**CITATION**: Panasonic Canada Inc. v XL Specialty Insurance Company, 2025 ONSC 4407
**COURT FILE NO.:** CV-23-00708788-0000
**DATE:** 20250730



**ONTARIO**

**SUPERIOR COURT OF JUSTICE**

| | |
|---|---|
| **BETWEEN:** | |
| PANSONIC CANADA INC.<br>Applicant | *Jeffrey Brown and Dylan Cox,* lawyers for the Applicant |
| **– and –** | |
| XL SPECIALTY INSURANCE COMPANY<br>Respondent | *Marcus B. Snowden and Dean P. Barlett,* lawyers for the Respondent |
| | **HEARD:** June 24, 2025 |

**REASONS FOR DECISION**

APPLICATION UNDER RULE 14.05(3)(D) OF THE RULES OF CIVIL PROCEDURE, R.R.O. 1990, REG. 194

**LEIPER J.**

**Introduction**

[1] Panasonic Canada Inc.(“Panasonic”) brings this application for a declaration that its claim for indemnity under its insurance policy with XL Specialty Insurance Company, (“XL”) is subject to a $1.5 million USD retention. It also seeks coverage for the replacement laptops it purchased as a reasonable mitigation.

[2] XL contends that a $3 million USD retention applies to this claim because the claim involved a “ransomware event”. XL submits that a plain reading of Endorsement 23 of the policy sets a $3 million USD retention in the event of any claim that is connected to a ransomware event,

whether or not the claim for coverage is made under Endorsement 23. XL submits that the parties allocated risk in such events and their intentions are clear on reading the policy as a whole. Separately, XL contends that Panasonic has not established that purchasing new laptops was reasonable in the circumstances, and ought to have explored other cost-effective options such as leasing. Finally, XL seeks to have an exclusion in the policy apply.

[3] For the reasons that follow, I find that Panasonic has established its claim for coverage under the policy such that a retention of $1.5 million USD applies to its losses, which were relative to an attempt at cyber-extortion by a person or persons external to the organization, in a "ransom-ware" event. I conclude that XL has not met its onus to show that the limitation in the form of a higher retention amount of $3 million USD, applies in these circumstances. I conclude that the laptop purchases were reasonable and supported by the evidence. Finally, I would not give effect to the exclusion cited by XL.



**Background Facts**

[4] Panasonic sells technology products and services to businesses and consumers. It is an affiliate of Panasonic Corporation of North America ("PNA").

[5] On February 15, 2022 Panasonic learned that persons outside the company had obtained access to its network and placed malicious software (malware) throughout its computer network. This was accomplished by sending an infected file to one of Panasonic's employees. When the employee downloaded and opened the infected file at their workstation, the malware entered Panasonic's system network. The attackers then downloaded confidential and sensitive files from Panasonic's network which they posted online.

[6] Panasonic responded immediately. IBM X-Force IRIS security (IBM) assisted Panasonic to disconnect from the web and shutdown its systems. Panasonic hired several other external companies as follows:

a) Avasek Security to bring the Panasonic network back online and reconfigure devices.

b) Consilio to assist IBM with determining the scope of damage and how the cyber-attack occurred.

c) Stikeman Elliott LLP & Goodmans LLP (the Law Firms) were hired to give Panasonic legal advice on matters relating to the cyber-attack including a demand letter from a customer.

d) Kroll to communicate with individuals affected by the cyber-attack about the breach of the network.

e) Trans Union to provide monitoring services to alert individuals affected by the cyber-attack if their credit or identity information was compromised.

f) Professional Electronics was hired to clear a backlog of product returns caused by the cyber-attack.

g) Other external IFT consultants were hired to help rebuild the servers, applications, networks and virtual environments.



[7] The attacker(s) posted a message asking Panasonic to contact them. Panasonic's company policy is that it does not negotiate with attackers, thus it did not make contact nor did it pay any ransom.

[8] Panasonic also retained CYPHER, a company which specializes in responding to cyber-attackers for a consultation. Panasonic does not seek reimbursement for this amount in these proceedings.

[9] Panasonic mitigated the effects of the cyber attack on its business by fixing the damage to its network. Panasonic notes that it was obliged to do this under its insurance policy with XL which requires the insured "take all reasonable steps to… mitigate any "loss" …"

[10] The cost of these mitigation efforts to Panasonic included $109,800 CDN in overtime, and payments to PNA of $158,659 CDN.

[11] Once Panasonic brought its network back online, it then took steps to ensure that no infected computers would be reconnected to the repaired network to avoid reinfection. There were 69 Panasonic employees who used Citrix devices that have no hard drives. These employees needed new computers to carry out their work and to connect to the repaired network. A further 65 laptops were found to have been infected during the cyber-attack. Panasonic began purchasing replacement laptops in tranches, in parallel to the tasks of scanning and checking all of its devices.

[12] In total Panasonic purchased 140 new laptops with adapters and extended warranties. Its employees scanned over 500 laptops and desktops to clear the malware. By the end of that process, it was clear that 134 replacement units were required.

[13] Panasonic spent $242,000 CDN to purchase 140 new laptops. In addition to the dispute over the amount of retention that applies to the claim, XL secondarily submits that the cost of new laptops to replace older hardware would not be covered, because this a "betterment" in favour of Panasonic, not merely a cost to put it in the position that it was in prior to the cyber-attack.

[14] Panasonic also incurred the hosting costs in a parallel virtual environment on Amazon Web services servers. Panasonic maintained this parallel environment until the damaged servers could be remediated.

**The Insurance Policy**

[15] At the time of the cyber-attack Panasonic was insured by XL under an insurance policy. This policy came into effect on April 1, 2021 for a one-year period.

[16] The policy included several types of insurance coverage. Each coverage is subject to a "retention" which functions as a deductible.

**The Three Types of Coverage in the Policy**

**Third party liability coverage**

[17] Under the first type of coverage in the policy, third party liability coverage required XL to pay on Panasonic's behalf any "claim expenses" above the applicable retention amount. Panasonic became legally obliged to pay as the result of any third party claim based on allegations against the insured that they had committed either a "technology wrongful act" or a "privacy and security wrongful act".

[18] "Claim expenses" are defined in the policy to include legal fees incurred to investigate and defend against such a "claim."

[19] The parties agree that the July 2022 demand letter made by a Panasonic customer was such a "claim" and that the letter alleged a "technology wrongful act" and/or a "privacy wrongful act" by the insured, Panasonic. Accordingly, XL agreed that the amount paid to the law firms to respond to the demand letter was covered subject to the applicable retention amount.

**Data Breach Response and Crisis Management Coverage**

[20] The second type of insurance coverage provided by the policy was data breach response and crisis management coverage. This coverage required XL to reimburse Panasonic for certain "data breach response and crisis management costs" resulting from a "cyber security breach". These amounts were also subject to the applicable retention amount under the policy, which I discuss below.

[21] The parties agree that the cyber-attack in this case was a "cyber security breach" and a "data breach "as those terms are defined by the policy.

[22] The policy defines "data breach response and crisis management costs" as reasonable and necessary costs charged by breach response providers to:

a) determine the legal applicability of and actions necessary to respond to a "data breach reporting requirement" (as defined);

b) notify affected persons of a breach of personally identifiable information;

c) perform computer forensics to determine the existence cause and scope of the cyber-attack;

d) notify affected individuals regarding the cyber-attack;

e) operate a call centre;

f) provide credit or identity monitoring.

[23] Some of the external companies and individuals hired by Panasonic were on XL's preapproved panel of vendors. XL approved others subject to a rate cap. Those amounts payable are not in dispute.

**First Party Coverages**

[24] The final type of insurance provided under the policy was for "first party coverages". This part of the policy provides for three types of coverage as follows:

i. "Business interruption and extra expenses" which would cover Panasonic for any "extra expenses" incurred in excess of the applicable retention resulting from a "cyber security breach" that itself directly caused an interruption in Panasonic's business operations; The policy defines "extra expenses" as "Reasonable and necessary expenses, including payroll, in excess of the Insured's normal operating expenses which are incurred to reduce or avoid loss of business income and/or restore business operations."

ii. "Data recovery" insurance which required XL to reimburse Panasonic for data recovery expenses in excess of the applicable retention amount that resulted directly from a cyber security breach. The policy defines "data recovery expenses" as follows:

    a. reasonable and necessary costs incurred by [Panasonic]… The prior written consent of [XL]… Such consent not to be unreasonably withheld, to:

        1. determine whether damaged or destroyed computer programs, software or electronic data can be replaced, restored or repaired; and

        2. replace, re-create, restore or repair such damage or destroyed computer programs software or electronic data residing on the "network" substantially the form in which it existed immediately prior to {the cyberattack]…

iii. Endorsement 23, paragraph 3, which grants cyber-extortion coverage as follows:

> The Insurer will reimburse the Insured for cyber-extortion expenses in excess of the applicable retention that the Insured incurs directly resulting from and in response to a cyber-extortion threat." "Cyber-extortion expenses" are defined to include reasonable and necessary amounts paid to qualified third parties to facilitate or negotiate an actual payment by or on behalf of Panasonic to eliminate mitigate or remove a "cyber-extortion threat."

**Policy Retention (Deductible) Amounts: $1.5M unless Endorsement 23 terms apply**

[25] The insurance coverage provided under the policy is subject to a retention amount of $1.5 million USD, except for Endorsement 23 coverage, which provides for a $3 million USD retention.

[26] Section III(B)(1)(a) of the policy states that: "if more than a single retention applies… Then [Panasonic] … is responsible for paying the highest applicable retention.

[27] Panasonic's position is that its claim does not engage the higher retention amount under Endorsement 23 because it made no claim for coverage under Endorsement 23. XL submits that because Endorsement 23 sets out a definition of "ransomware event loss" which applies to the circumstances of this claim, any claim of involving a "ransomware event loss" under any part of the policy, not only under Endorsement 23, attracts the higher retention amount of $3 million USD.

[28] Endorsement 23 is important to the first issue in the dispute. For that reason, I set it out here in full:



**ENDORSEMENT #023**

This endorsement:
effective 12:01 a.m., April 1, 2021,
forms a part of Policy No. CTP0910005-03,
issued to PANASONIC CANADA INC.,
by XL SPECIALTY INSURANCE COMPANY.

THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY

**RANSOMWARE SUBLIMIT ENDORSEMENT**

In consideration of the premium charged, it is understood and agreed that the Policy is amended as follows:

1. The following Endorsement Schedule is added to the Policy:

**ENDORSEMENT SCHEDULE**

| COVERAGE | SUBLIMIT | CO-INSURANCE % | | RETENTION | WAITING PERIOD |
|---|---|---|---|---|---|
| | | INSURED | INSURER | | |

| | | | | | |
|---|---|---|---|---|---|
| Cyber-Extortion Reimbursement | $5,000,000 USD | 0% | 100% | $3,000,000 USD | N/A |
| Ransomware Event | $5,000,000 USD | 0% | 100% | $3,000,000 USD | 12 Hours |

2. Insuring Agreement I.B.3. Cyber-Extortion and Ransomware is deleted and replaced with the following:

   3. Cyber-Extortion Reimbursement

   The Insurer will reimburse the Insured for cyber-extortion expenses in excess of the applicable retention that the Insured incurs directly resulting from and in response to a cyber-extortion threat.

3. Definitions IV.H. Cyber-extortion Expenses is deleted and replaced with the following:

   H. Cyber-extortion Expenses

      1. Reasonable and necessary money, digital currency, property, or other consideration surrendered as payment by or on behalf of the Insured Company in order to eliminate, mitigate, or remove a cyber-extortion threat; and

      2. Reasonable and necessary amounts paid to qualified third parties to facilitate or negotiate an actual payment by or on behalf of the Insured Company as set forth in paragraph 1. of this definition, including any transaction or currency exchange fees.

   Amounts surrendered as payment will be deemed reasonable and necessary cyber-extortion expenses only when the Insured shows by clear evidence that the amounts surrendered plus any loss of business income and data recovery expenses otherwise covered by this Policy is materially and measurably less than the sum of any loss of business income and data recovery expenses that would have otherwise been covered by this Policy. The Insured must prepare and submit a complete and final proof of loss to the Insurer in conformance with Notice VI.E.1(b) Insured's Claim and First Party Incident Obligations of the Policy for the Insurer to evaluate coverage under this provision. In no event will the Insurer pay or commit to pay any cyber-extortion expenses before such amounts are actually paid by the Insured and submitted to the Insurer for reimbursement in conformance with this provision.

4. Definitions IV.I. Cyber-extortion Threat is deleted and replaced with following:

   1. Cyber-extortion Threat

Any threat communication from a third party or rogue employee related in any way to an actual or potential threat to start or continue to:

1. Disrupt the network to impair business operations of the Insured Company;

2. Alter, damage, or destroy data stored on the network;

3. Use the network to transmit malware to third parties;

4. Deface the Insured Company's website;

5. Access, release, or otherwise misuse data, including personally identifiable information, protected health information, or confidential business information, stored or previously stored on the network;

6. Refuse to return data stolen from the network;

7. Prevent access to the network or data by using encryption and withholding the decryption key; or

8. Disclose any fact relating to the foregoing to the public or to any third party

5. Solely for the purposes of this Endorsement, the following new definitions shall apply:

- Threat Communication

A threat made demanding or seeking payment and/or other consideration in exchange for, or in connection with, the prevention, elimination, mitigation or removal of a threat against the Insured or any communications intended to initiate such communications with the Insured.

- Ransomware Event Loss

Any and all loss for, arising out of, in connection with, or in any way involving a cyber-extortion threat, regardless whether such loss consists of damages, claim expenses, regulatory damages, first party costs, or any other amounts paid by the Insurer under the Policy.

6. The Insurer's obligation to pay cyber-extortion expenses shall not exceed the Cyber-Extortion Reimbursement Sublimit set forth in the Endorsement Schedule. The Cyber-Extortion Reimbursement Sublimit shall be the Insurer's maximum liability for all cyber-extortion expenses for which this Policy affords coverage under any insuring

agreement and is part of, and not in addition to, the limit(s) of liability applicable under any other of the Policy's insuring agreements or applicable aggregate limit(s). The Cyber-Extortion Reimbursement Sublimit shall apply regardless of the number of cyber-extortion threats. No amount constituting cyber-extortion expenses as defined in this endorsement shall be afforded coverage under any other insuring agreement or provision of this Policy, including, but not limited to, as extra expenses or data recovery expenses. Coverage for all loss included within the definition of cyber-extortion expenses set forth above shall be available solely and exclusively under Insuring Agreement 1.B.3. as amended in this endorsement and shall be subject to the Cyber-Extortion Reimbursement Sublimit and Cyber-Extortion Coinsurance Percentage set forth in the Endorsement Schedule.

7. For any cyber-extortion expenses in excess of the highest applicable retention, the Insured shall be responsible for payment of the Cyber-Extortion Coinsurance Percentage set forth in the Endorsement Schedule of otherwise covered cyber-extortion expenses, and the Insurer shall pay only the remaining Insurer Percentage set forth in the Endorsement Schedule of any cyber-extortion expenses. Payment by the Insured of the Cyber-Extortion Coinsurance Percentage of such loss will not reduce the Cyber Extortion Sublimit or any other limit under the Policy. Only the Insurer Percentage set forth in the Endorsement Schedule of cyber-extortion expenses paid by the Insurer may erode and/or exhaust the Cyber-Extortion Reimbursement Sublimit. The Cyber-Extortion Coinsurance Percentage of cyber-extortion expenses shall remain uninsured and borne solely by the Insured at its own risk. The Cyber-Extortion Reimbursement Sublimit is part of, and not in addition to, the Ransomware Event Sublimit.

8. The Insurer is liable only for that portion of cyber-extortion expenses in excess of the Cyber-Extortion Retention amount set forth in the Endorsement Schedule. The Cyber-Extortion Retention shall remain uninsured and borne solely by the Insured at its own risk. The Cyber-Extortion Retention will be separate from any other retentions in the Policy applicable to cyber extortion expenses for which this Policy provides coverage, provided that if more than a single retention applies to a claim and/or first party incident, then the Insured is responsible for paying only the highest applicable retention.

9. The Insurer's obligation to pay ransomware event loss shall not exceed the Ransomware Event Sublimit set forth in the Endorsement Schedule. The Ransomware Event Sublimit shall be the Insurer's maximum liability for all ransomware event loss for which this Policy affords coverage under any insuring agreement and is part of, and not in addition to, the limit(s) of liability applicable under any other of the Policy's insuring agreements or applicable aggregate limit(s). The Ransomware Event Sublimit shall apply regardless of the number of cyber extortion threats, claims, first party incidents, or other events for which coverage may apply under any of the Policy's Insuring Agreements. The Cyber-Extortion Reimbursement Sublimit is part of, and not in addition to, the Ransomware Event Sublimit.

10. For any ransomware event loss other than cyber-extortion expenses in excess of the highest applicable retention, the Insured shall be responsible for payment of the Ransomware Event Coinsurance Percentage set forth in the Endorsement Schedule of otherwise covered ransomware event loss, and the Insurer shall pay only the Insurer Percentage set forth in the Endorsement Schedule of any ransomware event loss. Payment by the Insured of the Ransomware Event Coinsurance Percentage of such loss will not reduce the Ransomware Event Sublimit or any other limit under the Policy. Only the Insurer Percentage set forth in the Endorsement Schedule of ransomware event loss and any other ransomware event loss paid by the Insurer may erode and/or exhaust the Ransomware Event Sublimit. The Ransomware Event Coinsurance Percentage of ransomware event loss shall remain uninsured and borne solely by the Insured at its own risk.

11. The Insurer is liable only for that portion of ransomware event loss other than cyber-extortion expenses in excess of the Ransomware Event Retention amount set forth in the Endorsement Schedule. The Ransomware Event Retention shall remain uninsured and borne solely by the Insured at its own risk. The Ransomware Event Retention will be separate from any other retentions in the Policy applicable to ransomware event loss for which this Policy provides coverage, provided that if more than a single retention applies to a claim and/or first party incident, then the Insured is responsible for paying only the highest applicable retention.

12. Solely in connection with any ransomware event loss, Definition IV.AAA. Waiting Period of the Policy is replaced by the Ransomware Event Waiting Period set forth in the Endorsement Schedule.

13. The provisions of this Endorsement, including the relevant Cyber-Extortion Reimbursement Sublimit, CyberExtortion Coinsurance Percentage, Cyber-Extortion Retention, Ransomware Event Sublimit, Ransomware Event Coinsurance Percentage, Ransomware Event Retention, and Ransomware Event Waiting Period shall apply regardless whether any other cause or event contributes concurrently or in any sequence to any portion of cyber-extortion expenses or ransomware event loss.

14. Should the Insurer determine, in its sole discretion, that payment of any ransomware event loss might conflict with applicable laws or regulations (including but not limited to any Canadian, U.S. or foreign trade or economic sanctions laws or regulations), the Insurer has the right, but not the obligation, to seek relief or guidance from an appropriate regulatory authority or court of competent jurisdiction before it will pay any such ransomware event loss. If the Insurer exercises such right, payment for any ransomware event loss will not become due until thirty (30) days after payment of such ransomware event loss has been authorized by such regulatory authority or court or such additional time that the Insurer may reasonably require. Condition IX.K, Alternative Dispute Resolution, of this Policy shall not apply to or impair the rights of the Insurer as set forth in this paragraph.

15. To the extent any provision contained in this Endorsement is deemed inconsistent with any other provision of this Policy, the provisions of this Endorsement shall control.

All other terms and conditions of this Policy shall remain the same.



**The claim and XL's response**

[29] On February 22, 2022, Panasonic's insurance broker, Aon, reported the cyber-attack to XL. During July 2022, the manager for XL's North America cyber incident response team sent letters with XL's position on coverage.

[30] XL took the position that the claim engaged the third party liability coverage, data breach response and crisis management coverage, as well as first party coverage under Endorsement 23. As a result, XL asserted that the $3 million USD retention applied to any claims for payment under the policy.

[31] On August 8, 2022, Panasonic sent proof of loss with a cost tracker for Panasonic's claim. Panasonic reserved the right to update its proof of loss cost tracker. Panasonic also noted that it had never contacted the person or persons who committed the cyber-attack or paid a ransom.

[32] On May 8, 2023, Panasonic's coverage counsel Jeffrey Brown wrote to XL to advise that further to Panasonic's ongoing reservation of its rights, the company was updating its coverage claim and removing the amount paid to CYPHER for consultation regarding the attacker.

[33] Mr. Brown explains that in the circumstances, the only retention applicable to his client's claim was of the claims was covered under the insuring agreements without engaging Endorsement 23.

[34] On May 19, 2023, XL's coverage counsel wrote to Mr. Brown, asserting that even if Panasonic withdrew its claim for costs paid to CYPHER, the applicable retention was $3 million USD. Coverage counsel also said that Panasonic could not withdraw any prior claim under Endorsement 23.

[35] On this Application, counsel to XL does not press that position, but instead submits that the definition of "ransomware event loss" and the retention amount in Endorsement 23 apply to the whole policy and to any coverage sought by Panasonic for "ransomware event losses".

[36] In argument, counsel for Panasonic agreed that the incident involved fits the definition in paragraph 5 of Endorsement 23, that is it involves a "ransomware event loss" which is "Any and all loss for, arising out of, in connection with, or in any way involving a cyber-extortion threat, regardless whether such loss consists of damages, claim expenses, regulatory damages, first party costs, or any other amounts paid by the Insurer under the Policy." Counsel for Panasonic agreed that while the chart in Endorsement 23 appears to set out policy claim limits for both cyber extortion reimbursement (which it neither paid, nor sought coverage for) and for a "ransomware event loss", there are no words in Endorsement 23 which actually grant coverage for a ransomware event loss.

[37] Counsel for Panasonic submits that because paragraph 5 begins with the phrase, “Solely for the purposes of the Endorsement” this means that the ransomware event losses described in paragraph 5, apply only to the various limits and prescriptions in Endorsement 23.

[38] I discuss this position, and XL’s in response, in the analysis of the issues, below.

**The Expert Evidence Tendered by XL and the Preliminary Issue of Admissibility**

[39] In preparation for this application, XL retained David Youssef, managing Director of cybersecurity at FTI Consulting to provide an opinion on the nature of the incident that led to the claim. Mr. Youssef has 18 years of cybersecurity and cyber incident response experience.

[40] Mr. Youssef reviewed the affidavits filed on this application and conducted his own research. XL summarizes his expert opinion as bearing on the meaning of certain terms in the insurance policy, whether the incident gave rise to a “cyber-extortion threat” and his knowledge information of a hacker group known as “Conti” which has used similar methods to that employed here.

[41] Panasonic submitted that this evidence is not admissible because it is not necessary to assist the finder of fact in an application concerning the contractual interpretation of an insurance policy.

[42] XL submits that Mr. Youssef’s report is relevant to establish a fact in issue, namely the nature of the incident and whether it was a “ransomware attack” as that term is commonly understood in the cybersecurity industry. XL submits that I apply the rationale in *Workman Optometry Professional Corporation v. Certas Home and Auto Insurance Company,* 2023 ONSC 3356 (CanLII), aff’d 2024 ONCA 479 (CanLII), at paras 62–66.

[43] I disagree. First, it is not a matter of specialized knowledge that a person who obtains something valuable to another and seeks money for its safe return is engaged in a practice that is fairly described as holding something or someone for “ransom,” a term that is not technical but part of the English language. Second, merely because this is in the information technology environment, meaning that the term “ransomware” is used, does not require opinion evidence. The policy itself describes a “ransomware event loss”, and connects such losses to a cyber-extortion threat, which is in turn comprehensively described in Endorsement 23, reproduced above. This is a matter of reading, not expert evidence.

[44] Third, I distinguish the nature of the evidence tendered in *Workman Optometry* from that in this case. In *Workman Optometry*, the expert evidence concerned how viruses interact with inanimate surfaces, a matter demonstrably outside the expertise of a judge.

[45] Finally, the *concession* made by counsel to Panasonic that its claim arises from what can be described as a ransomware event means that this evidence is unnecessary.

[46] The issues on this application are squarely within the competence of a judge: to interpret an insurance policy in accordance with the case law and the principles that have been well established by the Supreme Court of Canda.

[47] I decline to admit the evidence of Mr. Youssef.

**Issues**

[48] The first issue on this application is whether Panasonic's coverage claim attracts the retention rate for ransomware event losses described in Endorsement 23 which is $3 million USD.

[49] The second issue is whether the policy covers Panasonic's claim for 140 new laptops, adapters and warranties.

[50] The third issue is whether the property damage exclusion in the insurance policy applies to limit coverage.

**Legal Framework**
**Principles of Policy Interpretation**

[51] The court interprets insurance policies by reading the policy language as a whole. Where the language is clear and unambiguous, the court will give effect to the policy and apply any definitions agreed upon by the parties: *Ledcor Construction v. Northbridge Indemnity Insurance,* 2016 SCC 37 at paras. 49-51; S*urespan Structures Ltd. v. Lloyds Underwriters*, 2021 BCCA 65 at paras 40-42.

[52] Words in the policy that are not defined are construed as they would be understood by the "average person applying for insurance": *Sabean v. Portage La Prairie Mutual Insurance Company*, 2017 SCC 7 at paras. 4, 13.

[53] If the language of the policy is unclear, the court will employ the rules of contract interpretation. The court looks to the shared reasonable expectations of the parties to aid in the interpretation of ambiguous wording, provided that such an interpretation is supported by the language in the policy: *Ledcor* at para. 50.

[54] If ambiguity remains, then the court will apply the *contra proferentum* rule and construe any ambiguity against the insurer.

[55] At the stage where a grant of coverage is in issue, the insured party bears the burden of proving that its claim is covered: *Ledcor* at paras 51-52.

[56] If the insured establishes coverage, then the onus shifts to the insurer to establish that there is an exclusion of coverage. If no policy exclusion applies, the insured's claim is covered: *Ledcor* at paras. 51-52.

[57] In *PCL Constructors Westcoast v. RSA*, the court applied these principles to determine that the insurer was required to establish a higher deductible, given that it functions as a limitation on coverage: *PCL Constructors Westcoast Inc.* v. *Royal & Sun Alliance Insurance Company of Canada*, 2019 BCSC 822 at paras. 31-32.

**Analysis of the Issues**

**Does Panasonic's coverage claim attract the $3 million USD retention rate for ransomware event losses as described in Endorsement 23?**

[58] XL submits that Endorsement 23 applies to the entire policy, thus Panasonic's claim under the parts of the policy outside of Endorsement 23, are nevertheless subject to the higher retention amount, because they involve "ransomware event losses".

[59] As I understand their position, XL is not arguing that Panasonic could or was required to seek coverage for their losses under Endorsement 23. This is consistent with the wording of Endorsement 23, which only has an explicit grant of coverage for cyber extortion reimbursement, which was not paid here to the cyber attacker(s). The parties agree, as do I, that had Panasonic done so, the grant of coverage for payment of a ransom to the cyber attacker(s) would have been subject to the retention amount of $3 million USD, on the clear wording of Endorsement 23.

[60] Turning back to the plain language of the ransomware event losses, notably the definitions in paragraph 5 of Endorsement 23, paragraph 5 reads

> Solely for the purposes of this Endorsement, the following new definitions shall apply:
>
> Threat Communication
>
> A threat made demanding or seeking payment and/or other consideration in exchange for, or in connection with, the prevention, elimination, mitigation or removal of a threat against the Insured or any communications intended to initiate such communications with the Insured.
>
> Ransomware Event Loss
>
> Any and all loss for, arising out of, in connection with, or in any way involving a cyber-extortion threat, regardless whether such loss consists of damages, claim expenses, regulatory damages, first party costs, or any other amounts paid by the Insurer under the Policy.

[61] I give effect to the clear language in paragraph 5, that these definitions are "Solely for the purposes of this Endorsement". This is not ambiguous. This means that these definitions apply "solely" for the purposes of Endorsement 23.

[62] Panasonic did not look to Endorsement 23 for their grant of coverage for attack that led to their losses. Thus, one must look to the language in the balance of the policy to assess the availability of coverage.

[63] In each of the claimed areas, the lower retention rate applies. Panasonic opted to make no claim for any expenses that might be also covered under Endorsement 23, and there is nothing in

the policy or the Endorsement that requires that they have recourse to Endorsement 23 only, in the event of a "threat communication", a "ransomware event loss" or "attempted cyber-extortion."

[64] In the context of motor vehicle claims, the choice of an insured to make a claim that is more advantageous to themselves and their family members, absent a clear limitation from doing so in the policy, is theirs to make: *Gostick (Litigation Guardian of) v. Squance Estate*, 2006 CanLII 31019 (ONSC) at paras. 1-3, 5, 6, 7-10, 13, -23, 27, 29, 31; *Gostick (Litigation Guardian of) v. Squance Estate,* 2007 ONCA 674 at paras. 5, 10, 23, 25-26, 36.

[65] On the definitions in the main part of the policy, Panasonic suffered a "First party incident" which is defined as a "cyber security breach, cyber extortion threat or data breach. It claimed for its expense under the provisions for variously, third party liability coverage, data breach response and crisis management costs" resulting from a "cyber security breach" and under the provisions for first party coverage under the headings of "Business interruption and extra expenses" and "data recovery."

[66] I find that these coverages attract a retention amount of $1.5 million USD. Endorsement 23 does not apply to these grants of coverage and thus neither does the higher retention amount of $3 million USD.

**Does Panasonic's claim for the replacement laptops fit within the coverage provisions of the policy?**

[67] XL takes the position that Panasonic should not be reimbursed for purchasing replacement laptops, complete with extended warranties, because this amounts to a "betterment not reasonably envisioned by the time-limited scope of extra expense coverage."

[68] Certainly, the parties can contract in such a way that "betterment" outcomes can be accounted for in the policy: *Bell Pole Co v. Commonwealth Insurance Co.*, 2003 BCCA 7 at para 40.

[69] There is no such accounting in the extra expense coverage in this policy. To trigger this coverage, Panasonic was required to establish that the costs incurred were "reasonable and necessary" and incurred during the "period of restoration".

[70] XL argues that during the "period of restoration", the policy contemplates that the insured will lease computers owned by third parties, not purchase permanent replacement devices. The policy does not impose such a limitation.

[71] The evidence tendered in this application by Panasonic establishes the new laptops were "commercially equivalent" to the old laptops. The affidavit in support from Ms. Oehrlein sets out in detail the steps that Panasonic took to identify which computers were compromised. She describes the 69 Panasonic employees using Citrix devices that could not access the Panasonic network for months until it could repair the damage to the network caused by the cyber-attack. Her evidence establishes that these employees needed new laptops immediately.

[72] The uncontradicted evidence tendered from Ms. Oehrlein was that Panasonic secured the lowest price for new laptops that its vendor was willing to offer. It purchased extended warranties because this was standard Panasonic operating procedure to ensure that the company received a sufficient return on its investment.

[73] Ms. Oehrlein detailed how the alternatives would not have been cost effective or efficient, and thus were not reasonable. For example, in her evidence, replacing only the hard drives would have been a time-consuming process that would have likely delayed the resolution of the cyber-attack, among other negative consequences, including a greater negative financial impact on Panasonic.

[74] XL did not tender evidence to show that leasing this number of laptops would have been less expensive, and thus a more reasonable alternative to purchasing new laptops.

[75] Panasonic purchased its laptops in tranches, in parallel with scanning the existing hardware to ensure it had detected all of the defective stock. All told, it needed to replace 134 laptops, and it purchased 140.

[76] I accept that the cost of 134 laptops, with adapters and warranties was "reasonable and necessary" and contemplated by the policy. I find in favour of Panasonic in this regard.

**Does the Property Damage Exclusion Apply in these Circumstances?**

[77] Finally, XL argues that Panasonic's laptop claim is excluded because the policy's property damage exclusion applies. To establish that the exclusion applies, XL must prove that the "first party incident" (i.e., the "cyber security breach") arose out of "property damage". On the facts of this incident, XL is not able to do so.

[78] The cyber-attacker(s) breached Panasonic's network by sending a Panasonic employee an Excel file created by the cyber-attacker, on February 2, 2022. Once that file was downloaded, the cyber-attacker(s) gained access to the employee's workstation.

[79] Once they had access to this workstation, the attacker(s) accessed Panasonic's network. On February 16, 2022, two weeks after obtaining access, the cyber-attacker(s) attempted to deploy the ransomware. The network breach had already happened.

[80] Thus, the network breach preceded the damage (i.e., the ransomware infection)., rather than the reverse, which is the language of the exclusion. The breach must be caused by the property damage to trigger the exclusion.

[81] I find that XL has not shown that the exclusion for property damage applies in the circumstances of the case at bar.

**Conclusion**

[82] I find in favour of Panasonic on this Application, save for the additional 6 laptops that were not shown to be “reasonable and necessary.”

[83] The parties have advised me that they have agreed on damages and on costs. They may provide an order in accordance with these reasons for signature.

Leiper, J.

**Released:** July 30, 2025

**CITATION**: Panasonic Canada Inc. v XL Specialty Insurance Company, 2025 ONSC 4407
**COURT FILE NO.:** CV-23-00708788-0000
**DATE:** 20250730

**ONTARIO SUPERIOR COURT OF JUSTICE**

**B E T W E E N:**

PANSONIC CANADA INC.

Applicant

**– and –**

XL SPECIALTY INSURANCE COMPANY

Respondent

---

**REASONS FOR DECISION**

---

Leiper, J.

**Released:** July 30, 2025