Editorial

EU cybersecurity policy in the financial sector

With the inexorable rise of e-commerce comes the inexorable rise of the e-criminal. Cybercrime is now the world's fastest growing crime. It has leapt to number two of the top ten business risks worldwide, from not even appearing in that list five years ago. For certain countries, cyberattack is now the risk of greatest concern. Gone are the days of concern about a low-level hack of a website by a script kiddie. Today's attackers are multi-faceted and increasing in sophistication, ranging from advanced persistent threats, corporate espionage, organised crime and "hactivists" to cyberterrorists, ever more competent, and ever better funded. Cybersecurity has moved from being a technical issue to a political and boardroom issue. Financial markets are particularly important as they oil the wheels of all member state economies.

So what should the priorities of cybersecurity be? There are three core themes to address:

(1) governance (at all of organisational, international and national levels);

(2) risk management (both contextually and intelligence driven); and

(3) capability (cybersecurity by design and by default, using a standard framework applied to context).

Amid several large cyberattacks in 2017, the European Commission adopted its multi-sector cybersecurity package. Nonetheless, a multitude of issues remain that the financial sector needs to address to bolster its resilience against current and future threats.

The EU Task Force on cybersecurity policy for the financial sector has recently released its report (www.ceps.eu/system/files/TFRCybersecurityFinance.pdf) on the main issues at play across the European financial sector, and they have come up with nine policy recommendations to advance the effectiveness of cybersecurity. First, convergence in the taxonomies of cyber-incidents is needed, we clearly need to know what each other is talking about, although this can be a challenge with tech speak. Second, the framework for incident reporting needs to be significantly improved to contribute fully to financial institution cyber-resilience. Third, cybersecurity data need to be shared and authorities should assess how and to what extent data held by the centralised hub should be shared, and with whom. Fourth, ambitious policies are needed to develop consistent, reliable and exploitable statistics on cyber-trends. Fifth, companies can do a lot themselves but best practices for cyber-hygiene should be continuously enhanced. Sixth, the European Cybersecurity Certification Scheme needs to be strengthened to contribute better to cybersecurity, cyber-risk management and capability. Seventh, cybercrime is largely cross border, and the reinforcement of cross-border cooperation and legal convergence remains a priority, both within the EU and more widely. Eighth, best practices in remedies in case of cyberattacks need to be further encouraged. Finally, policymakers should further assess the pros, cons and feasibility of creating an emergency fund in case of large cyberattacks. Let's look at these in more detail.

A common taxonomy for cyber-incidents

A common taxonomy across regulations, jurisdictions and sectors should ease the understanding of multi-country and multi-sector cyberattacks, and eventually strengthen the quality of responses. Given the ever-changing nature of cyberspace, the reference

Journal of Financial Crime
Vol. 26 No. 3, 2019
pp. 666-668

1359-0790
DOI 10.1108/JFC-07-2018-0073

taxonomy should be flexible enough to be revised regularly. This common taxonomy should include specific variants applicable to different sectors.

Wherever possible, convergence in templates for incident reporting is needed across legislation. However, given the diversity of purpose of legislation, full harmonisation in those templates remains challenging.

Incident reporting framework

The emergence of different reporting requirements (notably in GDPR, PSD2, NISD, ECB/SSM, eIDAS regulation and Target 2) raises questions as to the best cyber-incident framework to boost financial institution cyber-resilience financial.

First, national templates for the NISD and GDPR should be harmonised across the EU. Second, large firms active in different countries need to develop adequate consolidation processes of the "overall cyber-risk" at group level. Third, authorities should be able to exploit the content of incident reporting to inform and advise CSIRTs in return. For that purpose, policymakers and firms should assess together the risks and opportunities of developing a standard messaging system. Fourth, the creation of a European sectoral hub in charge of centralising all incident reports, dispatching the right information to stakeholders and advising both authorities and CSIRTs could greatly reinforce the incident reporting framework. Finally, to create a resilient cybersecurity framework that could efficiently handle multi-sectoral cyberattacks and prevent contagion from one sector to another, the hub should also be able to cover all economic sectors.

Data sharing by a centralised hub

Authorities should encourage the set up of platforms to facilitate voluntary exchange of cyber-information between financial institutions. In parallel, incident reporting requirements should fully contribute to financial institution cyber-resilience. Incident reporting data should be quickly shared with relevant stakeholders.

First, a centralised hub in charge of incident reporting should quickly provide relevant supervisors with the right information on cyberattacks. Second, the hub needs to share relevant information with financial institutions, provided there is balance between building up an efficient collective response to cyberattacks and safeguarding firms' interests. To provide technical assistance to those firms, the hub would need a clear mandate.

Sharing information with firms' potential clients through the development of cyber-ratings that mirror the cyber-risk to which each supplier, and therefore their potential clients, is exposed should be based on market rather than regulatory initiatives. Tight security of the data managed by the centralised hub should be the main priority.

Macro statistics benchmark

The absence of a macro statistics benchmark on cyber-trends and the poor consistency across sources raise the risk that the cyber-strategies of firms and cyber-policies are not well-founded. If a centralised framework is developed for incident reporting, robust and relevant macro statistics could be developed at national and European levels.

Specifically, robust statistics on the financial impact of cyberattacks will enable better understanding of the overall impact of attacks and inform cyber-policies and strategies. However, the complexity of measurement at firm level has so far made consistent methodologies impossible. A principle-based list should operate at EU level, with the aim of enhancing best practices to measure both "tangible" and "intangible" factors. Convergence should be achieved provided that collaboration is improved between cyber-authorities, CSIRTs, CFOs and CIOs, authorities, etc.

Promoting cyber-hygiene

Authorities should continue to enhance best cyber-hygiene practices. Principle-based lists should be updated on a regular basis. At present they should, for example, include conducting adequate education and awareness activities, updating programs regularly and patching systems, creating complex passwords and changing them frequently, using micro-segmentation, multifactor authentication and encryption of sensitive data, implementing the least privilege principle, developing an adequate strategy to handle shadow IT and establishing an incident response and reporting plan.

European cybersecurity certification scheme

Given the rising importance of digital technologies and their vulnerability to cyberattacks, authorities need to address information asymmetries and the fragmentation of standards in national certification. A European Cybersecurity Certification Scheme could be a powerful tool for reinforcing harmonisation, raising awareness and ensuring mutual recognition.

Yet the Commission's current proposal lacks practical operability and adds unnecessary complexity. As the scheme's success depends on voluntary participation, value added must exceed costs. With too many issues left unclear, the current European Cybersecurity Certification Scheme needs to be strengthened to have a positive impact on cybersecurity.

Reinforcing cross-border cooperation and legal convergence

The cross-border framework to facilitate exchange of information and electronic evidence for prevention, investigation and attribution of cross-border cybercrimes needs further development. When cyber-criminals are identified, convergence in national legal frameworks is needed to facilitate extradition.

Enhancing best practices in remedies after cyberattacks

Best practices in cyberattack remedies need encouragement by EU and national supervisors through core principles. These include robust methodologies to assess how firms and/or clients share cyber-liability. Principles should also cover the best remedies where data theft has no immediate financial loss.

Emergency fund in case of large cyberattacks

Authorities should assess the feasibility of developing an emergency cyber-fund to alleviate the risk of financial instability in case of major cyberattack. Criteria for a cyber-incident to qualify will have to be well defined in advance.

The benefits and costs of the different options to create such a fund require careful analysis. Could existing EU natural disasters funds be extended to cyberattacks or would it make more sense to create a fund that covers all operators of essential services?

The worlds of cyber security and cyber resilience are becoming ever more complex, but the above steps should go a long way to improving Europe's cybersecurity effectiveness.

Richard Parlour
Financial Markets Law International, St Albans, UK

About the Editor

Richard Parlour, Financial Markets Law International (www.fmli.co.uk), is the Chairman of EU Task Force on Cybersecurity in the Financial Sector (June 2018).