Cyber insurance exclusions: 4 examples of upgrades a policy may not cover after a breach

September 13, 2022

This is part two in a three-part series that also explores business interruption coverage under a cyber insurance policy and *how to lower your cyber insurance costs*.

A cyber breach is painful and expensive. The silver lining – if there is one – is that an incident can reveal an Achilles heel that a business can protect by improving its systems. Cyber insurance policies usually won't cover these improvements (often called "betterment") or will only cover a portion of the cost. This is because cyber insurance is designed to restore an organization's systems – to get them back to where they were pre-attack – not cover upgrades.

This article on cyber insurance exclusions explores four examples of upgrades that may not be fully covered, as well as insight into how insurers and insureds usually negotiate these issues.

Example 1: Software and hardware upgrades

After a cyber breach, cyber incident response and recovery professionals may recommend system upgrades. A common example is a recommendation to upgrade an on-premises Microsoft Exchange server to cloud-based Office 365. They may also suggest installing the latest version of software if an insured is unable to completely restore its systems from a backup after a ransomware attack.

The insured's position: This is the perfect time to upgrade our software. It will make us stronger and more attractive to insure.

The insurer's position: The policy does not cover upgrades that cost more than the original, require a switch to a subscription model or incur training costs for your staff.

The cyber insurance lawyer says: Insureds almost always have to pay out-of-pocket for software and hardware upgrades. One exception, however, is if upgrades are the only available option. Organizations should add the cost of regular upgrades to their IT budget to help them stay cyber safe – and improve the chances of obtaining and keeping cyber insurance.

Example 2: Extending endpoint detection and response monitoring

After a breach, it's common practice to deploy endpoint detection and response (EDR) software for a short period of time to keep an eye on network activity and identify malware.

The insured's position: It makes sense to maintain the contract with the EDR vendor longer-term to strengthen our defenses. We really want to avoid this happening again.

The insurer's position: Your cyber insurance policy covers eradication of the threat actor's presence on your system. EDR software is only covered as part of the immediate post-breach response. Ongoing contracts to prevent future threats are not covered.

The cyber insurance lawyer says: Extending your EDR engagement is forward-looking security enhancement. While it's a great idea (it's on our cyber hygiene checklist, along with regular upgrades to your software and hardware), it's something organizations are expected to pay for outside of their cyber insurance claim.

Example 3: Streamlining network infrastructure

Over time, an organization's IT infrastructure can become a patchwork of bespoke integrations, encrypted blind spots, old servers and decentralized IT service providers. This is particularly common when companies merge. A cyber attack can wreak havoc on these systems.

The insured's position : Our network is Frankenstein's monster. We'd never have built it this way if we'd been doing it from scratch. It will take much longer to try to re-create the original mess than to do it right the second time – and time is money. Our insurance company should cover the costs to get us up and running faster. It might even be cheaper!

The insurer's position : The insurance will ordinarily pay to restore systems to what they were before. But, if there is no cost difference between the options, the upgrades may be covered. If it costs more to upgrade, insurance may only cover part of the cost.

The cyber insurance lawyer says : It may be possible to get the cost of network improvements covered – insureds just have to prove it will be financially beneficial to the insurance company. Organizations should cost out two scenarios: returning the network to its pre-breach state and streamlining it. If it's less expensive to build back better, chances are the insurer will agree to cover it. Insureds should show their insurer the cost comparison and get agreement before embarking on a full IT restoration.

Example 4: Regaining the confidence of suppliers

A cyber breach can cause reputational issues, with the company that suffered the attack being seen as a higher risk to do business with. This can lead integration partners to

deny access to shared networks or databases until the company can prove it has improved its cyber security.

The insured's position : My suppliers have a list of upgrades I need to make, and I can't restart my business until those upgrades are complete. These upgrades should be covered under the restoration or business interruption coverages in our cyber insurance policy.

The insurer's position : The costs of upgrading to a supplier's standards are not covered because they don't relate to restoration of the pre-existing system.

The cyber insurance lawyer says : This one is tricky. Do the costs fit the definition of restoration, in that they're required to restore business operations? Or are they upgrades, in that that they're required to satisfy new standards? (Upgrades aren't often covered by cyber policies.) It also comes down to cause. Were the upgrades caused by the cyber incident? Or were they caused by new and more stringent standards from the supplier? Surely, the policy would not cover the cost if the supplier demanded upgrades without an incident having occurred. In instances like this, insurers and insureds must acknowledge this ambiguity and negotiate to reach an agreement.

So what's a business to do?

A home insurance policy won't pay to build a mansion if a modest bungalow burns down. Likewise, a cyber insurance policy won't pay to improve outdated systems after a cyber attack.

That doesn't mean that organizations should be satisfied with their pre-attack status. In fact, if they don't invest in their cyber hygiene, their insurance costs may go up, or they may be denied cyber coverage altogether.

Organizations that have experienced a cyber breach and need cost-effective solutions for recovery should start by framing their restoration efforts as less expensive than restoring to the previous condition. In our representation of the world's largest insurers on complex cyber claims, we've learned that insurers are often very reasonable in a cyber claims scenario if the proposed improvements are the more cost-effective route to restoring operations.

If you need to determine the aspects of a complex cyber claim that are covered or understand the fine print of your cyber insurance policy in the aftermath of a breach, connect with Eric Charleston or Michelle Doody.

By

Eric S. Charleston, Michelle Doody

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