The Hanover Insurance Group®

RESET SAVE PRINT

Data Breach & Cyber Liability

SUPPLEMENTAL QUESTIONNAIRE

Insured: ______________________________ Web Address: ______________________________

Mailing Address: ____

Agent: ______________________________ Producer: ______________________________

GENERAL SECURITY/CONFIDENTIALITY PRACTICES

1. Type of Data stored:

   □ Name & Address □ Medical Records

   □ Credit Card Information/Bank Account Numbers □ Other Financial Information

   □ Social Security Numbers

2. Number of CLIENT records the insured handles and stores that consists of a combination of Name/Address and any other data listed under question1. ______________________________

   % Electronic: ______ % Paper: ______

   Number of EMPLOYEE records the insured handles and stores that consists of a combination of Name/Address and any other data listed under question1. ______________________________

   % Electronic: ______ % Paper: ______

3. Do you pull or use credit bureau data on a regular basis? □ Yes □ No □ N/A

   If Yes, describe below.

   ____

4. Do you comply with Payment Card Industry (PCI) standards? □ Yes □ No □ N/A

5. A Compliance Officer has been designated to ensure compliance with established institutional standards for handling data. □ Yes □ No □ N/A

6. What percentage of Insured's sales are online? □ 0-25% □ 25-50% □ Over 50%

7. Hiring Practices:

   a. Are Criminal Background Checks completed? □ Yes □ No □ N/A

   b. Is there Data Security training given to employees? □ Yes □ No □ N/A

   c. Is there written Data Security protocol that has been established with all employees? □ Yes □ No □ N/A

8. Access to data files are restricted to specific project staff? □ Yes □ No □ N/A

9. Written and explicit policies are in place to deal with a Data Breach? □ Yes □ No □ N/A

10. The security practices of the firm have been audited without findings of deficiencies. □ Yes □ No □ N/A

    If deficiencies identified, please detail the deficiencies and resolution on a separate sheet

more ▼

ELECTRONIC SECURITY PRACTICES

1. All users with access to systems are authenticated by means of unique and individually assigned passwords, biometrics or digital ID. □ Yes □ No □ N/A
2. Access is controlled by role based authentication and an internal firewall. □ Yes □ No □ N/A
3. An audit trail that documents user activity is maintained. □ Yes □ No □ N/A
4. Firewalls, Spam Filters, Virus Protection etc. are used and updated at least quarterly. □ Yes □ No □ N/A
5. Does the Insured have secure email practices (i.e. automatically scan & filter emails)? □ Yes □ No □ N/A
6. Data that is sent, received and/or stored electronically is encrypted with the highest available encryption software? □ Yes □ No □ N/A
7. A specific data retention/destruction schedule is adhered to. □ Yes □ No □ N/A
8. Do you permit Private Personal Data stored on electronic devices (i.e. laptop, PDA, etc.) to be removed from your premises? □ Yes □ No □ N/A

   If Yes, describe authorization & control measures below.

   ____

9. Is remote access to the network permitted only if through Virtual Private Network (VPN) or equivalent system? □ Yes □ No □ N/A
10. Written data back-up and disaster recovery plan is created and adhered to. □ Yes □ No □ N/A
11. Do you require your service providers to maintain at least the same level of data security regimen that you maintain? □ Yes □ No □ N/A
12. Does your company allow use of file sharing or Peer to Peer networking technology? □ Yes □ No □ N/A
13. Does your company back-up network data and configuration of files daily? □ Yes □ No □ N/A

PAPER RECORD SECURITY PRACTICES

1. Do you have secure storage areas (i.e. locked rooms, locked file cabinets, limited access areas, etc.) for documents containing customer and/or employee personal identification information? □ Yes □ No □ N/A
2. Is access to such info restricted to only need to know employees? □ Yes □ No □ N/A
3. Do you have a sign out procedure when documents are removed from such areas? □ Yes □ No □ N/A
4. Do you have a written procedure for the secure transport of documents from one location to another? □ Yes □ No □ N/A
5. Do you have a regular document destruction policy? □ Yes □ No □ N/A
6. Do you supply shredding facilities/capabilities for paper documents? □ Yes □ No □ N/A
7. Do you outsource paper shredding and document destruction functions to 3rd parties? □ Yes □ No □ N/A
8. Do you have pre coded dialing numbers in fax machines used for sending personal information? □ Yes □ No □ N/A
9. Do you restrict the removal of paper documents containing personal identification information from your premises? □ Yes □ No □ N/A
10. Is the personal identification information of customers, employees, etc. regularly sent out via mail, FedEx, UPS, or other delivery service? □ Yes □ No □ N/A

more

RESPONSE PLANS & TESTING

1. Incident Response Plans (IRP)—please check all that apply:

   □ Network intrusion detection sensor alert

   □ Antivirus software alerts

   □ A system administrator

   □ A log for multiple failed login attempts

   □ An email administrator

   □ A network administrator to monitor unusual deviation from typical network traffic

2. Penetration Testing—please check all that apply:

   □ Subscription to Assessment Services (IT health check, Mail Server Deployments, Testing of mobile devices, etc)

   □ Formal Compliance, Risk and Audit procedures (ISO27001 Implementation, PCI ASV Testing, PCI QSA Audits and Consultancy, Third Party Risk Assessments)

   □ Physical Security, Data Asset Protection and Privacy Services (Telephone based social engineering, Physical social engineering, Building access security Audits, CCTV control reviews)

   □ Computer Forensics and Incident Response (Forensics Analysis, Information Security Incident Management, Secure Data Recovery & File Password Cracking)

   □ Automated Vulnerability Assessment

   □ IT CISO/Security Manager

BREACH HISTORY

Describe Prior Cyber or Data Breach incidents or losses (Date of Loss, amount, loss description) and steps taken to prevent deficiencies going forward.

____

____

____

____

Describe any particular security measures your firm employs (including use of security consulting firms, etc.):

____

____

____

____

Additional Clarification/Comments:

____

____

____

____

Signature of Applicant: ____ Date:____________________