WEI
WARSAW ENTERPRISE INSTITUTE
UL. ALEJE JEROZOLIMSKIE 30/7
00-024 WARSZAWA

SUMMARY

Cybersecurity requires well-thought-out regulation that avoids attempts to centrally control technology development and fetishize procedures in the form of a *security theater*. Significant investment in cybersecurity is needed, including on the business side, yet the state should be restrained in dictating detailed solutions. Our report suggests considering an Anglo-Saxon approach to regulation by streamlining liability for damages in cyber incidents. In this way, market forces can be harnessed to discover what detailed solutions will most effectively enhance security.

With high-profile attacks on institutions and individuals, including politicians, fewer and fewer people need to get convinced that cybersecurity is one of the biggest challenges of the coming years. Gartner predicts that global spending on cybersecurity will reach more than $150 billion in 2021, up 12.4% from 2020. The state and the law have a crucial role to play in cybersecurity, although they should guard against the seemingly attractive illusion that security can be achieved through detailed legal requirements coupled with heavy penalties. Threats in cyberspace are evolving so rapidly that attempts aimed at detailed top-down planning will bring more costs than benefits.

INFORMATION EXCHANGE AND CERTIFICATION

Among the positive regulatory models that are already being implemented in Poland and the EU are efforts to coordinate and exchange information on threats, incidents, and methods of counteraction. A system of legally regulated certification of suppliers, services, and equipment will also contribute to the production and dissemination of valuable knowledge. These solutions are of immense importance because, in cybersecurity, an attack is more favorable than defense. An attacker only needs one vulnerability in a complex system consisting of people, code, and hardware. No defender, not even the largest technology companies, can detect all possible threats on their own. Hence, the need to share detailed information. However, there is a risk that, in principle, the proper regulations for the creation and exchange of valuable knowledge are „gilded" with disproportionate obligations. For example, it is not evident that extending the obligation to have specialized internal operations centers to further categories of organizations will contribute to security. It would also be a mistake to hastily introduce mandatory security certificates, for example for public procurement. Above all, the zero-trust model — promoted for instance by the US NSA — should be implemented, whereby systems are configured on the assumption that any software or network connection is in danger of being taken over by the „enemy." For many technologies, the successful implementation of zero trusts may mean that a certification obligation would do little to improve security. And the costs of such requirements could be considerable, particularly in the sense of higher prices and reduced choice from a buyer's perspective.

LIABILITY AS REGULATION BY THE MARKET

The above does not mean that legal liability should not be a tool of regulation for cybersecurity. In our report, we argue that compensatory liability is a potentially better instrument than a criminal or administrative liability (e.g. fines imposed by authorities). As with ‚analog' products and services, technology manufacturers should be liable to their customers for damages, as it is much easier for manufacturers to prevent damage. Currently, the burden of risk and damages is imposed mainly on customers (especially consumers), while the liability is illusory. Proving that

the injury occurred as a result of force majeure, or that the trader exercised due diligence is still too easy (because market standards are still inadequate). Introducing effective strict liability, rather than empowering officials, could turn insurance companies into „regulators." They would have a strong economic incentive to condition insurance premiums on the use of truly effective methods of coverage - whether they became yet market standard or not. By competing with each other and looking after their profitability, insurance companies would have to experiment and constantly analyze the technological situation. „Administrative" alternatives in the form of bureaucratic central control of security methods and punishment for not using them are not adequate for today's technology. Hence, the idea of harnessing compensatory liability. It is not just a question of sharing the burden of risk fairly between traders and consumers, but using the market mechanism to discover what solutions could significantly reduce risk. The assumption behind this idea is that entrepreneurs, including insurers, are able to perform this function better than officials, while retaining an element of strong incentive, e.g. in the form of lower insurance premiums rather than financial penalties as in the bureaucratic model.

ETHICAL HACKING AND CRIMINAL LAW

Ethical hacking is a colloquial term for security analytics done by companies and individuals who have a vested interest in securing their own as much as products provided by others. „Anti-virus" software vendors may be involved in such hacking, as well as companies offering specialized enterprise security services. Another high-profile example is Google's pro bono team „Project Zero" (see page 24), which discovered, among other things, several security vulnerabilities in Apple systems. The benefits for ethical hackers themselves can be to build a reputation and improve their own security products. Given the relatively low cost of entering this market, this is a significant opportunity for Poland. However, activities such as Google Project Zero in Poland carry the risk of criminal liability, despite a positive attempt to rectify this situation in 2017. It is unlikely to expect Poland's security analytics industry to develop to its full potential when one of the primary types of this activity outside our country is, in principle, a criminal offense in Poland, which may not be punishable under certain conditions, but even these conditions may be difficult to meet.

RECOMMENDATIONS

- Cybersecurity regulation should focus on a dynamic process and not on reaching some momentary state. Due to technological developments, the gold standard of yesterday may be outdated today. Therefore, regulation should support a continuous process of identifying threats, assessing them, monitoring them, and adapting responses to these threats.
- Avoiding security theater is key. During the regulatory process, it is easy to fall into a fetishization of procedures, without a significant — or at least proportionate to the effort — increase in security.
- Regulation can contribute to cybersecurity by supporting the production and communication of information about threats, attack methods, and countermeasures.
  - The regulation of the coordination and exchange of information on cybersecurity at both national and EU levels is generally to be welcomed.
  - However, it is not clear whether state institutions set up to collect and process information on threats and incidents would be able to make proper use of mandatory reporting if the number of entities or situations covered by such an obligation were significantly increased.
  - Given the limitations of mandatory reporting systems, the role of voluntary — even public — information sharing should not be forgotten.

- Cybersecurity certification of suppliers, services, and equipment responds to the problem of asymmetric access to information: it is more difficult for users of technologies to assess their level of security.
  - The solutions proposed in the KSC 2.0 Act to create a framework for a national certification system are reasonable.
  - It is appropriate to adopt in KSC 2.0 the principle of voluntary certification.

- Promoting a zero-trust model is worth considering. If mandatory certification is ever considered, e.g. when purchasing services or products for public administration, its legitimacy and scope should be carefully weighed against the costs and benefits, especially in the context of implementing the zero-trust model.

- It is important to support external security research, even if it is carried out without a prior agreement between the researcher and the operator of the system under investigation.
- It is worth considering clarifying the provisions of the Criminal Code, which create the risk of criminal liability for actions undertaken in good faith in this area.
- It is also worth considering the establishment by state institutions in Poland of *bug bounty* programs (with remuneration) or free but publicly recognized reporting of threats.

- Regulation may directly increase the cost of undesirable practices from a cybersecurity perspective also for those who do not take sufficient action to protect themselves and those who rely on them (e.g. consumers).
- Given the practical and legal difficulties, in a fault-based model of liability for cyber incidents, the burden of risk and damage from such incidents in practice falls on those who are in the worst position to prevent harm: consumers and other end-users.
- In view of the above, consideration could be given to introducing the principle of strict liability. To a certain extent, such liability is established by Article 82 of the RODO, but in practice, it would be difficult to effectively hold a digital service provider liable under it.
- It is worth discussing a stronger strict liability model, where a trader holding consumer data would be liable for damages resulting from a cyber incident regardless of the fault — even negligence — of that trader and regardless of the trader's breach of the law.

- Regulation of cybersecurity in any model creates additional costs for traders. This is natural, as in each case additional obligations or risks are imposed on entrepreneurs. While all the models discussed should be implemented, the choice of specific solutions within these models must take into account the magnitude of these costs and the „return on investment". Such an assessment is not carried out with sufficient rigor in EU and Polish decision-making.
- It is likely that streamlining indemnification liability for vulnerabilities and incidents and the use of external security analytics would carry a more proportionate burden-benefit ratio for the private sector (especially with higher burdens) than, for example, requiring businesses to set up internal operations centers (SOCs) for cybersecurity, as is the case in the European Union.