Cyber hygiene checklist: Tick these boxes to lower your cybersecurity risk and insurance costs

February 09, 2022

It used to be that only big corporations that kept large volumes of highly sensitive personal data needed to worry about cybersecurity. Not so today. In November 2021, the Canadian Centre for Cybersecurity reported that nearly a quarter of small businesses in Canada had experienced some kind of cybercrime since March 2020 – a number believed to be an underestimate. Small- and medium-sized enterprises also accounted for almost two-thirds of known Canadian "name and shame" ransomware victims in the first half of 2021.

The good news is that businesses of all sizes can take steps to reduce their cybersecurity risk using this 11-point cyber hygiene checklist. By identifying and eliminating vulnerabilities in your systems, policies and practices, you reassure your executives, customers, suppliers and your insurance company that you take cybersecurity seriously. And, while there may be a cost to some of the items on the checklist, it's helpful to see this cost in context – the average data breach in Canada has a C$6.35 million price tag and cybercriminals often strike the same victim more than once.

Your cyber hygiene checklist

Review each of the items below. You should be able to respond to each item with a resounding "yes." If not, now's the time to take action - and we're here to help.

☐ **Multifactor authentication is in place for all users** . Multifactor authentication confirms the identity of a user in more than one way, for example, by password and security token or key fob and facial recognition software. Without multifactor authentication, your firewall, encryption technology and antivirus software offer little protection. Multifactor authentication is becoming a common requirement for business insurance coverage. Note that verifying identity via password plus a one-time code sent to a smart phone – the traditional two-factor authentication strategy – is falling out of favour, as phones and phone numbers can end up in the wrong hands.

☐ **We have endpoint detection and response software** . Endpoint detection and response software allows you to detect and investigate any suspicious activity on all endpoints within your network. It is different from antivirus software.

☐ **Network security monitoring is in place** . Used in conjunction with endpoint detection and response software, network security monitoring identifies unusual patterns of behaviour and validates suspicious activity. If you don't have firewall settings or they've been tampered with, the network security log becomes a secondary means of validating data staging or exfiltration.

☐ **Our regular employee cybersecurity training includes simulated attacks** . Just as a fire drill forces us to practice an emergency evacuation, a simulated cyberattack allows us to practice our response to a cyber threat. As an IT director or privacy officer, you'll learn where your people understand their risks and responsibilities and where they need more education. In-house cybersecurity training is certainly possible, but it can place an unreasonable burden on your already stretched IT resources. BLG can provide recommendations for external training vendors who will meet your curriculum and cost requirements – just reach out to Eric Charleston or Julie Gauthier.

☐ **We enforce mandatory password changes and complexity practices** . People are notoriously bad at setting complex passwords and changing them regularly. That's why the most important words in this checklist item are "enforce" and "mandatory." Use a password updating system that schedules regular password changes and requires passwords of a minimum complexity, so that timing and password strength are decided by a machine, not a human.

☐ **We follow policies that describe how and when our software and hardware is updated**. It's important that there is a policy, not just informal practices for updating and patching.

☐ **We restrict admin-level access** . Permissions should be assigned on a need-to-know basis to minimize the number of individuals who could succumb to a cyber scam or execute one themselves.

☐ **Our data map accurately represents all the data we have** . A data map is a comprehensive description of the data you collect, including anonymized data retained for demographic or market insights. A data map is a tool, not simply a document. Use it to determine whether you're collecting too much data, if you're retaining it for too long, and to know exactly what was accessed and stolen if there's a data breach. If there's a breach, your insurance company will expect that your map accurately reflects the amount and type of data that was compromised. If the two don't match, your claim may not be covered. BLG does data mapping and gap analyses to help organizations develop robust crisis management plans, privacy policies and ensure regulatory compliance.

☐ **We have a data retention policy** . An ever-expanding data repository is a liability. Retain data that you have permission to keep for the purpose you originally intended, and data required for mandatory reporting, such as tax. A lawyer can help explain your regulatory obligations regarding data retention and privacy, including for anonymized data. Eric, Julie and other members of BLG's cross-Canada cybersecurity, privacy and data protection team would be happy to discuss your situation with you.

☐ **Data is backed up to an off-site location** . This location needs to be disconnected from your network. Data can be backed up to a hard drive or the cloud. Make sure the location of the servers complies with privacy requirements.

☐ **We have a privacy compliance program** . Privacy laws vary around the world and even within countries, and they are always evolving. Québec's privacy law, adopted in September 2021, heralds an era of increased enforcement and accountability in Canada. Every organization needs to have a program to govern and manage its data use, based on its business activities; the type of data it collects, stores, processes and transfers; its legal, contractual and regulatory obligations; risks to data; and privacy principles. Managing consent is part of any privacy compliance program. Private sector organizations collecting personal information from Canadians must comply with Canadian consent law.

So there you have it – our 11-point cyber hygiene checklist. If you checked off every box, congratulations. Your cyber hygiene is impeccable–for now, at least. The pace of change in information technology and the genius of cybercriminals means that this checklist, like your cyber hygiene, will forever be a work in progress.

If some of the boxes remain unchecked, never fear. Use this newfound awareness of your vulnerabilities to take purposeful, well-informed steps to improve your cyber hygiene. BLG's cybersecurity, privacy and data protection team is here to help you identify the right third party service providers, understand your contractual and regulatory obligations, and dive into the details of your data collection, storage and use, so that cyber hygiene becomes almost as routine as washing your face and brushing your teeth.

By:

Eric S. Charleston, Julie M. Gauthier

Services:

Cybersecurity, Privacy & Data Protection, Technology

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