Cyber Insurance

Disclaimer: For informational purposes only, please consult insurance and legal professionals for more information.

Some information attributed to AIG and other sources.
As cyber risks grow, senior management and boards of directors of companies are increasingly focused on a **holistic response** to cyber threats that includes:

- **Risk Mitigation**
  - *How do we reduce the odds or severity of something happening?*

- **Risk Transfer**
  - *How can we contractually shift a portion of our risk to someone else?*

- **Response/Recovery**
  - *Something happened, now what?*

When thinking about cyber insurance, consider all three elements.
Identify the Exposure

Challenge = maintaining policies that tackle both internal and external threats

• External Threats
  – Hackers
  – Viruses
  – Social Media
  – Third Party Vendors (VERY COMMON)
    – According to many state laws the liability for the exposure of protected data resulting from the breach of a 3rd party, such as cloud or payroll providers, still falls to the organization that gave the information to the vendor.
  – A Changing Regulatory Environment
    – States are constantly amending laws
    – Federal agencies such as the FTC are finding ways to bring action against affected organizations
    – International laws are being created causing additional regulatory exposure

• Internal Threats
  – Rogue Employees
  – Human Error
  – Mobile Devices
Legal Landscape

• 47 out of 50 states have notification laws, no two are the same
• Each has a different definition of Personally Identifiable Information (PII), but common components include:
  • First name/first initial and last name in combination with:
    – Social Security Number
    – Driver’s License Number or State ID Card Number
    – Financial Account/Credit/Debit Card Number with access/security code
    – E-mail Addresses/Usernames and Passwords
• Transfer of data to a third party does not constitute a shift in responsibility (Data Owner vs. Data Aggregator)
• The laws that apply are by residency of the affected persons, not the residency of the affected organization
• Federal Laws (i.e. HIPAA, FTC, Gramm Leach Bliley, etc.) impose data security requirements and allow for regulatory action to be brought
• Contracts also pose an exposure (Merchant Service and Non-Disclosure Agreements – patents are not covered)
How Do Incidents Occur?

- Accidental:
  - Lost Devices & Inadvertent Publication of Data
- Intentional:
  - Disgruntled Employees
  - Hackers & Unsecured Websites

- Internal:
  - Vendors & Subcontractors
- External:
Breach Examples
Between 2005 – Present there have been over 5,000 breaches affecting more than 900M records

Yellow Front Grocery – Hack
Hackers were able to infiltrate the point of sale network and install malware by using compromised LogMeIn credentials.

CVS Pharmacy – Insider
A pharmacy technician admitted to stealing customer records and providing the information to their property manager who used the information to open up fraudulent credit cards.

Texas Health and Human Services – Physical Files
A storage contactor discovered that 15 boxes containing medical information had gone missing from the contractor’s premises.

Multi-Color Corporation – Portable Media
An unknown individual broke into the offices of a law firm representing Multi-Color Corporation and stole an external hard drive containing employee records.
What do you have to lose?

**Tangible Costs (typically covered)**
- Damage to Systems/Forensics Time and Expense
- Legal Damages/Communication Expenses
- Financial Compensation

**Intangible Costs (typically not covered, but mitigation is available)**
- Loss of competitive advantage
- Loss of customer and/or partner and/or public trust
- Loss of data integrity
- Damage to reputation and brand
Cyber Claims and Industry Trends (10 years) 
Triggers by Industry Segment  (as of 10/2015)

As the number of devices continues to increase, so does your risk exposure.
Cyber Claims Overview (10 years)
Average Cost of First Party Expenses (as of 10/2015)

Every Breach Response is Unique

Cost Range of Each Service:

- **Legal Fees:**
  Under $5,000 up to about $50,000

- **Forensics:**
  About $10,000 to Seven Figures

- **Notification & Call Center:** up to $80,000

- **Credit Monitoring:**
  $10 - $30/month ($120 - $360/annual)
  per employee and/or student

- **Crisis Management Costs**
Three Reasons to Consider Cyber Insurance

• Insurance places a dollar value on an organization’s cyber risk.

• The underwriting process can help organizations identify cybersecurity gaps and opportunities for improvement.

• Many cyber insurance policies bring supplemental value through the inclusion of risk mitigation tools as well as significant incident response assistance following a cyber incident.
Examples of Available Coverage

Insurers offer both first-party and third-party insurance for cyber losses.

**Third-party coverage** insures for the liability of the policyholder to third parties — including clients and governmental entities — arising from a data breach or cyber attack.

**First-party coverage** insures for losses to the policyholder’s own data or lost income or for other harm to the policyholder’s business resulting from a data breach or cyber attack.
3rd Party Coverage

• Network and Privacy Liability
  • Coverage for:
    • Claims arising from the unauthorized access to data containing identity information,
    • Failure to protect non-public information (PII/PHI/Corporate Confidential Information in your care, custody and control) – patents are not covered
    • Transmission of a computer virus, and
    • Liability associated with the failure to provide authorized users with access to the company’s website

• Payment Card Industry (PCI) Assessments
  • Coverage for fines/penalties assessed against merchants by payment card companies and banks arising from the breach of payment card data due to non-compliance with the PCI – Data Security Standard per the terms of a Merchant Service Agreement
3rd Party Coverage

• Media Liability –
  • Coverage for:
    • Claims arising from online content
    • Libel
    • Slander
    • Defamation
    • Emotional Distress
    • Infringement of copyright/trademark/etc.
    • Invasion of Privacy
  • Offered on either an online only or multimedia basis
3rd Party Coverage

• Regulatory Liability –
  • Covers defense expenses and, *where insurable by law*, penalties associated with legal action brought by governmental entities that enforce privacy statutes. Examples include:
    • State Attorney Generals (under applicable state privacy/consumer protection laws)
    • Office of Civil Rights (for entities subject to HIPAA/HITECH)
    • Federal Trade Commission (Federal Trade Commission Act)
    • International Regulators (e.g. European Union Privacy Law)

• Statutes *not* typically insurable:
  • Telephone Consumer Protection Act (telemarketing)
  • Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM)
  • Wrongful collection of information regulations
1st Party Coverage

• Crisis Management/Security Breach Response and Notification Expenses
  • Coverage for:
    • Expense to obtain legal assistance from privacy counsel
    • Forensic investigation expenses to determine how the breach occurred and what information was compromised
    • Public relations/crisis management services to mitigate reputational harm
    • Notification to those individuals of the security breach
    • Credit monitoring
    • Call center to handle inquiries
    • Identity fraud expense reimbursement
1st Party Coverage

• Computer Program and Electronic Data Restoration Expenses
  • Coverage for:
    • Expenses incurred to restore data lost from damage to computer systems due to computer virus or unauthorized access

• Cyber Extortion
  • Coverage for:
    • Money paid to investigate and, if necessary, pay ransom demands connected to threats made regarding an intent to destroy data, introduce a virus or attack on computer system, or disclose electronic data/information

• 1st Party Business Interruption and Additional Expense
  • Coverage for:
    • Loss of income, and the extra expense incurred to restore operations, as result of a computer system disruption caused by a virus or other unauthorized computer attack
New Coverage Offerings

• Carriers are constantly introducing new coverages, including (please note not all carriers can offer the following);
  – Telecommunications fraud
    • Reimburses insured for losses resulting from the unauthorized use of the insured’s telecommunications system (i.e. someone hacks in and uses the insured’s phone system to place long distance calls and insured gets stuck with the bill)
  – Social Engineering/Fraudulent Instruction
    • When a malicious 3rd party impersonates a trusted party (i.e. CFO, CEO, Controller, etc.) in an effort to get the insured to fraudulently transfer funds
    • Available via many crime carriers as well which may potentially offer broader wording
  – Reputational Harm
    • Coverage for the loss of revenue due to client turnover/“churn” as consumers/clients no longer feel that insured can be trusted with information after a breach is noticed/reported on
  – Dependent/3rd Party Network Interruption
    • Coverage for loss profit/extra expenses if an independent 3rd parties’ system is impaired by a virus/hacker causing the insured to suffer profit loss and/or incur extra expenses to continue operations (limitations may apply)
  – System Failure/Operational & Administrative Mistakes
    • Expands the 1st Party Network Interruption coverage to respond to situations where the system is taken offline due to negligence/mistakes made by an employee or vendor while working on the system (limitations may apply)
Cyber Claim Process

#1 • Notify the Cyber Liability carrier once your organization is made aware of a possible breach.

#2 • The carrier will assign a Breach Coach to your organization who will help you select the proper breach counsel and forensic team.

#3 • The Breach Coach and your organization will select a notification service provider to notify the affected individuals ensuring all regulatory requirements are met.

#4 • Your organization will approve the notification letters to be mailed to the affected individuals.

#5 • The Breach Coach will contract a call center service provider to handle any questions on your organization’s behalf.

#6 • Affected individuals receive their notification letters and may enroll in the credit monitoring service.

#7 • Your organization will receive reports on the progress of the notification letters and credit monitoring enrollment for continuous monitoring of the event.
“How much cyber insurance do we need?”

It depends.

What is at risk, your appetite for risk, the ‘cyber maturity’ of your organization, and your existing insurance coverages?
So, where do we start?
Start with an accepted framework to assess cyber risks and cybersecurity risk management.

Recommended: National Institute for Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity
www.nist.gov/cyberframework

NIST or similar assessment can identify areas to address PRIOR to seeking insurance which may strengthen your ‘cyber-maturity’ profile, resulting in lower premiums.
Or start with a cyber insurance **APPLICATION FORM** to help guide your review.

3. Check each of the following that apply to the Applicant’s information security program:
   - [ ] A formal risk assessment methodology which includes at least an annual review of organizational risks
   - [ ] Individual officially designated as a responsible security officer (CISO, CSO, etc…)
   - [ ] An Information Security Policy communicating how information is protected by the organization
   - [ ] An Acceptable Use Policy communicating appropriate use of data to users

4. Check each of the following technologies used by the Applicant:
   - [ ] Firewalls at the perimeter of the network
   - [ ] Firewalls in front of sensitive resources inside the network
   - [ ] Corporate antivirus/anti-malware software
   - [ ] Intrusion detection systems
   - [ ] Centralized log collection and monitoring
   - [ ] Proactive vulnerability scanning/penetration testing
   - [ ] Physical controls preventing access to the devices themselves

5. Does the Applicant have a formal process in place to automatically push updates to all computing resources for critical updates, patches and security hot-fixes?  [ ] Yes  [ ] No  
   If ‘No’, please describe:

5. Does the **Applicant** have processes in place to ensure that all confidential data is encrypted?  
   - [ ] Yes  [ ] No  
   If ‘Yes’, check all of the scenarios in which data is encrypted:
     - [ ] Data at rest  [ ] Data in transit  
     - [ ] Data transferred to removable media (backup tape, CDs, removable hard drives, etc…)

6. Is the **Applicant** subject to any laws or regulations dictating information security?  [ ] Yes  [ ] No  
   If ‘Yes’, check all that apply:
     - [ ] Health Insurance Portability and Accountability Act
You’ll evaluate your potential risk exposure

• What **types of information** does the organization have (i.e., social security numbers, direct deposit information, credit card numbers, passwords, health records, etc.)?

• What are the **potential ramifications** to the organization if this information is compromised or exposed (reputational damage, regulatory actions, litigation, inability to continue operations, repairs to network, etc.)?

• What steps has the organization **already taken** to protect this information?
You’ll examine Policies, Processes, and Practices, and more

Incident Response Planning:
• Is a formal incident response plan in place and will also inquire regarding regular testing through tabletops or simulation exercises.

Security Measures:
• Underwriters are typically interested in data retention, network segmentation, data classification, log monitoring, penetration testing, patch management and business interruption planning.

Vendor Management:
• As many recent data breaches have occurred through third-party relationships, underwriters are concerned with third-party vendor management. It will be important to describe whether the business has a formal third-party management process, due diligence and ongoing oversight performed on third parties, and the contractual obligations required of third parties.

Board Oversight:
• Underwriters will also likely ask how frequently cyber security risk issues are reported to the Board and whether there is Board-level approval or oversight of the information security program.

Coordinate Existing Coverage
• Cyber can overlap with many policies, especially professional liability/E&O. Proactively identifying and accounting for coverage duplication can simplify the claims process.
## Coverage & Gaps

<table>
<thead>
<tr>
<th></th>
<th>Property</th>
<th>General Liability</th>
<th>Crime / Bond</th>
<th>K&amp;R</th>
<th>E&amp;O</th>
<th>Cyber</th>
</tr>
</thead>
<tbody>
<tr>
<td>1st Party Privacy / Network Risks</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical damage to Data only</td>
<td>✅</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Virus / Hacker damage to Data only</td>
<td>✅</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Denial of service attack</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>B.I. Loss from security event</td>
<td>✅</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Extortion or threat</td>
<td>☣</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Employee sabotage of Data only</td>
<td>☣</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3rd Party Privacy / Network Risks</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Theft / Disclosure of private info.</td>
<td>✅</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Confidential corporate info. breach</td>
<td>✅</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Technology E&amp;O</td>
<td>✅</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Media Liability (electronic content)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Privacy breach expense / notification</td>
<td>✅</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Damage to 3rd party's Data only</td>
<td>✅</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Regulatory privacy defense / fines</td>
<td>✅</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Virus / Malicious code transmission</td>
<td>☣</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Coverage Provided?
Coverage Possible?
No Coverage?

*For reference and discussion only; policy language and facts of claim will require further analysis*
Check Current Insurance Coverage

- **First-Party Losses - Cyber**
  - Network interruption due to computer crime, employee sabotage, operational errors and mistakes, security breach, cyber terrorism
  - Restoration, recollection and rectification of digital assets

- **First-Party Losses – Data Privacy**
  - Data protection fines and penalties
  - Data protection investigation and defense expenses
  - Crisis management and public relations costs

- **Third-Party Cyber Losses**
  - Data breach caused by or to third-party outsourcer
  - Distributed Denial of Service (DDoS) attacks
  - Transmission of malicious code
  - Lost or stolen laptop or device
Shopping for a Cyber Policy

• Cyber insurance is relatively **new in the marketplace**
• Risk/price imbalance currently in favor of clients. Pricing often based on **revenue/size of organization**, not on amount of data at risk.
• **Many agents/insurers not familiar**, cyber a one-off.
• Many insurers developing cyber policies
• Consider ‘Big Three”: AIG, Chubb, Lloyd’s of London
Shopping for a Cyber Policy – Key Questions

• When is coverage triggered?
  • Unlike ‘slip and fall’ or ‘flood’ scenarios, where the triggering event is often straightforward, the interconnectedness of the data environment can be quite complex, sometimes resulting in delays between the event occurring and notification of the event.

• When is notice to the insurers required?
  • Typically, notice to the insurers is required at a very early stage of potential breach identification and consent from the insurers is often required for many expenditures following a breach. Best to do in advance rather than after event has occurred.

• How are breach counsel and vendors selected?
  • Typically, notice to the insurers is required at a very early stage of potential breach identification and consent from the insurers is often required for many expenditures following a breach. Best to do in advance rather than after event has occurred.

• What are the possible exclusions?
  • Portable devices, voluntary/intentional acts, social engineering, negligent security, insider malfeasance, information maintained and stored by third-parties, etc.
Your Next Steps

• Conduct organizational review
• Consult insurance and legal professionals
• If HCC can assist, please let us know.
Closing Thoughts

Organizations have the challenge of meeting risk management needs while adhering to a budget. Meanwhile, trends are showing that it is no longer a matter of *if* a breach will occur, but *when* it will occur... A cyber policy in conjunction with an experienced broker can work with you to address both challenges.