BUSINESS ANDMONEY

+2.91% SFC PLC

+0.57% MEDSERV PLC

+0.40% BOV PLC

-17.10% GO PLC

-4.14% MALTA PROPERTIES CO PLC

-1.71% MIA PLC

STOCK MARKET REPORT

» PAGE 32

CONSUMER AFFAIRS
WHEN IS IT WORTH BUYING AN EXTENDED WARRANTY?

» PAGE 33

FINANCIAL NEWS P30, 31

Cyber-risks for businesses

Ramon Cutajar

Ramon Cutajar is a senior manager at Mazars Malta, a member firm of Mazars International.

Over the past decade, various business sectors, such as remote gaming, have seen the introduction of new internet-based business models, content digitalisation, and the need to enable content to be used on different platforms. This technological evolution has exposed businesses to cyber-crime, as cyber-criminals find new and innovative ways to defeat security measures.

Data security has emerged as a major challenge, particularly in view of the very real threat that loss of data can represent to the continuity of a company's operations and the long-term effect on its reputation.

One of the trends that emerges from a recent global report by Mazars on the issue of cyber-security, is that cyber-risks do not seem to feature on the agenda of boards of directors, or as part of the risk management function. In most cases, cyber-security is sidelined and omitted from firms' enterprise risk management systems, simply because management can't figure out where it can fit in their firms' traditional structures.

Such a myopic perspective is dangerous, because the truth of the matter is that cyber-security risks can have grave, and sometimes fatal, repercussions on businesses. There should be no doubt as to the direct connection between technology risk and business risk.

Reducing exposure to cyber-crime requires both technical and operational investments.

The formulation of efficient and effective defence strategies addressing the numerous information technology risks to which companies, such as those in remote gaming, are exposed, is a critical first step.

The mapping of information technology risks and the allocation of the necessary resources to address each major risk should be at the top of the list.

At the same time, management, including the company's board of directors and its audit committee, must be made aware of cyber-security risks, and each of these should in turn understand their respective roles and responsibilities. This would normally include an assessment of the legal implications linked to an attack, and how such an attack might affect the reputation of the organisation.

One should also analyse and evaluate the implementation of regular and effective communication between the various management entities, which would be critical in such circumstances.

A typical checklist should also take into consideration the allocation of the appropriate human and financial resources, and the implementation of performance indicators for the cyber-security programme. Finally, it is the responsibility of management to ensure there is a change of culture in order to take into account the impact of these new risks on the organisation.

The Mazars report also highlights the importance of personnel training and the integration of security in all company projects. It specifies that some 30 per cent of hacks that occurred in 2014 were caused by errors committed by employees. The latter should therefore be fully aware of the risks of data hacking and consequences for the company. The key words are awareness, training and information.

Data security has emerged as a major challenge, particularly in view of the very real threat that loss of data can represent to the continuity of a company's operations and the long-term effect on its reputation.

Because of the technical nature of the risks involved, IT management must have in-depth knowledge of best practices, especially those established by the ISO 27001 standard on information security management systems, National Institutes of Standards and Technology (NIST), Information Systems Audit and Control Association (ISACA) and the Sans Institute.

Meanwhile, depending on the size of the company, the appointment of a Chief Information Security Officer (CISO) may prove worthwhile in ensuring that content, technologies and all company assets are being properly protected. The CISO must, however, be independent of the information technology function and report directly to top management.

While it is possible, and for smaller companies perhaps more practical and cost-effective, to outsource this function, one should understand the risks linked with such a choice.

Regular testing of existing capabilities and procedures will, of course, enhance the quality of the protection and its durability over time. These should be complemented by social engineering tests, such as e-mail phishing and phone pre-testing, to ensure users are able to detect a manoeuvre or any process aimed at extracting information from them that might facilitate an attack.

Meanwhile, depending on the type of data the company holds and its reputation, it may be subject to hundreds of attacks per day. If a breach appears, the implementation of a proper response plan may make the difference between a mere incident and a complete disaster.

Because of their potential vulnerability, the integration of security in applications or online games (security by design) requires strong awareness and professionalism on the part of organisations, particularly in terms of information systems management.

Considering this scenario, it is comforting to note that companies operating in the remote gaming sector are subject to robust regulation as far as security issues are concerned.

Also reflecting the strong regulatory framework in place in countries such as Denmark and France, where among others, operators are encouraged to take into account security risks from the very start of projects, the Malta Gaming Authority requires applicants for remote gaming licences to implement an information security policy that safeguards data, applications, equipment and network, as well as a strict system access control policy.

Compliance with these cyber-security policies are one of the requirements for remote gaming applicants to be issued a licence to operate their business from Malta.

Nevertheless, and despite this stringent regulatory framework, the fact remains that cyber-security remains a major strategic risk for exposed companies, and that the nature of cyber-crime is to constantly seek out and exploit vulnerabilities.

Eliminating threats is impossible, so protecting against them without disrupting business innovation and growth is a top management issue.

The big question mark therefore remains linked to the staying power of management to keep pace with the increasing sophistication and complexity of cyber-attacks and cyber-crime in general, and to protect itself against these effectively.

> **Management, including the company's board of directors and its audit committee, must be made aware of cyber-security risks**