Powered by ePlace Solutions, Inc.