CERT'S PODCASTS: SECURITY FOR BUSINESS LEADERS: SHOW NOTES

Cyber Insurance and Its Role in Mitigating Cybersecurity Risk

Key Message: Cyber insurance is best used in organizations that are effectively managing cybersecurity risks.

Executive Summary

"The goal of any cybersecurity investment is to reduce the potential impact from cyber risk. Initial investments should be in capability development—the implementation of controls to protect and sustain operations that depend on technology. As capability increases, additional capability investments produce diminishing returns—the curve flattens. At that point, investment in cyber insurance becomes an efficient means to further reduce risk." [1]

In this podcast, Jim Cebula, the Technical Manager of CERT's Cybersecurity Risk Management Team, and David White, Chief Knowledge Officer with Axio Global, discuss cyber insurance, its potential role in reducing operational and cybersecurity risk, and how organizations are using it today. We also discuss ongoing CERT research on this topic.

PART 1: DEFINING CYBER INSURANCE; POSITIONING IT AS A SECURITY CONTROL

Defining Cyber Insurance

Cyber insurance in the United States typically covers first-party costs associated with a security breach. This may include costs associated with, for example:

- hiring a forensics firm
- conducting the investigation
- making customers whole such as credit monitoring
- reissuing credit cards

There is a much bigger market for cyber insurance in the U.S. than in other parts of the world, driven largely by breach notification laws in 46+ states.

Europe does not currently have any breach notification laws but several countries are working on enacting these. Cyber insurance in Europe typically covers costs associated with non-physical business interruption, sometimes referred to as network business interruption. An example is covering costs associated with having a website knocked

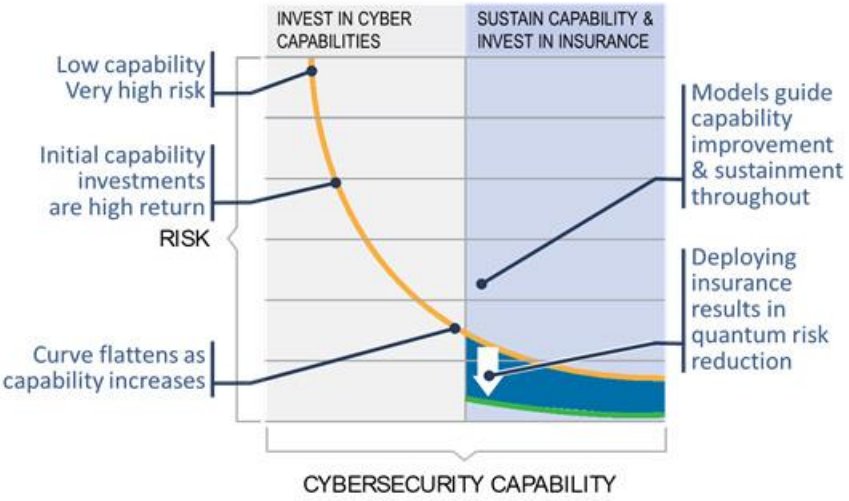
offline from a DDoS (Distributed Denial of Service) attack, resulting in lost revenue or sales.

Physical damage and bodily injury are covered under normal property and other more traditional types of insurance policies.

Cyber Insurance as a Security Control

As shown in the figure below, if an organization is doing nothing about cybersecurity, it has low capability and high risk (upper left corner). As they start to make investments in cybersecurity, the risk reduces and then starts to flatten out at the point of diminishing returns. There is a wide range of security controls that can be used to reduce risk.

The best time to consider cyber insurance is when an organization gets to the flat part of the risk curve. Cyber insurance moves the whole curve down as it functions directly on the financial impact that would hit an organization's balance sheet or bottom line.



To get a good price on insurance coverage, an organization needs to be on the right side of the curve vs. the left. In other words, an organization needs to have its cybersecurity house in order, have good security hygiene, and have a solid security program in place.

Insurers are improving their ability to conduct underwriting evaluations to figure out if an organization is a good risk, so as to avoid the "moral hazard."

Cyber insurance is basically another tool in the toolbox of controls. It works best in organizations that already have a handle on their cybersecurity risks – and they're making a decision to deal with residual and excess risks and liabilities through the purchase of insurance.

PART 2: HOW CYBER INSURANCE IS BEING USED TODAY; NEW, EMERGING PRODUCTS

U.S. Federal Government Exploring the Use of Cyber Insurance

The U.S. Department of Homeland Security is investigating the use of cyber insurance as an incentive for critical infrastructure owners and operators to adopt the NIST (National Institute of Standards and Technology) Cybersecurity Framework(CSF).

The NIST CSF provides a framework of cybersecurity practices for U.S. critical infrastructures. It was developed as a collaborative process with government, industry, and academia. The idea is if an organization adopts the NIST CSF, insurers would favorably consider this in setting insurance rates or perhaps higher insurance limits.

Current State of the Practice

On the consumer side, there is more uptake for cyber insurance in larger organizations. Chief Information Security and Chief Risk Officers are generally responsible for oversight of cybersecurity. This is much more challenging for small and medium enterprises as they typically do not have staff dedicated to cybersecurity issues.

Larger organizations typically want to buy more coverage and want higher limits that insurers are willing to provide. So they often obtain such coverages from multiple insurers.

On the insurer side, the market is still relatively new and much smaller compared to other forms of insurance.

David shared the following statistics from a recent industry roundtable conducted at the U.S. Treasury:

- 50 percent of the Fortune 250 firms are currently buying cyber insurance. The forecast is that this number will increase to 70 percent within 2 years.
- The primary sectors that buy cyber insurance are finance, health care, and retail, due to their handling of PII (personally identifiable information); secondary sectors include technology and educational firms.
- Total annual premiums for cyber insurance are approximately $1.3B; annual premiums for property insurance are well in excess of $100B.

New, Emerging Insurance Products

In the U.S., there are new products that address business interruption, similar to the offerings in Europe.

With respect to critical infrastructures, there are new products dealing with the intersection of software, technology, and physical devices such as control systems. These

would cover the risks of physical damage, property damage, and bodily injury resulting from a cyber event. A few examples include AIG CyberEdge PC and offerings from Aegis.

Companies that buy cyber insurance are struggling with how to fine tune their insurance program to best meet their risk exposure. For example, a utility that takes credit card or bank transfer payments and also faces critical infrastructure risks may need a spectrum or blend of coverages.

There currently are no products that covers costs associated with the loss of intellectual property.

PART 3: CHALLENGES FOR CONSUMERS AND INSURERS; CERT AREAS OF RESEARCH

Challenges for Insurers

Some of the current challenges that face insurers offering cyber insurance include:

- A shortage of people with cybersecurity skills. This affects their ability to supplement their underwriting teams with people who understand this risk.
- Understanding enough about an organization's state of cybersecurity during the typically brief interaction that occurs during the underwriting process, to assess the level of risk and if they want to insure the organization.
- Making underwriting a lightweight yet informative process.
- Treating underwriting as a measurement problem – knowing the appropriate metrics, indicators, and factors to collect.
- Understanding the basic and more advanced cybersecurity practices, tools, and techniques.
- Being able to translate the technical aspects of cybersecurity into business terms that are more meaningful for senior leaders, for example, being able to express risks in terms of business impact and monetary loss.

Challenges for Consumers

Many of the current challenges that face consumers are the same as those facing insurers. Some additional ones include:

- Those advocating for cyber insurance need to position this investment in the context of more established insurance investments.
- Fine tuning and optimizing cybersecurity and cyber insurance programs to an organization's tolerance for risk, all of which are moving targets.

One risk manager said it took 7 years to get his organization's cyber insurance program properly tuned to the organization's risk profile, which is not surprising given the dramatic changes that have occurred during this time.

CERT Areas of Research

CERT's research in cyber insurance is, in part, motivated by the need to be able to describe security vulnerabilities and incidents in business language. This includes being able to monetize cybersecurity risks.

Insurers have to do this every day so we are hoping to learn from and draw upon this body of knowledge and expertise as insurers evaluate organizations for insurance coverage. They are attempting to put a dollar figure on cyber risk exposure.

Measurement and analysis of data to support cyber insurance decisions are also of interest. Can we develop more repeatable, reliable (but not too onerous) ways of measuring the security state of an organization?

We also hope to explore all aspects of data analysis of cyber events and incidents, perhaps towards the objective of developing a repository of information with supporting analysis.

Resources

[1] White, David. "Axio Process & Services: A comprehensive approach to cyber risk management and transfer." Presentation, Axio Global, October 2014.

U.S. Department of Homeland Security Cybersecurity Insurance website

Advisen website

NetDiligence website and their 2014 cyber claims study

AIG website and CyberEdge product