Business interruption and cyber insurance: What's covered after a cyber attack?

September 13, 2022

*This is part one in a three-part series. Check out part two for **examples of cyber insurance exclusions** (plus insight into how insurers and insureds usually negotiate these issues) and part three for **how to lower your cyber insurance costs**.*

Fires. Floods. Labour disputes. Vandalism. Civil unrest. Regulatory changes. These are the usual suspects when it comes to causes of business interruption, but ever since Captain Zap's infamous 1981 hack into AT&T's network, cyber crime has become an important addition to the list. If your business has been hit, there's no time to waste – so here are the need-to-knows about business interruption coverage and your cyber insurance policy, including four scenarios that present coverage challenges.

Business interruption coverage in a cyber policy

Business interruption coverage eases the financial pain experienced by an organization that is unable to operate normally following a cyber attack. An important point: not all cyber insurance policies include business interruption coverage. For policies that do, typical coverages include lost income and extra expenses incurred to get the business up and running.

The organization, of course, must have experienced a disruption or incurred additional expenses in order for the business interruption coverage to be triggered – and this is where organizations and insurance companies often disagree. The rest of this article explores four common situations that result in complex business interruption claims.

New requirements from integrated partners

When an organization is impacted by a cyberattack, its integrated partners – third parties that maintain the organization's electronic medical records or leads databases, for example – often take a hard look at their own cybersecurity. If the partners' standards increase, the organization that suffered the attack may need to improve its security before being given the keys to the systems again.

Organizations usually expect that expenses related to their integrated partners' demands will be eligible for business interruption coverage under their cyber insurance policy. From the insurer's perspective, though, coverage is meant to return an organization to its original state, not pay for improvements. This type of claim is often denied and, in our experience, the ensuing dispute often goes to mediation.

Regular salaries and wages

When it comes to business interruption expenses related to labour, insurance companies usually require evidence that the organization's costs increased due to post-attack remediation efforts. Costs for new staff or consultants brought on to rebuild the organization's systems often qualify. So do overtime costs incurred by current employees. The regular salaries of existing employees who have been reassigned to restoration efforts during normal business hours are rarely covered.

Delays in sales or payments

The business interruption coverage in most cyber insurance policies will cover lost sales – those that could never be completed due to the security or privacy breach – but not sales that were simply delayed until systems were back online. If a customer or client can initiate, continue or complete a sale using approaches that weren't affected by the breach (think using the telephone, visiting a brick-and-mortar location, and putting a credit card in an old school manual credit card machine), the delay is not usually eligible for inclusion in the claim.

Excessive ransom demands

Many organizations are keen to pay a ransom as a way to return to normal business operations immediately. Some insurers, however, require some due diligence before authorizing a payment. They often encourage the insured to compare the cost to rebuild systems from backups plus the cost of projected business interruption expenses to the amount demanded by the attackers. Since most policies require insurer consent before a ransom payment can be made, insurers will often ask insureds to take a hard look at whether:

- The organization can operate, even at a reduced level, while its systems are restored
- The rebuild can be done relatively quickly
- The ransom is greater than the anticipated business interruption claim.

Your next steps

Cyber insurance is complicated. And it's getting more expensive. If time is on your side, one of the best things you can do is review your policy with an experienced cyber insurance broker to ensure your coverage matches your business situation. (A cyber insurance lawyer can sometimes help you reduce premium costs, too)

Not everyone has the luxury of time, however. If you're caught up in the panicked aftermath of an attack, our best advice is to communicate openly and often with your

insurer. Our four examples of complex business interruption claims are cautionary tales. If your understanding of your policy isn't the same as your insurer's, any well-meaning decisions with financial consequences you make may result in your claim being rejected.

We welcome inquiries from insurers and insureds alike. Reach out to Eric Charleston or Christine Kucey for answers to your business interruption coverage questions.

By

Eric S. Charleston, Christine Kucey

Expertise

Cybersecurity, Privacy & Data Protection, Insurance Claim Defence

---

BLG | Canada's Law Firm

As the largest, truly full-service Canadian law firm, Borden Ladner Gervais LLP (BLG) delivers practical legal advice for domestic and international clients across more practices and industries than any Canadian firm. With over 725 lawyers, intellectual property agents and other professionals, BLG serves the legal needs of businesses and institutions across Canada and beyond – from M&A and capital markets, to disputes, financing, and trademark & patent registration.

blg.com

BLG Offices

Calgary
Centennial Place, East Tower
520 3rd Avenue S.W.
Calgary, AB, Canada
T2P 0R3
T 403.232.9500
F 403.266.1395

Ottawa
World Exchange Plaza
100 Queen Street
Ottawa, ON, Canada
K1P 1J9
T 613.237.5160
F 613.230.8842

Vancouver
1200 Waterfront Centre
200 Burrard Street
Vancouver, BC, Canada
V7X 1T2
T 604.687.5744
F 604.687.1415

Montréal
1000 De La Gauchetière Street West
Suite 900
Montréal, QC, Canada
H3B 5H4
T 514.954.2555
F 514.879.9015

Toronto
Bay Adelaide Centre, East Tower
22 Adelaide Street West
Toronto, ON, Canada
M5H 4E3
T 416.367.6000
F 416.367.6749