1st ANBIMA Survey on Cybersecurity | 2017

December/2017

ANBIMA

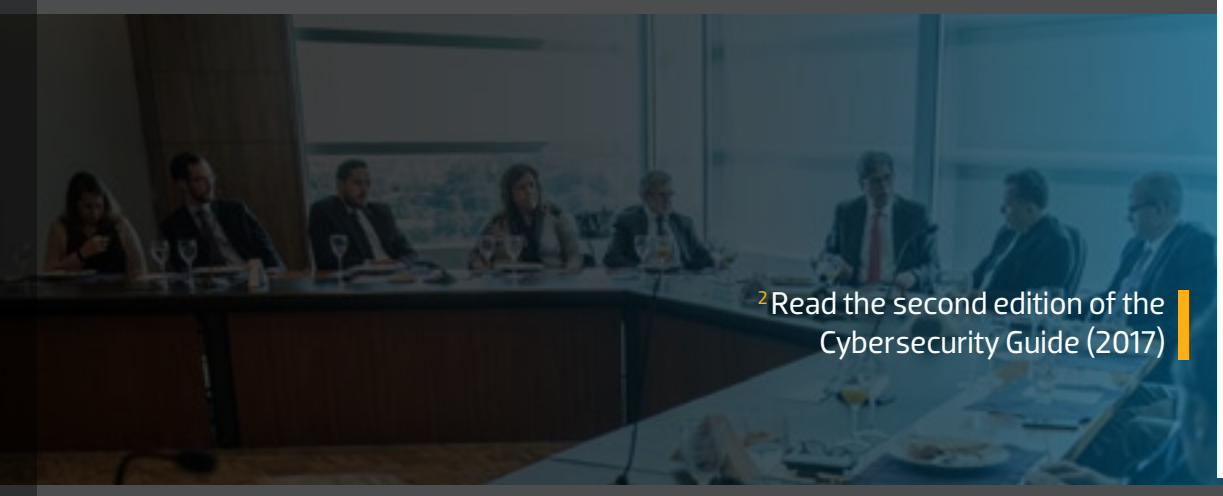
Summary

INTRODUCTION

The increase in cyberthreats in recent years is remarkable: they have grown in volume, but stand out mainly because of their sophistication. The many players of the financial and capital markets have been paying increasing attention to that issue to set up procedures that institutions should adopt to verify if their structures are prepared to identify and mitigate cyber risks and recover from possible incidents.

Our goal

The topic has been on our radar since 2015. The purpose is to contribute to the improvement of cybersecurity in the financial and capital markets in Brazil. Since then, we have launched the Cybersecurity Guide that recommends practices and procedures for establishing cybersecurity programs for institutions, and for educating teams on that matter. As a result, in April 2017 the Cybersecurity TEchnical Group was created. The agenda of that council focuses on the continuous updating and complementation of the guide[2], the coordination of actions to share information and to improve cybersecurity initiatives in the local market, and on the exchange and dissemination of information on the subject.



[2] Read the second edition of the Cybersecurity Guide (2017)

The survey

To gauge the Brazilian market's maturity level in cybersecurity, we conducted a survey among our associates. That assessment is important because it will help guiding other activities such of education, support to tests and sharing information. The survey was developed by the Cybersecurity Technical Group, and the first edition of that guide served as a benchmark: one year after its launch, we measured the compliance of our associates to the recommended practices.

The survey focused on the development of programs by local institutions and asset managers, the occurrence of issues deemed ordinary and other control and monitoring aspects adopted by participants.

Profile of surveyed institutions

We interviewed our **262** associates: asset management firms, banks, distributors, brokerage firms, among others. We received feedback from 151 institutions, or 58% of the total. Most of those who took part in the survey are asset management firms (46%) and have between 11 and 100 employees (46%).

Type of institution

- 46% Asset management firms
- 32% Banks
- 16% Brokerage and Distributors
- 6% Other institutions

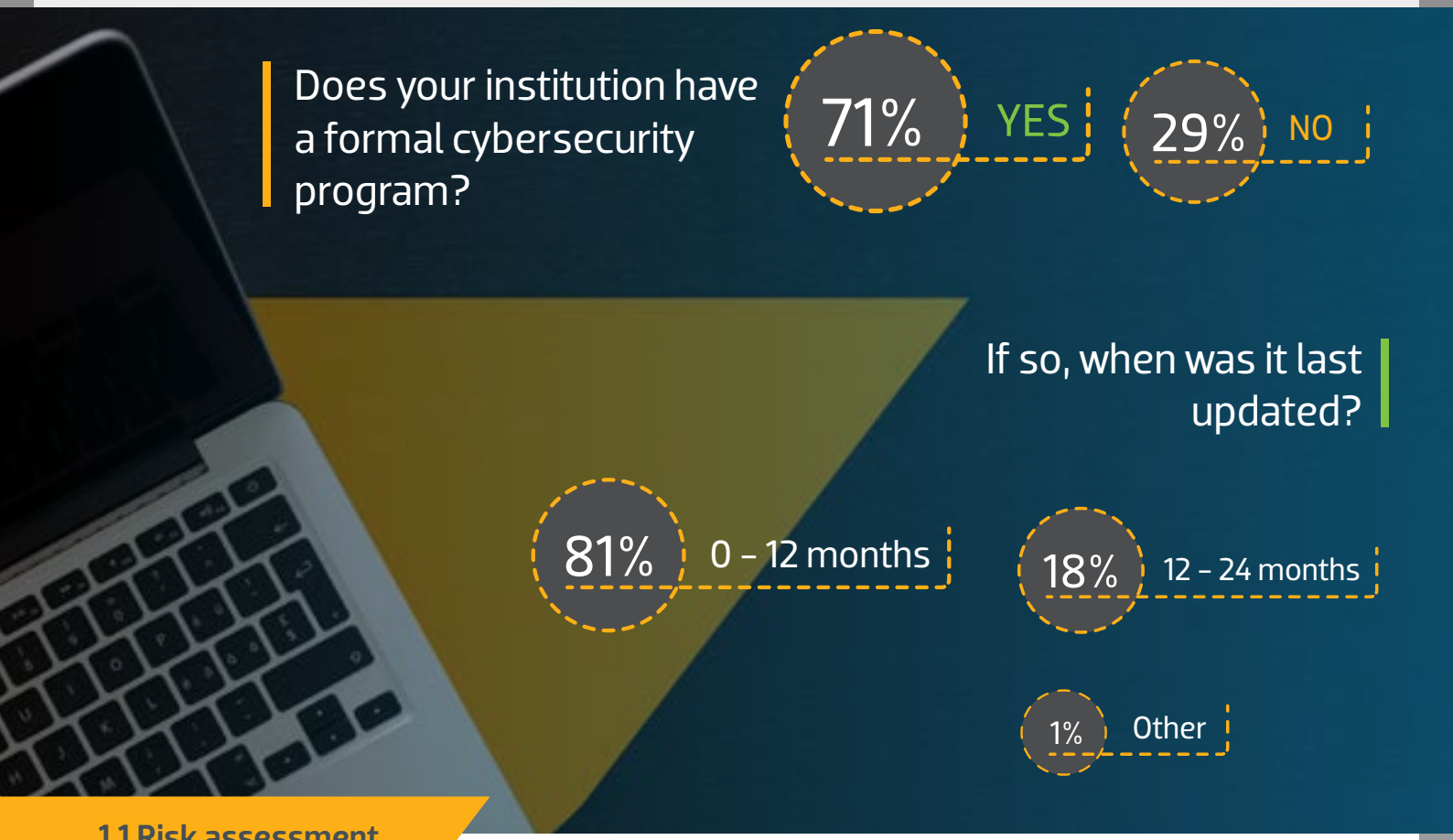
Number of employess

- 46% 11 – 100
- 20% 101 – 500
- 16% 501 – 5,000
- 11% 1 – 10
- 7% 5,001 or more

1. The cybersecurity programs

An efficient cybersecurity program should contain at least five well-defined functions, according to our Cybersecurity Guide: risk assessment; prevention and protection actions; monitoring and testing; creation of the incident response plan; and recycling and review.

That is an aspect that members pay attention to: **71%** said they have implemented a formal program and **81%** have updated it in the last year. Among those who did not deploy any program, **73%** intend to set it up in 2018.



1.1 Risk assessment

The identification of internal and external cyber risks, and of hardware and software assets and processes that need to be protected, called risk assessment, is done by 84% of the institutions. Among them, 59% measure possible financial, operational and reputational impacts, and 48% devise and employ methodology to assess cyber risk.

With respect to governance, only 42% of the institutions that perform risk assessment said to have created a specific committee, forum or group to address cybersecurity internally, with appropriate representation and governance. Among asset management firms, that proportion was 27%.

1.2 Prevention and protection actions

The topic that almost every institution (99%) pays attention to is cyber-attack prevention.

Among those companies, the clear majority responded that they adopt measures such as backup services, access controls, edge security (including firewalls) and minimum rules for setting passwords, among others. Seventy-four percent stated they have implemented controls to prevent the installation and execution of software and unauthorized applications.

When hiring third party services, 72% perform due diligence in the process, examining legal issues and confidentiality clauses, and require security controls in the supplier structure.

1.3 Monitoring and tests

Does your institution adopt monitoring and testing routines to detect threats in time?

YES 83%

NO 17%

Threats are detected by 83% of institutions and 94% of brokerages. If necessary, both groups tighten controls and identify possible irregularities in the technological environment, such as unauthorized users, components or devices.

Among those institutions, only half (51%) test the incident response plan, 42% of them do so every year and 58% within a 6 month-period.

1.4 Creating the incident response plan

As for reaction to attacks, 75% of institutions stated they have an incident response, treatment and recovery plan, including an internal and external communication plan, if needed.

Within the companies, the teams responsible for devising the plan are technologicalsecurity (92%), legal (38%) and communications departments (26%). Other mentioned areas included compliance, risk and business teams.

The threats foreseen in the risk assessment were included in the response plan of 75% of institutions surveyed, and 78% have defined roles and responsibilities within the action plan.

1.5 Recycling and review

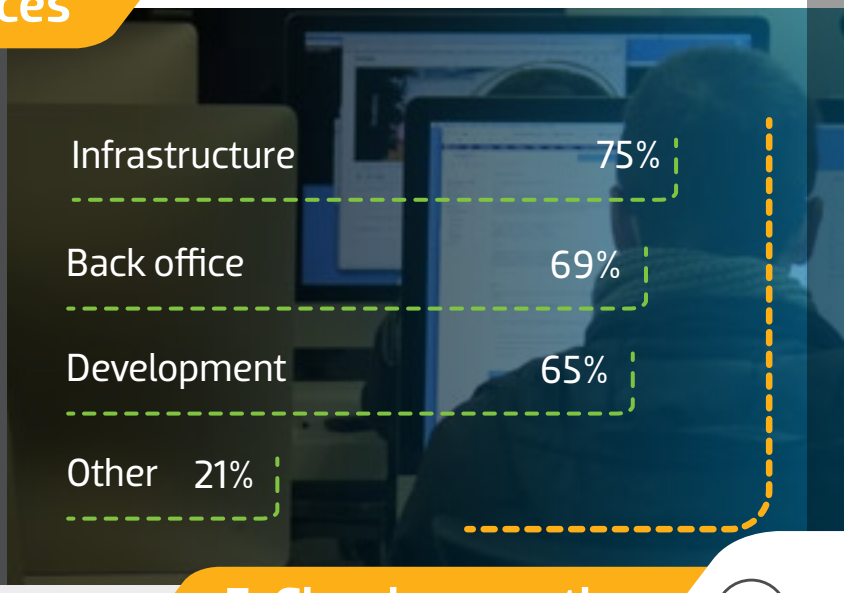
Identifying new risks, assets and processes, reassessing the residual risks of the cybersecurity program and keeping it updated are some of the actions taken by 77% of institutions.

The groups of professionals involved in the program also revise their knowledge about vulnerabilities and threats, according to 86% of the members. Among those institutions, information are obtained from internal sources (85%); from specialized suppliers (75%); and from participating in information-sharing groups (56%).

Out of the total number of respondents, 75% promote and foster a cybersecurity culture by creating internal communication channels to disseminate the cyber security program and offer training. Key performance indicators, which help raise awareness and involve top management and other institutions, are defined and maintained by only 30% of the members.

2. Outsourcing IT services

IT services are outsourced by 83% of the institutions, mainly in infrastructure and back office departments. Periodic reports on quality control are required by only 55% of the institutions that employ those services.



3. Cloud computing

Institution assets may be placed internally or externally, often in the cloud. The latter is the choice of 75% of the institutions, which said to have some service or asset located in that environment. That percentage reaches 90% in the case of asset managers.

Most institutions use cloud computing to storage critical data and systems, including other services such as file backup, e-mail, services provided by third-party systems, servers, non-critical systems, websites, and financial controls.

60% Data

36% Critical systems

35% other

21% Assets

Cloud computing can be considered as a service outsourcing, according to international organizations such as NIST and FFIEC , thus involving certain risks that should be considered by institutions. In this sense, it was found that a large part of the interviewees ensure that the configuration of resources is done under security frameworks, and most also perform due diligence with contractors for that matter.

When outsourcing cloud-computing services,

do you make sure that the configuration of resources is done under security frameworks?

YES 86%

NO 14%

do you perform due diligence with contractors?

YES 68%

NO 32%

Learn more

[3]Nactional Institute of Standards and Tecnology. Refer NIST Cloud Computing Program – NCCP

[4]Federal Financial Examination Council Refer to "Outsourced Cloud Computing" (FFIEC, 10/7/12).

4. Tests

4.1. External penetration tests

Last year, 53% of companies run external penetration tests, performed every year by 80% of them. In 84% of cases, the test is conducted by third-partys. Among the 47% who did not perform external penetration tests last year, 77% have plans to do so. As for brokerage firms, 56% do not perform such tests, out of which 56% have plans to carry them out.

If you do...

how often do you run penetration tests?

80% 0 – 12 months

20% 12 – 24 months

The test was conducted...

84% by third parties

16% internally

If you don't...

are there any plans to carry out those tests?

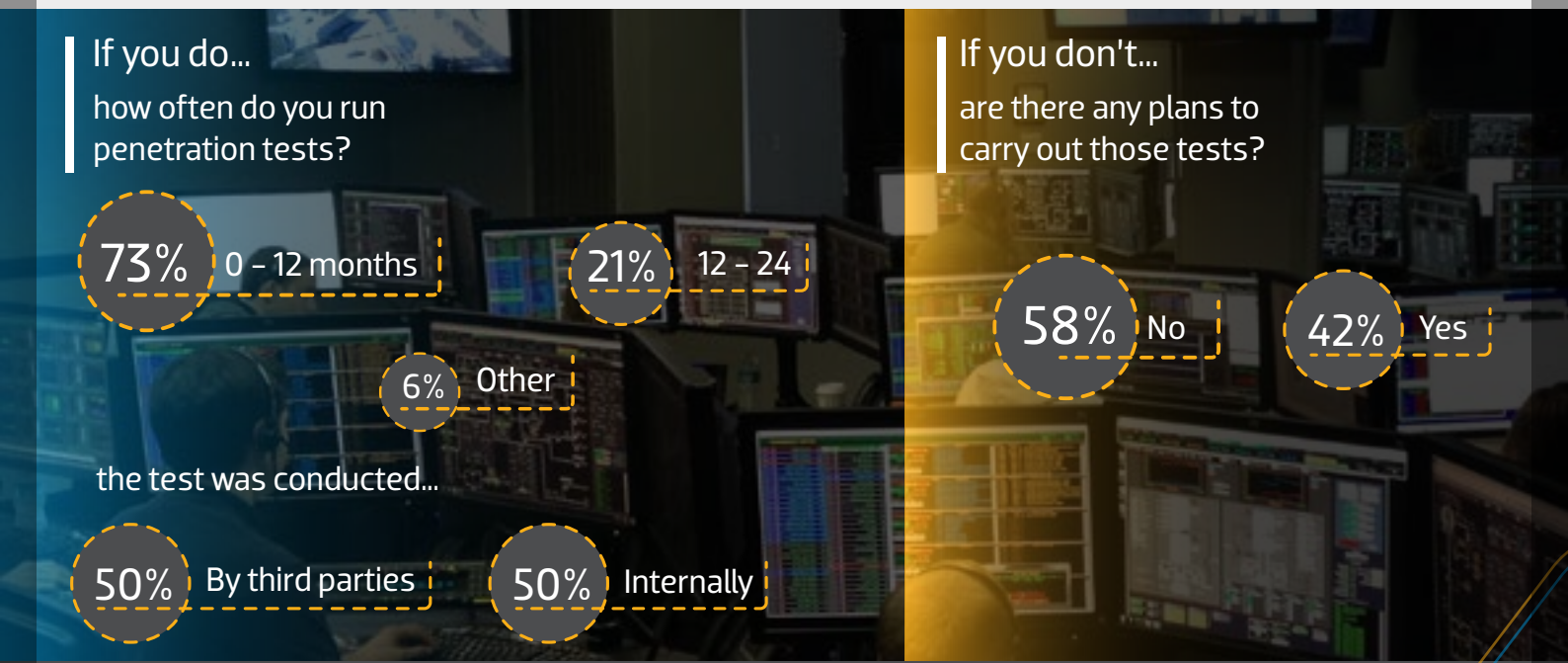
77% Yes

23% No

4.2. Internal penetration tests

Internal tests are performed by 63% of the institutions: 73% of them do it annually and 50% rely on third-party services to handle those services.

Out of those who did not run internal penetration tests, only 42% have plans to carry them out.



4.3 Phishing

Phishing tests were run by 44% of companies and by 29% of asset management firms last year. Those tests include sending e-mail links that simulate an official statement from a trusted person or company, with the purpose of obtaining confidential information.

Conclusions

The first edition of our survey on cybersecurity in the local market sought to contribute to the improvement of cybersecurity practices in financial and capital market institutions. The results reveal that participating institutions have shown satisfactory maturity in how they handle the main cybersecurity issues. The majority employs a formal cybersecurity program and reported to follow many procedures recommended by our Cybersecurity Guide, such as conducting risk assessment processes, adopting prevention, protection and monitoring actions and running tests. A significant number of companies have revealed that they outsource IT services.

Cloud-based services were also addressed: in addition to the widespread adoption verified among institutions, especially for storing data, a large number perform due diligence with third parties. Nevertheless, external penetration and phishing tests still require attention.

As a result, in addition to stimulating the debate among members and other market representatives to build up proper cybersecurity governance, these answers will lay the foundations for the Cybersecurity Technical Group's agenda in 2018. These plans will essentially focus on sharing actions between institutions, both for information and activities aimed at increasing resilience in the local market and among participants.

Further information

Survey support

Cybersecurity Technical Group

Rio de Janeiro
Avenida República do Chile, 230, 13th floor
ZIP 20031-170
Phone: +55 21 3814 3800

São Paulo
Av. das Nações Unidas, 8501, 21st floor
ZIP 05425-070
Phone: +55 11 3471 4200

ANBIMA

www.anbima.com.br