



## NCSIP Position Paper

### Cyber Insurance

Prepared on behalf of NCSIP with input from Committee Members by

Gary Perkins/BRITISH COLUMBIA

2017-11-09

---

#### **INTRODUCTION**

Cybersecurity is an issue of business enterprise risk. Cyber insurance is a service intended to assist businesses and individuals with managing risk. Cyber insurance may help organizations offset costs of cyber breaches, navigate through breaches when they occur, and assist in evolving organizations' security posture.

#### **POSITION**

It is the position of NCSIP that the marketplace for cyber insurance is very "immature with room for improvement"<sup>1</sup>. Insurers have not anticipated the variety of scenarios that may arise and under what conditions the insurance companies will accept and reject claims. Organizations are encountering varying levels of success when submitting claims against cyber insurance policies in seeing the return on value for their premiums. Organizations that have adopted cyber insurance policies early are learning the boundaries where cyber insurance will and will not pay. For example, in the case of *Brick Warehouse v. Chubb Insurance*, the courts found that although email was used to facilitate the crime, the root cause was social engineering, which was not covered by the cyber insurance policy.<sup>2</sup>

Many insurers are using scare tactics to market offerings to organizations. This tactic is used despite the fact that actuarial data is still not available for insurers to adjust premiums "based on what security controls and products are most effective"<sup>2</sup>. Cybersecurity is one of many enterprise risks that organizations face. For governments that choose to self-insure for these risks, cyber risks would be no different.

The primary reason organizations purchase cyber insurance is to compensate for financial losses incurred as a result of cyberattacks. The most significant losses often relate to intellectual property or information about proprietary artefacts that give the organization an edge over competitors. Private sector organizations should consider insuring against cyberattacks just as they would insurance against fire and other risks. Purchasing cyber insurance may be seen as another item on the list that organizations can point to as evidence of preparing for the inevitable when faced with scrutiny from the media, auditors, or Boards of Directors. After all, no organization globally is immune and the impacts of cyberattacks can have significant costs.

Government is not an optimal use case for cyber insurance as no amount of compensation will offset brand and reputational damage, or the loss of trust from stakeholders. Reputational damage is rarely covered by cyber insurance policies. Insurers admit that reputations are difficult to measure and thus difficult to insure.<sup>3</sup> Based the above statement as well as the fact that cyber insurance is still immature, **NCSIP members agree that cyber security insurance is not a value add that is required at this time for public sector organizations.**



Cyberattacks may have impacts that are wide reaching or even global in nature. There is concern that large-scale cyber incidents with immediate repercussions will result in too many claims by organizations over a short amount of time. This surge in claims may lead to solvency issues, bankruptcy, and inability to reimburse claims by insurance organizations. With increasing convergence between logical and physical environments it remains to be seen whether cyber insurance will cover physical damage caused by cyberattacks. This will become even more significant in the case of attacks targeting critical infrastructure.

Businesses and insurers should be concerned with risk aggregation, given the possibility of single attacks leading to losses across a large number of firms, which can create counter-party risk for the insured and potential failure for the insurer.<sup>4</sup>

It is essential that organizations conduct research to determine whether cyber insurance and a policy exist that is right for them. Reading the fine print might ensure that organizations know in advance of a specific firm they may be mandated to work with as a cyber breach coach, cybersecurity breach handler, or cyber breach negotiator. When experiencing a breach, an organization may find upon making a claim that a third party is now in charge of responding to the incident. Additional cyber insurance policy requirements may include mandatory reporting to law enforcement, federal departments, or other parties.

Following a successful claim against a cyber insurance policy, organizations may find that they are still not whole as the settlement may not cover business disruption or theft of intellectual property that is impossible to recover from. The research and costs involved in re-creating intellectual property may be so prohibitive as to force the organization out of business. Organizations in this situation will conclude it is more valuable to invest in hygiene controls required to prevent the incident than recover than try to make up for the loss of priceless IP.

Regardless of whether an organization intends to purchase cyber insurance they should invest to reach a level of security maturity that is aligned with their appetite for risk. Otherwise they will risk the insurance company not paying to cover the breach for reasons that the organization did not take reasonable steps to prevent the problem in the first place. If an organization isn't prepared to at least achieve a basic level of security then cyber insurance is not worth the premiums paid by the organization. Cyber insurance is not a substitute for a maintaining a solid cybersecurity program. Cyber insurance may be worth the premiums in order to cover third party liability.

In Public sector, data breaches routinely involve sensitive information including the personal information of citizens. Citizens deserve to be able to conduct their online transactions knowing that the information entrusted to government is secure. When there is a breach, citizens lose faith in government's ability to protect their information. This results in loss of confidence in government and adversely impacts brand and reputation. Insurance involves the transfer of risk and reputational risk cannot be transferred. Thus, cyber insurance is of limited benefit to public sector organizations and not a replacement for a robust security program.

## **REFERENCES**

- 1: <https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/risk/lu-cyber-insurance-cyber-risk-management-strategy-03032015.pdf>
- 2: <http://www.insurancebusinessmag.com/ca/news/cyber/court-rules-social-engineering-attacks-not-covered-under-cyber-policy-83950.aspx>
- 3: <https://www.ft.com/content/25bf97e8-3a27-11e7-821a-6027b8a20f23>
- 4: [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/415354/UK\\_Cyber\\_Security\\_Report\\_Final.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/415354/UK_Cyber_Security_Report_Final.pdf)