15 October 2019

Cyber and Data Breach Liability Insurance: Protecting Small Businesses and Our Nation

Primary Author

Charles Tupitza, RightExposure LLC

A licensed insurance consultant

Contributors

Carter Schoenberg, IPKeys Power Partners

Chip Block, Converged Security Solutions

Dr. Tony Lopez, INDUS Technology, Inc

Herb Bennett, The Baran Agency

Susan Yankaitis, Independent editor

Contact: Charles Tupitza cyber@rightexposure.com 202 839-5563

 © RightExposure 2019 v10.9.6

FORWARD

This document is for small and mid-sized businesses who are considering acquiring "cyber and data breach liability insurance" to protect themselves against the increasing velocity and complexity of cyber and data breach attacks.

It is also for larger businesses and governments to help them understand the value of the insurance for their contractors and extended supply chain members. Some may wish to require subcontractors and suppliers to have proper insurance in place, as a stipulation to providing goods or services to them.

Detailed guidance is provided to help small and mid-sized businesses identify value for them in coverage. Example language is provided for larger businesses to use in requests of subcontractors and suppliers to have proper insurance in place, as a stipulation to providing goods or services to them. Additional protection and services available from some insurance providers are identified as extra value businesses can gain from a policy beyond what they could afford on their own.

Preventable risk in the application process itself is addressed.

This is a living document. Threats will continue to change, along with the needs of businesses. The insurance industry is moving as fast as they can to provide value. This paper will be updated on a regular basis. We welcome input for updates.

Author Perspectives

This document takes a look at insurance from the perspective of value for small and mid-sized business owners, as well as large corporations or governments concerned about their contractors and supply chains.

- **Small and mid-size businesses (SMB)** need to understand the business value of insurance. A SMB in this document is defined as a company with less than 500 employees and an annual gross revenue of $100,000,000 or less. The Small Business Administration may have a lower employee threshold and a higher revenue threshold, but the insurance industry seems to address small businesses in these terms.

- **Large corporations** and governments are trying to understand the business value of requesting contractors and supply chain members to have insurance for protection against cyber and data breach threats for sustainability. They are also interested to see if their contractors and supply chain partners can get help from insurers they normally could not afford. They are trying to decide if it is "reasonable and prudent" to require contractors, subcontractors, and others within a supply chain to have a Cyber and Data Breach Liability insurance policy. If so, what should they include in their request to them?

Interviewed Entities

A market survey was conducted to address the above perspectives. Interviews were conducted with insurance companies, insurance brokers, consultants and agents, managing general agents and national insurance packagers, representatives from the National Institute of Standards and Technology, Department of Defense, Department of Energy, Federal Trade Commission, Department of Homeland Security, Small Business Administration, large federal civilian and defense contractors, large private sector businesses, the Americas Small Business Development Centers advisors, and members of the FBI InfraGard.

Also interviewed were the National Association of Insurance Commissioner members, representatives from major professional and trade associations representing millions of small businesses, local and national members of the US Chamber of Commerce, and over one hundred small businesses directly.

This document is a direct result of these interviews.

Table of Contents

BACKGROUND

All organizations have the responsibility to be aware of their cyber and data breach risks, to protect themselves, and if applicable, to be in compliance with state, federal and industry regulations. They also have the responsibility to work with other companies within their business ecosystem and supply chain, including individuals, to ensure they are also doing the same. Insurance is a part of an overall cyber and data breach risk management plan.

Many governments and larger private corporations now include a Cyber and Data Breach Liability Insurance requirement in bid specifications as a prerequisite to a subcontractor providing any goods or services to them.

This requirement is being put in place in order to help provide additional resources and financial protection to ensure the sustainability of the smaller sub-contractor post-breach, thus helping to protect the larger company's overall supply chain.

It is common business practice to transfer business risk to the insurance industry, much as companies would do with other risk concerns such as insuring property (against fire, theft, flood or other damages), or insuring the business against General Liability, Professional Liability, Employment Practices Liability, Workers Compensation or other types of losses.

These types of insurance are typically required to be in place by a contractor in order to secure or maintain a contract with a larger contracting entity. Understanding the complexities of how Cyber and Data Breach Liability Insurance is procured, what should be covered by a policy, along with what can be required in contracting specifications, is important for all involved parties.

It should be understood no representation is made that the minimum insurance requirements recommended in this survey are sufficient to cover the indemnity or other obligations of the SMB subcontractor.

WHAT IS CYBER AND DATA BREACH LIABILITY INSURANCE

There is a real urgency to understand the current value of Cyber and Data Breach Liability Insurance. Both large and small businesses and governments need information to be able to make informed business decisions about insurance. Blanket statements about mandating insurance need to be accompanied by coverage guidance or a bad policy that could satisfy a request and fail to cover the business and their business eco-system partners.

The value of Cyber and Data Breach Liability Insurance transcends beyond the single company insured, into the entire business ecosystem, thereby helping to protect the entire supply chain by ensuring they are all able to sustain a breach event. It is important for businesses to be able to understand the amount of financial coverage needed for each cause (Peril) that is reasonable and consistent with the anticipated exposure to loss.

Insurance companies need to articulate their value in terms of the cyber controls or help the client inherit from their policy just like other product and service providers. Conversely, the applicant should understand that having coverage does not negate their obligations to protect confidential information, their obligation to disclose breaches as required by each State Attorney General, and their responsibility to manage the likelihood of system disruption.

Definitions

The term **"Peril"** describes a specific cause of damage covered by the policy.

Some perils are covered only in certain situations, and others (like neglect) are excluded from insurance entirely.

The term **"Cyber"** implies coverage only for incidents involving electronic hacking or online activities.

The theft of electronic records in mass or as basic as someone stealing individual identity information or other critical information from an individual while online. In a "cyber event", someone was able to take control of the computer or server of a business without permission or knowledge, and stole information, records, intellectual property, or held those records for ransom, system disruption, or created other harm to the business.

"**Cyber Insurance**" needs to be addressed as "Cyber and Data Breach Liability Insurance"

This is more holistic in support of the loss of any confidential information, including information which may not be in an electronic form. Someone stole a sensitive document from a desk or paper files. Someone left their laptop, phone, or briefcase containing paper files at a coffee shop. Someone purchased a used copy machine and found the information on its hard drive from the previous owner of everything they had ever copied.

"Cyber and Data Breach Liability Insurance" coverage is specifically designed to protect an organization from:

- Costs associated with the response and recovery from a Cyber or Data Breach event, and;
- Liability claims involving the unauthorized release of information for which the organization has a legal obligation to keep private or confidential, and;
- Liability claims alleging invasion of privacy and/or copyright/trademark violations in a digital, online or social media environment, and;
- Liability claims alleging failures of computer security resulting in deletion/alteration of data, the transmission of malicious code, denial of service, ransomware, etc., and;
- Regulatory fines, penalties, and proceedings involving violations of State or Federal privacy law(s), and;
- Defense costs in State or Federal courts, and;
- The provision of expert resources and monetary reimbursement to the insured for the out-of-pocket (First Party) expenses associated with the appropriate handling of the types of incidents listed above.

Elements to Consider

Risk Transfer

It is normal industry practice to recognize certain business risks have a potential for sizable losses, and to then transfer some, or all, of that risk to other parties, (like an insurance company) when and where appropriate. This document is not meant to replace good proactive practices associated with protecting organizations from cyber and data breach events. Rather, it is to help ensure organizations have the capability to survive and to continue to operate at the same level following a breach event, by having a comprehensive Cyber and Data Breach Liability Insurance plan in place for their business.

Sustainability

Costs and losses associated with cyber-attacks and data breaches are high enough to put an SMB contractor out of business or impact their ability to perform. Proper insurance coverage protects them and all who depend on them.

- **Business ecosystem** members depend on contractors and suppliers to stay in business and perform their contract and/or mission.
- **Clients** depend on contractors to be responsible and protect the confidential information shared with them by the client intentionally but exposed by the contractor unintentionally.
- **Other stakeholders,** such as stockholders of the organization, depending on the protection of their investments and the organization's ability to perform their obligations.

Unified Messaging

Business risk is confusing. Cyber messaging comes from many directions and can be confusing. The insurance industry, as a stakeholder, can help unify messaging and enable the sharing of good practices by contractor size and industry type and support the use of these practices and standards.

Leverage of Resources

Many businesses lack the resources, capability, and capacity to best protect themselves or to adequately respond to breach events. Once a company becomes insured, then the insurer, as a stakeholder, can provide products and services which are normally unaffordable to the insured, especially in the area of breach detection, response, and recovery.

Value to the Supply Chain and Business Ecosystem

A 360-degree view of cyber insurance relating to overall business risk management and opportunity to sustain a cyber or other breach event has greater value and potential for impact larger than just a single contractor. Supply chain members are a critical part of many company's overall business eco-systems. If a member of the supply chain fails others are impacted.

WHAT TO LOOK FOR IN OFFERING

The following are key components of what should be taken into consideration for a company when considering the purchase of a comprehensive Cyber and Data Breach Liability Insurance policy.

1) Authorized/Domicile of the Insurance Carrier

The insurance carrier issuing the policy to the insured company should be domiciled in the USA, UK or an approved U.S. ally. Furthermore, the insurance carrier should provide insurance for claims incurred regardless of the originating source of the breach event, (i.e. provide worldwide coverage).

2) Security Breach Hotline

The insurance carrier issuing the policy to the company should provide the company with access to a call center, or other telephone support, staffed and available 24/7/365, that the company may call to notify the insurance carrier of a security breach (suspected or known).

The call center or hotline provided by the insurance carrier should provide the company with access to breach response legal counsel and breach response team(s) and access to other resources provided by the insurance carrier to promptly develop a response plan and to promptly begin recovery and response activities.

3) Minimum Coverage Limits by Policy Face Amount and Coverage Perils

NOTE: *No representation is made that the minimum insurance requirements outlined herein are sufficient to cover the indemnity, losses or other obligations of the policyholder and are only a "recommendation" of what is typically viewed within the insurance industry as reasonable minimum liability coverage limits*.

Any insurance policy should meet minimum coverage limits of no less than $1,000,000.00 USD per claim or in the aggregate of no less than $1,000,000.00 USD (limits should be set based on the revenue/size of the company to be insured or contract to be awarded. It is recommended that minimum policy coverage limits be set at no less than or equal to ten percent (10%) of the annual revenue of the company to be insured or contract to be awarded.

Thus, it is suggested that a company with $50,000,000 of annualized revenue or value of the contract should maintain no less than a $5,000,000 Cyber and Data Breach Liability Insurance policy) with no sub-limit for any coverage unless noted as such below. A policy with a perceived face value of $2,000,000 but has an "each cause for a claim sub-limit" of $150,000.00, means the company really only has a $150,000.00 policy.

4) Coverage Should Extend to Types of Losses (Perils)

Many policies have limits and conditions for each peril covered. Be sure to consider all limits associated with each peril.

a. Security Breach Response Coverage:

Coverage for costs incurred to respond as a result of a security breach event. Breach response costs include the costs of fees, charges or expenses incurred after the discovery of a security breach, including the following:

i. Computer forensic professional fees and expenses to determine the cause and extent of the Security Breach;

ii. Costs to notify any company, client, subcontractor or persons affected, or reasonably believed to be affected; including; printing costs, publishing costs, postage expenses, call center costs or costs of notification via phone or e-mail;

iii. Legal fees and expenses;

iv. Credit Monitoring Expenses for those affected by the security breach.

b. Privacy Liability (Including Employee Privacy)

Coverage for a claim arising out of any privacy wrongful act causing harm to any Third (3rd) Party or Employee. The coverage should provide liability protection for the company for the losses due to the unauthorized release of confidential or protected data and information, Personally Identifiable Information (PII), Protected Health Information (PHI), and any corporate confidential information of third parties and employees, and for any privacy breach violation of a person's right to privacy regardless of State or Federal specific definitions of confidential or protected data and information, PII or PHI.

c. Privacy Regulatory Claims Coverage

Provides coverage for both legal defense and the resulting fines/penalties (where insurable by law) emanating from a regulatory claim, alleging a privacy breach or a violation of a Federal, State, local or foreign statute or regulation, (including GDRP) with respect to privacy regulations.

d. Security Liability Coverage

Coverage for the company for allegations of a security wrongful act, including the inability of a third-party, who is authorized to do so, to gain access to the company's computer systems due to the failure to prevent unauthorized access to or use of a computer system, and/or the failure to prevent false communications such as phishing resulting in corruption, deletion of or damage to electronic data, theft of data and denial of service attacks against websites or computer systems of a third party. This coverage protects against liability associated with the company's failure to prevent transmission of malicious code from their system to a third party's computer system.

e. Multimedia Liability Coverage

Coverage for defamation, libel, slander, emotional distress, invasion of the right to privacy, copyright and other forms of intellectual property infringement (patent excluded) in the course of the company's communication of media in electronic (website, social media, etc.) or non-electronic forms.

f. Cyber Extortion Coverage

Coverage for expenses and payments (including ransom payments if necessary) to a third party to avert potential damage threatened against the company such as the introduction of malicious code, system interruption, data corruption or destruction or dissemination of personal or confidential corporate information.

g. Business Income and Digital Asset Coverage

Coverage for lost earnings and expenses incurred because of an authorized third-party's inability to access the company network due to disruption of the company's computer system(s) including restoration costs from the alteration, destruction, damage or loss of digital assets.

Business Interruption coverage should also provide for reimbursement of lost earnings and expense the insured incurs in the event a network disruption event occurs on a system of an IT service provider (i.e.: cloud provider) for whom the insured is reliant upon (and with whom they have a contract) to operate their business.

h. Payment Card Industry Data Security Standard (PCI-DSS) Assessment Coverage

If the company maintains or processes credit or payment cards, then the company should maintain at least $100,000 of PCI-DSS fines and assessment coverage to respond to any fines, penalties or other costs to respond to, or levied by, the Payment Card Industry Security Standards Council, under the Payment Card Industry Data Security Standards, as well as have coverage for expenses associated with a mandatory audit performed by a Qualified Security Assessor (QSA), certified by the PCI Security Standards Council, after a data breach event.

i. Cyber Deception Coverage

The company should maintain at least $100,000 of cyber deception coverage for losses from the intentional misleading of the company by means of a dishonest misrepresentation of a material fact contained or conveyed within an electronic or telephonic communication(s) and which is relied upon by the company believing it to be genuine which results in a financial loss to the company.

j. Funds Transfer Fraud Coverage

The company should maintain coverage of no less than $100,000 for losses incurred from an unauthorized electronic funds transfer, theft of company money or other financial assets from the insured company's bank by electronic means, or theft of money or other financial assets by electronic means, or any fraudulent manipulation of electronic documentation while stored on company computer system(s) that lead to a transfer of funds based on the fraudulent electronic documentation.

k. Duty to Defend and Defense, Settlement, and Investigation Cost Coverage

The policy should have coverage and wording noting the insurance carrier should defend (Duty to Defend), the company for any claim made against the company seeking damages which are potentially payable under the terms of the insurance policy, even if any of the allegations of the claim are groundless, false, or fraudulent.

l. TRIA/Acts of Cyber Terrorism Coverage

The policy should include coverage for any act certified as an "Act Of Cyber Terrorism" for those acts perpetrated electronically, pursuant to the federal Terrorism Risk Insurance Act of 2002 or otherwise declared an "Act Of Terrorism" by any government or; any act committed by any person or group of persons designated by any government as a terrorist or terrorist group or any act committed by any person or group of persons acting on behalf of or in connection with any organization designated by any government as a terrorist organization, whether acting alone or on behalf of or in connection with any organization or government, committed for political, religious, ideological, or similar purposes, including the intention to influence any government and/or put the public, or any section of the public, in fear.

m. Ransomware Coverage

The policy should include coverage for ransomware. This will most likely come in the form of reimbursement versus the insurance company directly being in involved with the criminal directly. Ransomware insurance should be coupled with an effective risk management program.

5) Attorney-Client Privilege

The insurance company that will issue the policy to the insured company should provide for the attorney-client privilege at the start of, (or at the time of) the reporting of a cyber or data breach event or claim.

Attorney-client privilege refers to a legal privilege that works to keep confidential communications between an attorney and his or her client secret. The privilege is asserted in the face of a legal demand for communications, such as a discovery request or a demand that the lawyer testifies under oath.

From Cornell Law School Legal Information Institute "Attorney-Client Privilege"

6) Assistance with Data Breach Reporting Requirements

Most data breaches expose information about companies or individuals in multiple states. Breach notifications required by each of these states vary. Many public and private contracts require specific notification of a breach, such as the Department of Defense requirement of notification within 72 hrs.

Penalties can be high if these reports are not provided in the time required. Small businesses can leverage the capability and capacity of the insurance industry via hotline support. *(It's not reasonable to think small businesses understand these requirements and have the resources to report accurately and on time without help).* Check to see I there is an additional charge for this service.

7) Assistance with Response/Recovery from Cyber Threat or Incident

It is critical to be able to respond to a threat and recover from an incident as quickly as possible. On their own, individual companies may not have the capability or capacity to respond and recover in a timely or effective manner. Often help is needed. Seeking credible resources when under the pressure of a cyber-attack threat is difficult. Valuable time can be lost which will affect the company's ability to perform its mission. The insurance company as a stakeholder can provide assistance.

8) Business Type, Class, or Industry in the Application Process

Many potential insured companies may have characteristics that are common across different types of businesses or industries. This makes it difficult for a potential insured to accurately label or classify their business for the insurance carrier; who may determine rates and coverages based upon the type of business or industry that is disclosed in the application process.

The insurance carrier will use this information when determining their rates for a business based upon the underwriting rates they have established for a particular industry, business type or underwriting "class". It is important for the insured to document the rationalization of choice and have formal recognition from the Insurer if unclear how to answer this underwriting question. A contractor's business class may not be covered by an Insurer. Representing a business class to "fit" the application versus the actual class, will jeopardize coverage at the time of a claim filing.

9) Coverage Limitations Due to Cyber Terrorism

Some Cyber Insurers have specific language to deny claims for "Cyber Terrorism", thereby excluding coverage for these claims. As such, a company should maintain coverage that will extend not only to Cyber Terrorism, (as well as elect to maintain the TRIA endorsement (See 5(l) above), but also ensure that they have coverage that will extend coverage for "foreign acts", whether tied to cyber terrorism or not, as long as such acts are perpetrated electronically.

SUGGESTED COVERAGE REQUIREMENTS FOR COMPANIES/CONTRACTORS

The company to be insured, should have the following coverage in place and take into consideration the following while considering the provision of adequate protection.

Coverage should be secured for losses incurred for both Cyber and Data Breach events and the liability and potential expenses that could be incurred by a company from a range of threats and incidents, including the following First-Party and Third-Party exposures:

First-Party

a. Legal expertise and advice regarding breach response and requirements
b. Costs to notify all affected individuals and organizations
c. Forensic costs to investigate the cause of the breach
d. Business interruption costs
e. Public regulations and crisis management costs
f. Data recovery and restoration costs
g. Cyber extortion and ransomware costs

Third-Party

h. Payment to those affected by the breach
i. Regulatory fines and penalties
j. Defense costs in state and federal courts
k. Costs incurred to respond to the regulatory actions and review
l. Settlements, damages and judgements

The term "Cyber Breach" implies coverage only for incidents involving electronic hacking or online activities and "Data Breach" is in reference to coverage of any private data and communications in different formats, including paper. A company should maintain a policy from an authorized insurance carrier providing acceptable levels of coverage for both Cyber and Data Breach events

CONCERNS DURING APPLICATION PROCESS

A company should not disclose, in an unsecured environment, details about the company (other than publicly available information such as name, address, contact information, etc.) or any information about past cyber and data breach events or losses, as well as the company's current cybersecurity processes or procedures (other than to answer basic underwriting questions). A general recommendation would be that for a small contractor, that the question set should not need to exceed twelve (12) underwriting questions pertaining to past events or losses or to current cybersecurity processes and procedures).

	COMMON OBJECTIONS	AVAILABLE SOLUTIONS
Length of Application Process	*Lengthy and Complicated* Some carriers have a written paper application process that can take as much as thirty (30) days for a company to receive a bound policy from the start of a written, paper application that is submitted to the carrier's underwriting department for review.	*Short and Simple* Some policies are available all online with simplified underwriting, allowing a contractor to obtain coverage and download a policy and proof of insurance within minutes of starting the application process.
Ease of Application Process	*Multi-Person Applicants Required* Complex underwriting process requiring the need to engage multiple disciplines such as HR, IT, Legal and other departments of the company to be insured.	*Single-Person Application Process* Carriers are offering an online application process based on a single person applicant process, thus minimizing the effort for a contractor.
Security of Application Process	*Risky Application Process* Some Insurers request the completion of detailed and lengthy underwriting questions which are answered by the applicant company on paper with few if any, security controls in place to protect this information once submitted to the insurance carrier, putting the applicant company and their business supply chain partners at risk.	*Simplified and Secure Process* Policies asking as few as 8 -12 underwriting questions all online are available and minimize the risk of critical information getting into the wrong hands. Companies with over $100m of revenue need to be assured their application be stored on an independently secure cloud with strong access controls. (example FedRAMP certified)
Cost of Policy	*Costs Too Much* Some rates are very high, with average annual policy costs over $15,000.00/ year for $1,000,000 policy.	*Cost Within Reason* Competition has driven rates down. One carrier pricing starts at below $1,000/ year for a $1,000,000 policy

Coverage Availability Within States	*Coverage issued by a Non-Admitted or Non-U.S. Domiciled Insurance Carrier* There are many insurance carriers who provide coverage that are not domiciled in the U.S.A. and may offer insurance offerings that will differ substantially in different states.	*Coverage issued by a U.S Based Insurance Carrier* Look for an Insurer who is domiciled in the United States and offers the same policy in all 50 states, thus providing a consistent strategy to protect the company.
Confusion Of Policy Coverage	*Policy Coverage is Not Clear* Some insurance applications provide very little information about the policy offered until the company actually pays for it and receives its bound policy.	*Clarity of Policy Coverage* Look for a policy offering a comprehensive FAQ, written in simple easy-to-understand language, and a specimen policy for review prior to binding/purchase.
Number of customer records	*Difficult to Accurately Answer* Some Insurers request the total number of customer records in the custody of applicant (in control or maintained on the company's systems) If an incident occurs this number could create a problem for your coverage even though you did not intentionally misrepresent this number	*Avoid Answering this Question* Look for an Insurer who does not ask this question. This question can have a major impact on an insurance premium. Consider the implications of having a large number of records on your need for proper coverage.
Potential For Claim Denial	*Excessive Amount of Questions* Lengthy applications inherently produce more warranty information from which an insurance company can use to deny a claim.	*Concise and Reasonable Application* A shorter application inherently produces less warranty information which can be used to deny a claim.

If an underwriting insurance company asks for more detailed questions as part of the application process, (i.e. more than 12 basic underwriting questions in Appendix I) or requires the company to provide details to fully answer the basic underwriting questions, then the application for the purchase of the insurance should be done in a "secure" format. "Secure" is defined as "the application should be conducted and stored in a certified secure cloud storage system with proper controls of access to the information contained in the application".

APPENDIX I

Examples of Basic Underwriting Questions

Past Events or Losses

a. Is your company aware of any current or past circumstances, within a reasonable time frame, which may indicate your company has suffered a cyber or data breach?

b. Has your company ever experienced a cyber or data breach resulting in a state, federal or other regulatory fine or penalty?

c. Has your company ever been sued or had other litigation that resulted from a cyber or other form of a data breach?

d. Has a subcontractor, under the direct supervision of your company, ever reported to you a cyber or another form of a data breach that may have compromised data provided by your company to the subcontractor?

e. Has your company ever experienced any system intrusions, tampering, viruses or malicious code attacks that resulted in the loss of data; or had any hacking incidents, extortion attempts, or other forms of data theft?

f. Has your company experienced a financial loss due to the transfer of funds in excess of $10,000 due to cyber deception?

Current Cyber Security Processes and Procedures

a. Does your company back up your data and systems?

b. Does your company store these backups in an offsite location, or does someone regularly do this on your behalf?

c. Does your company utilize firewalls?

d. Does your company utilize anti-virus applications?

e. Does your company utilize multifactor authentication for systems maintaining controlled unclassified information, including financial records?

f. Does your company have a process for dual authorizations for the electronic payments or transfer of funds over $10,000.00?

g. Does your company provide training to those employees and staff who are responsible for the transfer of funds in excess of $10,000 externally?

APPENDIX II

Sample Cyber and Data Breach Insurance Requirements for Most Contracts

The following is suggested wording for an organization to include as part of vendor insurance requirements when creating a request for proposal, etc.

Vendor shall procure and maintain for the duration of the contract insurance against claims which may arise from or in connection with the performance of the work hereunder by the Contractor / Vendor ('Company"), its agents, representatives, or employees. Contractor / Vendor shall procure and maintain for the duration of the contract insurance against claims arising out of their services and including, but not limited to loss, damage, theft or other misuses of data, infringement of intellectual property, invasion of privacy and breach of data.

1) Minimum Coverage Amounts and Limits

Contractor / Vendor shall maintain coverage in an amount of no less than $ X,000,000 per claim and $ Y,000,000 in the aggregate (unless noted below as acceptable per peril / claim sub-limit) to cover the replacement value of, or damage to, alteration of, loss of, or destruction of electronic data and/or information "property" of "XXXXXXXX" that will be in the care, custody, or control of Contractor/Vendor.

Furthermore, the insurance policy must contain coverage for the following:

a. Security Breach Response Coverage

Coverage for costs incurred to respond as a result of a security breach event. Breach response costs include the costs of fees, charges or expenses incurred after the discovery of a security breach, including:

i. Computer forensic professional fees and expenses to determine the cause and extent of the Security Breach;
ii. Costs to notify any Vendor / Contractor, client, subcontractor or persons affected, or reasonably believed to be affected; including; printing costs, publishing costs, postage expenses, call center costs or costs of notification via phone or e-mail;
iii. Legal fees and expenses;
iv. Credit Monitoring Expenses for those affected by the security breach.

b. Privacy Liability (including employee privacy)

Coverage for a claim arising out of any privacy wrongful act that causes harm to any Third (3rd) Party or Employee. The coverage must provide liability protection for the Vendor / Contractor for the losses due to the unauthorized release of data and information, Personally Identifiable Information (PII), Protected Health Information (PHI), and any corporate confidential information of third parties and employees, and for any privacy breach violation of a person's right to privacy regardless of State or Federal specific definitions of such data and information, PII or PHI.

c. Privacy Regulatory Claims Coverage

Coverage must be provided for both legal defense and the resulting fines/penalties emanating from a regulatory claim, alleging a privacy breach or a violation of a Federal, State, local or foreign statute or regulation, (including GDRP) with respect to privacy regulations.

d. Security Liability Coverage

Coverage must extend for all allegations of a security wrongful act, including the inability of a third party, who is authorized to do so, to gain access to the Contractor / Vendor's computer systems due to the failure to prevent unauthorized access to or use of a computer system, and/or the failure to prevent false communications such as phishing that results in corruption, deletion of or damage to electronic data, theft of data and denial of service attacks against websites or computer systems of a third party. This coverage protects against liability associated with the Contractor or Vendor's failure to prevent transmission of malicious code from their system to a third party's computer system.

e. Multimedia Liability Coverage

Coverage for defamation, libel, slander, emotional distress, invasion of the right to privacy, copyright and other forms of intellectual property infringement (patent excluded) in the course of the Contractor / Vendor's communication of media in electronic (website, social media, etc.) or nonelectronic forms.

f. Cyber Extortion Coverage:

Coverage for expenses and payments (including ransom payments if necessary) to a third party to avert potential damage threatened against the Vendor / Contractor such as the introduction of malicious code, system interruption, data corruption or destruction or dissemination of personal or confidential corporate information.

g. Business Income and Digital Asset Coverage

Coverage for lost earnings and expenses incurred, and reimbursement to the insured for their loss of income resulting from their inability to access their own network – or the network of IT service providers for whom they are contractually reliant upon in order to transact their business and resulting from an authorized third-party's inability to access the Vendor / Contractor network due to disruption of the Vendor / Contractor's computer system(s) including restoration costs from the alteration, destruction, damage or loss of digital assets.

h. PCI-DSS Assessment Coverage

If the Vendor / Contractor maintains or processes credit or payment cards, then the Vendor / Contractor must maintain at least $100,000 of PCI-DSS fines and assessment coverage to respond to any fines, penalties or other costs to respond to, or levied by, the Payment Card Industry Security Standards Council, under the Payment Card Industry Data Security Standards, as well as have coverage for expenses associated with a mandatory audit performed by a Qualified Security Assessor (QSA), certified by the PCI Security Standards Council, after a data breach event.

i. Cyber Deception Coverage

The Vendor / Contractor must maintain at least $100,000 of cyber deception coverage for losses from the intentional misleading of the Vendor / Contractor by means of a dishonest misrepresentation of a material fact contained or conveyed within an electronic or telephonic communication(s) and which is relied upon by the Vendor / Contractor believing it to be genuine which results in a financial loss to the Vendor / Contractor.

j. Funds Transfer Fraud Coverage

The Vendor / Contractor must maintain coverage of no less than $100,000 for losses incurred from an unauthorized electronic funds transfer, theft of Vendor / Contractor money or other financial assets from the insured Vendor / Contractor's bank by electronic means, or theft of money or other financial assets by electronic means, or any fraudulent manipulation of electronic documentation while stored on Vendor / Contractor computer system(s) that lead to a transfer of funds based on the fraudulent electronic documentation.

k. Duty to Defend and Defense, Settlement, and Investigation Cost Coverage:

The policy must have coverage and wording that notes that the insurance carrier must defend (Duty to Defend), the Vendor / Contractor for any claim made against the Vendor / Contractor seeking damages which are potentially payable under the terms of the insurance policy, even if any of the allegations of the claim are groundless, false, or fraudulent.

l. TRIA/ACTS of Cyber Terrorism Coverage for Acts that Are Perpetrated Electronically:

The policy must include coverage for any act certified as an "Act of Cyber Terrorism" pursuant to the federal Terrorism Risk Insurance Act of 2002 or otherwise declared an "Act of Cyber Terrorism" by any government or; any act committed by any person or group of persons designated by any government as a terrorist or terrorist group or any act committed by any person or group of persons acting on behalf of or in connection with any organization designated by any government as a terrorist organization; whether acting alone or on behalf of or in connection with any organization or government, committed for political, religious, ideological, or similar purposes, including the intention to influence any government and/or put the public, or any section of the public, in fear.

2) Acceptability of Insurers

Insurance is to be placed with insurers authorized to conduct business in the state with a current A.M. Best's rating of no less than A:VIII, unless otherwise acceptable to "XXXXXXXX". Furthermore, The insurance carrier issuing the policy to the Vendor / Contractor to be insured must be domiciled in the USA, UK or an approved U.S. ally, that insures the Company, based in the USA, regardless of the originating source of the breach event, (i.e. worldwide coverage).

3) Security Breach Hotline

The insurance carrier issuing the policy to the Company must provide the Company with access to a call center, or other telephone support, that is staffed and available 24/7/365, that the Company may call to notify the insurance carrier of a security breach (suspected or known). The call center or hotline provided by the insurance carrier must provide the Company with access to breach response legal counsel and breach response team(s) and access to other resources provided by the insurance carrier to promptly develop a response plan and to promptly begin recovery and response activities.

4) Self-Insured Retentions

Self-insured retentions must be declared to and approved by "XXXXXXXX". At the option of "XXXXXXXX", either: The Vendor / Contractor shall cause the insurer to reduce or eliminate such self-insured retentions as respects this agreement and, "XXXXXXXX" its officers, officials, employees, and volunteers; or the Contractor shall provide a financial guarantee satisfactory to "XXXXXXXX", guaranteeing payment of losses and related investigations, claim administration, and defense expenses.

5) Other Insurance Provisions

The insurance policies are to contain, or be endorsed to contain, the following provisions:

a. Primary Coverage: For any claims related to this contract, the Vendor / Contractor's insurance coverage shall be primary insurance primary coverage.

b. Notice of Cancellation: Each insurance policy required above shall state that coverage shall not be canceled, except with notice to "XXXXXXXX".

c. Subcontractors: Vendor / Contractor shall require and verify that all subcontractors maintain insurance meeting all the requirements stated herein.

d. Special Risks or Circumstances: “XXXXXXXX” reserves the right to modify these requirements, including limits, based on the nature of the risk, prior experience, insurer, coverage, or other special circumstances.

e. Insurance Obligation: The insurance obligations under this agreement shall be the greater of all the insurance coverage and limits carried by or available to the Company; or the minimum insurance requirements shown in this agreement.

f. Use of Excess Proceeds: Any insurance proceeds in excess of the specified limits and coverage required, which are applicable to a given loss, shall be available to “XXXXXXXX”.

g. No representation is made that the minimum insurance requirements of this agreement are sufficient to cover the indemnity or other obligations of the Vendor under this agreement. If the Vendor maintains broader coverage and/or higher limits than the minimums shown above, “XXXXXXXX” requires and shall be entitled to the broader coverage and/or the higher limits maintained by the Vendor / Contractor.

APPENDIX III

Cybersecurity Maturity Model Certification (CMMC)

The risk and opportunity to our supply chain is obvious. The Department of Defense (DoD) has recognized the threat and is addressing it in the upcoming Cybersecurity Maturity Model Certification program.

Insurance has a direct role to help small businesses become CMMC certified by taking advantage of support articulated in this document by insurers.

Some insurance companies help businesses protect themselves by providing products and services along with the policy that may not be affordable outside the policy.

This appendix will be updated soon as more details are revealed about the CMMC and its use beyond the DoD.

For more information about the CMMC: *https://www.acq.osd.mil/cmmc*

PRIMARY AUTHOR

Charles Tupitza is a licensed insurance consultant in the Commonwealth of Virginia and president of RightExposure LLC. He is an active member of the Software and Supply Chain Assurance Forum sponsored by the DHS, GSA, NIST, and DoD. He was a charter member of a Presidential Directive PPD-21 working group to determine federal contracting officer's needs for cyber and another seeking common cyber contracting terms. He supports America's Small Business Development Centers Cybersecurity First Steps program and support of the Cybersecurity Maturity Model Certification. He was formerly the Head of Cyber Resilience in the US for Axelos and led discussions about how to incorporate cyber resilience in enterprise IT systems utilizing the international framework of ITIL. As CEO of the National Forum for Public and Private Collaboration, he led the collaboration between the private sector and Defense Department about cyber resilience in enterprise service management and IT systems.

CONTRIBUTORS

Carter Schoenberg is the Executive Vice President of Cybersecurity Solutions with IPKeys Power Partners. Mr. Schoenberg is a Certified Information System Security Professional (CISSP) with over 25 years of combined experience in criminal investigations, cyber threat intelligence, cybersecurity, risk management, and cyber law. His specialized experience in where cyber, legal and insurance considerations converge has helped both private and public sector leaders address Supply Chain Cyber Risk Management (SCRM) issues. His products are used by the DHS and DoD, the Information Sharing and Analysis Center (ISAC) communities, and the Georgia Bar Association for Continuing Learning Educational (CLE) credits on the topic of cybersecurity risk and liability. His expertise has been profiled at conferences including the National Association of Insurance Commissioners (NAIC) Annual Conference, Council for Insurance Agents and Brokers (CIAB), ISC2, SecureWorld Expo, ISSA, Latin American Insurance & Reinsurance Forum, and InfosecWorld.

Chip Block is the Vice President and Chief Solutions Architect at Converged Security Solutions. Mr. Block has over thirty years of advanced technology research and development. He is a frequent speaker and author including "And Then the Accountants Showed Up…How The Insurance Industry Will Drive Cybersecurity." His research has included federal projects with DARPA and the Air Force Research Laboratory (AFRL) in the development of advanced cyber technologies and commercial work with Internet of Things with a focus on medical devices. Mr. Block is a recipient of an R&D 100 Award for the top research achievements for a year as awarded by R&D magazine. He received the ACT-IAC Individual Contributor of the Year Award in 2016 and is a certified Open FAIR™ analyst.

Dr. Tony Lopez is a Vice President and Chief Information Security Officer at INDUS Technology, Inc. and as stated above was responsible for the development and implementation of both INDUS' NIST 800- 171and INDUS' Internal Threat Program, so he has firsthand knowledge of the NIST 800-171, DFARS 7012 and the Cyber Maturity Model Certification (CMMS) requirements and what it takes to meet these requirements. Dr. Lopez Chaired a NIST 800-171 Small Business Task Force to study the impact of NIST 800-171 and DFARS 7012 small business by the San Diego NDIA Chapter. This Task Force recently published a final paper discussing the impact. Dr. Lopez has over 25 years working in the Defense Industry and for Federal Agencies, 16 of these as Director of Information Systems INDUS Technology and today Vice President of Operations and CISO. Other recent experience includes Director of Instructional Systems and Technology at the Navy Center for Information Technology and Program Manager of NASA's SOLAR e-Learning Program. Dr. Lopez's holds a bachelor's degree from Cal State San Luis Obispo in Mechanical Engineering, a Master's Degree in Business Administration from the University of Phoenix and a Ph.D. from Cal Southern University in Business Administration

Herb Bennett is Director of Cyber Security and Compliance Operations at the Baran Agency, a veteran-owned cybersecurity and compliance as a service company that utilizes a workforce of highly trained ex-military. The Agency specializes in working with Dept. of Defense and other government contractors, as well as high profile cybersecurity targets in the private sector. He is also the founder and Chief Training Officer of Veterans Re-Entry Training (VRT), an educational center dedicated to assisting military veterans transitioning back to civilian employment in cybersecurity after military service. Prior to his civilian career, Herb served in the United States Army 82nd Airborne Infantry and Special Operations. He is also certified in CompTIA IT Fundamentals, A+, Network+, Security+, CySA, PenTest+, Project+, CTT+, and a EC-Council Certified Ethical Hacker (CEH).

Susan Yankaitis, Independent technical writer and editor.

We would like to hear from you.

Please contact us with comments.

We will be updating this document on a regular basis and giving credit to contributors.

Contact: Charles Tupitza cyber@rightexposure.com 202 839-5563

This document is for the use of any organization including governments for the purpose of making informed general business decisions regarding the value of Cyber and Data Liability Insurance.

RightExposure LLC and the authors are not responsible for decisions made by the readers as a result of the information disclosed in this document. Conditions regarding the value and use of this information continuously change.