The Ohio Data Protection Act

SOPHOS
Cybersecurity made simple.

The Ohio Data Protection Act (Senate Bill 220) went into force on November 2, 2018. The Act provides a legal safe harbor to businesses that implement a specified cybersecurity program by providing compliant businesses with an affirmative defense to tort actions brought under Ohio law or in Ohio courts. To be eligible for this affirmative defense, the business must create, maintain, and comply with a written cybersecurity program that contains administrative, technical, and physical safeguards for the protection of personal information and restricted information, and that reasonably conforms to an industry-recognized cybersecurity framework. Some examples of acceptable frameworks include NIST, HIPAA/HITECH, FedRAMP, GLBA, CIS Controls, FISMA, ISO 27000 Family, and PCI DSS. Read more about the Act here: https://www.ohioattorneygeneral.gov/Business/CyberOhio/Data-Protection-Act

The particular design of the cyber security program will vary by business, taking into account a business's size and complexity, nature and scope of activities, sensitivity of information, cost and availability of tools to improve security, and resources available to the business. Thus, a smaller business may face different threshold requirements for implementing an effective cyber security regime than a larger business.

Sophos products can support your efforts to build a robust cybersecurity program that aims at protecting the security and confidentiality of information, protecting the security and integrity of information against anticipated threats or hazards, and protecting against unauthorized access to and acquisition of the information that may result in identity theft or other fraud. For more Sophos solutions that can reinforce your regulatory compliance efforts, please visit: https://www.sophos.com/en-us/solutions/compliance.aspx

SECURITY GOAL FROM CYBERSECURITY FRAMEWORK	SOPHOS PRODUCT	HOW IT HELPS
REQUIREMENT 1 OF THE ACT: PROTECT THE SECURITY AND CONFIDENTIALITY OF THE INFORMATION		
Install and maintain a firewall configuration to protect data.	Sophos XG Firewall SG UTM	Allows for granular rule-based traffic control to specific ports and services at perimeter ingress and egress points, and can control remote access authentication and user monitoring at the perimeter. Creates granular and manageable firewall rule sets that specify addresses, ports, protocols, and specific application traffic and behavioral patterns. Sophos firewalls can also perform Network Address Translation (NAT), detect and block spoofed IP addresses, and perform stateful traffic inspection.
	Sophos Intercept X Sophos Intercept X for Server	Includes a powerful local firewall (endpoints) and host-based intrusion detection and traffic control and monitoring, and creates detailed log events of all malicious activity on endpoint and servers, helping to identify suspicious activity on systems.

The Ohio Data Protection Act

SOPHOS
Cybersecurity made simple.

SECURITY GOAL FROM CYBERSECURITY FRAMEWORK	SOPHOS PRODUCT	HOW IT HELPS
Ensure integrity, confidentiality, and availability of data	Sophos XG Firewall SG UTM	Enables role-based administration for delegating secure network security management; blocks traffic, services, ports, and protocols except those explicitly allowed and defined as appropriate and necessary for the organization. High availability with active-active load balancing or active-passive fail-over and WAN link balancing ensures availability of critical systems and resources at all times.
	Sophos XG Firewall SG UTM Sophos Intercept X	Data Leakage Prevention (DLP) capabilities in Sophos products can detect credit or debit card numbers and can prevent leaks of credit and debit card details via email, uploads, and local copying.
	Sophos Intercept X Sophos Intercept X for Server	HIPS, deep learning, anti-exploit, anti-adversary, and malicious traffic detection combine to proactively detect malicious behaviors occurring on the host.
	Sophos SafeGuard Encryption Sophos Central Device Encryption	Encrypts data on Macs, Windows, and mobile devices. Device Encryption provides centrally-managed, full disk encryption using Windows BitLocker and Mac FileVault. Sophos application-based (synchronized) encryption is automatic and always-on, i.e. content is encrypted as soon as it is created and it stays encrypted even when shared or uploaded to a cloud-based file-sharing system or removable devices. Role-based management is available to separate authorization levels and your encryption policies, keys and self-service key recovery can be centrally managed.
	Sophos Mobile	Integration with Sophos UTM, Sophos Wireless access points, and other UTMs provides integrated and consistent security and compliance enforcement for mobile devices accessing the network and other services.

The Ohio Data Protection Act

SOPHOS
Cybersecurity made simple.

SECURITY GOAL FROM CYBERSECURITY FRAMEWORK	SOPHOS PRODUCT	HOW IT HELPS
	Sophos Email Appliance Sophos XG Firewall SG UTM	Prevents messages containing sensitive data from leaving the organizations with data loss prevention rules providing policy driven encryption in transit and at rest. SPX encryption is able to dynamically encapsulate email content and attachments into a secure encrypted PDF to help protect email content from unauthorized access.
	Sophos Phish Threat	Provides simulated phishing cyberattacks and security awareness training for the organizations end users. Courses cover a wide range of topics from phishing and cybersecurity overview lessons, through to data loss prevention, password protection and more.
Ensure business continuity and disaster recovery planning	Sophos XG Firewall SG UTM	High availability with active-active load balancing or active-passive fail-over and WAN link balancing lets you easily double your performance when you need it.
	Sophos Email on Central	In the event of third-party cloud email service provider outages, alerts are provided if mail can't be delivered to a server/service; email is then queued for delivery to ensures no email is lost, and access to that queued email is provided from a 24/7 emergency inbox inside the end user portal. Retry period for queued email is 5 days.
	Synchronized Security feature in Sophos products	Shares telemetry and health status, enabling coordinated isolation, detection, and malware remediation across servers, endpoints, and firewalls. The Security Heartbeat also shares this information with Sophos Encryption, which revokes the encryption keys on the affected machine until the problem is fixed to prevent any data theft. After the systems have been automatically returned to their initial, clean state, the XG Firewall restores network access to the device, the encryption keys are returned, and your network is botnet-free.
	Sophos Intercept X Sophos Intercept X for Server	Includes rollback to original files after a ransomware or Master Boot Record attack, along with Sophos Clean which provides forensic-level remediation by eradicating malicious code as well as eliminating nasty registry key changes created by malware as well.

The Ohio Data Protection Act

SOPHOS
Cybersecurity made simple.

SECURITY GOAL FROM CYBERSECURITY FRAMEWORK	SOPHOS PRODUCT	HOW IT HELPS
REQUIREMENT 2 OF THE ACT: PROTECT AGAINST ANY ANTICIPATED THREATS OR HAZARDS TO THE SECURITY OR INTEGRITY OF THE INFORMATION		
Identify and assess internal and external cybersecurity risks that threaten the security and integrity of stored data	Synchronized Security feature in Sophos products	Shares telemetry and health status, enabling coordinated isolation, detection, and malware remediation across servers, endpoints, and firewalls – stopping advanced attacks.
	All Sophos Products	Generate security event logs that can be integrated into a centralized monitoring program for incident detection and response.
	Sophos Mobile	Monitor mobile devices for jailbreaking and side-loading of applications. Deny access to email, network, and other resources if device is not in compliance with policy.
	Synchronized Security feature of Sophos Email and Sophos Phish Threat	Sophos Email 'At Risk Users' report highlights exactly which users are clicking email links re-written by Time-of-Click URL protection. Identifying users who have either been warned or blocked from visiting a website due to its risk profile. It's then simply one-click from the report to enroll users in Phish Threat simulations and security awareness training – increasing their threat awareness and reducing risk.
	Sophos Intercept X for Server	Server Lockdown allows only trusted whitelisted applications and associated files to run.
	Sophos Intercept X Sophos Intercept X for Server	HIPS, deep learning, anti-exploit, anti-adversary, and malicious traffic detection combine to proactively detect malicious behaviors occurring on the host. Endpoint Protection application control policies restrict the use of unauthorized applications.

The Ohio Data Protection Act

SOPHOS
Cybersecurity made simple.

SECURITY GOAL FROM CYBERSECURITY FRAMEWORK	SOPHOS PRODUCT	HOW IT HELPS
Secure transmitted data	Sophos Mobile	Provides enterprise mobility and security management capabilities for traditional and mobile endpoints, including security and device policies. Flexible compliance rules monitor device health and can automatically deny access to sensitive data in case of a compromised device. Emails and documents can be stored in the secure and encrypted Sophos Container and accessed with the Sophos Secure Email and Sophos Secure Workspace apps. The Sophos Secure Workspace app secures sensitive data with AES-256 encryption, allowing a secure way to manage, distribute, and edit documents and view web content on mobile devices.
	Sophos XG Firewall SG UTM	Facilitates two-factor authentication for VPN connections, with granular RADIUS/TACACS integration. Sophos RED (Remote Ethernet Device) extends a secure network to a remote location easily by establishing a secure, dedicated VPN tunnel.
	Sophos SafeGuard Encryption	Encrypts information at rest and in transit on Macs, Windows, and mobile devices. Manages BitLocker and FileVault full disk encryption as well as always-on file encryption for information stored on hard disks, USB sticks, cloud storage, file shares, memory cards, and CDs/DVDs. All data encrypted remains encrypted as files move across the network.
	Sophos Email Appliance Sophos XG Firewall SG UTM	Sophos SPX encryption provides encryption in transit and at rest. SPX encryption is able to dynamically encapsulate email content and attachments into a secure encrypted PDF to help protect email content from unauthorized access.

The Ohio Data Protection Act

SOPHOS
Cybersecurity made simple.

SECURITY GOAL FROM CYBERSECURITY FRAMEWORK	SOPHOS PRODUCT	HOW IT HELPS
Respond to identified or detected Cybersecurity Events to mitigate any negative effects	Synchronized Security feature in Sophos products	Shares telemetry and health status, enabling coordinated isolation, detection and malware remediation across servers, endpoints, and firewalls – stopping advanced attacks.
	Sophos Email on Central Sophos Email Appliance Sophos XG Firewall SG UTM	Uses real-time threat intelligence to detect and block unwanted email at the gateway, and our anti-spam engine catches the rest – including the latest phishing attacks, malicious attachments, and snowshoe spam.
	Sophos Intercept X Sophos Intercept X for Server	Integrates innovative technology like deep learning, anti-exploit, and anti-adversary into malicious traffic detection with real-time threat intelligence to help prevent, detect, and remediate threats with ease. Get a root cause analysis of an attack with complete visibility on the how and where of the attack, along with recommendations on what your next steps should be.
	Synchronized Security feature of Sophos Email and Sophos Endpoint	Sophos Synchronized Security now connects Sophos Email with Sophos Endpoint. Delivering automatic detection and clean-up of infected computers sending outbound spam and viruses.
	Sophos XG Firewall	Includes IPS, APT, antivirus, sandboxing with deep learning and web protection to monitor and block malicious, anomalous, and exploitive traffic from in-bound or out-bound access. Sophos Sandstorm, optional cloud-sandbox technology, inspects and blocks executables and documents containing executable content before the file is delivered to the user's device.

The Ohio Data Protection Act

SOPHOS
Cybersecurity made simple.

SECURITY GOAL FROM CYBERSECURITY FRAMEWORK	SOPHOS PRODUCT	HOW IT HELPS
REQUIREMENT 3 OF THE ACT: PROTECT AGAINST UNAUTHORIZED ACCESS TO AND ACQUISITION OF THE INFORMATION THAT IS LIKELY TO RESULT IN A MATERIAL RISK OF IDENTITY THEFT OR OTHER FRAUD TO THE INDIVIDUAL TO WHOM THE INFORMATION RELATES		
Identify and authenticate access to system components	Sophos XG Firewall SG UTM	User awareness across all areas of our firewall governs all firewall polices and reporting, enabling next-gen control over applications, web surfing, bandwidth quotas, and other network resources by user/group. Sophos XG Firewall with Security Heartbeat™ allows next-generation endpoint and network security to continuously share meaningful information about suspicious events across extended IT ecosystem; detects compromised / unauthorized endpoint device; allows automated and near instantaneous isolation of this endpoint, preventing it from leaking confidential data.
	Sophos SafeGuard Encryption	Authenticates users for access to specific protected devices, files, and/ or folders with the use of user- or group-specific keys. Supports multi-factor authentication, tokens, and smart cards for user authentication.
	Sophos Central	Protects privileged and administrator accounts with advanced two-factor authentication. Keeps access lists and user privileges information up to date. Provides procedures to ensure that access rights are revoked if individuals no longer meet the conditions to receive access (e.g., because they change position or leave the company).
	Sophos Mobile	Sophos Secure Email and Sophos Secure Workspace in Sophos Mobile store content on mobile devices securely with AES-256 encryption. Access to the content in the apps can be restricted based on device health, compliance rules, time, Wi-Fi, or geo-location.

The Ohio Data Protection Act

SECURITY GOAL FROM CYBERSECURITY FRAMEWORK	SOPHOS PRODUCT	HOW IT HELPS
Get Audit Trails	All Sophos products	Generate security event logs that can be integrated into a centralized monitoring program for incident detection and response.
	Sophos XG Firewall SG UTM	iView Reporting provides intelligent, centralized reporting and analytics across multiple firewalls or sites; easy monitoring and analysis of security risks across entire network; convenient backup and long-term storage for security information.

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

2019-01-09 CC (PC)

SOPHOS