development ASIA
An initiative of Asian Development Bank
sharing development know-how

INSIGHT

The Cost of Underestimating Cybercrime

Top government and private sector leaders need to focus on improving cybersecurity. Photo credit: ADB.

A cyber-attack could mean global economic losses of between $121 billion and $234 billion and insurance losses of between $27 billion and $40 billion.

Introduction

Cybercrime is the most underestimated economic risk. Without proper understanding and a managed-risk approach to handling cyberattack, countries, organizations, and individuals are severely exposed to economic losses that could eventually cause broad reputational harm and unexpected financial losses, damages, and liabilities.

As industries continue to adopt new technologies and companies place more value on intangible assets (e.g., intellectual property, reputation, brand, knowledge, and customer data), the risks of attacks or failures are higher because there are more unknown variables.

For example, real-time connectivity has become vital for various business activities such as order-anticipation, just-in-time supply, stock-optimization, predictive maintenance, incident/accident forecasting, and in the future, autonomous driving. Such dependence on technology opens institutions to a targeted, massive cyberattack.

Thus, one cannot emphasize enough the importance for government and industry leaders to truly understand cyber threats and risk perceptions as well as trends, economic losses, and insurance damages so they could improve their cybersecurity and enterprise risk management response.

And if there’s one thing that the coronavirus disease (COVID-19) pandemic has shown us, it is that we need to be prepared to handle abnormal circumstances.

Analysis

We looked at combinations of various scenarios that can affect everyday activities in cases where there is massive power outage or major cloud operation or the failure of domain name servers due to a coordinated global cyberattack. The global attacks use the combination of high volume and intensity-driven distributed denial of service attack with up to 4 attack vectors, one of which is a highly sophisticated ransomware called "wiper" which does not come with an immediate kill switch. An attack vector is a way for an attacker to gain unauthorized access to a computer or network.

Global economic damages can range from $121 billion to $234 billion while insurance losses will run from $27 billion to $40 billion. Depending on the region, sector, and scenario, we consider an interference and/or interruption for a period of 2 to 5 days in the public and/or private sector—with an estimated low of 359,000 to a high of 776,000 companies impacted globally.

In 2020, industries most at risk of attacks are: financial services, power/energy, telecommunications/utilities, healthcare, airlines, information technology, education and hospitality, defense, retail and governmental entities—sectors critical to a country's productivity, development, and security. Disruption of these services could significantly impact commerce and a country's gross domestic product (GDP).

Organizations need to be aware of the different types of cybersecurity threats that they face since cybercriminals have also evolved over time. Some of these threats are: (i) distributed denial of service attack—a malicious attack floods the target infrastructure with traffic, disrupting its services; (ii) system compromise—unauthorized access to an organization's computer system; (iii) ransomware; (iv) financial theft; (v) threat to intellectual property; and (vi) insider threats.

In extreme catastrophic cyber cases, individual companies may require between 9 to 24 months for full business and productivity recovery. This number includes the original incident triage, discovery, and investigation periods. Cybersecurity is a marathon and not a sprint. The "battle" is not won in just the first 2 to 3 days but in the first 3 to 6 months after the incident. Only at a later stage do institutions realize the full impact of the attack because of business interruption and interference, and customer losses.

The case of Asia

Examples of major data breaches reiterate that many Asian companies continue to underestimate weaknesses in the area of cybersecurity and data protection. This results in exponentially longer compromise, detection, and resolution periods following an attack—compared to the United States and Europe.

The take-up of cyber insurance remains strongest in North America (28%–35%), followed by Europe (7%–10%), and much smaller in the Asia–Pacific region (3%–5%).

The major difference between the Asia–Pacific region (mainly outside Australia) and North America or Europe is the Asian institutions' perceived lack of priority and investment when it comes to countering cybersecurity and enterprise risk management. Too often top management still pays little attention to the need for continuous cybersecurity investments, training, and engagement because they think they cannot be hacked and that only large corporations, such as financial services, critical infrastructure providers, and retail industries, are at risk. In addition, they believe the cost to implement these needed measures are high.

Broad cybersecurity laws and aligned data directives across Asia are also lacking, unlike the European Union's General Data Protection Regulation (GDPR) that enforces potential fines and penalties following a major breach.

Implications

As organizations and institutions continue to move toward digital technologies, cybersecurity is likely to have a unique adverse impact on every organization and individual. The criticality of intangible assets for business success has created unprecedented vulnerabilities for many industries and countries. Aviation, communications, media, technology, defense, healthcare, financial institutions, retail, and utilities are some of the highly exposed industries.

However, many may not realize that traditional industries like manufacturing are also exposed since they also have intellectual property, brand, customer data, supply chain management, or use software.

It is not a matter of "if" but "when" you will be hacked. This is why it is essential that governments and companies learn to identify, evaluate, mitigate, transfer and control parts of this risk at top management or ministerial level. The consequences of cybercrime can result in loss of revenue, additional costs to remedy the cybersecurity breach, third-party liability claims, fines or penalties and worst of all—damage to reputation or harm to the brand.

Recommendations

Cybersecurity requires very close cooperation between the public and private sectors to tackle this unaccustomed risk. Cyber risk is global, highly volatile and severe. It is contagious, fully man-made, and criminal intent-driven. No government or company is big enough to solve the entire security problem. The private sector, government, and individuals need to work together to come up with cybersecurity solutions that go beyond conventional means, such as risk pooling or government-funded structures.

To respond successfully to cyberattacks, governments and businesses need to focus proactively on these three core areas:

- address and embed cybersecurity at the highest level;
- craft and stress real-time crisis management (not just as a table exercise), supply chain management, business interference, and forensic plans; and
- identify and establish broad cybersecurity (threat intelligence, penetration stress-tests, defense), risk transfer measures (cyber insurance), regulatory and crisis management (public relations and branding), and partnerships (internal and external resources).

Organizations should establish plans and conduct stress tests against the possibility of a cyberattack, and top management and government leaders must be actively engaged in these exercises. New real-time defense capabilities, such as artificial intelligence—for instance in data breaches—should be carefully reviewed and integrated if and where feasible and applicable.

Peter Hacker discussed "Cyber Crime: The Known Unknown Emerging Exposure" at the 3rd Asia Finance Forum: The Future of Inclusive Finance, *an event organized by the Asian Development Bank in Manila in November 2019.*

Resources

ADB Knowledge Events. 3rd Asia Finance Forum: The Future of Inclusive Finance.

A. Ladbury. 2019. Single coordinated cyberattack could cause $40bn insured losses. *Commercial Risk: Insurance & Risk Management News.* 6 November.

A. Sadiq. 2019. Keeping up with Asia. *Asia Insurance Review.* July.

European Union. 2016. The General Data Protection Regulation (GDPR).

M. Beasley. 2016. *What is Enterprise Risk Management (ERM)?.* Raleigh. Enterprise Risk Management Initiative North Carolina State University Poole College of Management.

P. Hacker and H.J. Guenther. 2019. Cyber risks – the stakes are high for reinsurers. *Asian Insurance Review: Singapore International Reinsurance Conference Supplement.* October–November. pp. 14–16.

Peter Hacker
Cybersecurity Expert

Peter Hacker has 2 decades of cyber risk, advisory, underwriting, and technical cybersecurity leadership experience in London, New York, Singapore, and Zurich. The focus of his work and research has been for many years at top management level of leading global companies, successful midcap niche players and regional and international organizations. In November 2018, he was engaged by the Singapore Reinsurance Association to advise on the world's first Cyber Risk Insurance Pool in Singapore.

Last updated: June 2020