IVASS
ISTITUTO PER LA VIGILANZA SULLE ASSICURAZIONI

Il valore della cooperazione per lo scambio informativo e l'analisi delle minacce nel settore finanziario

Intervento di

Stefano De Polis - Segretario Generale IVASS e

Pietro Franchini - Vice Capo del Servizio Studi e Gestione Dati IVASS

Tavola rotonda nel Convegno "La cooperazione pubblico-privato per la resilienza cyber del settore finanziario italiano - Le opportunità per gli operatori e il ruolo del CERTFin"

Roma, 4 luglio 2024

Good morning to all participants.

Many thanks to CERTFin and the organisers for inviting IVASS to this seminar on cooperation between public and private operators for cyber resilience in the financial sector. The participation of the insurance sector in this initiative is relevant for enhancing the cooperation and promoting security and operational resilience.

We would like to develop two key points: the importance of information exchange and the need to add a third actor to our policies: the broad customer base. We can do more and better on both issues.

1. The insurance industry plays a peculiar role in cyber resilience issues.

On the one hand, insurance companies have to manage their own cyber risks just like every other financial intermediary. On the other hand, they sell protection, via insurance contracts, to policyholders covering, at least in part, remediation costs and economic damages incurred as a result of cyber-attacks, reducing the exposure to operational risks. On the

specific topic of policies covering cyber risk, IVASS published a thematic survey last October 2023[1].

IVASS supervises insurance companies with a focus, among other issues, on ICT governance and cyber security to ensure business continuity and data protection. IVASS, as the national insurance supervisor (unlike banks there is no EU supervision mechanism) has been collecting reports on cyber incidents for years now, on the assumption that sharing this information with the Authority is a crucial factor in assessing risks for individual companies and the market. So far, most of the reports of cyber-attacks received have only served to assess the impacts on the affected companies and verify the restoration of reliable operating conditions. However, they have not benefited the system.

The various entities in the insurance and financial sectors must have the opportunity to learn from the experience of others to promptly identify emerging threats and take effective preventive or corrective measures, thereby keeping their cyber risk at an acceptable level. The system needs to be reactive and proactive simultaneously, pre-empting future attacks.

The Clusit Association reports that in 2023, partly due to the geopolitical environment, there was a deterioration in cyber security in Italy, with a significant increase in serious incidents, especially in the financial/insurance sector. However, maybe due to some reluctance on the part of companies to report incidents, the number of reports received by IVASS has been tiny, only 5 in 2022 and 4 in 2023, of which the reporting companies classified just two as serious incidents. In the first half of 2024, there were no reports of cyber incidents; it was only thanks to the cooperation of CERTFin that we have been aware of incidents involving ICT outsourcers.

We hope that this will change with DORA which requires incident reporting by insurance companies and technology providers, with stricter reporting criteria and timeline. Structured information sharing should indeed make it possible to constantly and more effectively mitigate cyber risk at the national and European levels. Information sharing should also aim to guide companies toward extensive compliance with the new DORA obligations across the full insurance value chain (e.g. including providers, agents, brokers, and so on).

In Italy, a positive example of cooperation is the network for real-time sharing of information and expertise among CERTFin members, in which, however, only six insurance firms (about 10 per cent of the members) have participated so far. Establishing improved collaboration and procedures with the National Cybersecurity Agency (ACN) is essential.

Information sharing, including on attacks on critical outsourcers, is fundamental for prevention, early detection of threats, preparation of coordinated and, therefore, more effective responses, and finally, increasing overall resilience, creating a safer environment for all participants.

[1] https://www.ivass.it/pubblicazioni-e-statistiche/pubblicazioni/altre-pubblicazioni/2023/indagine-cyber-risk/index.html

2. Awareness and education are relevant to improve the cyber security for financial firms and customers.

We have recently opened dedicated cyber security pages on IVASS' website[2] aimed at insurance operators and policyholders since we believe that awareness of the risks and the role each component can and should play is key to making the system more resilient.

In the digital age, online security has become a shared responsibility involving all members of society. Citizens play a crucial role in preventing and managing cyber risks: they are the first line of defence against digital threats.

Thus, awareness and education are of paramount importance. Ongoing training is essential in a constantly changing cyber landscape. Citizens must understand online risks, adopt good digital hygiene practices, and actively protect their data. The reference here is to use strong passwords, update software regularly, and be careful when dealing with suspicious content online. Getting people to understand that online security is a shared responsibility is crucial. Each individual contributes to the resilience of the entire digital ecosystem. The actions of one individual can affect many, highlighting the interconnectedness of online security.

In conclusion, investing in citizen education on cyber security is not only a preventive measure but a social imperative. In recent years, CERTFin has made a significant contribution in this regard through its training and information campaigns. By creating a digital awareness and responsibility culture, we can work together to build a safer and more reliable online environment for everyone.

As evidence of the results that dissemination of information and consequent awareness of cyber risks can yield, it is relevant to point out the experience of IVASS in countering scams implemented through unauthorised websites offering citizens fake insurance policies. In the beginning, IVASS' offices had the task of identifying suspicious sites, with limitations due to the limited availability of resources; today, thanks to the work of our Communication Department and extensive information in the press, radio, TV and social media about the risks and methods of these scams, 95 per cent of the reports of suspicious sites come from companies, intermediaries and citizens themselves who, suspicious, decide to contact our call-centre. We make the appropriate checks and proceed to shut them down.

To sum up, we are convinced that cooperation, appropriate information dissemination, and full customer involvement can strengthen resilience more than proportionately.

We can ensure a high level of cyber security and maintain confidence in our financial and insurance system through a coordinated and collaborative approach. Widespread knowledge of the seriousness of the cyber threat, also on the part of customers, is an additional key driver of the system's resilience.

[2] https://www.ivass.it/cyber/index.html