Cyber Protection during an emergency

Cyber liability is todays equivalent to General liability and every business is susceptible to a breach and loss.

What Is Cyber Liability Coverage? Cyber liability insurance covers financial losses that result from data breaches and other cyber events. ... First-party coverages pay expenses your firm directly incurs as result of the breach, such as the cost of informing your customers about a breach.

Cyber liability policies protect your business from claims and expenses resulting from a data breach. Policies aren't standardized and contain unique terminology. Most policies are flexible so you can choose the coverages you want.

Most notably, but not exclusively, cyber and privacy policies cover a business' liability for a data breach in which the firm's customers' personal information, such as Social Security or credit card numbers, is exposed or stolen by a hacker or other criminal who has gained access to the firm's electronic network. The policies cover a variety of expenses associated with data breaches, including: notification costs, credit monitoring, costs to defend claims by state regulators, fines and penalties, and loss resulting from identity theft.

In addition, the policies cover liability arising from website media content, as well as property exposures from: (a) business interruption, (b) data loss/destruction, (c) computer fraud, (d) funds transfer loss, and (e) cyber extortion.

Claims emanate from Stolen laptops or smart phones, rogue employees, 3rd party hackers, manufactures duped, spyware, dumpster diving (looking in business trash bins) cyber extortion and data theft, opening and or responding to emails that are traps,

Everyone is susceptible as the media reports about claims when it is a name brand such as Amazon, NASA, Porsche Audi, Church of Scientology, eBay, and yahoo...

Ten Tips to Stay Cyber-Safe When Working Remotely

Whether for work or personal use, our reliance on technology has never been higher. As this reliance grows, so do the associated cyber risks. And when more people are working or studying from home, the potential for a cyber incident increases in different ways.

Cyber criminals know that when more people are communicating online, they're interacting with technology in different ways - even sometimes using networks or software for the first time. Bad actors often attempt to take advantage of such situations, using deception to gain access to protected information. At the same time, corporate IT and operations teams are working overtime to keep networks running without interruption - potentially impacting their ability to detect malicious activity quickly.

This makes protecting confidential information more challenging than ever. At Chubb, we look for ways to do more for our clients, like suggesting ways to possible help you prevent issues from happening in the first place. Following these ten tips may help your business and your employees stay cyber-safe, even in periods of uncertainty.

1. **Prepare for IT resourcing issues from both a people and a technology perspective.** When more people are connecting remotely, technology call centers may face a higher call volume than normal, and more resources may be needed outside of standard business hours. Simultaneously, network bandwidth, data storage capabilities, and computing power are put to the test. Despite this increase in traffic, attention to detail cannot falter. Businesses are encouraged to keep a close eye on these needs, prepare a plan to reallocate resources as necessary, and recognize that this dependency may increase over time.
2. **Ensure your network, software, and applications are up-to-date.** Remote access technologies have known vulnerabilities - and are all too often the weak link that bad actors use to gain access to protected information. Make sure all software and applications are updated, and patch any weaknesses that are identified.
3. **Make sure your resources are aligned - before an incident occurs.** Organizations should make sure their business continuity plans, disaster recovery teams, and cyber incident response plans are in alignment. Bad actors know that dependency on your network and its availability is never higher than when more people are accessing it remotely, and will attempt to take advantage of the situation.
4. **Review your existing policies, and closely monitor any necessary security exceptions.** When IT resources are stretched, organizations may need to make some exceptions to published security policies, standards, or practices. Implement a thorough review process to ensure such exceptions are closely monitored and solved. Also, most work-from-home policies weren't originally drafted to address a global conversion to remote work; organizations should carefully review those as well.

5. **Only connect to the Internet through a secure network.** When connected to a public network, any information you share online or via a mobile app could be accessed by someone else. Always use a Virtual Private Network (VPN) to encrypt your activity. Most organizations provide a VPN to their employees to ensure secure, remote access for work use, and personal VPN accounts are available from various service providers.
6. **Use strong passwords.** Many people use the same or similar version of a password for everything, even between work and home. Unfortunately, this means a single stolen password can be reused on multiple sites to unlock dozens of accounts for hackers. Remembering secure and complex passwords for every account can be difficult, if not impossible. Use password management software to ensure you have strong, unique passwords for everything, because passwords are the foundation of sound online security practices.
7. **Use multifactor authentication - now is the time to implement if you haven't already.** Traditional user login and password accounts are easy for bad actors to penetrate. Whenever possible, set up multifactor authentication on your accounts. This requires you to provide at least two authenticating factors, or proofs of identity, before you can access protected data, giving you a second line of defense against criminal activity. This additional level of protection is particularly critical when more people are accessing networks remotely, giving bad actors more entry points to access private networks.
8. **Only click on links, open attachments, and download software from trusted resources.** Most people want to stay informed with the latest information, especially during periods of uncertainty. Bad actors know this, and will attempt to take advantage by masking malicious links as something informative. Once clicked, that malicious link can be used to gain access to an individual's or organization's private information and/or freeze their computers or networks. If you're unsure of the source, go to the organization's website. If it's important, the information will be posted there as well.
9. **Verify website URLs before sharing confidential information.** Bad actors can create fake websites where both the URL and homepage look remarkably similar to a site you trust - such as your healthcare provider, bank, or email provider. Instead of following a link in an email, type the URL in by hand. Also, make sure the site you visit has HTTPS in the URL; these sites are more secure than those with HTTP.
10. **Don't respond to requests for information from unknown sources - especially if the request is for personally identifiable information or passwords.** Bad actors will attempt to con people into sharing confidential information by pretending to be someone you know or work with. Take extra care in identifying who you're sharing information with - even if you think the request came from a trusted resource or organization. Don't feel rushed; take the time to research the request and whether it's appropriate before responding.

Minimize Your Cyber Risks
Every commercial Chubb cyber policy provides access to a variety of resources to help organizations prepare for and quickly respond to disruptive cyber incidents, including:

- Online cyber security training that can be shared with employees to educate them on how to identify potential threats, protect sensitive data, and escalate issues to the right people when necessary.
- Password management software that can be deployed to employees, ensuring they always use secure and complex passwords.
- Cyber security rating services, providing objective, quantitative measurements on your company's security performance.
- Ransomware identification software, to help identify ransomware attacks from incoming malware, then mitigate the spread to other exposed devices on a company's network.

Chubb's personal cyber policyholders also have access to premier consulting, investigative, and crisis management services to help prevent incidents from happening.

Visit www.chubb.com/cyber to learn more about keeping your organization protected against cyber risk, or www.chubb.com/online-you-protected for additional tips on protecting your personal data at home.

Chubb. Insured.SM

This checklist contains general information only. Chubb does not have any obligation to oversee or monitor any insured's adherence to any guidance or practices set out in this document, or to any other risk control practices. The content of this document is presented for informational purposes only, and is not intended as a substitute for consultation with your insurance broker, or for legal or other professional advice. No liabilities or warranties are assumed or provided by the information contained in this document. Chubb is the marketing name used to refer to subsidiaries of Chubb Limited providing insurance and related services. For a list of these subsidiaries, please visit www.chubb.com. Product highlights are summaries only. Please see the actual policy for terms and conditions. Products may not be available in all locations, and remain subject to Chubb's underwriting criteria. Surplus lines insurance is sold only through licensed surplus lines producers.

Courtesy of
Schechner Lifson Corporation

CYBERRISKS&LIABILITIES_

Coronavirus and Managing Remote Work Cyber Risks

Given the implications of the coronavirus (COVID-19) outbreak, countless employees across a variety of industries are working remotely. While this allows businesses to remain operational, it can create a number of risks, particularly for those who fail to take the proper precautions.

Above all, information security is one the greatest challenges for companies allowing remote work during the COVID-19 outbreak. When an employee is at the office, their work is protected by safety standards that keep your company's network and data secure. However, an employee working from home may not have the same safety measures in place to protect your organization's devices and information.

In order to safeguard your business and employees from data breaches, cyber scams and viruses, consider the following strategies:

- **Train employees on how to detect and respond to phishing attacks.** Criminals prey on unfortunate circumstances, seeking to capitalize on victims during times of panic and hardship. Unfortunately, the COVID-19 pandemic is no exception. Cyber criminals have been known to pose as charities and legitimate websites to lure victims into sending money and revealing personal information. Individuals should scrutinize any emails, texts and social media posts related to COVID-19 and be cautious when clicking any links and attachments. Specifically, employees should be instructed to:
    - Avoid clicking links from unsolicited emails, and be wary of email attachments.
    - Use trusted sources when looking for factual information on COVID-19, such as CDC.gov.
    - Never give out personal or financial information via email, even if the sender seems legitimate.
    - Never respond to emails soliciting personal or financial information.
    - Verify a charity's authenticity before making any donations.
- Have a virtual private network (VPN) in place, and ensure employees are using it to access company systems and data when working remotely. VPNs encrypt internet traffic, which can be particularly useful when your employees are connected to a home or public network. Furthermore, it could be beneficial for your company to prohibit employees from accessing company information from public networks altogether.
- Mandate the use of security and anti-virus software. This software should be up to date and include the latest patches.
- Educate your employees on the kinds of sensitive data they are obligated to protect. This could include confidential business information, trade secrets, intellectual property and personal information. When working with sensitive data, employees should take to the same precautions

This Cyber Risks & Liabilities document is not intended to be exhaustive nor should any discussion or opinions be construed as legal advice. Readers should contact legal counsel or an insurance professional for appropriate advice.

they would if they were at the office. They should avoid using their personal email for company business and think critically about the documents they are printing at home. If they must print sensitive information, they should shred the document when it is no longer needed. Encrypting sensitive information can also help you protect any data that is stored or sent to remote devices.

- Prohibit employees from sharing their work devices with friends and family members. Doing so reduces risks associated with unauthorized or inadvertent access of company information.
- Have employees update their contact information. That way, if your systems are compromised, you can easily contact your staff and provide the appropriate updates and instructions.
- Create and communicate a system that employees can use to report lost or stolen equipment. This will help your IT department respond quickly and mitigate potential data loss threats.
- Require two-factor authentication for all company passwords. Two-factor authentication adds a layer of security that allows companies to protect against compromised credentials. Through this method, users must confirm their identity by providing extra information (e.g., a phone number or unique security code) when attempting to access corporate applications, networks and servers. This additional login hurdle means that would-be cyber criminals won't easily unlock an account, even if they have the password in hand.
- Consider security precautions for mobile devices. Proper phone security is just as important as a well-protected computer network. A smartphone could grant access to any number of applications, emails and stored passwords. Depending on how your organization uses such devices, unauthorized access to the information on a smartphone or tablet could be just as damaging as a data breach involving more traditional computer systems.

For additional protection, employers should consider backing up data and bolstering network protections as best as they can. For more cyber security guidance, contact Schechner Lifson Corporation today.

NEWS BRIEF

Provided by: Schechner Lifson Corporation

Cyber Criminals Seeking to Capitalize on Coronavirus

Criminals prey on unfortunate circumstances, seeking to capitalize on victims during times of panic and hardship. Unfortunately, the coronavirus disease 2019 (COVID-19) pandemic is no exception.

The Cybersecurity and Infrastructure Security Agency (CISA), part of the U.S. Department of Homeland Security, told individuals to be vigilant about scams related to COVID-19.

Cyber criminals have been known to pose as charities or legitimate websites to lure victims into sending money or revealing personal information. Individuals should scrutinize any email, text or social media post related to COVID-19 and be cautious when clicking any links or attachments.

CISA offered specific guidelines for individuals to avoid being scammed online:

- Avoid clicking links from unsolicited emails, and be wary of email attachments.
- Use trusted sources when looking for factual information on COVID-19, such as CDC.gov.
- Never give out personal or financial information via email, even if the sender seems legitimate.
- Never respond to emails soliciting personal or financial information.
- Verify a charity's authenticity before making any donations.

It's not always easy to disregard messages from senders that seem reputable, like banks. If individuals have any doubts about an email from a seemingly legitimate source, they should navigate to the organization's website and use the contact information there to reach out. Individuals should never respond to the initial message.

If individuals have any doubts about a message's sender, links or attachments, they shouldn't click anything in the message.

What Can Employers Do?

Employers should consider notifying employees about the existence of these COVID-19 cyber scams. Especially during times of crisis, scammers will pose as reputable sources and use fear to solicit personal information. Employers should also communicate best practices so employees know how to respond to such solicitations.

It may also benefit employers to back up data and bolster network protections in case an employee clicks the wrong link and compromises the entire system.

Speak with Schechner Lifson Corporation for more cyber security guidance.

CHUBB

ACE American Insurance Company
436 Walnut St.
Philadelphia, PA 19106

Chubb Cyber Enterprise Risk Management Policy

Cyber and Privacy Insurance

New Business Application

NOTICE

***NOTICE*: THE THIRD PARTY LIABILITY INSURING AGREEMENTS OF THIS POLICY PROVIDE CLAIMS-MADE COVERAGE, WHICH APPLIES ONLY TO CLAIMS FIRST MADE DURING THE POLICY PERIOD OR AN APPLICABLE EXTENDED REPORTING PERIOD FOR ANY INCIDENT TAKING PLACE AFTER THE RETROACTIVE DATE BUT BEFORE THE END OF THE POLICY PERIOD.**

AMOUNTS INCURRED AS CLAIMS EXPENSES UNDER THIS POLICY SHALL REDUCE AND MAY EXHAUST THE APPLICABLE LIMIT OF INSURANCE AND WILL BE APPLIED AGAINST ANY APPLICABLE RETENTION. IN NO EVENT WILL THE INSURER BE LIABLE FOR CLAIMS EXPENSES OR THE AMOUNT OF ANY JUDGMENT OR SETTLEMENT IN EXCESS OF THE APPLICABLE LIMIT OF INSURANCE. TERMS THAT ARE UNDERLINED IN THIS NOTICE PROVISION HAVE SPECIAL MEANING AND ARE DEFINED IN SECTION II, DEFINITIONS. READ THE ENTIRE POLICY CAREFULLY.

INSTRUCTIONS

Please respond to answers clearly. Underwriters will rely on all statements made in this **Application**. This form must be dated and signed.

1. Applicant Information

Desired Effective Date
Mm/dd/yyyy

Applicant Name
Click here to enter text.

Applicant Address (City, State, Zip)
Click here to enter text.

Please list all Subsidiaries for which coverage is desired:
Click here to enter text.

Applicant Type Choose an item.	**Ownership Structure** Choose an item.
Website Address Click here to enter text.	**Year Established** Click here to enter text.
Global Revenue (Prior Fiscal Year) Click here to enter text.	**% Domestic Revenue** Click here to enter text.
Global Revenue (Current Projected Fiscal Year) Click here to enter text.	**% Online Revenue** Click here to enter text.

Total Number of Employees
Enter a number or choose an item.

Number of Records Containing Protected Information:

What is the maximum total number of unique individual persons or organizations whose **Protected Information** could be compromised in a not-yet-discovered **Cyber Incident**, or will be stored or transmitted during the **Policy Period** on the Applicant's **Computer System** or any **Shared Computer System** combined that relate to the Applicant's business?

This should include **Protected Information** of employees, retirees, customers, partners and other third parties that the Applicant is responsible for securing, including **Protected Information** that is secured by third parties under contract with the Applicant. Multiple records or types of **Protected Information** relating to the same unique individual person or organization should be considered a single record.

Enter a number or choose an item

2. Nature of Operations

Class of Business

Describe nature of business operations, products or services in layperson terms.

Does the Applicant currently or will the Applicant potentially operate as any of the following?

- Accreditation Services Provider
- Adult Content Provider
- Credit Bureau
- Cryptocurrency Exchange
- Data Aggregator/Broker/Warehouse
- Direct Marketer
- Gambling Services Provider
- Manufacturer of Life Safety Products/Software
- Media Production Company
- Payment Processor
- Peer To Peer File Sharing
- Social Media
- Surveillance
- Third Party Claims Adminstrator

Or does the Applicant derive more than 50% of its revenue from technology products and services (e.g. software, electronics, telecom)?

☐Yes ☐ No

If Yes, please provide details:

Click here to enter text.

3. Current Loss Information

Within the past three years, has the Applicant had any actual or potential **Incidents** or **Claims** to which the **Policy** would apply; or is the Applicant aware of any fact, circumstance, or situation that could resonably be expected to give rise to an **Incident** or **Claim** to which the **Policy** would apply? ☐ Yes ☐ No

If Yes please provide details:

Click here to enter text.

4. Cyber and Media Controls

Which of the following IT security controls does the Applicant have in place?	
1) Antivirus and Firewalls (Windows 7 or higher qualifies)	□ Yes □ No □ Unknown
2) Encryption of Sensitive Data	□ Yes □ No □ Unknown
3) Encryption of Mobile Computing Devices	□ Yes □ No □ Unknown
4) Critical Software Patching Procedures	□ Yes □ No □ Unknown
5) Critical Data Backup and Recovery Procedures	□ Yes □ No □ Unknown
6) Formal Cyber Incident Response Plan	□ Yes □ No □ Unknown
Does the Applicant accept payment card (Credit/debit card) transactions?	□ Yes □ No
If Yes, is the Applicant PCI compliant? (via assessment or self-attestation)	□ Yes □ No □ Unknown
Does the Applicant deal with protected health information as defined by HIPAA?	□ Yes □ No
If Yes, is Applicant compliant with HIPAA and the HITECH Act?	□ Yes □ No □ Unknown
Does the Applicant have operations or customers in California, or any responsibilities under the California Confidentiality of Medical Information Act?	□ Yes □ No □ Unknown
Has the Applicant obtained legal review of its use of trademarks, including domain names?	□ Yes □ No □ Unknown

5. Current Coverage

Does the Applicant currently purchase Professional Liability or E&O insurance? **If Yes**, what is the Retro Date? Click here to enter a date.	□ Yes □ No
Does the Applicant currently purchase Cyber or Privacy Liability insurance? **If Yes**, what is the Retro Date? Click here to enter a date.	□ Yes □ No
Does the Applicant currently purchase Media Liability Insurance? **If Yes**, what is the Retro Date? Click here to enter a date.	□ Yes □ No
Does the Applicant intend to purchase E&O and/or Media coverage on a separate and distinct policy? (e.g. with a separate set of limits, or with another carrier?)	□ Yes □ No

6. Desired Coverage (Only Enter Information For Desired Coverages)

	Retention	Limit	Commentary
Cyber and Media Coverages	$	$	

Enter any further commentary about desired coverage options.
Click here to enter text.

Notice to Puerto Rico Applicants: Any person who knowingly and with the intention of defrauding presents false information in an insurance application, or presents, helps, or causes the presentation of a fraudulent claim for the payment of a loss or any other benefit, or presents more than one claim for the same damage or loss, shall incur a felony and, upon conviction, shall be sanctioned for each violation with the penalty of a fine of not less than five thousand (5,000) dollars and not more than ten thousand (10,000) dollars, or a fixed term of imprisonment for three (3) years, or both penalties. Should aggravating circumstances are present, the penalty thus established may be increased to a maximum of five (5) years, if extenuating circumstances are present, it may be reduced to a minimum of two (2) years.

Notice to New York Applicants: Any person who knowingly and with intent to defraud any insurance company or other person files an application for insurance or statement of claim containing any materially false information, or conceals for the purpose of misleading, information concerning any fact material thereto, commits a fraudulent insurance act, which is a crime and shall also be subject to: a civil penalty not to exceed five thousand dollars and the stated value of the claim for each such violation.

MATERIAL CHANGE

If there is any material change in the answers to the questions in this **Application** before the **Policy** inception date, the Applicant must immediately notify the **Insurer** in writing, and any outstanding quotation may be modified or withdrawn.

DECLARATION AND SIGNATURE

For the purposes of this **Application**, the undersigned authorized agents of the person(s) and entity(ies) proposed for this insurance declare to the best of their knowledge and belief, after reasonable inquiry, the statements made in this **Application** and any attachments or information submitted with this **Application**, are true and complete. The undersigned agree that this **Application** and its attachments shall be the basis of a contract should a policy providing the requested coverage be issued and shall be deemed to be attached to and shall form a part of any such policy. The **Insurer** will have relied upon this **Application**, its attachments, and such other information submitted therewith in issuing any policy.

The information requested in this **Application** is for underwriting purposes only and does not constitute notice to the **Insurer** under any policy of a Claim or potential Claim.

This **Application** must be signed by the risk manager or a senior officer of the **Named Insured**, acting as the authorized representative of the person(s) and entity(ies) proposed for this insurance.

Date Signature Title

________________ ________________________ __________________________