RISK NOTE

Cyber Risk FAQs

Q.1 What is Cyber Risk?

According to the Institute of Risk Management, cyber risk means "any risk of financial loss, disruption or damage to the reputation of an organisation from some sort of failure of its information technology systems."[1] This includes computer networks, electronic data, and mobile devices.

Q.2 What does Cyber Risk Insurance Cover?

Cyber risk insurance covers costs related to data breaches or cyber-attacks caused by crimes such as phishing, malware, ransomware, identity theft and fraud. These attacks and breaches can lead to the release of confidential information and cause significant disruption and reputational damage to an organization. Cyber risk insurance can cover first party losses for costs incurred in dealing with the breach such as business interruption, IT damage, cyber extortion, ransom payments, IT forensics, data restoration and ransomware negotiation. It can also cover legal expenses, fines, and defence costs including settlement of third-party losses such as libel, slander and intellectual property rights infringement.

Q.3 Does HCPP provide Cyber Risk Insurance?

No, HCPP does not generally respond to cover cyber risk.

While cyber risk losses are largely managed and paid for by Health Authorities, HCPP does offer Limited Social Engineering Fraud Coverage under crime coverage for a limit of $100,000. Terms and conditions apply. For further details please refer to HCPP's Social Engineering Program Bulletin.[2]

Q. 4 Why does HCPP not provide Cyber Risk Insurance?

The decision not to provide cyber risk insurance is the position taken by the Risk Management Branch (RMB) and this decision is not unique to the publicly funded health sector. RMB undertook a cross-sector client consultation and in-depth analysis of cyber risk

[1] https://www.theirm.org/what-we-say/thought-leadership/cyber-risk/
[2] Program Bulletins | British Columbia Health Care Protection Program (login required)

insurance products available in the commercial insurance markets. It was determined that the coverage is expensive, and many clients would not be able to meet the rigorous underwriting processes of commercial insurers. To minimize exposure commercial insurers were carefully selecting what is insurable, restricting coverage limits, imposing high deductibles, warranties and exclusions and charging high rates. Cyber risk is evolving at a fast rate. Traditional 'cyber' coverage agreements were not written to cover cyber risks that have evolved. Many Health Care Agencies (HCAs) were also concerned with only some elements of cyber risk and did not require a full spectrum of cyber coverage. Not much has changed with how cyber risk insurance is handled in the open and specialized markets.

Q.5 How does HCPP help protect HCAs from cyber risk?

The province utilizes various corporate supply arrangements (CSAs) as part of its mitigation strategies. Rather than providing coverage via the various self insurance programs, RMB instead offers broader public sector entities with access to these CSAs. HCAs can purchase CSAs according to each organization's needs where funds can be directed to cyber risk mitigation rather than the purchase of cyber risk insurance in commercial markets. Given the high cost of cyber risk coverage, the variations in wordings, exclusions and warranties, and high deductibles; funds are likely better directed towards mitigation through internal cyber risk management rather than the purchase of commercial cyber risk insurance.

Q.6 How to Purchase Corporate Supply Arrangements (CSAs)

For managing cyber risks, HCAs have the option to purchase "cyber security" (IM/IT) risk management services direct from pre-selected vendors. Access to these services is via the Province of BC's Corporate Supply Arrangements which are available to all public sector organizations. These CSAs can assist HCAs in building, assessing, validating, or improving its information systems and effective cybersecurity practices. These may include an assessment of an existing system or architecture, the development of security policies and procedures, recommendations and guidelines, and identification of threats or vulnerabilities. The CSAs are currently available for the following IM/IT services:

- Firewall Advisory Services
- Public Key Infrastructure Advisory Services
- Identity and Access Management Advisory Services
- Security Advisory Services
- Security Awareness Advisory Services
- Security Governance Advisory Services
- Security Incident and Event Management Advisory Services
- Web Vulnerability Scanning Advisory Services

- Mobile Application Security Testing Advisory Services
- Penetration Testing Advisory Services
- Security Threat and Risk Assessment Advisory Services
- Security Incident Response Advisory Services

The CSAs are an open framework where services can be added / updated at any point in time. Please visit the following Province of BC website for the most up to date services catalogue and detailed guidance on what the above services entail:

https://www2.gov.bc.ca/gov/content/bc-procurement-resources/buy-for-government/goods-and-services-catalogue/im-it-security-services

To access Vendor pricing on the CSA (locked down on the public website as pricing is confidential), registration is required. There are two steps required to receive direct access which are outlined at the following website:

https://www2.gov.bc.ca/gov/content/bc-procurement-resources/buy-for-government/goods-and-services-catalogue/access-pricing

Q.7 When should HCAs require Cyber Risk Insurance from their contracted parties?

When HCAs enter a contract, we recommend including insurance requirements for the other party to obtain cyber risk insurance when:

- Other party will store your confidential data such as personal information of patients or others or sensitive information on their proprietary software. (e.g. employee personal information, proprietary information, legal documents, etc.).
- Other party is integrating their software with yours and confidential data may be accessed
- There may be exceptions dependent upon actual risk exposures. Please contact HCPP for consultation if necessary

When HCAs require a contractor to carry cyber risk coverage, we recommend the following language:

"Computer Security and Privacy Liability in an amount not less than <$fill-in> inclusive per claim and in the aggregate insuring against errors or omissions in the Contractor's performance of the Services including, without limitation, unauthorized use/access of a computer system, defense of a regulatory action involving a breach of privacy, failure to protect confidential or personal information from disclosure, and notification costs whether or not required by statute, and including:

i. the HCA as an additional insured to the full extent of coverage provided, but only with respect to liability arising out of the Contractor's performance of this Agreement;
ii. a cross-liability clause; and
ii. an endorsement to provide thirty (30) days prior written notice of reduction in limits, cancellation or non-renewal, or any adverse material change.

If this insurance is provided on a claims-made basis, the policy must include an extended reporting period of not less than two years with respect to events which occurred but were not reported during the term of the policy."

The recommended limit depends on the details of the service or product. Generally, $1,000,000 to $2,000,000 limits are acceptable.

Q.8 What can HCAs do to reduce cyber risk exposures?

Undertaking a robust risk assessment such as security threat risk assessment (STRA) and developing defensible security will help to pinpoint and reduce cyber risk exposures.

Q. 9 What is STRA?

STRA is a process that can help determine potential cyber vulnerabilities within an organization. This in turn will help HCAs make well informed risk-based decisions about cyber security and implement strategies to mitigate these risks. The key components of a STRA are as follows:

1) Identify potential cyber-related threats before they occur
2) Assess vulnerabilities that could enable these threats
3) Rate the vulnerabilities on the likelihood of them occurring and the potential impact on the organization
4) Develop a risk treatment plan and mitigation strategies
5) Document, track and follow-up on the treatment plan

More information on STRA can be found at the following BC Government website:

https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/security-threat-and-risk-assessment

Q. 10 What is Defensible Security?

No organization is immune to cyberattacks. Organizations must be able to prevent the majority of attacks, detect them, and respond. One way to do this is by establishing Defensible Security. Defensible Security is a series of controls you can use to help support your security program, such as access control and incident management. It helps organizations know what they need to be doing at a minimum to achieve security posture that is defensible.

The Defensible Security Manual developed by the BC Government OCIO can be found here:

https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/defensible-security

Q.11 What can HCAs do when asked to insure against Cyber Risk?

Sometimes other parties insist on HCAs obtaining cyber risk insurance. If this is the case, we recommend taking a risk-based approach in negotiations:

- Decide if the ask is reasonable. Are you providing a software or IT data storage service where the system(s) you provide could be breached by a cyber-attack? Is the data you are storing for the other party sensitive in nature?
- Are there mitigation strategies in place already to reduce HCA cyber risk exposures such as firewalls, IT upgrades, virus detections, security schedules, etc. If so, these mitigation strategies can be used in negotiations.
- Some cyber losses are "uninsurable" or exceed what is reasonably available. Consider if it is even possible to obtain the type of cyber risk coverage the other party is requesting. For example, cyber related claims stemming from human error or negligence, pre-existing vulnerabilities, internal breaches, world cyber attacks, or data loss are not widely available.

If obliged to purchase cyber risk insurance, HCA can investigate commercial insurance options with a licensed insurance broker. HCPP can assist in evaluations of the broker's proposals.

In summary, cyber risk is a complex and rapidly evolving risk exposure for all individuals and corporations globally. Insurance markets are also varied, and coverage is not

consistent across the commercial insurance industry. Careful assessment and consideration are important when managing cyber risk exposures and the focus for HCAs should be on cyber risk mitigation strategies.

Created August 2025

Published by the Health Care Protection Program