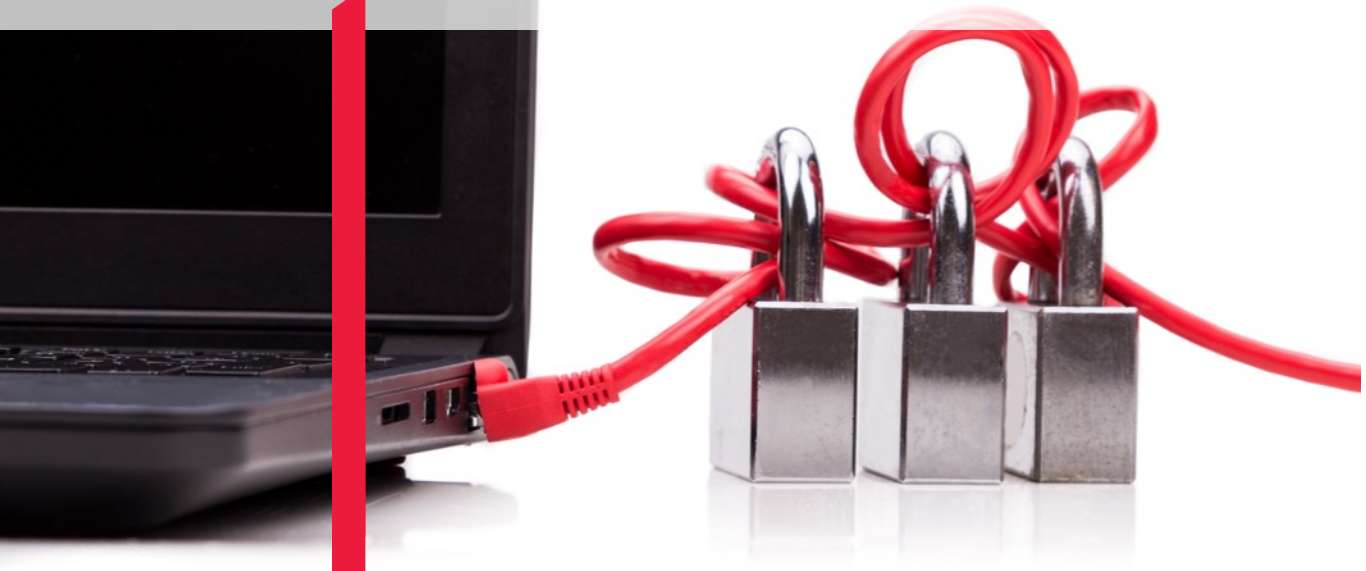
BDO FLASH NOTE

Cyberattacks and their implications to financial statements



Cybersecurity is one of the major risks businesses face nowadays, no matter their size and geographic location. Wannacry highlighted some of the vulnerabilities that businesses encounter: lack of supervision to internal users, weak network defenses, outdated software, etc. Ransomware is rapidly growing, attacking all types of businesses. In their Report of Internal Security Threats of April 2017, Symantec set out some startling facts:

- In 2016, Ransomware detection increased 36% compared to 2015, going from an average of 933 daily to 1,270;
- The yearly number of ransomware has tripled, from 30 in 2015 to 101 in 2016;
- The average recovery went from USD294 in 2015 to USD1,077 in 2016;
- Only 47% of the victims who reported payment received their return of information.

It is estimated that cyberattack losses exceeded USD1.3 trillion in 2016 (according to the FBI's IC3 report).

Cyber Threats, an internal or external malfunction?

Computer experts point out that most of the risks are at the periphery of the system and not at the core of the network. In view of the speed with which business move nowadays, companies have adopted policies such as "bring your own device" to work (BYOD), which allows employees to use their mobile devices (cell phones, tablets, Laptops, etc.) to carry out their functions. This together with the use of the cloud increases the possibilities of improper use / access of information by the companies, their operating processes and clients.

Lastly, at internal level, the threat begins with the distracted, careless or inadvertent employee who does not pay attention to safety suggestions, until a malicious person steals confidential information from the company for illegal acts.

Hackers are becoming more sophisticated, persistent and able to evolve their techniques according to changes in technology. More critically, they are able to move using legitimate tools (operating systems, cloud services) to compromise networks.

Effects on business

- Theft of sensitive information affecting production, as well as extortion by criminal groups;
- Loss of intellectual property due to information leakage;
- Loss of reputation and market share due to attacks that prevent the provision of services;
- Loss of client's personal information, affecting the trust of clients and investors.

Effects on financial statements

Once the company suffers a cyber attack, there are issues related to the preparation of its financial statements that must be analyzed. Here are some sensitive areas to consider:

- **Liabilities and contingencies related to claims:** due to breach of contract, counterparty claims due to losses incurred, investment costs to remedy damages, etc.
- **Impairment of assets:** The incident might cause a decrease in the cash flows of operation, which could result in an impairment of intangible assets (goodwill, brand) and tangible assets (property, plant and equipment).
- **Going concern:** the extent of the occurrence might evaluate the going concern of the company. Even the need to include a mention in the financial statements if there is a matter of significant uncertainty on the occurrence and its possible consequences.
- **Occurrences after the closing:** it is necessary to consider in which period the effects of the incident should be recognized at the level of the financial statements; i.e. at the closing date or in the subsequent period.

Final recommendations

Despite grand advertisements on the subjects, many companies continue to operate under a false sense of security since they have not been victims to a cyberattack. You must keep in mind that there are two types of businesses: those who have been victims to attacks and does who haven't. It is nearly impossible to stop a cyberattack. However, there are some general recommendations to consider:

Work on the human element. Training programs to educate employees about the threat posed by a ransomware and how it is delivered.

Risk mitigation plan. Identify key assets to be protected such as customer, employee, product / service information, and assess the level of risk of internal and external threats to which they are exposed to.

Continuous monitoring. From the technical point of view, reinforcing IT policies, keeping IT security programs up to date, installing mechanisms and procedures to detect undue access as soon as possible in order to limit their impact, evaluate security processes throughout the chain of production.

To conclude, we recommend that employers avoid looking at the subject of "cyberattack" as a matter exclusive to the IT department. On the contrary, it is a matter of business, brand and reputation. You have to be prepared to have control over the occurrence, talk to customers, market and allow the business to continue.

To be considered

According to a survey made by BDO:

- More and more Directors recognize the seriousness of the ramifications that a cyberattack can have on the organization.
- 80% of them indicated that the budgets to defend themselves against cyberattacks have increased by 22%.
- Only 27% said that their company is sharing information on cyberattacks with entities outside their business.
- Seventy percent of Board members believe that the large number of disclosures required in the financial statements today creates confusion when determining which information is most important.

Contact

F&F Tower, piso 30
Calle 50 y Calle 56 Este
Tel.: +507 280 8800

Edificio BDO
Urb. Los Ángeles, Ave. El Paical
Tel.: +507 279 9700

www.bdo.com.pa
www.bdo.global

Prepared by:

Juan Moreno Real
Partner, Director of Regional Audit
jmoreno@bdo.com.pa