OFFICE OF THE
Auditor General
of British Columbia

Managing Cybersecurity Risk in the Telework Environment

An independent audit report

March 2022

bcauditor.com

OFFICE OF THE
Auditor General
of British Columbia

623 Fort Street
Victoria, British Columbia
Canada V8W 1G1
P: 250.419.6122
F: 250.387.1230
www.bcauditor.com

The Honourable Raj Chouhan
Speaker of the Legislative Assembly
Province of British Columbia
Parliament Buildings
Victoria, British Columbia
V8V 1X4

Dear Mr. Speaker:

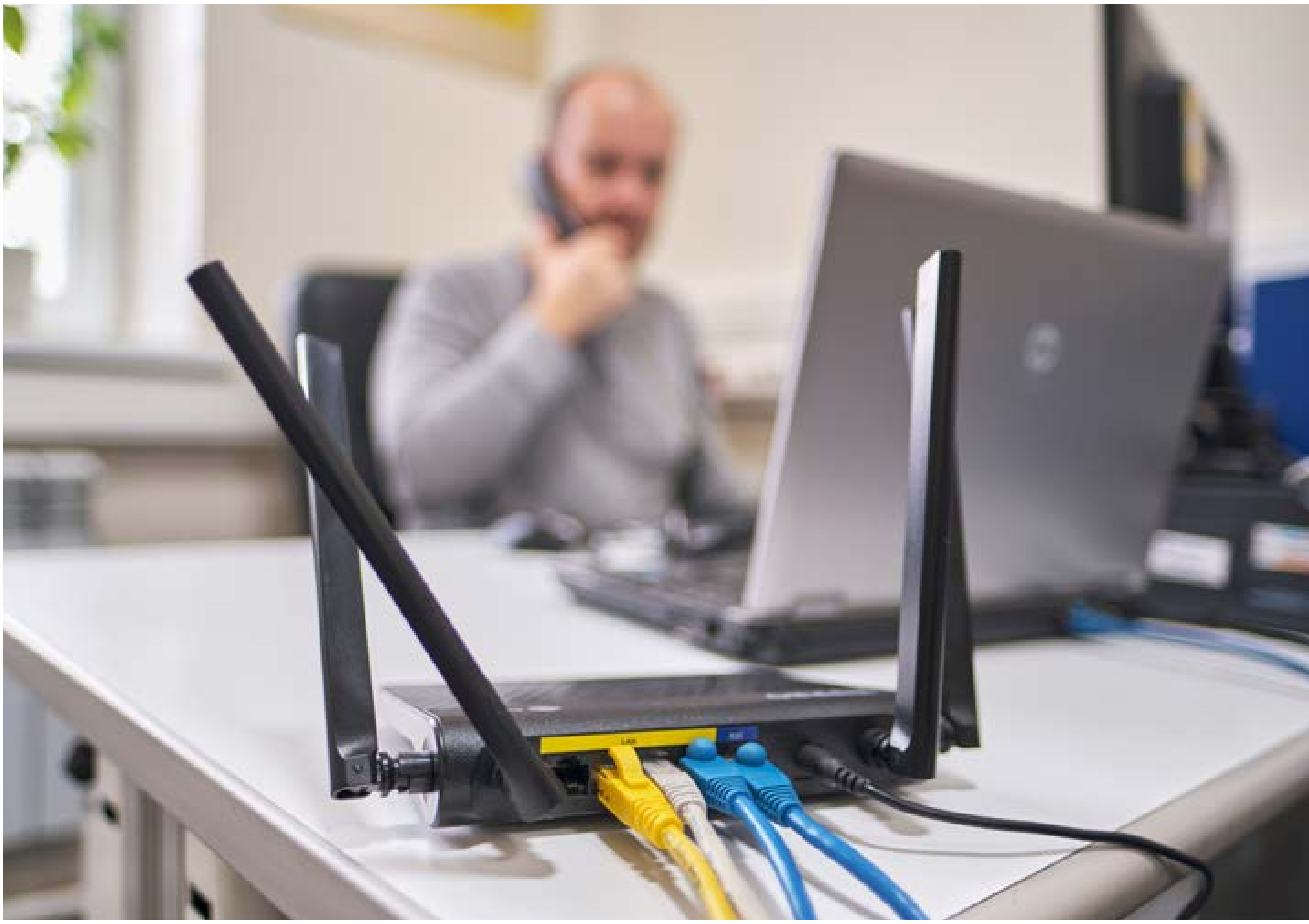
I have the honour to transmit to the Speaker of the Legislative Assembly of British Columbia the report: *Managing Cybersecurity Risk in the Telework Environment.*.

We conducted this audit under the authority of section 11(8) of the *Auditor General Act*. All work in this audit was performed to a reasonable level of assurance in accordance with the Canadian Standard on Assurance Engagements (CSAE) 3001—Direct Engagements, set out by the Chartered Professional Accountants of Canada (CPA Canada) in the *CPA Canada Handbook—Assurance*.

Michael A. Pickup, FCPA, FCA
Auditor General of British Columbia
Victoria, B.C.

March 2022

Contents



The Office of the Auditor General of British Columbia acknowledges with respect that we conduct our work on Coast Salish territories, primarily on the traditional lands of the Lekwungen-speaking people (Esquimalt and Songhees Nations) and the W̱SÁNEĆ people (Pauquachin, Tsartlip, Tsawout, Tseycum First Nations).

Audit at a glance

Why we did this audit

- Twenty times more British Columbia government employees have been teleworking since the COVID-19 pandemic began.
- To do their work, employees and contractors remotely access government data, some of which is sensitive.
- Teleworking provides many benefits, but also exposes government data to increased risk that must be managed.

Objective

To determine if the Office of the Chief Information Officer (OCIO) has established processes and practices to effectively manage cybersecurity risk to government data in the telework environment.

Audit period:

July 2021 to February 2022

Conclusion

The OCIO has established processes and practices to effectively manage cybersecurity risk to government data in the telework environment.

We made one recommendation on detecting and responding to the use of devices not managed by government.

The ministry has accepted this recommendation.

What we found

Planning, governance, and strategic activities

In the telework environment the OCIO:

- uses an established risk assessment framework to evaluate cybersecurity risk to government data.
- has implemented and maintains policies, procedures, and standards to manage cybersecurity risk.

Data protection

The OCIO:

- protects government data transmitted to and from telework devices.
- protects government data stored on telework devices provided by government.
- prohibits the use of personal devices for teleworking but is unable to detect whether these devices are being used and if government data is stored on them.

RECOMMENDATION 1

Training and awareness

- The OCIO provides cybersecurity training and guidance for teleworkers to protect government data.
- 92% of public service employees have completed mandatory data security and privacy training.
- The OCIO assesses cybersecurity awareness and updates training and guidance for teleworkers.

Audit at a glance *(continued)*

After reading the report, you may want to ask the following questions of government:

1. *What more could the OCIO do to protect government data accessed by teleworkers?*
2. *What are ministries responsible for when it comes to protecting government data?*
3. *How will the OCIO detect and respond to the use of prohibited personal devices?*

Background

Cybersecurity is a large and growing concern at all levels of government. As more public services move online, and with many more employees and contractors working remotely during the pandemic, digital information and systems security is more complex.

British Columbia (B.C.) government employees and contractors work with confidential information (personal health records, personal or government financial information) that needs to be protected.

According to the Office of the Chief Information Officer (OCIO), 20-times more public service employees have been working outside of the traditional office setting since the start of the COVID-19 pandemic. Teleworking has had many benefits, but it has also increased cybersecurity risk to government data.

Cybersecurity is the protection of information by reducing risk to information processed, transmitted, or stored on computers. Cybersecurity risk management addresses:

- Confidentiality – can unauthorized individuals view the data?
- Integrity – can unauthorized alterations to the data be made?
- Availability – can the data be destroyed or made unavailable?

Teleworking creates higher cybersecurity risk than working in traditional office settings because of network and human factors.

Network risk factors include:

- Telework requires internet connectivity, which is often less secure.
- Teleworkers connect to externally controlled networks that are not subject to government policy and standards.

Human risk factors include:

- Employees and contractors working remotely may take shortcuts that compromise the confidentiality, integrity, and availability of government information either knowingly or unknowingly (for example, saving documents on their local hard drives instead of on government servers).
- Teleworkers may miss cybersecurity awareness training or guidance and updates.
- Teleworkers may use their own unsecured devices, which is prohibited by government policy.

These cybersecurity threats and the risk they present are best managed through a combination of strategic activities, such as telework planning and governance, technical data protection measures (including encryption), and training and guidance.

The B.C. government's core policy and procedures manual delegates responsibility for the protection of government's electronic information to the Ministry of Citizens' Services. The ministry is also responsible for working with all ministries to monitor, report, and manage risk to the security of government's IT infrastructure. The OCIO leads cybersecurity risk management, and it has executive support at the assistant deputy minister level for cybersecurity risk management in the telework environment.

Objective

The purpose of this audit was to determine if the Office of the Chief Information Officer has established processes and practices to effectively manage cybersecurity risk to government data in the telework environment.

Scope

Our audit focussed on the OCIO's areas of responsibility in the telework environment, including strategic activities (such as risk assessment and telework-related policies, procedures, and standards) data protection measures on telework devices (including controlling connections to government services by authenticating users and vetting their devices) and telework-related cybersecurity training and guidance.

We did not look at the cybersecurity responsibilities of the OCIO pertaining to the regular office environment or the cybersecurity responsibilities of individual ministries.

We conducted this audit from July 2021 to February 2022.

Learn more about the audit criteria.

Learn more about how we did this audit.

Conclusion

We concluded that the Office of the Chief Information Officer has established processes and practices to effectively manage cybersecurity risk to government data in the telework environment.

We identified one control gap related to the use of personal devices for teleworking, which are prohibited by policy, and we have provided a recommendation.

Findings and recommendations

Planning, governance, and strategic activities

Cybersecurity threats are greater in the telework environment than the traditional office. The threats need to be mitigated with planning, governance, and strategic activities (such as risk assessments) and with telework policies, procedures, and standards.

The OCIO has assessed cybersecurity risk to government data in the telework environment

What we looked for

To understand and mitigate cybersecurity risk in the telework environment organizations must assess each risk and identify appropriate responses. To do this effectively the OCIO should have a well-defined risk assessment framework, with documented assessment processes, and the risk assessments must be done by qualified staff.

We looked to see if the OCIO had:

- Assessed cybersecurity risk to government data in the telework environment.
- Prioritized areas of risk in the telework environment and identified responses.
- Qualified personnel to assess cybersecurity risk to government data in the telework environment.

Learn more about the audit criteria.

What we found

Cybersecurity risk to government data in the telework environment has been assessed

The OCIO assesses cybersecurity risk to government data in the telework environment. Its risk assessment framework includes: risk identification and analysis, existing controls evaluation, residual risk treatment, and monitoring. Its process involves having ministries track security risk using their own risk documents (risk registers). The OCIO reviews ministries' submissions and identifies security risk elements that have potential to harm broader government systems and adds them to the OCIO's risk register.

Areas of risk and responses have been identified

The OCIO provided us with a copy of its risk ranking assessments. Each risk has been ranked using a four-level scale: extreme, high, medium, and low. A threat response, or a series of threat responses, have been identified and documented in the form of immediate response or future response to address residual risk.

The OCIO has qualified staff to assess cybersecurity risk

We reviewed relevant job profiles and staff credentials at the OCIO and concluded it has hired qualified staff to assess telework cybersecurity risk as part of their roles and responsibilities.

Why this matters

The above findings matter because iterative processes to assess and address risk helps prevent unauthorized individuals from viewing, altering, deleting, or blocking access to government information.

The OCIO has implemented and maintains policies, procedures, and standards for telework cybersecurity risk

What we looked for

Some cybersecurity risk can be mitigated through technical means; however, employees invariably need to be a part of an organization's defense. To that end the OCIO must develop and maintain telework-related policies, procedures and standards for employees and contractors to follow.

We looked to see if the OCIO developed policies, procedures and standards that protect government data in the telework environment that:

- Require teleworkers receive cybersecurity training.
- Specify permitted remote access methods and tools.
- Specify permitted telework devices and device classes.

We also looked to see whether the OCIO updated policy documents to reflect threat and technology changes.

Learn more about the audit criteria.

What we found

Policies, procedures, and standards have been implemented

Cybersecurity training

The government has mandated that public service employees, including all teleworkers, must complete the on-line course on protection of privacy, access to information and records management, which includes cybersecurity content.

Remote access methods and tools

The OCIO policies are specific about remote access methods that are permitted. Its Appropriate Use policy says employees must use a virtual private network (VPN) portal when accessing government information while teleworking.

The OCIO's Working Outside the Workplace policy stipulates that, in addition to VPN connection methods, desktop terminal services (DTS) may be used.

Employees have also been directed not to transmit, open, or print confidential government data, or information, using Microsoft Outlook web-access services, or to save government data to computer hard drives or external storage locations not managed by government.

Telework devices and device classes

The OCIO's Teleworking Security Standard sets the requirements for teleworking controls, including appropriate teleworking devices and device classes. The standard requires teleworking agreements between employers and employees to be formally authorized and documented.

Ministries must demonstrate annually, through annual information security reviews, that teleworking agreements are documented, and home technology assessments have been completed.

The OCIO's Mobile Device Security Standard for Information Protection applies to all mobile devices that are used to access, process or store B.C. government information. The standard requires these devices to access government services via the B.C. government Enterprise Mobility Management (EMM) system – also known as the Mobile Device Management Service (MDMS).

The OCIO's standards are consistent with their policies. The standards support staff and ensure they use secure remote access methods and tools to protect government information.

Policies, procedures, and standards are maintained

We concluded that the OCIO's most significant telework-relevant policies, procedures and standards are being maintained. The OCIO has documented and dated changes they have made and has communicated them to employees.

Why this matters

Policies, procedures, and standards are the foundation for effective cybersecurity governance. They set clear expectations for employees complementing the technical measures in the next section to create a robust control environment. Having employees and contractors who know what is expected of them and what to do to fulfil those expectations helps to reduce cybersecurity risk.

Data protection

Data protection refers to a combination of technical and procedural methods to ensure information is not accessed by unauthorized individuals. Government information must be secured both while it is being transmitted to and from telework devices and while it is being stored on telework devices.

Government protects data transmitted to and from telework devices

What we looked for

We looked to see if the OCIO implemented validated encryption protocols (defined in its standards) for government data transmitted to and from telework devices.

Learn more about the audit criteria.

WHAT IS ENCRYPTION?

Encryption is the scrambling of data so that only an authorized person can read it. Validated encryption uses mathematical procedures (algorithms) which are deliberately made public. The algorithms must be strength tested by experts and judged sufficiently difficult to undo without the password. For validated encryption, only the password needs to be kept secret not the algorithm.

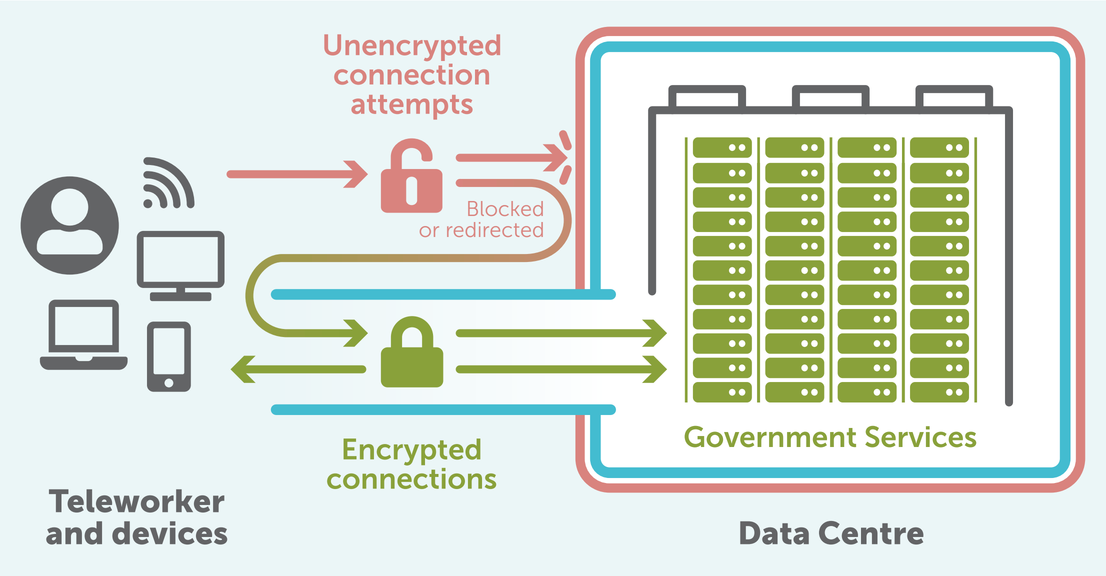
What we found

The OCIO enforces validated encryption protocols for government data transmitted to and from telework devices.

The OCIO's Information Security Policy defines encryption methods for protecting information and reducing the threat of government information being accessed by unauthorized users. The OCIO's Cryptographic Standards for Information Protection specifies that only validated encryption technologies are allowed.

We examined the system set-up at the government's data center, where all core government services are hosted, and found that users are only provided access through encrypted channels. If attempted connections to government services do not meet OCIO's encryption standards, they are rejected and re-directed to channels using validated encrypted technologies.

FIGURE 1: Data path from telework device to government data centre



SOURCE: Adapted from a National Institute of Standards and Technology publication.

The OCIO conducts weekly scans of ministry systems and flags those that are not in compliance with its cryptographic standards. These findings remain on weekly reports to ministries until they are addressed. These are effective preventative and detective control activities.

The OCIO also keeps logs of connection attempts that were rejected. These logs demonstrate the firewalls are working.

Why this matters

Telework and remote access places government information at higher risk than working in the traditional office environment due to the nature of the networks that must be used:

1. The internet — government information must be transmitted over the internet which exposes the information to internet-based threats
2. Home and other privately-controlled networks — teleworkers connect from home or non-government Wi-Fi networks which they share with users who are not subject government cybersecurity policy and standards. These users and their unsecured devices increase risk to government information.

By encrypting all government data transmitted to and from telework devices, OCIO mitigates the risk presented by these threats.

Data stored on government-managed telework devices are protected but there is risk if personal devices are used

What we looked for

One way to protect government information stored on teleworkers' government-managed devices (such as desktop and laptop computers, or mobile smartphones and tablets) is to encrypt the storage on these devices. Another way is to configure settings to:

- require a password of a defined length before access is granted
- lock device screens after a defined period of inactivity
- lock device screens after multiple unsuccessful attempts to gain access
- force security software updates regularly

We looked to see if the OCIO:

- Enforces validated encryption technology for government data stored on telework devices.
- Prevents unauthorized users from accessing government data stored on telework devices by configuring settings as described above.

Learn more about the audit criteria.

What we found

Government data stored on government-managed devices is protected with validated encryption

We looked at the OCIO's settings at its network border to confirm whether validated encryption technology is used, and standards enforced, for data storage on telework devices.

Encryption for data stored on mobile devices (i.e., smartphones and tablets) is enforced by requiring users to connect to government services through the government's mobile device management (MDM) service. This service requires validated encryption for storage of government information.

When government issues computers for employees to use they are configured with validated encryption technologies.

Controls have been implemented to prevent unauthorized users from accessing government data stored on telework devices

The OCIO has configured government-provided devices to have:

- minimum passcode lengths
- automatic screen locks after a set period of inactivity
- system lockouts after a set number of unsuccessful password attempts for most devices
- and receive essential security software updates

Controls to prevent the use of personal devices have not been established

OCIO policy prohibits the use of personal devices for telework. However, the OCIO has not established technical controls to prevent the use of personal devices, except for devices that connect through the mobile device platform. With no controls to enforce this policy, there is a risk of government data being stored in an unencrypted format on teleworkers' personal devices.

Why this matters

Allowing employees and contractors to access government systems with their own telework devices leaves government unable to determine how government data is being stored on those devices. If unauthorized users gain access to the devices, and sensitive information is not encrypted, they may be able view and copy information in breach of government information privacy and protection policies.

Recommendation

We recommend the OCIO implement detective controls to determine to what extent teleworkers are using personal devices and identify a risk response to address the threat that personal devices pose.

See the response from the auditee.

Training and guidance

Training and guidance are key to maintaining the security of government information. If employees and contractors know what is expected of them – and they know how to conduct their business activities safely – they are far less likely to inadvertently put government data and information at risk.

It's also important to check in with employees to find out if the training and guidance being provided is making a difference, and to update it when new cybersecurity threats emerge.

Guidance and training for teleworkers to support the protection of government data is provided

What we looked for

We looked to see if the OCIO provides training and guidance on:

- securing devices used for teleworking
- securing home networks used for teleworking
- using public networks
- the threat of phishing emails
- use of teleconferencing services

Learn more about the audit criteria.

WHAT IS PHISHING?

Phishing is where an attacker attempts to deceive email recipients into providing sensitive information or installing malicious software when the recipient clicks a link or downloads an attachment.

What we found

The OCIO provides cybersecurity training for teleworkers. It contributed to the development of the online course, Information Management: Protection of Privacy, Access to Information and Records Management, and created the course, Information Security and Awareness.

Employees must complete the Information Management course every two years, and newly hired staff within their first three months. The optional Information Security and Awareness course is complementary and provides more detailed cybersecurity training.

The OCIO has also developed, delivered, updated, and shared additional training for teleworkers to support the protection of government data.

It has also prepared public guidance documents for employees and contractors, on:

- Password best practices
- Cyber-safety for mobile workers
- Security 101 Guidebook
- Tip Guide: how to protect your home computer
- Protect your mobile devices

It has also posted public training videos on securing telework devices on YouTube, including:

- Information security for mobile workers
- How to create a strong password
- Multi factor authentication – learn how to protect your account
- Patch Management

Why this matters

Cybersecurity training addresses the vulnerability of government data accessed and used by teleworkers. For example, phishing emails are one of the primary ways attackers gain unauthorized access to government networks and data. Teleworkers need to be trained to spot these malicious emails, which have increased and often target remote workers.

Teleworkers' knowledge of cybersecurity is assessed, and results are used to update guidance and training

What we looked for

We looked to see if the OCIO assesses teleworkers' cybersecurity awareness and uses assessment results to update training and guidance.

Learn more about the audit criteria.

What we found

The OCIO has assessed teleworker knowledge of cybersecurity risk and updated training and guidance.

The OCIO conducted a large-scale phishing exercise to assess B.C. public service employees' knowledge and practices in 2018. Sixteen per cent of employees failed, indicating a need for additional training and guidance.

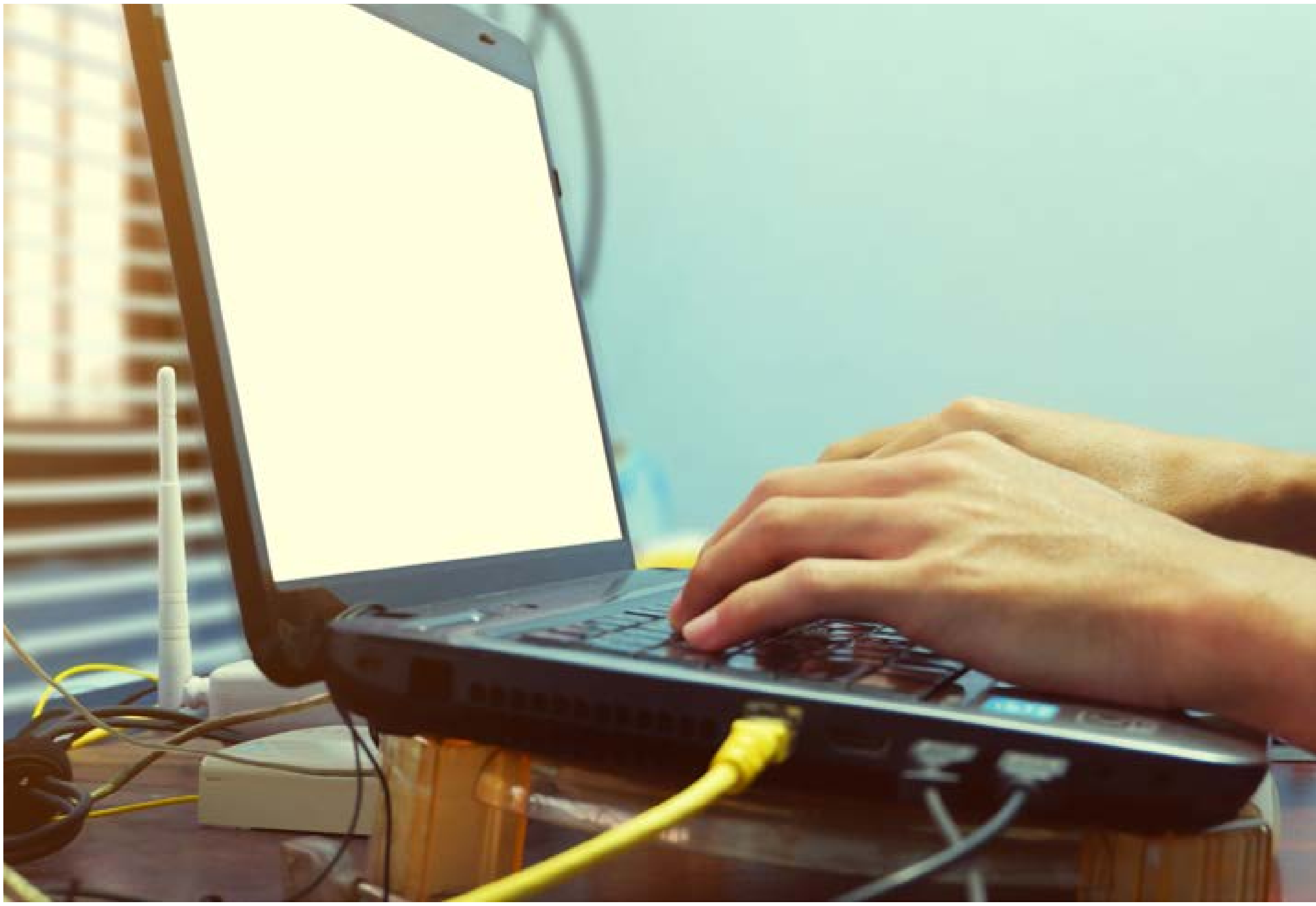
In response to this and other phishing exercises, the OCIO gathered feedback from employees and updated the online Information Security and Awareness course, adding more training on phishing. The OCIO also plans to conduct more phishing tests in 2022.

When employees take online courses, learning is assessed as employees take the training. In total, 92 per cent of public service employees completed the mandatory Information Management course at the time of our audit.

The OCIO updates their courses to keep the content current. They also host security awareness events and track the registrations and attendance.

Why this matters

Regularly updating training materials to reflect changing technology and threats supports the OCIO in managing cybersecurity risk to the confidentiality, integrity and availability of government data and information.



About the audit

We conducted this audit under the authority of section 11(8) of the *Auditor General Act* and in accordance with the Canadian Standard on Assurance Engagements (CSAE) 3001—Direct Engagements, set out by the Chartered Professional Accountants of Canada (CPA Canada) in the *CPA Canada Handbook—Assurance*. These standards require that we comply with ethical requirements and conduct the audit to independently express a conclusion against the objective of the audit.

A direct audit involves understanding the subject matter to identify areas of significance and risk, and to identify relevant controls. This understanding is used as the basis for designing and performing audit procedures to obtain evidence on which to base the audit conclusion.

The audit procedures we conducted included: examining and analyzing relevant documents, interviewing OCIO staff, and walking through government systems and documenting cybersecurity controls that have been implemented to mitigate threats in the telework environment.

We believe the audit evidence we have obtained is sufficient and appropriate to provide a basis for our conclusion.

Our office applies the Canadian Standard on Quality Control (CSQC 1), and we have complied with the independence and other requirements of the code of ethics issued by the Chartered Professional Accountants of British Columbia that are relevant to this audit.

Audit report date: March 18, 2022

Michael A. Pickup, FCPA, FCA
Auditor General of British Columbia
Victoria, B.C.

Appendix A: Recommendations and auditee response

RECOMMENDATION 1: We recommend that the OCIO implement detective controls to determine the extent of personal telework device use (in violation of policy) to aid the OCIO in its risk response.

RECOMMENDATION 1 RESPONSE: **The auditee accepts this recommendation.**

The B.C. government takes the security of its systems seriously and accepts this recommendation. The Office of the Chief Information Officer (OCIO) continues to implement technical controls to prevent, detect, and respond to cyber-attacks and have implemented some controls to address this gap and laid the groundwork for additional controls to be implemented shortly. The Province will continue these efforts and expand them going forward to ensure cybersecurity of teleworking remains secure.

Appendix B: Audit criteria

1. The OCIO assesses cybersecurity risk to government data in the telework environment

1.1 The OCIO has qualified personnel responsible for assessing cybersecurity risk to government data in the telework environment.

1.2 The OCIO assesses risk to government data in the telework environment using a risk assessment framework.

1.3 The OCIO prioritizes areas of risk in the telework environment and identifies its responses.

2. The OCIO implements and maintains policies, procedures, and standards for managing cybersecurity risk in the remote (telework) environment

2.1 The OCIO develops policies, procedures and standards that protect government data in the remote (telework) environment.

2.2 The OCIO updates policy documents to reflect threat and technology changes.

3. The OCIO protects government data transmitted to and from telework devices

3.1 The OCIO enforces validated encryption protocols for connections to government data transmitted to and from telework devices.

4. The OCIO protects government data stored on telework devices

4.1 The OCIO enforces validated encryption technology for government data stored on telework devices.

4.2 The OCIO prevents unauthorized users from accessing government data stored on telework devices.

5. The OCIO provides cybersecurity training and guidance for teleworkers to protect government data

5.1 The OCIO provides training and guidance on securing devices used for teleworking.

5.2 The OCIO provides training and guidance on securing home networks (when used for teleworking).

5.3 The OCIO provides training and guidance on the use of remote connections from public networks.

5.4 The OCIO provides training and guidance on the threat of phishing emails.

5.5 The OCIO provides training and guidance on the use of teleconferencing services.

6. The OCIO assesses cybersecurity awareness to update training and guidance for teleworkers

6.1 The OCIO assesses teleworkers for cybersecurity awareness.

6.2 The OCIO uses the results of cybersecurity awareness assessments to update training and guidance.

OFFICE OF THE
Auditor General
of British Columbia

AUDIT TEAM

Malcolm Gaston
Assistant Auditor General

René Pelletier
Executive Director

David Lau
Director

Jacqueline McDonald
Director

John Bullock
Sr. IT Audit Specialist

Greg Morhart
Director

LOCATION

623 Fort Street
Victoria, British Columbia
Canada V8W 1G1

OFFICE HOURS

Monday to Friday
8:30 am – 4:30 pm

Telephone: 250-419-6100
Toll-free through Enquiry BC: 1-800-663-7867
In Vancouver: 604-660-2421

FAX: 250-387-1230
EMAIL: bcauditor@bcauditor.com
WEBSITE: www.bcauditor.com

This report and others are available on our website, which also contains further information about the office.