BCNET 30 Years

Shared Services for Higher Education & Research

Privacy Impact Assessment: Sophos Central and Intercept X

Name of Organization	BCNET		
PIA Drafter	Hooper Access and Privacy Consulting Ltd. – Jo-Ann Bellamy		
Email	bev@hooperconsulting.ca jbellamy@hooperconsulting.ca	Phone	250 896-4272 250 208-3431
Program Manager	Dean Crawford - Director Shared Systems and Technology		
Email	dean.crawford@bc.net	Phone	250 721-8477 250 418-0593

1. Description of the Initiative

BCNET is a federally incorporated not-for profit services and information technology organization that represents the interests of its member institutions comprised of 25 publicly funded universities, colleges, institutes, and research organizations across British Columbia. It represents all public, post-secondary education institutions in the province and provides shared services to its members in the areas of networks, procurements, licensing, and IT services.

This unique, collaborative shared services model provides a multitude of benefits to its members from reducing and containing costs and increasing spending power, to decreasing duplication and improving service quality and productivity. The model cultivates a strong community, where members actively engage with peers to share, explore, and develop innovative ideas and solutions as they tackle a broad spectrum of common and unique research and education technology challenges and topics. BCNET strives to add value to its membership by leveraging an advanced network that provides economies of scale to maximize efficiencies and drive down collective costs, while at the same time, continuing to facilitate collaborative innovative solutions that meet the needs of their stakeholders in support of world-class research and education.

Cybersecurity is a growing and important issue for BCNET member institutions. With the number of new cyberthreats facing the community, cybersecurity has become a top priority. On behalf of its members and affiliations, BCNET is taking the lead on the development of this Privacy Impact Assessment on the Sophos Central and Intercept X cybersecurity system. BCNET members will be able to purchase licenses for the Sophos system through BCNET's VAR (value-added reseller). Users (members and students) will have a self-service portal to customize their security status, recover their password, and receive notifications.

Sophos Intercept X is a comprehensive endpoint protection built to stop a wide range of threats. Intercept X is managed by Sophos Central, an intuitive security platform that enables IT teams to see, manage, and control everything through a single web-based interface. Products share real-time information via a "Security Heartbeat", enabling IT teams to respond automatically to threats and deliver unprecedented cross-estate cyber risk visibility.

This Privacy Impact Assessment is addressing Sophos Central including Intercept X Advanced, and Intercept X Advanced with Endpoint Detection and Response services. Sophos Managed Threat Response (MTR) is outside the scope of this PIA.

The features of Intercept X include:

> Endpoint Detection and Response – automatically detects and prioritizes potential threats and allows users to quickly see where to focus attention and know which machines may be impacted
>
> Anti-Ransomware – provides ransomware file protection, automatic file recovery, and behavioural analysis enabling users to stop ransomware and boot record attacks
>
> Deep Learning Technology – built in artificial intelligence that detects both known and unknown malware without relying on signatures
>
> Exploit Prevention – enables users to block the exploits and techniques used to distribute malware, steal credentials, and escape detection
>
> Active Adversary Mitigations – prevents persistence on machines, credential theft protection, and malicious traffic detection

Sophos Central allows organizations to have one place to manage endpoint, mobile, encryption, web, email, server, and wireless security. Using a synchronized security management platform, organizations benefit from security intelligence sharing, policies that follow users, easy configuration, detailed and summary reporting, and automatically prioritized alerts. By using Sophos Central, organizations do not have to install or deploy servers to secure endpoints. Sophos Central provides default policies and recommended configurations to ensure organizations get the most effective protection. The Sophos Central dashboard provides a snapshot of the organization's security protection at any given time.

This privacy impact assessment is intended to ensure the use of Sophos Central and Intercept X is compliant with FIPPA.

2. Scope of this PIA

This PIA has been developed with a focus on the privacy protection and security measures for Sophos Central and Sophos Intercept X.

Notes:

- This PIA does not address the use of Sophos Managed Threat Response. If a member uses MTR, a separate or amended PIA should be completed by the member.

- This PIA does not address the use of a Managed Security Service Provider (MSSP). If a member uses an MSSP, a separate or amended PIA should be completed by the member.

3. Related Privacy Impact Assessments

No other PIA's have been completed on this initiative.

4. Elements of Information or Data

Data Provided Voluntarily

The following information may be requested when a user registers an account with Sophos, subscribes to marketing communications, purchases products or services, and/or submits enquiries. In general, the personal data that users are asked to provide, and the reasons why they are asked to provide it, will be made clear to the user at the point they are asked to provide personal data. The personal information may include:

- Name
- Company position
- Postal address
- Telephone number
- Mobile number
- Fax number
- Email address
- Credit card or other payment details
- Age or date of birth
- Account usernames
- Passwords
- Gender

Data Collected Automatically

When using the Sophos site, products, or services, data may be collected automatically including:

- IP address
- Device type
- Operating system details
- Unique device identification numbers (including mobile advertising identifiers)
- Browser-type
- Browser language
- Operating system
- Geographic location
- How the user's device has interacted with the Site, products or services, including the pages or features accessed and links clicked, the amount of time spent on particular pages, mouse hovers, the date and time of the interaction, error logs, referring and exit pages and URLs

For Sophos' cloud-based solutions, Sophos processes data (generally as data processor) about the assets the user manages through those solutions (e.g. endpoint or network device configuration information), diagnostic and activity logs generated by use of Sophos' cloud-based solutions and any assets the user manages through those solutions, information about potential threats detected by Sophos products, and any other information shared with Sophos from such assets. Many Sophos products can be configured to send data (e.g. files, URLs, emails) about potential security threats to Sophos for further scanning, analysis, and research. In such cases, the nature of the data processed by Sophos depends on what the customer decides to send to Sophos.

Many Sophos products (both on-premise and cloud-based), also send telemetry data to Sophos. Telemetry is usually non-identifying statistical and diagnostic data about product configuration, usage, and performance that allows Sophos to understand how their products are used so they can improve them and fix any problems. To the very limited extent that telemetry includes personal data, Sophos acts as data controller.

Sophos' primary data centres are provided by Amazon Web Services and are located in the European Union and the United States. There is currently no Canadian data storage centre available. Customers using Sophos' cloud-based solutions may be able to choose which data centre facility their data should be stored in. This choice, if available, is made at the time of account setup, and may not be changed afterwards. In addition to these data centres, Sophos processes data from its headquarters in the United Kingdom and may share data with various of its affiliates around the world for reasons including customer support, account management, and provision of other services. Sophos affiliates are located in various countries listed at https://www.sophos.com/en-us/company/contact.aspx.

5. Storage or Access outside Canada

Personal information is stored outside of Canada. Sophos Central is hosted on Amazon Web Services, across a number of virtual machine instances and services that dynamically scale to handle the current Sophos Central workload. When a user creates a Sophos Central account, they are provided with the choice of region where they wish to set up their account. The regions are completely independent, and data is not moved between them. At present, the options are Germany, Ireland, and the United States.

6. Data-linking Initiative

In FOIPPA, "data linking" and "data-linking initiative" are strictly defined. Answer the following questions to determine whether your initiative qualifies as a "data-linking initiative" under the Act. If you answer "yes" to all 3 questions, your initiative may be a data linking initiative and you must comply with specific requirements under the Act related to data-linking initiatives.	
1. Personal information from one database is linked or combined with personal information from another database;	No
2. The purpose for the linkage is different from those for which the personal information in each database was originally obtained or compiled;	N/A
3. The data linking is occurring between either (1) two or more public bodies or (2) one or more public bodies and one or more agencies.	N/A
If you have answered "yes" to all three questions, please contact your privacy office(r) to discuss the requirements of a data-linking initiative.	

7. Common or Integrated Program or Activity

In FOIPPA, "common or integrated program or activity" is strictly defined. Answer the following questions to determine whether your initiative qualifies as "a common or integrated program or activity" under the Act. If you answer "yes" to all 3 of these questions, you must comply with requirements under the Act for common or integrated programs and activities.	
1. This initiative involves a program or activity that provides a service (or services);	Yes
2. Those services are provided through: (a) a public body and at least one other public body or agency working collaboratively to provide that service; or (b) one public body working on behalf of one or more other public bodies or agencies;	No
3. The common or integrated program/activity is confirmed by written documentation that meets the requirements set out in the FOIPP regulation.	No

Please check this box if this program involves a common or integrated program or activity based on your answers to the three questions above.	□

8. Personal Information Flow Diagram and/or Personal Information Flow Table

Personal Information Flow Table – Users			
	Description/Purpose	**Type**	**FOIPPA Authority**
1.	Users enter their personal information into Sophos for the purpose of receiving services from Sophos.	Collection	*Section 26*
2.	Sophos uses the personal information for the purpose of providing services, communications, and support related to their site and products.	Use	*Section 32*
3.	Sophos may disclose personal information to Sophos group companies, third party services providers, suppliers, agents, and other organisations who provide data processing services to Sophos; third parties who process orders or provide technical/customer support; or for anti-spam/security threat research. Detailed information can be found in the Sophos privacy policy https://www.sophos.com/en-us/legal/sophos-group-privacy-notice.aspx	Disclosure	*Section 33*

9. Risk Mitigation Table

BCNET members are responsible for the management and administration of physical and technical security risks related to their use of Sophos.

Risk Mitigation Table				
	Risk	**Mitigation Strategy**	**Likelihood**	**Impact**
1.	Unauthorized individuals at Sophos could access the personal information and use or disclose it for personal purposes.	Sophos protects all personal data using reasonable and appropriate physical, administrative, technical, and organizational measures, and in accordance with their internal security procedures and applicable law. These safeguards vary based on the sensitivity of the information that Sophos collects, processes, and	Low	High

		stores, and the current state of technology.		
2.	Unauthorized individuals at third party providers could access the personal information and use or disclose it for personal purposes.	Except as set out in the Sophos Privacy Policy, Sophos does not disclose personal data except to enforce their privacy policy, End User License Agreements, rights generally, or where required or permitted by law. Sophos takes all reasonable steps to ensure personal information is treated securely and in accordance with their Privacy Policy.		
3	Personal information is compromised during transmission	Technical security measures are in place as detailed in #12 below.		

10. Collection Notice

Each BCNET member is responsible for ensuring the appropriate collection notification is in place prior to the collection of personal information. An example of a collection notice that may be used by members follows:

> *The personal information that you provide when activating your Sophos account will be used by Sophos to create and administer your account, send you marketing communications, provide you with the products and services you request, and to respond to your enquiries. Sophos may also collect certain data automatically from your computers or devices (including mobile devices). The data Sophos collects automatically may include your IP address, device type, operating system details, unique device identification numbers (including mobile advertising identifiers), browser-type, browser language, operating system, geographic location, and other technical information. Sophos may also collect data about how your device has interacted with the Sophos Site, products or services, including the pages or features accessed and links clicked, the amount of time spent on particular pages, mouse hovers, the date and time of the interaction, error logs, referring and exit pages and URLs, and similar information. This information will be used and disclosed only for purposes directly related to and required by Sophos to provide its products and services, and to communicate with you. Your personal information will be processed and stored on a secure server in the region that you select (either Germany, Ireland, or the United States), until your account is deactivated and deleted.*
>
> *For more information about Sophos privacy policies and practices please see https://www.sophos.com/en-us/legal/sophos-group-privacy-notice.aspx*

By registering with Sophos and activating your account you consent to the collection, use, and disclosure of your personal information as described above.

11. Please describe the physical security measures related to the initiative (if applicable).

BCNET members are responsible for ensuring the physical security of all data while in their custody and/or control (including data at rest or in transit) and must meet applicable physical security standards required by their organization.

Sophos:

As the physical infrastructure for Sophos Central is maintained by Amazon, there is a separation of responsibilities. In brief, Amazon takes responsibility for security of the cloud itself, and Sophos takes responsibility for security in the cloud. The AWS Shared Responsibility Model details these responsibilities: https://aws.amazon.com/compliance/shared-responsibility-model/.

For details on what steps Amazon takes to secure the infrastructure and services they offer, see their security whitepaper:
https://d1.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf

12. Please describe the technical security measures related to the initiative (if applicable).

BCNET members are responsible for ensuring the technical security of all data in their custody and/or control (including data at rest or in transit) and must meet applicable technical security standards required by their organization. Members are accountable for Security Risk Assessments for their respective organization.

Sophos:

Every piece of data is stored in database clusters that is, at a minimum, triplicated. Event-driven clustered replication, with a replication factor of at least three, ensures two database instances in the cluster can fail and data will remain available. Being event-driven, any database change is immediately pushed to all instances in the cluster, rather than changes being replicated on a schedule, making sure that even when an instance fails, the full dataset is available on failover instances.

Each instance of a database is supported with its own storage volume which is snapshotted hourly. These instances are transient, with only the storage volumes persisting. This enables Sophos to destroy database instances without fear of data loss thanks to the cluster replication factors. Vulnerabilities in database applications, operating systems, etc. can be rapidly addressed without data loss.

All data at rest is encrypted using volume-level encryption – storage volumes, object storage, and virtual drives of virtual machines.

For sensitive user data, Sophos uses field-level encryption within storage volumes using a per-field multi-part key. These parts are formed from several different locations, including a key management system. Each key is unique to every customer, and every field.

Transport-level encryption is used to secure management communication between the client software and Sophos Central platform via certificates and server validation.

Sophos never stores nor sends users' passwords in plain text. When a user signs up for an account, this new user must set a password as part of the activation process.

Sophos Central Device Encryption does not store encryption keys but, instead, recovery keys for BitLocker and FileVault-encrypted volumes.

A recovery key is randomly generated on the Windows/Mac endpoints. This recovery key is obfuscated and sent to Sophos Central via their Management Communication System (MCS) protocol, protected with Transport Layer Security (TLS). Once it has reached Sophos Central, the recovery key is de-obfuscated and stored in the relevant storage volume. The recovery key is transparently encrypted using AES, in addition to residing on an encrypted volume. Recovery key metadata is not stored alongside the recovery key.

As soon as an admin or user reads a recovery key from the database (such as via the Sophos Central Admin or Self-Service Portal), this recovery key is marked as 'expired'. When the recovery key is used to recover an endpoint, and the endpoint boots and synchronizes with Sophos Central, it is informed the recovery key is expired. The endpoint generates a new recovery key and sends this to Sophos Central as detailed above. Once Sophos Central confirms it has received the new recovery key, the old recovery key is invalidated on the endpoint so that it no longer can be used. This ensures that recovery keys can only be used once. Recovery keys are never deleted in Sophos Central.

Threat Protection

Anti-Malware

Sophos Central is architected so that all machines are user-less, requiring no interaction, allowing machines to be locked down and hardened. Machines are built from pristine sources, thanks in part to Sophos' secure digital code signing process, and only execute the prescribed software from engineering as part of creating the machine gold image.

Similarly, to database server instances, machines that comprise Sophos Central can be destroyed and rebuilt at any time without data loss.

Patching

Every 3 weeks, the gold images for virtual machines are upgraded with the latest software libraries and applications. No virtual machine instance exists for longer than 3 weeks, with old instances being destroyed and new instances deployed based on the new gold images. Should a vulnerability be found via the vulnerability dependency framework, internal or external testing, bug bounty program, or other means, patching and redeployment take place as part of the vulnerability response program.

Security Monitoring and Response

Sophos' global security team monitors all logging data from Sophos Central and its related services 24/7/365. Central has forensic capabilities in the event of a data breach for rapid incident response.

13. Does your branch/department rely on any security policies?

BCNET members are responsible for the administration of organizational security policies as it relates to the management of personal information in their custody and/or control.

Sophos:

https://www.sophos.com/en-us/legal/sophos-group-privacy-notice.aspx
https://www.sophos.com/en-us/legal/product-privacy-info.aspx#SophosCentral
https://www.sophos.com/en-us/legal/sophoslabs-information-security-policy.aspx

14. Please describe any access controls and/or ways in which you will limit or restrict unauthorized changes (such as additions or deletions) to personal information.

BCNET members are responsible for the management and administration of user access based on "need to know" principles including maintenance and enforcement.

Sophos:

Network Access Control Lists

Security Groups and Network Access Control Lists are in place using the principle of least privilege. By default, any service that is built for use in Sophos Central is placed on a private subnet that is not exposed outside of the virtual network. Additionally, services are not given permission to talk to other services unless explicitly needed and access has been granted by the Sophos Central Infrastructure Services (CIS) team. Only services that must expose an external interface are given a public-facing interface.

Database Access

Databases are not exposed to the internet, are only accessible within the virtual network, and are kept on separate, private subnets from the other Sophos Central infrastructure. Services wishing to interact with any database must do so through the Data Access Layer (DAL).

Maintenance Access

Maintenance access to Sophos Central is only available via a VPN tunnel originating from a specific network within Sophos' IT infrastructure. The tunnel cannot be established outside of Sophos' network even with credentials, keys, and certs.

15. **Please describe how you track who has access to the personal information.**

BCNET members are responsible for ensuring that access to all personal information in their custody and/or control is secure, monitored and reviewed/audited on a regular basis.

<u>Sophos</u>

Sophos' global security team monitors all logging data from Sophos Central and its related services 24/7/365. Central has forensic capabilities in the event of a data breach for rapid incident response.

16. **How is an individual's information updated or corrected? If information is not updated or corrected (for physical, procedural, or other reasons) please explain how it will be annotated? If personal information will be disclosed to others, how will the public body notify them of the update, correction, or annotation?**

Users can request that Sophos correct or update their personal information by contacting Sophos directly using the contact details provided on the Sophos website. Users can also access, delete, or request portability of their personal data by completing on online form available on the Sophos website.

17. **Does your initiative use personal information to make decisions that directly affect an individual(s)? If yes, please explain.**

No.

18. **If you answered "yes" to question 17, please explain the efforts that will be made to ensure that the personal information is accurate and complete.**

N/A

19. **If you answered "yes" to question 17, do you have a records retention and/or disposition schedule that will ensure that personal information is kept for at least one year after it is used in making a decision directly affecting an individual?**

N/A

20. Does the initiative involve systematic disclosures of personal information? If yes, please explain.

No.

21. Does the program involve access to personally identifiable information for research or statistical purposes? If yes, please explain.

No.

22. Will a personal information bank (PIB) result from this initiative? If yes, please list the legislatively required descriptors listed in section 69 (6) of FOIPPA. Under this same section, this information is required to be published in a public directory.

No.

Signed on Behalf of BCNET:

Bev Hooper
Privacy Advisor

August 27/20
Date

Dean Crawford

Dean Crawford
Director
Shared Systems and Technology

29 September, 2020
Date