ASSESSING CYBER SECURITY 2015

Michel RADEMAKER

Abstract: The article is based on the HCSS Report on Assessing Cyber Security. Following the introduction, it identifies fragmentation of reporting and presents threat assessment. Then it highlights the trends in cyber security, followed by a discussion on the importance of developing national cyber strategies. Last but not least, the authors provide general recommendations. The article is based on a review of 70 studies published by public authorities, companies, and research organizations from 15 countries over the last few years, and calls for international efforts to develop shared, commonly agreed definitions, metrics, and reporting standards to enhance threat assessments; to systematically anticipate trends and attempt to foresee potential new threats; to develop evidence-based cyber security policies that rely more on data and indicators, rather than subjective perceptions; and to consider setting up a mechanism to harmonize the collection and reporting of cyber statistics.

Keywords: cyber security, strategies, awareness, trends, cyber attacks.

Introduction

Over the years, a plethora of reports has emerged that assess the causes, dynamics, and effects of cyber threats. This proliferation of reports is an important sign of the increasing prominence of cyber attacks for organizations, both public and private, and citizens all over the world (see Figure 1). In addition, cyber attacks are drawing more and more attention in the media. Such efforts can help to enhance better awareness and understanding of cyber threats and pave the way to improved prevention, mitigation, and resilience. The Hague Centre for Strategic Studies (HCSS) assessed what is to be known about cyber security threats based on a review of 70 studies published by public authorities, companies, and research organizations from about 15 countries over the last few years (see the bibliography at the end of this article). The questions where: what do we know about the number, origin, and impact of cyber attacks? What are the current and emerging cyber security trends? And how well are we prepared to face these threats?
Figure 1: Cyber incidents reported per year (PWC, 2015).

Reporting is Fragmented

The focus of the examined reports differs widely. Some reports look at all possible cyber attacks, while others zoom in on specific threats such as Distributed Denial of Service (DDoS) attacks or malware. Some reports focus on a specific sector, or one country, others have a global scope. Methodologies used by the reports are often inconsistent and sometimes opaque: some are based on self-reporting (e.g., surveys), while others use data generated by software. One of the main observations out of the analysis is that the range of estimates in the examined investigations is so wide, that even experts find it difficult to separate the wheat from the chaff.

This leads to the conclusion that, although there is no shortage in the number of reports, well defined and comparable cyber threat data and risk assessments are missing.

Threat Assessment

In general, the number of registered cyber attacks is on the rise, partly due to an increase in cyber activity and reporting itself, with estimates of the growth in the number of cyber attacks ranging from a few percent to a tenfold increase. Most of these attacks are motivated by criminal, financial intent. There also seems to be a rise in espionage incidents. The picture furthermore differs per type of attack: in 2013, over a quarter of all cyber crime activities emanated from computers in the US, according to Symantec. And an assessment by Verizon suggests that almost half of all cyber espionage activities come from East Asia. The exact identity of who is behind these attacks remains unclear.
Most of the attacks originate from outside organizations, although many reports note that a sizable share of the attacks is conducted with help from current or former employees, ranging from 6 to 28% of all attacks. Governments, together with the financial sector and industry, stand out as main targets.

There is agreement on the fact that the costs of cyber attacks are significant. Most reporting focuses on larger companies (e.g., with over 500 employees). Existing estimates point to significant costs, which rise per person per organization in parallel to company size. On a national level, this leads to significant losses. McAfee estimates that the average loss due to cyber attacks amounts to over 0.8% of GDP annually, with the Netherlands and Germany topping the chart with over 1.5%. However, the range of estimates is large (Figure 2).

![Figure 2: Countries where IP addresses of attack are located (HCSS, 2015).](image-url)
Trends in Cyber Security

Highlighted are three trends that point to the changing nature of perpetrators. First, a new cyber crime economy is on the rise. An expanding zero-day exploits’ market increases the vulnerability of a large share of users. Secondly, state actors and organized criminal groups are converging capabilities: state actors are increasingly hiring such groups as ‘cyber-mercenaries.’ Third, because states are rapidly developing offensive capabilities, the threat of cyber weapons becoming a major ingredient in warfare is increasing.

As for targets, increasing interdependencies, partly due to the advent of the Internet of Things (IoT), are leading to cascading risks. Big Data hosting companies and digital certificate providers have become a focal point for attacks. In addition, our IDs are more and more the target of attacks, with perpetrators focusing more on ‘who you are’ than ‘what you own.’ Finally, GPS positioning, navigation, and timing stand out as a ‘weak link’ in critical systems.

Countering cyber attacks is becoming more difficult because perpetrators have expanding options available. Increasing availability of anonymization and abuse of Big Data analytics has helped to create a thriving cyber crime industry providing data and software for almost any type of cyber attack on a commercial basis. Even encryption might no longer be able to compete with the vastly improved computing power combined with backdoors in software. Finally, cyber attacks are taking place out in the open but camouflaged: increasingly, legitimate acts will become a means to gain an unfair advantage through cyber attacks (Figure 3).

![Figure 3: Estimated cost of cyber crime as a percentage of GDP (McAfee, 2015).](image-url)
Responses to Cyber Risk Factors

More and more nations see cyber security as a serious issue as evidenced by their development of national cyber strategies. However, several countries have still to develop or publish a strategy on cyber security. Another indicator of the rising importance of cyber security in the public and private sector is the rapidly growing spending of cyber security hardware, software and services.

The meta-analysis of five rankings of cyber security at the national level indicates that the Netherlands, UK, and the US are noted as best prepared and protected. These countries are followed by Japan, Germany, Finland, Canada, Australia, South Korea, and Sweden.

General Recommendations

The picture that emerges from the meta-assessment of cyber threat analyses is one where it has become difficult to see the forest for the trees. There are clearly a lot of reports around, but definitions and methods are difficult to compare. To be able to provide a more encompassing and comparable assessment of cyber threats, and create greater awareness thereof, organizations should:

- in line with emerging efforts on the international level, develop shared, commonly agreed definitions, metrics, and reporting standards to enhance threat assessments. This will provide more targeted investments in cyber security both on company and government level;
- systematically anticipate trends and developments in an early stage to include potential new threats;
- develop evidence-based cyber security policies that rely more on data and indicators, rather than subjective perceptions.
- consider setting up a mechanism to harmonize the collection and reporting of cyber statistics.

Notes:


Bibliography


About the Author

Michel RADEMAKER is the deputy Director of HCSS. He has fifteen years of hands-on experience as an officer in The Royal Netherlands Army, where he held various military operational and staff posts and also served a term in former Yugoslavia. He has a masters degree obtained at the University of Tilburg. After leaving the armed forces, Mr. Rademaker went on to work at the Netherlands Organisation for Applied Scientific Research (TNO) as a project and program manager and senior policy advisor on security topics for ten years. Eg. as NATO RTO project leader, he and his team developed serious gaming assessment methods and conducted several assessments of security technologies, and worked on numerous strategic security topics. E-mail: Michelrademaker@hcss.nl.