News release

Date	29 May 2017
Contact	Mihnea Anastasiu Media Relations Manager Tel: +40 21 225 3546 Email: mihnea.anastasiu@ro.pwc.com

Investments in security efforts are driven more by regulatory requirements and not by the actual awareness of the ongoing IT security threats, shows a joint PwC Romania and Microsoft survey

According to a joint PwC Romania and Microsoft Romania survey launched today, "*Security in the Digital World*", investments in cybersecurity are mostly driven by regulatory requirements instead of the organizations awareness of the actual and ongoing IT security threats. On the plus side, companies acting in highly regulated sectors such as the financial industry, for example, are usually better prepared to tackle cyber threats.

Almost 60% of the organizations responding to this survey are planning to increase their cybersecurity budget in the next financial year, with 20% counting on maintaining the current spending level, while 23% still don't not have a clear picture as to their next year's budget.

With 40% of the surveyed Romanian companies not having a formal cybersecurity strategy, and only 10% having reached a maturity level where the strategy is defined, implemented and optimised, the study reveals the fact that information security is not yet fully understood and supported at Board of Directors level.

"Information Security Officer appears not to be heard at Board level unless there is a crisis or a compliance issue – they need more support, including hiring more resources or acquiring security intelligence, as technology is a business wide matter today – information security risks are business wide risks" stated Mircea Bozga, Risk Assurance Partner, PwC Romania.

While relying mostly on internal existing resources, organizations in Romania responding to this survey need to scale up their information security intelligence This remains a hallmark of emerging markets, with the more mature organizations from developed economies relying more heavily on external specialized cyber security providers. As the Romanian companies grow and are confronted with more and more sophisticated cyber threats as well as more stringent regulatory requirements, it is likely that they will address the challenge by engaging specialized IT security providers and exploring the benefits of cloud computing.

In terms of perceived cybersecurity challenges, 87% of respondents declared that they are preoccupied with potential data leaks, 73% worry about malware (including ransomware), 70% are concerned about potential disruptions in business continuity, with another 70% preoccupied to ensure protection against targeted attacks.

“With less than 1 year until enforcement the European Directive for the General Data Protection Regulation (GDPR) is becoming an increasing concern for local organizations. However, the study reveals that very few respondents have already created an execution plan in relation to the provisions of the GDPR”, stated Oana Terteleac, Digital Sales Incubation Unit Lead Microsoft Romania.

As for the potential factors that could have a positive effect on cybersecurity, vast majority of respondents considered that increasing awareness (including training) of the employees regarding threats combined with increasing awareness and support of the management board are critical factors to improve digital security. Another positive factor is considered the enforcement of regulatory requirements as a major driver to improve digital security (77%). This may reflect the compliance requirements they are faced with, especially in highly regulated markets.

The need to hire additional security resources (67%) and to exchange security information with others (57%) were also considered by the large majority of respondents very important to improve digital security. This may reflect the current understaffed state of security in most of organizations and the hope that the experience of others may help.

When we discuss infrastructure security, 3 areas of priority emerge, focusing on data backup/ recovery, DLP and IAM.

Most of respondents would invest in data backup / recovery process (20%), improving access management to systems (19%) and data leak prevention solutions (16%). This may show that respondents prefer to invest in areas that have a quick and major impact on their security risk posture, access and data protection.

More than two thirds of respondents use a Data Loss Prevention (DLP) solution and this points out that DLP became a common security measure, similar with antivirus solutions. On the other hand, almost one fifth of respondents are not using a DLP solution. A possible explanation may be the lack of an information classification policy.

One challenge raising increased interest is related to how companies address access control. Across the entire organization, managing identity and controlling access are topics that encourage more companies to go for Identity Access Management “IAM” solution, with almost two thirds of respondents having implemented or planning to implement solutions to manage access across the entire ecosystem (Identity Access Management “IAM” solution).

In order to improve their information security, PwC and Microsoft recommend the following actions to be considered by organizations:

- **Have adequately scaled resources (the specialized personnel enabled by the right technologies and guided by validated processes) responsible for reporting to an information security officer CISO** (chief information security officer). The CISO should report directly to the Board of Directors or to one of the Board Members.
- **Perform regular security assessments** including information security strategy and vulnerability assessments, by using independent external providers
- **A thorough assessment of the cloud computing services should be undertaken** to identify the benefits of cloud services for security, privacy and compliance
- **Invest in employees training and awareness programmes** related to information security. It is a critical success factor in every security programs
- **Robust business continuity planning and exercising -** ensuring that individual user systems and key servers can be restored rapidly from backups, and that the frequency of backups aligns to the volume of data your organisation is prepared to lose in the event of any system being rendered unusable;
- **Crisis and incident response planning and exercising -** ensuring that there are formal procedures in which employees and those responsible for the management of high priority incidents are well versed to streamline the organisation’s reaction to unexpected events and its ability to restore service to employees and customers;

- **Strong security hygiene policies and user awareness -** preventing malware entering your IT environment through the most common delivery vector, phishing, by enforcing strong controls at your email gateways, and developing vigilant employees through robust awareness campaigns;

- **Rigorous patch and robust vulnerability management** programme will help reduce the likelihood of exploitation.

About the survey

The “Security in the Digital World” report was undertaken by the PwC cybersecurity team at the request of Microsoft Romania. The survey is based on the answers of 30 companies active in Romania and have been collected between March and April 2017. 76% of responses came from organizations with over 500 employees.

About Microsoft

Microsoft (Nasdaq “MSFT” @microsoft) is the leading platform and productivity company for the mobile-first, cloud-first world, and its mission is to empower every person and every organization on the planet to achieve more.
In Romania, Microsoft and its more than 3,000 local business partners offer companies a wide array of mobility solutions and growth of business efficiency. At the same time, small and medium-sized businesses have a Microsoft Romania-based contact service for additional information and advice (021 529 7174), and examples of Romanian companies using mobility and cloud solutions in order to increase their competitiveness are available on www.microsoft.com/studiidecaz.

About PwC

At PwC, our purpose is to build trust in society and solve important problems. We’re a network of firms in 157 countries with more than 223,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.

“PwC” refers to the network of member firms of PricewaterhouseCoopers International Limited, each of which is a separate and independent legal entity. Please see www.pwc.com/structure for further details.