CyberRiskOoooooo: Delivering expertise, solutions & innovation

We appreciate your business and look forward to partnering with you.

UNDERWRITING & CLAIMS: A PARTNERSHIP

Our Underwriters and Claims professionals are a tight-knit, customer-focused team. Day in and day out, we work together to support our Insureds with exceptional service. Underwriters have the acumen to deliver consistent and tailored coverage offerings. Our Claims team, who are all attorneys, work with our Insureds to deliver sensible resolutions. Remember that your XXX XX Cyber & Technology policy includes a lot more than just coverage. It comes with our dedicated claims team who can help you navigate through a cyber security breach. Use the Cyber Claims Road Map as a quick reference for what to do.

COMPREHENSIVE POLICY

CyberRiskOoooooo provides comprehensive coverage for Cyber, Technology and Media risks. The policy terms and conditions are broad and written with a simplified approach allowing our customers to easily understand coverage.

CYBERRISKOOOOOOO.COM

Policyholders have access to our proprietary portal, CyberRiskOoooooo.com. Resources are available to you and your organization related to incident response planning, privacy awareness training and access to educational videos.

PROACTIVE BREACH SERVICES

Lower your cyber security risk and mitigate potential exposures through our proactive breach services. Please visit CyberRiskOoooooo.com for a list of our current pre-breach service providers. Discounted pre-breach services with these partners include:

- Network Vulnerability Testing
- IT Risk Assessments
- Incident Response Planning
- Security Awareness Training
- PCI Compliance
- Social Engineering and Phishing Campaigns

BREACH RESPONSE SERVICES

As an Insured, you have access to an extensive global network of cyber security experts, one of the largest in the marketplace. You work directly with our breach response partners and have the ability to choose the right vendor for your organization. Our claims team will be there to guide you through the process.

If you suspect a cyber security incident has occurred, our dedicated response team, staffed with our claims experts, is ready to help you recover. We are available at all hours every day to take calls on our breach hotline (1-000-566-0000). Services available include:

- Computer Forensics
- Credit and ID Monitoring
- Data Breach Notification
- Call Center Operations
- Expert Legal Counsel
- Public Relations

Cyber Liability

Quick wins to reduce your cyber risk

Keep software and hardware up to date

There are many free tools that conduct vulnerability scans of your network, both internal and external, to identify any existing vulnerabilities, whether on a server, operating system or application in use. According to Verizon's 2020 Data Breach Investigations Report, the exploitation of unpatched vulnerabilities was the second most common breach cause. Vulnerability scanning tools, like OpenVAS, are easy to use, free, and can identify vulnerabilities that should be remediated to avoid such common breaches.

Implement Multi-Factor Authentication

Multi-factor authentication is an essential security control for any organization. However, if there are constraints on rolling out MFA to all users, at a minimum, organizations should enforce it for access to administrator accounts. This means that when a threat actor gains a foothold in a network, they won't be able to laterally compromise the administrator account using tools like Mimikatz and other credential stealing malware.

Manage use of remote services

In 2020 the FBI published a warning regarding vulnerabilities related to Remote Desktop Protocol as it remains the primary entry point for hackers. We recommend disabling or removing remote services wherever possible. Do not allow remote access directly from the internet and instead require access via VPN, again, with MFA enforced. Ensure that separate credentials are used for remote access to users' devices and whitelist IP addresses that are allowed to connect via RDP.

Perform phishing training

Many successful cyber security incidents still rely on human error. As such, basic user security awareness training focused on the threat of phishing can significantly reduce cyber risk. Free phishing training can be found online and is generally simple to use. This training should be repeated at least quarterly to ensure users remain aware of the threat.

Use a password manager

Passwords are the first – and often only – layer of defense for systems and applications. Due to the ever-increasing number of applications and accounts employees use for professional and personal use, many employees re-use weak passwords across different accounts so that they can remember them all. When passwords are compromised, this endangers all accounts that share the compromised password. A password manager overcomes these issues by issuing and securely saving unique passwords for all accounts, only requiring the employee to remember one strong password to access the password manager, instead of dozens of weak passwords.

Backup your data securely

To respond effectively to a wide range of different cyber attacks, an organization needs to ensure it has recent backups. Hackers, particularly in ransomware incidents, target backups, by either deleting or encrypting them so that they cannot be used to restore data. As such, it is crucial to keep backup data off of the corporate network. Cloud backups with versioning are a good option, especially for small and mediums sized organizations.

Separate professional and personal account usage

Many organizations lack visibility for the applications in use on their devices, particularly when their employees are working from home. It is important to ensure that employees are aware that they are prohibited from using personal accounts for operational reasons. This provides a virtual firewall between an individual's professional and personal cyber risk.

Block macro-embedded email attachments

One of the most common ways a threat actor will gain access to a network is through a phishing email containing a malicious attachment. Once opened, the attachment's payload exploits a vulnerability or directly executes on the user's system. Use restrictions such as blocking emails with macro-embedded attachments (.docm, .XXsm, etc.) unless absolutely necessary for business purposes.

Enable logging and increase log retention

One of the most important aspects of incident investigation and response is an examination of the relevant server / device / application logs that serve as evidence during an incident investigation. Many organizations have not enabled logging or have a retention period so short that it will not be useful for investigation. XXX's 2020 Cost of a Data Breach Report states that data breaches take an average of 280 days to detect and contain.

Check for involvement in data breaches

One quick method of checking whether employees have been involved in previous data breaches is to run their enterprise email address through XxxxxXxenXxxed. This allows users to check whether their email address has been involved in any data breaches that have been uploaded to the platform. If any users have been involved in a data breach, they should immediately change the password to the affected account and any other accounts that use the compromised password. This risk emphasizes the importance of not reusing passwords across multiple accounts.

1. According to Verizon's 2020 Data Breach Investigations Report 2
According to XXX's 2020 Cost of Data Breach Report

To learn more, contact your XXX XX Cyber underwriter.

X-XX is a global consultancy that helps clients manage regulatory, reputational and operational risks.

CyberRiskOoooooo

Privacy, Security and Technology Insurance

BINDER LETTER

January 17, 2025

Please be advised that the below referenced account, subject to the terms and conditions below is bound and shall remain in force for a period not to exceed sixty (60) days from the effective date of this binder.

BROKER

Dummy Broker
Dummy Account
,

NAMED INSURED

Test MTP
75-20 Astoria Blvd
Queens, NY 11370

POLICY PERIOD

11/04/2024 - 11/04/2025

POLICY NUMBER

MTP9999999 00

INSURER

Indian Harbor Insurance Company

PRODUCT

CyberRiskOoooooo TRD 444 4444 Click here to access our Policy Form.

COVERAGE SCHEDULE

OPTION # 1

COMBINED POLICY AGGREGATE LIMIT	$ 124

THIRD PARTY LIABILITY			
COVERAGES	**LIMIT**	**RETENTION**	**RETRO DATE**
Technology Products and Services	N/A	N/A	N/A
Professional Services	N/A	N/A	N/A
Media	N/A	N/A	N/A
Privacy and Cyber Security	N/A	N/A	N/A
Privacy Regulatory Defense, Awards and Fines	N/A	N/A	N/A

FIRST PARTY				
COVERAGES	**LIMIT**	**WAITING PERIOD/RETENTION**		
Business Interruption and Extra Expense	N/A	Loss of Business Income	Waiting Period	N/A Hours
		Extra Expense	Retention	N/A
		RETENTION		
Data Recovery	N/A			N/A
Cyber-Extortion and Ransomware	N/A			N/A
Data Breach Response and Crisis Management Coverage	N/A			N/A

OPTIONAL BUSINESS INTERRUPTION AND EXTRA EXPENSE ENHANCEMENTS – ADDED BY ENDORSEMENT				
COVERAGES	**LIMIT**	**WAITING PERIOD/RETENTION**		
System Failure	N/A	Loss of Business Income	Waiting Period	N/A Hours
		Extra Expense	Retention	N/A
Dependent Business Interruption	N/A	Loss of Business Income	Waiting Period	N/A Hours
		Extra Expense	Retention	N/A
Dependent Business Interruption System Failure	N/A	Loss of Business Income	Waiting Period	N/A Hours
		Extra Expense	Retention	N/A

PREMIUM:	$ 12,000,000

NOTICES AND ENDORSEMENTS - *the following will be added to the Policy*		
Number	**Form Number**	**Title**
Notice	NTD 111 1111	Claims Reporting Information
Notice	PN CW 55 5555	O.O. Xxxxxxxx Department's Office of Foreign Assets Control ("OOOO")
Notice	PN CW 11 1111	Fraud Notice
Notice	PN CW 22 2222	Privacy Policy
Notice	IL MP 3444 4444 IHIC	In Witness - Indian Harbor Insurance Company
Notice	CyberRiskOoooooo Breach Hotline 1111	XXX XX Cyber Breach Hotline
1	TVI 999 9999	Terrorism Insurance Coverage and Premium Disclosure
2	TRD 444 4444	Amended Definition of Executive Officer (CEO, CIO, CISO, RM and GC)
3	TRD 444 4444	Amended Subsidiary Threshold Endorsement (% threshold)
4	TRD 444 4444	Dependent Business Interruption Coverage Endorsement
5	TRD 444 4444	Dependent Business Interruption - System Failure Coverage Endorsement
6	TRD 444 4444	System Failure Coverage Endorsement
7	TRD 444 4444	PCI DSS Coverage Amendatory Endorsement ($,000,000)
8	TRD 444 4444	Law Enforcement Cooperation Endorsement
9	TRD 444 4444	Consequential Reputation Loss Endorsement ($,000,000 Limit; Period of Indemnity 6 Months; Waiting Period 2 Weeks)
10	TRD 444 4444	Bricking Coverage Endorsement ($,000,000 Limit)
11	TRD 444 4444	Privacy Regulatory Endorsement
12	TRD 444 4444	Voluntary Shutdown Endorsement ($,000,000 Limit)
13	TRD 444 4444	Utility Fraud Endorsement ($00,000 Aggregate Limit): Crypto-Jacking: $00,000 Limit Telecommunications Fraud: $00,000 Limit
14	TRD 444 4444	Cyber Crime Endorsement ($00,000 Aggregate Limit): Social Engineering Fraud: $00,000 Limit Funds Transfer Fraud: $00,000 Limit Invoice Manipulation: $00,000 Limit
15	TRD 444 4444	Amended Definition of Network Endorsement - BYOD/WFH
16	TRD 444 4444	Cyber-Extortion Threat Loss Endorsement: Sublimit: $ Coinsurance: Insured 0% / Insurer 100% Retention: $ Waiting Period: 12 Hours
17	TRD 444 4444	SEC Analysis & Reporting Costs Sublimit Endorsement- $25K Limit: $25,000 Retention: $
18	TRD MANOO	MANUSCRIPT ENDORSEMENT
19	XX-YYSOP 0118	Service of Process
20	TRD 803-XX 2222	NY Amend Definition of Damages

PROFESSIONAL SERVICES

N/A

SUBJECTIVITIES

Issuance of this policy of insurance to which this binder applies is contingent upon the Company's receipt and approval of the following information:

1. Current Fiscal Year net profit of net loss before income taxes
2. Estimated number of Individuals for which you collect, store or transmit Personally Identifiable Information
3. Signed and currently dated XXX XX warranty statement
4. Insured Contact Name and Email Address

Additional information must be received within (30) thirty days of the date of this binder at which time, the company, in reliance upon such information will make a determination as to policy issuance. Failure to remit all requested information within (30) thirty days of the date of this binder will result in the immediate termination of this binder.

COMMISSION

This coverage is provided by a non-admitted (surplus lines) insurance company. It is the responsibility of the surplus lines broker to collect and remit any applicable surplus lines tax and stamping fee and any applicable state surcharges.

Premiums must be remitted within (30) thirty days of the effective date.

If you have any questions, please contact me at 99999999999. Thank you for thinking of XXX XX for your Cyber and Technology risk needs. We look forward to working with you on other opportunities in the near future.

Sincerely,

Test UW
Underwriter
Cyber and Technology
XXX XX, a division of XXX
99999999999
testunderwriter@email.com

NOTICE OF TERRORISM INSURANCE COVERAGE

POLICYHOLDER DISCLOSURE

Coverage for “certified acts of terrorism” for the types of insurance subject to the Terrorism Risk Insurance Act is already included in your current Policy. “Certified act of terrorism” means an act that is certified by the Secretary of the Treasury, in accordance with the provisions of the federal Terrorism Risk Insurance Act, to be an act of terrorism pursuant to such Act. The criteria contained in the Terrorism Risk Insurance Act for a “certified act of terrorism” include the following:

1. The act resulted in insured losses in excess of $5 million in the aggregate, attributable to all types of insurance subject to the Terrorism Risk Insurance Act; and

2. The act is a violent act or an act that is dangerous to human life, property or infrastructure and is committed by an individual or individuals as part of an effort to coerce the civilian population of the Xooiii Xiiiii or to influence the policy or affect the conduct of the Xooiii Xiiiii Government by coercion.

You are hereby notified that if aggregate insured losses attributable to terrorist acts certified under the federal Terrorism Risk Insurance Act exceed $100 billion in a calendar year and we have met our insurer deductible under the Terrorism Risk Insurance Act, we shall not be liable for the payment of any portion of the amount of such losses that exceeds $100 billion.

Under your existing coverage, any losses resulting from “certified acts of terrorism” may be partially reimbursed by the Xxxxxx Xxxxxx Government under a formula established by federal law. Under this formula, the Xxxxxx Xxxxxx Government generally reimburses 99% through 2015; 99% beginning on January 1, 2016; 99% beginning on January 1, 2999; 00% beginning on January 1, 2999; 00% beginning on January 1, 2999; and 00% beginning on January 1, 2999, of covered terrorism losses exceeding the statutorily established deductible paid by the Insurer providing the coverage. However, your policy may contain other exclusions that may affect your coverage. The terms and limitations of any terrorism exclusion, or the inapplicability or omission of terrorism exclusion, do not serve to create coverage for any loss that is otherwise excluded under this Policy.

The portion of your annual premium that is attributable to coverage for “certified acts of terrorism” is:
$ waived. Any premium waiver is only valid for the current Policy Period.