REPRINT FINANCIER WORLDWIDE

DECEMBER 2016

FINANCIER WORLDWIDE corporatefinanceintelligence

RISK MANAGEMENT

Cyber risk and its enterprise implications

PETER S. SELVIN

TROYGOULD PC

The variety, permutations and forms of cyber incidents are constrained only by the limits of human imagination. For example, a hospital discovers that its patient records have been encrypted by an unknown hacker, thereby disabling its ability to provide patient care and its overall operations. The hacker demands payment from the hospital in exchange for providing the 'key' to encryption. The hospital pays the ransom in order to unlock access to those records.

Perhaps a motion picture production company's computer system has been infiltrated with malware, with the result that the names, addresses and other personal information concerning its employees have been accessed and then publicly released. In the meantime, its email system has been disabled and its accounting and financial systems have also been rendered inoperable and inaccessible.

Or in another example, a financial institution has received written instructions in the form of an email which appears to originate from a longstanding customer. The email has all the markings of genuineness, including the customer's email

Peter S. Selvin is an attorney at TroyGould PC. He can be contacted on +1 (310) 789 1230 or by email: pselvin@troygould.com.

address and the distinctive trademark of the customer's business. The instruction requests that the institution wire money from the customer's account to a certain offshore bank account. The financial institution complies, only to discover that the email is a fraud – a hacker has successfully impersonated its client.

The question for businesses of any material size is how to mitigate the risk of these incidents. In the words of a former FBI official, there are two kinds of companies: those have been hacked and those that don't know that they have been hacked.

The liability and regulatory equation is fairly straightforward. Companies, and in certain cases also their executives and directors, face potential liability exposure arising out of cyber incidents from persons whose private information has been compromised; from banks and other financial agencies which may be called upon in the wake of a data breach to implement credit monitoring and other mitigation measures for the affected persons; shareholders, especially where the cyber event can be correlated with a drop in the company's stock; and governmental agencies, such as the Federal Trade Commission in the US.

Importantly, these liability and regulatory exposures may extend beyond the enterprise itself, but also to its officers and directors. In this regard, shareholder derivative actions were filed against individual board members for breach of fiduciary duty in the *Target, Wyndham* and *Home Depot* cases in the US.

The filing of those cases follows upon the recent pronouncement from an SEC commissioner that "cyber-risk must be considered as part of the [board of director's] overall risk oversight".

In addition to civil liability risk, there is also a regulatory dimension to this issue. In the US, the Federal Trade Commission has been particularly active in this area, and it has commenced investigations and civil proceedings where it has found the risk mitigation measures or disclosure protocols at particular companies to have been lacking.

A key risk transfer device is insurance. Traditional policies may offer some protection, but they are inadequate principally because losses arising from cyber risks are, in the current policy forms, often expressly excluded from coverage. While a company's directors and officers liability policy may often pick up the defence of company executives or board members in a suit by shareholder arising from a cyber event, claims by employees, vendors and others (whose personal data may have been compromised or whose privacy has been invaded) will often be excluded from coverage in such a policy.

For this reason, there is now a developed market for what is termed 'cyber insurance'. While the particular policy forms vary from issuer to issuer, companies seeking such protection ought to be sure that their policies insure both first-party risk (e.g., damage to their own networks, data and infrastructure) and third-party risk (e.g., liability claims from third parties such as employees or others where, for example, personal information is disclosed in connection with a data breach).

Importantly, in many cases, these policies provide coverage for, among other things, crisis management expenses incurred in connection with mitigating any actual or potential negative publicity arising from a data breach or other compromise of a company's computer systems; security breach notification and remediation expenses; and computer program and data restoration expenses.

For companies, especially in the financial services and health-care sectors, these policies have now become 'must-haves' given the magnitude of the risks associated with data breaches in these particular industries.

But while insurance looks backwards (i.e., it may cover losses arising from events that have already occurred), companies and their executives also have to ask themselves what steps can be taken to prevent such events from

happening in the future.

There are emerging best practices in this area. First, since sophisticated hackers can often bypass or circumvent security measures, companies ought to consider upgrading their security infrastructure to include several layers of protection against cyber intrusion. Second, companies need to be proactive in modifying and adapting their defensive measures to emerging risks. Put simply, as hackers are constantly innovating their technology and methods, so it is that companies need real-time intelligence on these developments in order to continuously adapt, adjust, upgrade and calibrate their protective measures in response to the changing risk environment. Third, companies ought to have backup and contingency plans in place so that when a cyber event occurs, their operations are not disabled and they are not obliged to pay ransom in order to access critical records or resume normal operations. In the brick and mortar world, this is akin to conducting fire drills or evacuation plans so that there is an established protocol for responding on a going-forward basis to a potentially disabling cyber event.

The bottom line is that cyber incidents are now the 'new normal'. For this reason, and aside from the liability and regulatory risks, and the availability of 'backward looking' cyber risk insurance, companies need to formulate plans on a proactive basis to deal with these risks. ■