Data privacy and information security

GRI 205-2; GRI 418-1

SASB: TC-TL-220a.1-2-3-4; TC-SI-220a.1-2-3-4; TC-TL-230a.1-2-3-4; TC-SI-230a.1-2-3-4

Our customers, team members and investors expect us to demonstrate that we collect data appropriately, use it for purposes that advance their interests and keep it secure. Our approach to data governance encompasses the protection and appropriate use of data across its lifecycle, and we incorporate data governance proactively as a core consideration in all of our business initiatives and technology decisions.

The BCE Inc. Board of Directors adopted an enhanced data governance policy in 2020, bringing together multiple existing policies and programs in the interrelated areas of privacy, information security, data access management and records management. We have implemented mandatory data governance training for all employees as part of our biannual code of business conduct training program. We have also created an internal data governance site to centralize resources and answer frequently asked questions for team members. In 2022 we continued to review and rationalize our data inventory.

Privacy

WHY IT MATTERS GRI 103

Customer awareness about the importance of protecting their personal information, and privacy considerations relating to their use of our services continue to increase. This has attracted the attention of lawmakers and regulators. Changes to privacy laws have been proposed in a number of Canadian jurisdictions. There has also been increased regulatory scrutiny over the use, collection and disclosure of personal information in Canada. Our continued focus in this area aligns with our Strategic Imperative to champion the customer experience.

WHAT WE ARE DOING

We value the trust our customers place in us when sharing their personal information. We make every effort to be transparent about our privacy practices and are committed to being accountable for how we collect, use and disclose personal information. Our privacy policy sets out what information we collect, how and why we collect, use and sometimes disclose it, how and when we may request informed consent from our customers, how customers can access their personal information and how they can contact us if they have questions or concerns

Our privacy commitment

1. We commit to being accountable to you for how we collect, use and disclose your personal information.
2. We will inform you of the ways your personal information is being collected, used or disclosed. We may do this through our Privacy Policy, our Terms of Use or our websites.
3. We only collect, use or disclose your personal information if we have your consent, or in circumstances where your consent isn't necessary (such as an emergency situation).
4. We only collect your personal information in fair and legal ways. We limit our collection of your personal information to the purposes identified in advance to you.
5. We use or disclose your personal information for the reasons it is collected, when it is otherwise allowed or as required by law. We keep the information only as long as we need to, or as required by law.
6. We correct your personal information when you inform us of mistakes or let us know updates are required.

7. We do our best to keep your personal information safe, and ensure we use appropriate physical, technical and administrative safeguards appropriate to the sensitivity of the information. If we transfer your personal information to our suppliers we ensure your information is appropriately protected.
8. We make information available to you about our information management policies and practices.
9. We will provide you with access to the personal information we hold about you upon written request, unless restricted by law.
10. We are here to listen, and to help. If you have concerns, please contact us at privacy@bell.ca.

Bell and its affiliated companies have long been focused on maintaining the accuracy, confidentiality, security and privacy of personal information for customers and team members. To do this, we use technical and administrative safeguards appropriate to the sensitivity of the information. When we become aware of a suspected breach of privacy, we follow strict protocols to investigate and assess the issue and, if appropriate, to develop and implement mitigation strategies to prevent a reoccurrence in the future. Since November 1, 2018, we have also been obligated by law to report all privacy breaches that present a "real risk of significant harm" to impacted individuals to the Office of the Privacy Commissioner of Canada. In 2022, we updated our breach tracking tools to enhance our internal and external reporting capabilities.

Every year, all Bell team members must individually review and sign the Bell Code of Business Conduct. reinforcing the importance of safeguarding customer information and using it only in alignment with our privacy policy.

User consent and purpose of data collection

Bell's privacy policy explains how and when we collect, use and disclose personal information, including how we share personal information within the Bell group of companies.

We collect personal information with the customer's consent and clearly specify the purpose for which the collected information is used. We retain only the amount of information necessary for the purpose for which it was obtained. We keep information only as long as we need to or as required by law.

Moreover, Bell does not disclose a customer's confidential information to government agencies, unless it is required or permitted by law (such as where it is necessary to investigate the contravention of a law or to prevent fraud and secure our networks) or in the case of an emergency where there is an imminent danger to life or property. To view our Lawful Access Request Transparency Report, please see Appendix 1 at the end of this document.

Our privacy policy, including answers to frequently asked questions, is available on our website at Privacy at Bell.

Team member training and privacy tools

We provide our team members with information and ongoing training regarding the importance of respecting the privacy of our customers' and team members' personal information. We publish information on our intranet site that clearly defines roles, processes, training support and more. In 2021, we implemented mandatory data governance training for all employees as part of our biannual code of business conduct training program.

In 2022, Bell continued to make significant investments in people, processes and technology in order to protect confidential and personal information from evolving cyber security threats and to enhance our privacy management and reporting capabilities. Team members and customers are also able to address questions about privacy and obtain support from the Bell Privacy Team through our privacy mailbox, which is continuously monitored.

Number of unresolved well-founded privacy complaints from the Office of the Privacy Commissioner of Canada

2022	2021	2020
0	0	0

Information security

WHY IT MATTERS GRI 103

Our industry, like many others, is subject to constant cyber threats. We need to be able to identify and address information security risks in a timely manner in order to protect systems and information and help deliver on our Strategic Imperative to champion customer experience. Avoiding information security incidents can also limit increased expenses associated with remediation efforts and legal exposure, aligning with our Strategic Imperative to operate with agility and cost efficiency.

WHAT WE ARE DOING

We strive to maintain the security of our systems and customers' data. To do this, we implement prevention, detection and response programs related to security threats. As we provide ongoing training to our team members on data protection, we also continue to help define industry security and risk management practices.

Our information security goal:
To be recognized as the information security leader in our industry and a trusted partner for our customers.

At Bell, we seek to protect our networks, systems, applications and the personal information they contain against all threats, including cyber attacks, unauthorized access or entry, damage from fire and natural events, among others. We strive to protect the competitiveness of Canadian businesses using Bell's services, by seeking to maintain network security and stability. We make continual investments to improve the performance and availability of our services and networks, and deploy layers of security controls to protect against cyber threats.
Cyber security threats continue to evolve as new technologies emerge – such as 5G, cloud computing and IoT. Bell's Information Security program addresses the confidentiality, integrity and availability of existing and emerging technologies. Embedding a security mindset and appropriate protections into everything we do describes Bell's security-by-design approach.

Oversight

BCE's full Board is entrusted with the responsibility for identifying and overseeing the principal risks that our business is exposed to and seeking to ensure there are processes in place to effectively identify, monitor and manage them. While the Board has the overall responsibility for risk, the responsibility for certain elements of the Risk Oversight program is delegated to Board committees. This ensures that these elements (which are reported to the Board regularly) are treated with the appropriate expertise, attention and diligence. BCE's Risk and Pension Fund Committee is accountable for overseeing Bell's information security risks and strategy.
Operational business unit leaders are central to the proactive identification and management of risk on a daily basis. Business unit leaders have access to a range of corporate support functions that provide independent expertise to reinforce the implementation of risk management approaches.

The Corporate Security function is responsible for all aspects of security. Our Corporate Security professionals have a deep understanding of the business, the risk environment and the external stakeholder environment, and they set the standards for the organization in our security policies and monitor the organization's performance against these requirements. They also collaborate with operational business unit leaders to develop strategies and action plans to mitigate areas of risk.

BCE has established a Health and Safety, Security, Environment and Compliance Oversight Committee (HSSEC) that includes a number of our most senior leaders, to oversee progress throughout BCE's strategic security program (including information security).
For more information on Bell's risk management culture, see the Corporate governance and risk management section of our Integrated Annual Report.

Framework, policies and certification

To protect existing assets, we have developed a framework based on industry best practices and standards, including, but not limited to, those of the Information Security Forum (ISF), the International Organization for Standardization (ISO), the National Institute of Standards and Technology (NIST) and the Payment Card Industry Data Security Standard (PCI DSS). This framework consists of 10 strategic Information Security pillars and is supported by a series of policies, directives and standards defining security controls to protect our assets and data.

In 2021, we completed a third-party evaluation of Bell's information security management system (ISMS) and strategy, reinforcing our alignment with best practices and leadership in the industry. We have assessed and aligned 80% of our ISMS against the ISO standard, with the intent to align our ISMS to the ISO 27001 standard and obtain certification by the end of 2023. We already conduct Service Organization Control (SOC 1 & 2) audits on specific services across Bell to provide independent assurance on security, availability and privacy controls to our customers.

We rely on a robust assurance process to conduct assessments on projects, identify areas of risk and establish action plans to ensure systems are deployed with the appropriate level of security. In consideration of the evolving nature and sophistication of information security threats around the world, we rapidly adapt our security policies and procedures.

Bell’s information security pillars

1. Asset management and visibility
2. Access control and authentication
3. Secure system development and operations
4. Application, network and endpoint security
5. Security testing
6. Policies, requirements and risk prioritization
7. Supplier risk management
8. Security skills, education and awareness
9. Cyber threat intelligence and detection
10. Incident response and recovery

Threats and incidents

We have an internal Cyber Threat Intelligence team that identifies threats facing Bell and our customers, and complements the intelligence we gather from other industry sources. For example, Bell is a founding member of the Canadian Cyber Threat Exchange (**CCTX**), a national, cross-sector threat forum where security professionals exchange actionable threat intelligence and mitigation measures with peers.

In 2022, a cybersecurity incident occurred within Bell Technical Solutions, and some operational company and employee information was accessed. The incident was disclosed on Bell's website, a breach report was filed with the Office of the Privacy Commissioner of Canada, and the impacted employees and required customers were notified. There have not been any regulatory investigations or lawsuits to date, actual or threatened.

Awareness and training

Information security training has always been a part of team member onboarding and mandatory training at Bell.

In February 2021, we launched our Be Cyber Savvy information security training program. This training program includes onboarding to our specialized Cyber Savvy platform and performing phishing simulations. The program spans four courses that team members have a year to complete once they are onboarded. This program broadens mandatory training for team members and offers them an extensive catalogue of general awareness learning modules. In addition to general awareness, it also reinforces security-by-design principles. We have onboarded 100% of targeted team members in 2022, and plan for team members to fully complete the training cycle by the end of 2023. As of December 31, 2022, 88%[1] of targeted members have completed the full training program. We have adjusted the training completion target to have 90% of onboarded team members complete the yearly Be Cyber Savvy information security training. Our 2022 phishing simulation report rate is at 25%[2], and we observed a 155% increase in reported phishing simulations from fully trained employees compared to non-trained employees. These initiatives enable a stronger cybersecurity culture and a greater awareness of cybersecurity risks.

1 PwC provided limited assurance over our 2022 indicator. See PwC's assurance statement.

2 PwC provided limited assurance over our 2022 indicator. See PwC's assurance statement.

Customers

Consistent with Bell's position as an established provider of security services for Canadian businesses and organizations, our Managed IoT Security Service provides comprehensive security to keep our customers' networks and systems safe and secure as they adopt IoT technologies.

Our suite of security services is monitored by Bell's Security Operations Centre, a team of security professionals providing 24/7 incident management, policy management and reporting on all security-related incidents.

Suppliers

Supplier due diligence

We have an extensive supplier assurance program that assesses third and fourth-party partners in multiple ways. We work to understand the supplier's operations and security maturity to ensure service and product development is done in a secure manner, and we leverage industry tools and vendor ratings to evaluate risk. Finally, we mitigate risk by evaluating how suppliers access our systems and information in order to put the appropriate controls in place.

Contract requirements

Third-party data processors are required to implement adequate measures to ensure information security. We hold suppliers accountable through contractual clauses, requiring that the appropriate controls are in place to protect Bell’s data and systems.
Where a supplier handles sensitive information that belongs to a Bell company, a Bell customer or one of our team members, the supplier must comply with all applicable privacy laws in the jurisdiction in which they operate, as well as the contractual obligations set forth in the agreement. Bell reserves the right to assess and monitor suppliers' practices regarding information security protection.
Suppliers must notify Bell immediately of all actual or suspected privacy breaches, information security incidents or loss of Bell's data, and the supplier must assist Bell in managing the consequences of such events.

External collaboration and partnerships

As a Canadian chapter member in the not-for-profit, member-driven ISF, Bell helps drive the evolution of security and risk management practices. We also adhere to a number of international security standards and frameworks, including the Information Security Forum Standard of Good Practice, NIST and PCI DSS.

Bell is a founding member of CCTX, which aims to help public and private organizations share cyber threat and mitigation information across industries and sectors in Canada. Bell is also a founding member of the Canadian Security Telecommunications Advisory Committee (CSTAC), where we work together to drive best practices and improve the security and resiliency of Canada's connected world along with other Canadian telecommunications providers, government departments and law enforcement agencies.

Bell is recognized as a Canadian security leader by IDC Canada. IDC Canada evaluates security providers on their current capabilities and future strategies for delivery of security services. Bell's leadership was recognized in the 2015, 2016, 2017, 2018, 2019, and 2022 IDC Canada reports.[3]

We also aim to align our program to ISO 27001 by the end of 2023.

[3] IDC MarketScape: Canadian Security Services 2022 Vendor Assessment.

2022 Lawful Access Request Transparency Report

Bell may disclose a customer's confidential information to law enforcement or government agencies when specifically compelled to do so by lawful authority or in the case of an emergency where the life, health or security of an individual is threatened. Below is a summary of such requests that Bell responded to in 2021.

Requests from law enforcement and government agencies

	Number of Requests	Number of Customers[4]	Comments
Emergencies or exigent circumstances (including support to 9-1-1 calls)	59,463	60,106	Disclosures made to assist public authority in situations involving serious or imminent harm to life or property without authorization by a judge. Governed by relevant provisions of the Criminal Code including ss. 184.1, 184.4 and 487.11, and other relevant statutes and the common law)

[4] Number of Customers disclosed; based on the number of customers impacted

Legislative demands	496	1206	Compellable requests made by government agencies under the express authority of federal or provincial legislation
	324	36,844	Basic subscriber information [5]
Court Order/Warrant	9,899	15,320	Disclosures in compliance with production orders, summons, subpoenas, and search warrants issued by a judge or other judicial officer
	7	18	Foreign agency requests (court ordered) e.g. Mutual Legal Assistance in Criminal Matters Act
	36,775	470,041	Basic subscriber information[2]

[5] Basic subscriber information refers to customer name and address and/or a service provider identification

Canadian Radio-television and Telecommunications Commission tariffed services[6]

	Number of Requests	Number of Customers[7]	Comments
Government agencies	1,352	2,462	Publicly listed basic subscriber information for landline and/or service provider identification
Law enforcement	17,222	34,830	Publicly listed basic subscriber information for landline and/or service provider identification

Rejected or contested orders: We do not track rejected or contested orders. Our lawful access governance process and practice is to validate all requests and work with the requesting party to reduce the scope or withdraw the request if it is deemed too broad or invalid.

Voluntary disclosure: Bell does not disclose personal information voluntarily unless Bell is assisting in the investigation of a breach of Canadian laws (e.g. a crime against Bell). Such disclosure, if any, is made in accordance with relevant privacy legislation, including section 7(3)(d) of the Personal Information Protection and Electronic Documents Act (PIPEDA).

[6] Reference to CRTC tariffs: **Tariff Applications (8740) | CRTC**
General Tariffs Bell Canada: **Bell Canada Tariffs | BCE Inc.**
Item 2175 – Customer Name and Address: **2175.pdf (bce.ca)**
Item 2177 – Service Provider Identification: **2177.pdf (bce.ca)**
[7] Number of Customers disclosed; based on the number of customers impacted

To the extent this information sheet contains forward-looking statements including, without limitation, outlooks, plans, objectives, goals, targets, strategic priorities, commitments, undertakings and other statements that do not refer to historical facts, these statements are not guarantees of future performance or events, and we caution you against relying on any of these forward-looking statements. Forward-looking statements are subject to inherent risks and uncertainties and are based on assumptions that give rise to the possibility that actual results or events could differ materially from our expectations expressed in, or implied by, such forward-looking statements. Refer to BCE Inc.'s most recent annual management's discussion and analysis (MD&A), as updated in BCE Inc.'s subsequent quarterly MD&As, for further information on such risks, uncertainties and assumptions. BCE Inc.'s MD&As are available on its website at bce.ca, on SEDAR at sedar.com and on EDGAR at sec.gov.