Cyber Liability Insurance

Risk Management for the 21st Century

Dedicated to National Security Since 1920
Haas & Wilkerson Insurance is a third generation, family-owned Kansas City based business that is passionate about people and relationships.
Background

• In business locally and nationally since 1939.
• We are currently licensed to do business in 49 states.
• H&W specializes in providing risk management solutions middle market sized companies.
• Solutions include Property, Liability, Auto, Workers Compensation, D&O, E&O, Cyber and Employment Practice Liability Insurance
Defining Data Breach & Personal Identifiable Information (PII)

− A **data breach** is a security incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so.

− **(PII) Personal Identifiable Information** is any data that could potentially be used to identify a person.

  - Full name, Social Security number, driver’s license number, bank account number, passport number, and email address.
Legislation relating to Cyber Security

• **1996 HIPAA-Health Insurance Portability and Accountability Act**
  – Framework on how to maintain (PII) & healthcare data for the healthcare industry

• **1999 Gramm-Leach-Bliley Act**
  – AKA Financial Services Modernization Act

• **2002 Homeland Security Act**
  – Created the United States Department of Homeland Security

• **Federal Information Security Management Act of 2002 (FISMA)**
  – Requires each federal agency to develop, document, and implement an agency wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.
  

• **European Union -EU GDPR-General Data Protection Regulation**
1) In 2016, 3,000,000,000 Yahoo accounts were hacked
   One of the largest breaches of all time.
2) In 2016, Hackers stole the information of over 57,000,000 Uber riders and drivers.
3) In 2017, 147,900,000 consumers were affected by the Equifax Breach.
   The Equifax breach cost the company over $4 billion in total.
4) In 2018, 150,000,000 users of the Under Armour owned MyFitnesspal app and website were affected by a data breach.
5) 100,000 groups in at least 150 countries and more than 400,000 machines were infected by the Wannacry virus in 2017, at a total cost of around $4 billion.
6) In 2017, 5.4 billion attacks by the WannaCry virus were blocked.
Cyber Liability Insurance

**FIRST PARTY CYBER LIABILITY INSURANCE**
- This is an insurance policy that covers the cost to respond to a hack or data breach on your computers.
  - First-party Cyber Liability Insurance offers coverage for business owners in the event that a data breach compromises sensitive client information
  - Loss Exposures
    - Property
    - Business Interruption Net Income Loss

**THIRD PARTY CYBER LIABILITY INSURANCE**
- Third-party cyber liability insurance provides liability protection for any business whose action (or failure to act) may cause a client data breach or cyberattack.
  - Liability for Customer Data
    - Negligence, Fraud
    - Breach of Fiduciary, Invasion of Privacy
    - Breach of Contract
2018: Organizational Impact – Cyber Incidents

Average organizational cost to a business in the United States after a data breach from 2006 to 2018 (in million U.S. dollars)

Percent of Business Executive Responses

- Business Interruption
- Reputational Damage
- Breach of Customer Information
- Data or Software Damage
- Extortion / Ransomware
- Liability to 3rd Party Data Breach

Sources:
Ponemon Institute; IBM; Digital Commerce 360
© Statista 2019

Dedicated to National Security Since 1920
CLAIMS EXAMPLES

- **Privacy Liability**
  - An employee of an architecture firm lost a flash drive containing confidential information on several large construction contractor clients.

- **Cyber Extortion**
  - ABC Engineering held confidential information on many of their clients and information on merger opportunities. A hacker gained access to their computer system and sent an email with a copy of a merger plan scenario and files on of the firm's clients. The hacker threatened that unless they are wired $250,000 they would shut down the firm's computer systems and publish all the data obtained from the system.

- **Network & Information Security Liability**
  - An employee inadvertently downloads a destructive computer virus that spreads to other files housed on the computer network. Their client then downloads information from the organization's website, allowing the virus to spread to the client's computer systems.

- **Business Interruption – Loss of Income**
  - ABC Engineering launches a new website allowing users to create their own account, upload project bids, use a limited design tool, and process payments. The website is compromised by a DDoS attack by a hacker and takes a week for IT Staff to bring back online.

- **Computer Fraud Coverage**
  - Bad actor gains unauthorized access to your accounts payable in your computers system and alters the bank routing information on outgoing payments.
BEST PRACTICES Managing Cyber risk (Individuals)

- Personal Awareness & Standard Security Practices
  - Firewall, Antivirus/Antispyware software, Encryption Software
  - Only initiate web-based transactions on websites begins with “https”
  - Restricting type and amount of content shared on social networking
  - Declining to open any emails/attachments sent from unrecognized email addresses
  - Using a secure wireless network with secure mobile devices
  - Password management
BEST PRACTICES Managing Cyber risk (Organizations)

• Avoiding a Cyber Incident
  • Leadership should have a good understanding of network operations and security measures
  • Including regular monitoring and testing of network security
  • Procedures for access to network’s hardware and software
  • Data protection policy and procedures should be written and followed
  • Firewalls and antivirus protection continuously update

• Responding to a Cyber Incident
  • A clear Business Continuity Plan that can quickly read and executed
    – All relevant parties have a copy of the plan and receive appropriate training and periodic rehearsals
  • Identify a 3rd Party data vendor to utilize in assisting with how to handle the network and breached data.
  • Legal counsel should immediately be involved to advise on legal and regulatory requirements or potential litigation
  • Cyber Liability insurer should be contacted
  • Appropriate person to handle media communications should be designated in the response plan.
CONCLUSION

Any questions, concerns, or comments? Don’t hesitate to contact via phone or email.

Thank you for your time!

Josh Goodman, CPCU, AIC
Haas & Wilkerson Insurance
W#913-676-9323
josh.goodman@hwins.com
“Land of the Free, Home of the Brave”