Client Advisory: Twelve Takeaways to Consider When Obtaining Cyber Insurance

Richard Austin, Jennifer Davidson and Steffi Tran March 11, 2022

Introduction

Cyberattacks are increasing in frequency and sophistication and can affect any organization, regardless of size. Attacks are becoming more disruptive and damaging, leading to longer recovery times and greater economic consequences. The Emsisoft Malware Lab estimates that Canada experienced over 4,200 ransomware incidents in 2020, costing almost $660 million USD.[1] Fitch Ratings reports that cyber insurance pricing is increasing at an accelerating rate.[2] In addition, in 2020, direct written premiums for the property/casualty industry rose 22% to over $2.7 billion USD, reflecting the growing demand for cyber coverage.[3]

Recent case law illustrates that organizations without a cyber insurance policy may discover serious gaps in their coverage when impacted by a cyber incident.[4] Moreover, traditional or general insurance policies may provide limited or no coverage for certain losses stemming from cyber incidents. With costs of responding to a cyber incident now averaging $4.24 million USD, as estimated by IBM and the Ponemon Institute's annual *Cost of a Data Breach Report 2021*, it is crucial for organizations to consider obtaining coverage for cyber incidents and to ensure that their policies account for the costs involved in incident response.[5]

> *"There are only two types of companies: those that have been hacked, and those that will be… even they are converging into one category: companies that have been hacked and will be hacked again."*
>
> Robert Mueller, Former FBI Director[6]

With this in mind, Deeth Williams Wall has prepared a checklist to assist your organization with the review of your cyber insurance coverage; each point is discussed in further detail below:

1. Assess your organization's exposure risk
2. Ensure your cyber insurance application is accurate and complete
3. Evaluate your existing coverage
4. Evaluate first-party and third-party coverage provisions
5. Consider vendor/subcontractor risks
6. Understand activation obligations
7. Identify exclusion clauses
8. Understand limitation of liability clauses
9. Understand insurer consent provisions
10. Be aware of situations *not* mentioned in the policy
11. Consider policy renewal provisions
12. Prepare a cyber response plan that aligns with your policy

[1] "The cost of ransomware in 2021: A country-by-country analysis" (27 April 2021), Emsisoft Malware Lab, online at: blog.emsisoft.com/en/38426/the-cost-of-ransomware-in-2021-a-country-by-country-analysis/.
[2] "Cyber Insurance Losses Spark Rate Increases" (26 May 2021), Fitch Ratings, online at: www.fitchratings.com/research/insurance/cyber-insurance-losses-spark-rate-increases-26-05-2021.
[3] *Ibid*.
[4] See *Family and Children's Services of Lanark, Leeds and Grenville v. Co-operators General Insurance Company*, 2021 ONCA 159 and *Future Electronics Inc. (Distribution) Pte Ltd. c. Chubb Insurance Company of Canada*, 2020 QCCS 3042.
[5] "How much does a data breach cost?" (28 July 2021), IBM, online at: www.ibm.com/security/data-breach.
[6] "Combating Threats in the Cyber World: Outsmarting Terrorists, Hackers, and Spies" (1 March 2012), Federal Bureau of Investigation, online at: archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies.

DWW's Twelve Takeaways

1. Assess your organization's exposure risk

In order to obtain cyber insurance coverage that best suits your organization, it may be necessary to assess your business, consider any risks of exposure, and consider the potential consequences of a cyber incident. For example, to obtain an accurate assessment of the risks that your organization may be exposed to, your organization may: (i) identify the information your organization handles, uses, and/or processes; (ii) determine how the information is protected or secured; (iii) identify the potential risks to the information; and (iv) learn about the legal obligations that may apply with respect to such information.

The level of coverage an organization requires can vary widely depending on the organization's assets, risks, confidentiality obligations, and other needs. Understanding this information can help your organization ensure that the risks identified are within the scope of the cyber policy you choose, and can help your organization decide on appropriate policy limits.

2. Ensure your cyber insurance application is accurate and complete

Cyber insurance applications vary in length and in the type of information requested. Your organization should be aware that incomplete, vague, or inaccurate answers to cyber insurance applications may delay the claim process or allow the insurer to deny coverage for claims.

Your organization may therefore wish to review any cyber insurance application(s) provided to your insurer(s) to ensure that the information set out in such application(s) is accurate and complete, particularly once the cyber insurance policy is up for renewal.

Organizations may also consider implementing periodic reviews of their cyber insurance application(s). The adoption of new technology or other business changes can introduce new risks to your organization that may not fall neatly within the scope of the most recent application for cyber insurance; these changes may potentially undermine coverage. Therefore, organizations should consider introducing checkpoints in their procurement and change management processes (or otherwise on a periodic basis). This will allow your organization to evaluate whether the newly adopted technology or other business changes require your cyber insurance application(s) to be updated.

Moving forward, organizations should have a clear understanding of the type of information required during the application process for cyber insurance so that future applications are completed thoroughly and accurately.

3. Evaluate your existing coverage

It is important to understand what coverage, if any, is available under your existing policies. Traditional or general insurance policies may contain broad language that appear to provide comprehensive coverage in the event of a cyberattack, but in reality, the coverage may be limited by certain data exclusion clauses or policy limits.

For example, some cyber policies may appear to provide coverage for cyber incidents that stem from the actions of the organization's employees. However, the policy may contain a specific

definition of "employee", which may not be consistent with the organization's normal understanding of the term. It is therefore important to understand the range of actors that your organization's insurance policy covers.

In addition, consistent with our discussion of cyber insurance applications above, your organization may wish to identify any new or existing gaps in your insurance coverage. For instance, cyber insurance policies obtained prior to the COVID-19 pandemic may not provide coverage for cyber incidents that stem from working remotely. If your organization has experienced significant changes in its business operations from the time of your insurance application, assessing whether such changes impact your cyber coverage will enable your organization to identify whether further steps are required to ensure that it has the coverage that it needs and that such coverage is not invalidated by the changes in your business.

4. Evaluate first-party and third-party coverage provisions

First-party cyber coverage can insure an organization for the damages that it suffers as a result of certain cyber events. First-party provisions may provide coverage for events such as:

- Ransomware attacks where your organization's data is being withheld;
- Attacks by malicious actors that result in any loss of your organization's data;
- Denial of service attacks;
- Accidental destruction of data caused by an employee or other member of your organization; and
- Natural events, such as storms, that result in damage to your organization's servers or computer hardware.

As each cyber insurance policy is unique, it is important to understand the specific first-party losses that are covered under your policy and assess whether the coverage adequately addresses your organization's needs, including whether the level of coverage is aligned with your organization's level of risk-exposure. This is further discussed below.

Third-party coverage can protect your organization if it is sued (or threatened to be sued) by a third party for the damages the third party suffered as a result of your organization's data breach or a cyberattack affecting your organization. Third-party cyber insurance provisions may cover losses arising from:

- Litigation claims brought by employees, customers, or third-party suppliers against your organization for damages suffered in a data breach;
- Claims alleging that your organization was negligent or breached the terms of a contract due to the occurrence of a cyber incident;
- Claims relating to libel, slander, or copyright infringement due to the occurrence of a cyber incident; and
- Fines imposed on a third party by a regulatory authority arising from a data breach for which your organization was responsible.

The Ontario Court of Appeal's recent decision in *Family and Children's Services of Lanark, Leeds and Grenville v. Co-operators General Insurance Company*, 2021 ONCA 159, (*Family and Children's Services of Lanark*), highlights the importance of obtaining adequate cyber

insurance coverage and demonstrates why both first-party and third-party provisions should be considered.

Family and Children's Services of Lanark, Leeds and Grenville ("FCS") suffered a data breach, whereby threat actors successfully exfiltrated and published online the personal information of 285 individuals. The affected individuals brought a $75 million class action lawsuit against FCS. FCS was insured by Co-operators General Insurance Company ("Co-operators") under their commercial general liability insurance and professional liability insurance policies, and commenced an action asserting that Co-operators had a duty to defend FCS against the class action.

Additionally, FCS initiated a claim for indemnity against its service provider, Laridae Communications Inc. ("Laridae"), for alleged breach of contract and negligence. Laridae was also insured by Co-operators and argued that Co-operators had a duty to defend it against FCS' claim.

Co-operators refused to defend either claim on the basis that each respective insurance policy included clauses that excluded coverage for claims arising from the "distribution or display of data". The Ontario Court of Appeal agreed with Co-operators, concluding that no duty to defend existed, as the claims fell under the unambiguous exclusion clauses within the insurance policies.

In these circumstances, FCS may have benefitted from proper first-party coverage, while Laridae may have benefitted from proper third-party coverage. This case illustrates the importance of: (i) obtaining cyber insurance that responds to your organization's needs, rather than relying on general insurance coverage; and (ii) understanding and obtaining the first-party and/or third-party cyber coverage that is appropriate for your organization.

5. Consider vendor/subcontractor risks

Many organizations outsource services such as website development, payment processing, data processing, and data storage to third-party vendors. However, not all cyber insurance policies protect against losses suffered due to the acts or omissions of your third-party vendors.

More organizations are now experiencing supply chain attacks, which occur when threat actors target the organization's third-party vendors and exploit the vendors' security vulnerabilities to gain access to the organization's systems and data. Symantec's *2019 Internet Security Threat Report* found that the occurrence of supply chain attacks increased by 78% in 2018.[7]

If your organization engages third-party vendors or subcontractors, or may do so in the future, you may wish to review your cyber insurance policy to ensure it provides coverage for claims that arise due to inadequate security practices or misconduct by one of your vendors or subcontractors. In these situations, you may also consider whether your vendors will engage their own supply chain in providing services to you, and if so, whether such sub-vendors will be covered under your cyber policy or if a specific endorsement or rider is required to ensure they are covered.

[7] "2019 Internet Security Threat Report" (February 2019), Symantec, online at: docs.broadcom.com/doc/istr-24-executive-summary-en.

6. Understand activation obligations

It is important to understand the timing and circumstances that will activate coverage under your cyber insurance policy. Some cyber insurance policies may require policy holders to submit a claim and wait for the claim to be approved by the insurer before providing any coverage. It is often critical that cyber incidents are responded to immediately, and organizations can inadvertently incur substantial non-recoverable expenses before they submit a claim to their insurer, or in the period of time after the claim is submitted but prior to the insurer's approval.

Consider the example of a cyber insurance policy where the insurer requires up to 48 hours to approve a claim, and coverage only begins once the claim has been approved. In this example, policy holders could be in the unnerving situation where they must decide between taking immediate measures to mitigate the cyber incident and bearing these costs, or decide to wait until the insurer provides approval that activates the cyber coverage.

It is therefore critical to understand what circumstances trigger coverage and whether there is a gap in coverage for expenses incurred prior to the insurer's approval, where such expenses may be non-recoverable by your organization.

7. Identify exclusion clauses

Your organization should understand the exclusion clauses outlined in your cyber insurance policy in order to minimize gaps in your cyber coverage and understand whether your organization may be subject to any residual risk. For example, some cyber policies may contain clauses that exclude coverage in scenarios involving losses related to:

- Cyber incidents that occur as a result of outdated software;
- Data breaches that occur in relation to unencrypted mobile devices and data;
- Decreased value in intellectual property due to cyber theft; and
- War or cyber operations carried out in the course of war.[8]

As previously mentioned, the Ontario Court of Appeal in *Family and Children's Services of Lanark* concluded that the insurer had no duty to defend either of the insured organizations due to exclusion clauses in the relevant insurance policies.

Similarly, in *Future Electronics Inc. (Distribution) Pte Ltd. c. Chubb Insurance Company of Canada*, 2020 QCCS 3042, (*Future Electronics*), an insured organization suffered approximately $2.7 million USD in losses as a result of a fraudulent scheme and tried to claim full indemnity for its losses under its crime insurance policy, asserting that the policy provided coverage for "Computer Fraud by a Third Party" or "Funds Transfer Fraud by a Third Party". However, the Québec Superior Court found that the losses did not fall under the coverage provisions, as coverage was limited by certain definitions and exclusions set out in the insurance policy.

It is therefore important to pay close attention to any exclusion clauses contained in a cyber policy, as such clauses may severely limit or completely exclude coverage in certain instances.

[8] In November 2021, Lloyds of London recommended four new model clauses to insurers for inclusion in their cyber insurance policies. The model "Cyber War and Cyber Operation Exclusion Clauses" can be found online at: www.lmalloyds.com/LMA/News/LMA_bulletins/LMA_Bulletins/LMA21-042-PD.aspx.

8. Understand limitation of liability clauses

The costs of a cyberattack are often substantial. It is therefore important that your organization is aware of the limits of the cyber insurance policy and that these amounts are in line with your organization's level of risk, risk-tolerance, and financial ability to withstand uninsurable expenses. Similarly, your organization should be aware of any sub-limits in the cyber insurance policy, which may specify a separate maximum amount to cover specific losses.

For example, in *Future Electronics*, discussed above, the insured organization suffered losses of nearly $2.7 million USD. However, the organization's insurance policy contained a sub-limit of $50,000 USD for incidents captured by the policy's "Social Engineering Fraud" endorsement. The Québec Superior Court found that the organization's losses resulted from an incident that fell squarely within the "Social Engineering Fraud" endorsement and concluded that the insurance coverage was therefore limited to $50,000 USD.

Any limits and sub-limits in a cyber policy should be carefully considered, as these could severely restrict the amount that your organization may claim in respect of certain losses.

9. Understand insurer consent provisions

Some cyber insurance policies may contain provisions that require policy holders to obtain consent from the insurer prior to taking certain actions or incurring certain expenses related to the cyber incident. For example, some policies may require your organization to obtain the insurer's consent before incurring expenses related to:

- The notification of third parties of the occurrence of a data breach;
- Investigating the cyber incident; or
- Actions to defend or prepare your organization against third-party claims relating to the cyber incident.

Additionally, some policies may require your organization to obtain consent or approval from the insurer prior to incurring any incident response expenses. Some provisions may also require your organization to only engage professionals (e.g., lawyers, breach coaches, forensic auditors, etc.) that are pre-approved or selected by the insurer. These provisions could mean that your organization's preferred incident response service providers would be acting outside the scope of your policy when responding to an otherwise insurable cyber incident.

Your organization may therefore consider developing an incident response plan that specifically incorporates such provisions. Alternatively, your organization may wish to negotiate, clarify, and/or remove such provisions if specified in the cyber insurance policy offered by your insurer. If such provisions cannot be removed from the policy, your organization may wish to ensure that the insurer's consent or approval must be provided promptly, and such consent or approval will not be unreasonably withheld.

10. Be aware of situations *not* mentioned in the policy

Insurance providers may be reluctant to fully indemnify you if the cyber incident is not expressly set out in your cyber policy. Before obtaining a cyber insurance policy, your organization should

determine whether there are any notable gaps in the coverage as stated, and ask for further clarification if any terms or events are missing or unclear.

For example, if your cyber insurance policy does not specifically address or outline coverage in the event of a ransomware attack, your organization may be left without recourse in the event that it experiences such an attack and pays a ransom amount.[9] Thus, it may be desirable for your organization to understand what cyber coverage will be provided in the event that a cyber incident occurs which has not been expressly set out within the policy.

Consider proactively asking your insurer for clarifications, and if necessary, require your insurer to amend the wording of the cyber policy to better suit your organization's needs. Being proactive can help ensure that your organization remains covered in the event that a cyber incident occurs.

11. Consider policy renewal provisions

As the cybersecurity landscape is rapidly evolving, your organization should consider actively reviewing its cyber insurance policy, particularly when it is up for renewal. Specifically, your organization may wish to be cautious of automatically renewing a cyber insurance policy without checking for changes to the policy provisions. For example, some policies may implement changes such as increased deductibles, new sub-limits, and/or co-insurance requirements. Reviewing the amendments to your policy will help you understand what changes may affect your organization during the policy period. It is also important to assess such changes in the context of the information provided in your policy application, and to ensure that your application remains current and accurate.

Your organization may also wish to inquire about the existence of any upgrades or add-ons to the policy. Lastly, your organization may wish to consider re-negotiating existing policy provisions in the event that significant gaps in coverage are identified, or if your organization's cyber insurance needs have changed.

12. Prepare a cyber response plan that aligns with your policy

Your cyber insurance policy is only one part of a comprehensive cyber preparedness strategy. Every organization should have a cyber incident response plan in place to respond to cyber threats and cyber-related losses. The contents of that plan must align with your cyber policy. In preparing or reviewing your cyber incident response plan:

(i) your organization should determine whether its cyber insurance policy(ies) require the organization to have a cyber incident response plan in place; and
(ii) if a cyber incident response plan is required by your insurer, your organization should confirm that it has implemented a cyber incident response plan, that the plan's

[9] Reuters has reported that some insurers have halved their coverage amounts due to the increase in ransomware attacks following the pandemic, and Lloyd's of London, which has around a fifth of the global cyber market, has discouraged its syndicate members from taking on cyber business in 2022. See "Insurers run from ransomware cover as losses mount" (19 November 2021), Reuters, online at: www.reuters.com/markets/europe/insurers-run-ransomware-cover-losses-mount-2021-11-19/.

provisions align with the requirements of the insurance policy(ies), and that the plan is reviewed and updated on a periodic basis, consistent with the policy(ies)' requirements.

For instance, some cyber policies require policy holders to have a general cyber preparedness strategy in place. Other cyber policies may outline specific requirements, such as requiring policy holders to update their software within 48 hours of the release of a new software patch. Policy holders could therefore unknowingly vitiate their cyber insurance coverage if they fail to implement the appropriate measures into their operational procedures.

Concluding Comments

> *"From cybercriminals holding our personal information for ransom, to state-sponsored actors threatening our critical infrastructure, the cyber threats Canadians face are increasing in sophistication and severity."*
>
> Scott Jones, Former Head of the Canadian Centre for Cyber Security[10]

The risks associated with cyberattacks are increasing, as are their consequences. The costs associated with responding to a cyber incident may vary greatly based on organization size and sensitivity of the information processed. However, these costs are almost always likely to be significant.[11] With these ever-present risks, it is vital for organizations to engage in comprehensive cyber preparedness, which includes obtaining cyber insurance.

If your organization has made the assessment to obtain cyber insurance, it is worth putting in the time to ensure that your organization obtains the right cyber insurance policy. The above checklist is designed to assist your organization in reviewing and obtaining cyber insurance, as such policies often vary widely in language and in the coverage provided.

However, obtaining cyber insurance is only one step in developing a comprehensive approach to cybersecurity for any organization. All organizations should take preparatory steps to anticipate and manage cybersecurity incidents, which can be formally incorporated into an incident response plan that aligns with your cyber policy.

Deeth Williams Wall is providing this Client Advisory as part of an ongoing series of advisories on cyber preparedness.

[10] "Canadian Centre for Cyber Security releases the Canadian National Cyber Threat Assessment 2020" (18 November 2020), Canadian Centre for Cyber Security, online at: cyber.gc.ca/en/news/canadian-centre-cyber-security-releases-canadian-national-cyber-threat-assessment-2020.
[11] "How much does a data breach cost?", *supra* note 5.