Cyber-attacks Projected to Spike in 2013: Are Companies Prepared?

by KENNETH C. OH *on JANUARY 4, 2013*

Cyber-attacks against U.S. companies have been skyrocketing in recent years, with 2011 seeing an increase of nearly 44 percent according to the National Security Agency. While many businesses have implemented and continue to strengthen their security measures to deter and detect cyber-attacks, the threat is only expected to grow in 2013.

Financial institutions are frequent targets of cyber-attacks. For instance, McAfee Labs recently cautioned U.S. banks and other financial companies to be on the alert for an attack in the spring of 2013 using malware that allows hackers to conduct fraudulent online banking transactions. The warning highlights that cyber-attacks are also expected to transition from disruptive to destructive in the coming year.

This past fall, several large U.S. banks, including Bank of America and JPMorgan Chase, fell victim to a large distributed denial of service attack. While the hackers were able to significantly disrupt the banks' online operations, customer funds were not impacted. However, security experts are warning that banks may not be so lucky the next time around.

Of course, large national banks are not the only New York and New Jersey businesses targeted by cybercriminals. In fact, small businesses make attractive targets for hackers because they often do not have the money and resources to implement sophisticated security measures. According to a Verizon Business study, 72% of reported security breaches committed by hackers involved businesses with 100 or less employees.

Businesses , large and small, should be taking pro-active steps to protect themselves against cyber attacks. Even a small business can implement some basic IT security measures to significantly reduce its vulnerability. Firewalls, antivirus software, and email security can all help prevent an attack. Training employees to detect phishing emails and other security threats can also go a long way in protecting your company.

Should your business still fall victim to a cyber-attack, it is imperative to consult with an experienced business attorney to determine what legal remedies might be available. For example, if you can identify the responsible party, such as an employee or a competitor, criminal or civil remedies may be pursued.

If you have any questions cyber-attack liability or would like to discuss what your company can do to protect itself, please contact me, Kenneth Oh, or the Scarinci Hollenbeck attorney with whom you work.