On Tuesday, December 27, 2016, the United States Attorney for the Southern District of New York charged three Chinese men with hacking into the networks and servers of seven corporate law firms and using the stolen information to buy and sell stocks, thereby illegally profiting in an amount exceeding $4 million.

The charges accuse the men of using unlawfully obtained credentials of law firm partners to hack into network systems of law firms engaged in merger and acquisition deals. Once the firms’ email systems were penetrated, the men targeted the accounts of lead partners involved in these transactions.

The SEC complaint also charges the men with “installing malware on the law firms’ networks, compromising accounts that enabled access to all email accounts at the firms, and copying and transmitting dozens of gigabytes of emails to remote internet locations.” The case is U.S. v. Hong et al, U.S. District Court, Southern District of New York, No. 16-cr-360.

Law firms hold information valuable to a wide range of attackers, including fraudsters, hacktivists, or state actors seeking to trade on inside information, acquire trade secrets or other confidential information. As such, law enforcement, national intelligence agencies and, especially law firms and their clients have been increasingly concerned about the security of law firm client information.

Therefore, many firms have recently taken steps to strengthen their information security and training. Collectively, the profession has been working to improve the flow of threat information, most notably through the Legal Services Information Sharing and Analysis Organization and training provided by the American Bar Association.
Nevertheless, the recent attacks dramatically underscore the need for constant vigilance. Law firm decision makers should be asking themselves many questions regarding:

- The security of their networks
- Their ethical and legal obligations to their clients
- If proper information security training is in place for employees
- What systems they have in place to recover from cyber incidents
- What the financial consequences of such an attack could be

Law firms should also consider conducting a full review of the information security provisions of their retainer agreements and non-disclosure agreements with clients and vendors to gain as much certainty as possible regarding the extent of any additional legal obligations. Firms should pay particular attention to indemnification and insurance provisions.

**Insurance coverage implications**

In determining the potential financial consequences, firms should assess the nature and extent of their cyber coverage, beginning with their lawyers professional liability coverage.

A gap analysis could highlight the need to purchase a stand-alone cyber policy to address exposures not covered under a lawyers professional liability policy. A cyber coverage extension, which may be attached to an LPL policy, often does not provide the robust coverage addressed by a stand-alone cyber policy.

The following two loss scenarios, using the cyber securities fraud example described above, illustrate how a typical lawyers professional liability policy and a typical stand-alone cyber policy may respond.

**Scenario 1: First-party costs.** A law firm will almost certainly incur first-party costs for a forensic investigation to determine the actual existence of a breach, the point of compromise, the timing and extent of the breach, and whether the attackers left any malware in the system. This can be a long and expensive process, with costs often reaching into the millions.

A law firm may also incur additional direct costs to hire a public relations firm, crisis management firm or law firm to address the media and determine what legal and client notification obligations the firm owes clients whose confidential information was breached.

Although it is arguable that forensics or legal fees would be covered if directly associated with a liability claim by a client, the typical lawyers professional liability policy would not respond to the direct costs noted above.

If a lawyers professional liability policy has a cyber-endorsement in line with several versions available from some insurers, there could be coverage for certain first-party costs, but the breadth of this coverage could be limited and may not include public relations or breach notification costs if not specifically required by law.

Regarding first-party coverages intended to be covered under a stand-alone cyber policy, the breach would be considered a security failure or privacy event, often the trigger for an event management or data incident response coverage.

Most insuring agreements of this kind respond once the security failure or privacy event is discovered and reported. In the case above, it appears that the impacted law firms were hacked sometime in 2015, but only “discovered” the hack when notified by law enforcement. The affected law firms would likely be entitled to first-party costs to conduct a forensic investigation, costs for a public relations, crisis
management or law firm, and costs to notify the clients whose confidential corporate information was breached.

**Scenario 2: Third-party claims.** A law firm client could file a third-party claim against the law firm for its failure to properly safeguard its network which allowed hackers to access the client’s sensitive confidential corporate information. Such a claimant could seek to recover forensic and legal fees and damages arising from a hacker’s use of the stolen corporate information, possibly a trade secret, to profit.

Although it is possible that there would be coverage for such a third-party claim under a traditional lawyers policy, coverage for such claims, likely would depend on the breadth of the professional services definitions within the particular policy.

Certain cyber endorsements could ensure that coverage exists for these types of claims. A stand-alone cyber policy is also designed to provide coverage for such a claim under the security and privacy insuring agreement, which would be triggered by a claim alleging a security failure or privacy event. Such a stand-alone form could also provide the option for more robust limits and a lower retention under certain circumstances.

One final consideration with respect to both above scenarios is the potential impact of the other insurance provision. To optimize the benefit of a cyber policy when the lawyers professional liability policy does not have a cyber endorsement, the other insurance provision of the cyber policy may need to be amended to align with the law firm’s interest or contractual obligation.

When the lawyers professional liability policy has a cyber endorsement, the goal should be to avoid conflicts between the two policies, which could hinder an effective breach response. Other goals include maximizing recovery, minimizing the retained loss and protecting the professional liability policy from adverse claim experience unrelated to professional liability. Therefore, an approach that takes all these goals into consideration is recommended to avoid coverage disputes or gaps.

For more information, please contact your Client Relationship Director, Jason Krauss at jason.krauss@willistowerswatson.com or 212 915 8374; or Geoff Allen at geoffrey.allen@willistowerswatson.com or 818 915 4311.

---

**About Willis Towers Watson**

Willis Towers Watson (NASDAQ: WLTW) is a leading global advisory, broking and solutions company that helps clients around the world turn risk into a path for growth. With roots dating to 1828, Willis Towers Watson has 40,000 employees serving more than 140 territories. We design and deliver solutions that manage risk, optimize benefits, cultivate talent, and expand the power of capital to protect and strengthen institutions and individuals. Our unique perspective allows us to see the critical intersections between talent, assets and ideas — the dynamic formula that drives business performance. Together, we unlock potential. Learn more at willistowerswatson.com.