TOLMAN & WIKER INSURANCE SERVICES, LLC

INNOVATIVE RISK ADVICE SINCE 1923™

BAKERSFIELD | SALINAS | SANTA MARIA | VENTURA

You've Suffered a Cyber-Security Breach—How Will You Respond?

July, 2013

Property Casualty 360

No matter how prepared a company may be, or thinks it may be, a cyber-security breach can still occur. What the company does next can have a profound impact on its reputation, according to the book, "Cyber Liability and Insurance: Managing the Risks of Intangible Assets," available through the National Underwriter Company bookstore.

"Companies trade on their names, and spend years branding and building reputations," the book states. "In the blink of an eye, all of that hard work can be unwound and the company's reputation left spinning out of control."

Aside from reputational risks, companies can run afoul of state laws and regulations if they fail to notify the appropriate parties in a timely fashion following a breach. Companies should therefore develop an effective communications strategy to minimize potential damage to a company's reputation, customer loyalty, employee morale, and, ultimately, shareholder value, the book recommends.

Following are key quesitons companies should consider when preparing an effecitive communication strategy to put into action following a cyber-security breach:

Do you fully understand the impact—both financially and on the firm's reputation—of communicating with your key stakeholders (customers, employees, business partners) in the event of a cyber security crisis? Have you evaluated the ways in which different types of security breach incidents could impact your relationships with key stakeholders? Have you budgeted for communications responses in the event of various types of cyber security incidents?

- Communications activities surrounding the theft by a current or former employee of important confidential client information would likely be handled quite differently than the loss or theft of thousands of employees' Social Security numbers.

Do you have a crisis management process plan and does it include specific steps to communicate with key stakeholders and the media? Have you identified all of the internal and external resources required to execute the plan?

- Unless it might impede a criminal investigation, notification to key regulatory bodies is mandated in some cases, and an important courtesy in others.
- The plan should prepare for media inquiries in a manner that delivers a clear message for parties affected directly or indirectly.
- The plan should also anticipate activities to help victims of a breach communicate with the company to ask additional questions or obtain recommendations to minimize potential harm.

Have staff roles and responsibilities, in the event of a cyber security crisis, been clearly outlined and understood? Is your company spokesperson qualified and adequately prepared (e.g., media trained) to handle a crisis?

- Do not panic. Call everyone together. Find out the nature of the incident.
- Legal counsel should be prepared to carefully review the method and content of any communications in order to identify any potential issues.
- Use of external legal experts is highly recommended.

Do you have contacts at specialist crisis communications firms in the event you need their services?

- In selecting a crisis communications firm, you should consider whether the firm is knowledgeable of your industry, experienced in handling the type of events and constituents anticipated by your plan, and capable of speaking to the media on your behalf, as necessary.
- Many outside experts tend to prey upon companies that are victims of security breaches, knowing the management wants to do the right thing quickly to stay in compliance with the ever increasing number of regulations and statutes. Let your outside legal experts or your insurance carrier negotiate this agreement. They are more objective.

Do you have a system in place to quickly determine who should be notified, and a process for notifying the appropriate individuals (e.g., customers, employees) in case of a security breach? Do you know what contact methods you have available—mailing addresses, email addresses, or home phone numbers? Are you aware of the legal requirements regarding notification to individuals regarding loss of sensitive information?

- Because state laws may require prompt notification, it is important to determine in advance how individuals will be contacted.
- Understand your obligations under all the applicable statutes and regulations. Consult with outside legal exerts. They can help you understand what your timelines are for reporting.
- Immediately consider the size of the affected population impacted and the risks from exposure, all data elements exposed, and the predicted response of the affected constituents.
- Communicate accurately and as soon as practical. Appoint a single company spokesperson. Be honest, direct, and contrite. Let your actions mirror your words.

Have you considered that, depending on the situation, you may need to craft different messages for different types or levels of clients or employees?

- It may be appropriate to have a different message and method of delivery for your most important relationships, such as highest value customers or most-senior employees, or for individuals who may be particularly sensitive, such as the elderly, the disabled, and minors.

Have you conducted a mock "fire drill" to test the communications plan? Have you had to actually execute the plan? If so, did it work? Did you update the plan following the event?

- Many businesses have discovered holes in their incident response plans after failing to consider the impact an incident can have on daily operations and key departments, or in underestimating the attention the event may draw.
- An organization should carefully analyze past events and responses to improve their incident response plan and minimize the likelihood of future events.

Return to Article Index

Forward this article to a colleague

Address To | Recipient Name

Subject

Message

Send | Reset