Digital catastrophes and cyber insurance

In 2020, the Israel National Cyber Directorate (INCD) prevented several widespread infectious malware outbreaks in Israel. Earlier this month, the INCD has published findings of its technology-based policy study aimed to depict extreme cyber events scenarios and their economic impact on the Israeli economy. Such digital catastrophes, in general, include cause damage to computers and information systems in many organizations in a scope and scale that causes national harm and cumulative damage to masses simultaneously.

Building on digital catastrophe models created by CyRim group, the Israeli "Cyber-Epidemic" scenario narrates a cyber-attack of 40,000 organizations by means of infectious malware exploiting a common technological vulnerability that leads to the unavailability of systems for 2.7 business days on average. An additional scenario - "Death of the Firstborn" - estimated the economic impact of an attack directed at specific publicly traded enterprises, causing 10 days business interruption on average.

The "Cyber-Epidemic" scenario has the characteristics of a pandemic. Infectious malware first "sprays" the entire economy, obtains access to organizational credentials through a security vulnerability in commonly-used software, and then jumps on to other trust-giving business partners. The attackers achieve large-scale compromise before they exploit the authorizations and access privileges to encrypt data systems and extort ransom. The working assumption is that when these types of events occur, no nation is an island, and other countries will suffer from the same attack. dazzled by their clientele's enormous loss, software and security companies quickly offer an automatic patch for the security vulnerability, thus "vaccinate" the other companies that have yet to be compromised. We also assumed that most of the companies that incur damage will be able to recover within two to three days, but a substantial number of organizations suffer encryption for up to 30 days. Certain sub-scenarios vary in the identity of companies that will suffer damage for such a prolonged period. The price tag of an event of some sub-scenarios could be between NIS 4 billion to NIS 60 billion (roughly 10% of government budget), dependent on the economic importance of the companies hit.

Contagious cyber-attack scenarios cannot be prevented entirely, but the frequency of their occurrence can be reduced. Outbreaks of infectious malware in Israel were prevented a few times over the past year thanks to proactive steps taken by the INCD, combined with the capabilities and vigilance of cyber defenders that detected the attack

and notified the INCD in real-time. Thus, the collaboration of actors of high expertise and joint interests, stopped the spread of the attack and prevented significant damage.

The massive SolarWinds cyber-attack in the US at the end of 2020 is a good case study for a widespread compromise. Businesses in US capitol allegedly returned to "business as usual" since no visible damage was caused, but the expensive process of rebuilding secured networks may take months, if not years. Valuable and sufficient time for the attackers to exploit the data and credentials obtained in order to cause additional damage. SolarWinds cyber-attack also emphasized the global nature of these catastrophes and the blur of the standard distinction between government, public and private sectors, as an attack on private software company results in an outbreak that might jeopardize national economy and governance.

In both scenarios that were published, the initial loss alone would exceed the costs of a physical combat, such as Israel participated in over the past few years. Other catastrophe scenarios also come to mind: Cloud outage, Critical infrastructure outage (as happened in the recent colonial pipeline cyber-attack) - all high financial burdens. That is why the INCD has taken on itself, as the state agency responsible for securing Israel's national cyberspace and maintaining its proper functioning, to maximize the prevention of digital catastrophes and to promote national financial preparedness, private cyber insurance included.

Importance and challenges of cyber insurance

Cyber insurance companies offer relief to insureds for cyber events - but will they be able to cover extreme events? Most cyber insurance products cover financial losses resulting of an attack on the insured organizational network, including business interruption, additional immediate investment in cybersecurity, response teams that mitigate the attack and ensure that it will not reoccur. But insurance is not likely to cover an extreme event. On top of the already given exclusions regarding state-sponsored cyber incidents and infrastructure outage, Insurance giant "AXA" recently announced that it would stop covering cyber extortion, since ransomware cumulative losses is making it an uninsurable cyber risk.

Some formal financial statements published by public companies that were attacked lately, as well as surveys carried out by Israel's Central Bureau of Statistics and similar agencies in other countries, reveal the costly nature of extreme cyber events on the businesses level. Covering massive losses of thousands of insureds simultaneously might

drive the insurance companies out of the cyber risk market due to substantial aggregated loss. Furthermore, the increasing frequency of extreme events may render useless the attempt of insurance companies to distribute the risk over decades, as they successfully do in some natural disaster scenarios. A materialization of a digital catastrophe would spike insurance premiums like happened with terrorism insurance after the 9/11 attacks, resulting in public pressure on governments to implement national insurance schemes and share the risk with the private insurers.

Israel's Cyber National Strategy identifies cyber insurance market as an essential component of economic resiliency to cyber-attacks. Insurance companies serve as key actors in encouraging an increased, tailor-made cyber security level of businesses.

In June 2021 the State of Israel will host the Annual OECD Global Forum on Digital Security for Prosperity, led by the INCD. Our aim is to encourage governments to map the global systemic cyber risk factors that endanger the stability of the digital economy. Analyzing magnitude and frequency of catastrophe scenarios, leading to a surety model costumed for each scenario including indicators of stability, reliability, and responsibility allocation facets. Collaboration between governments, cyber security experts and insurance professionals is the key to raising the national and international digital security, and allow resilience, even in the most extreme scenarios.

Written by Itai Benartzi, Director for Policy at the Israel National Cyber Directorate. Please direct thoughts and feedback to itaib@cyber.gov.il.