Financial Services Sector Coordinating Council
for Critical Infrastructure Protection and Homeland Security

Purchasers' Guide to Cyber Insurance Products

Introduction

Seeking improved cybersecurity in the face of ever-evolving cyber threats is one of the great challenges of our time. There are numerous tools and frameworks that can assist organizations attempting to identify cyber vulnerabilities and improve cybersecurity. However, little assistance is available for an organization that wants to not only mitigate the risks of cyber incidents, but also transfer those risks through the purchase of insurance products. As a result, some organizations are unaware of or intimidated by cyber insurance products.

This document, a *Purchasers' Guide to Cyber Insurance Products*, is intended to provide resources and advice to organizations—particularly small and medium-sized enterprises—that are considering the purchase of cyber insurance. It provides an overview of the cyber insurance market and identifies key questions that a prospective policyholder should ask itself, its broker or agent, and its insurer when considering the purchase of cyber insurance. A Glossary is included as Appendix A.

Please note that this guide provides only limited background on cyber insurance, and, in all cases, organizations should consult with knowledgeable professionals before placing coverage.

Cyber Risk and Cyber Insurance

In its December 2014 paper, *Cyber Resilience: The cyber risk challenge and the role of insurance*, the CRO (Chief Risk Officers) Forum explained that "cyber risk covers the risks of doing business, including managing and controlling data, in a digital or 'cyber' environment."[1] More specifically, "cyber risk" refers to "any risks that emanate from the use of electronic data and its transmission, including technology tools such as the internet and telecommunications networks. It also encompasses physical damage that can be caused by cyber attacks, fraud committed by misuse of data, any liability arising from data storage, and the availability, integrity, and confidentiality of electronic information – be it related to individuals, companies, or governments."[2] The level of threat that such attacks pose was highlighted recently when the World Economic Forum identified technological

[1] CRO Forum, *Cyber Resilience Paper* at 3 (December 2014).
[2] *Id*. at 5.

risks, in the form of data fraud, cyber-attacks, or infrastructure breakdown, as one of its top 10 risks facing the global economy in its 2015 Global Risk Report.[3]

These risks are real and widespread. In the fall of 2014, PricewaterhouseCoopers' (PwC's) annual global information security survey of corporate executives, which included 9,700 participants, reported that almost 43 million cybersecurity incidents were detected during the past year, a 48 percent increase over 2013.[4] The number of cybersecurity incidents reported to the 2015 PwC survey increased by another 38 percent.[5] The costs associated with cybersecurity incidents often include disruption of business, erosion of customers, loss of revenue, forensic investigations, customer notification, regulatory fines, legal penalties, attorney fees, brand and reputational damage, loss of intellectual property, and the exposure of sensitive or confidential personal and business information. Data breaches can cost businesses millions of dollars.[6]

The insurance industry has responded to these risks with a variety of products collectively referred to as "cyber insurance." Such insurance is offered as an endorsement to existing policies or as a stand-alone policy, and may include a variety of different coverages. Most cyber insurance carriers provide data privacy coverage, which generally includes liability coverage for loss or breach of data, coverage for the remediation costs associated with loss or breach of data (*e.g.*, customer notification and forensic investigations), and coverage for regulatory fines and/or penalties associated with data breaches. Policyholders can also purchase coverage for, among other things, costs and liability arising out of cybersecurity incidents not involving data breaches, business interruption, contingent business interruption, cyber extortion, and media liability. These products will be discussed in further detail below.

Cyber Insurance Market

The U.S. cyber insurance market is growing, with most industry analysts estimating that the market reached $2 billion in premium in 2014.[7] The market has over sixty carriers, but only a small number of these insurers write aggregate premiums in excess of $100 million. Brokers help policyholders construct "towers" of coverage by placing a primary layer of insurance and then adding excess layers of coverage to reach a desired limit; even the largest of these towers generally provide no more than $400 million in coverage.[8] Although these towers often cover a variety of cyber risks, coverage limits vary by type of claim. For

[3] World Economic Forum, *Global Risks 2015* (2015), *available at* http://www3.weforum.org/docs/WEF_Global_Risks_2015_Report15.pdf.
[4] PwC, *Managing Cyber Risk in an Interconnected World: Key Finding from The Global State of Information Security Survey 2015*, at 7 (Sept. 30, 2014).
[5] PwC, *Turnaround and Transformation in Cybersecurity: Key Findings from The Global State of Information Security Survey 2016*, at 2 (September 2015).
[6] Ponemon Institute, 2014 Cost of Cyber Crime Study: United States, at 3 (Oct. 2014) (noting that financial loss from cyber attacks in the U.S. at surveyed organizations ranged from $1.6 million to $61 million annually per company); Experian, 2015 Data Breach Industry Forecast, at 8 (2015) (finding that "the average data breach costing organizations $3.5 million").
[7] Dan Schutzer, CTO Corner, Financial Services Roundtable, *An Assessment of Cyber Insurance* (February 2015); The Betterly Report, *2014 Cyber/Privacy Insurance Market Survey* (June 2014).
[8] Willis Re, *Marketplace Realities 2015: Spring Update* (April 2015).

example, while some policies cover contingent business interruption (*i.e.*, a cyber incident at a third party causes a business interruption for the policyholder), the sublimit for such coverage usually is very limited. Due to recently paid claim activity, cyber risk insurance premiums generally have grown more expensive, though this increase depends upon the particular coverage. At the same time that cyber-specific insurance products have developed, many traditional policies have begun explicitly excluding coverage for losses arising from cyber incidents. Additionally, some courts have found that traditional policies do not cover cyber losses.

Prospective policyholders have the opportunity to negotiate policy terms with most cyber insurance carriers. The vast majority of cyber risk insurance policies are sold by non-admitted insurers (*i.e.*, insurers, usually subsidiaries of larger insurance groups, licensed only in the state or country of the insurer's domicile) or by admitted carriers through deregulation exceptions for sophisticated buyers, both of which are subject to less regulation and are not legally tied to specific policy forms. Consequently, most cyber risk insurers have more freedom to negotiate with prospective policyholders, modify underwriting standards and rates, and adopt new policy provisions than do carriers of other insurance products.

While a variety of cyber insurance products are available in the U.S. market, the large majority of cyber insurance is for data privacy coverage. This focus on data breach coverage is largely due to U.S. regulatory complexity, which includes federal laws regarding health records and data breach notification laws in 47 states.[9]

The European market for cyber insurance products is also growing,[10] although differently from the U.S. market. Lloyds of London experienced a 50 percent increase in demand for cyber insurance products during the first quarter of 2015 as compared to the first quarter of 2014.[11] Cyber insurance demand in Europe has not been focused on data privacy coverage, as the European Union lacks the type of data notification laws that many U.S. states have. However, proposed EU General Data Protection Regulation (GDPR) legislation, which is focused on empowering national data commissioners by providing them with powers to fine companies who violate EU data rules up to 4% of global annual turnover.[12]

The Value Proposition for Cyber Insurance

As cyber risks grow, the senior management and boards of directors of companies have increasingly focused on a holistic response to cyber threats that includes risk mitigation, risk transfer, and response/recovery. This holistic approach necessarily includes insurance. For

[9] Insurance Information Institute, *Cyber Risks: The Growing Threat* (June 2014).
[10] Wall Street Journal, Digits, *Cyber Insurance Demand Said Rising in Europe* (Jan. 28, 2015), *available at* http://blogs.wsj.com/digits/2015/01/28/cyber-insurance-demand-said-rising-in-europe/.
[11] The Telegraph, *Cyber risk the most serious threat to business, says Lloyd's chief* (April 7, 2015), available at http://www.telegraph.co.uk/finance/11516277/Cyber-risk-the-most-serious-threat-to-business-says-Lloyds-chief.html.
[12] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML and http://europa.eu/rapid/press-release_MEMO-15-3802_en.htm.

example, 74% of respondents of a recent survey on cyber-related issues that did not have cyber coverage in place stated that they are considering purchasing coverage in the next 1-2 years.[13] In addition, regulators may also focus increasingly on cyber insurance as a key facet of a regulated entity's operational resilience. Indeed, the SEC has issued guidance noting that cybersecurity risk disclosures must "adequately describe the nature of the material risks and specify how each risk affects the registrant" and that appropriate risk factors related to cybersecurity include a "[d]escription of the relevant insurance coverage."[14] However, as evidenced by the low take-up rates for cyber insurance products, many organizations – particularly small and medium size entities – lack awareness that cyber insurance is a viable risk transfer option for companies of all sizes. In fact, not only can cyber insurance products help transfer some of the risks associated with cyber threats, but the insurance underwriting process can also help identify cybersecurity vulnerabilities and improve cybersecurity.

Three Reasons to Consider Cyber Insurance

1. Insurance places a dollar value on an organization's cyber risk. This metric is useful when discussing security budgets with senior management. A non-technical CFO may not be fully versed in the performance of Denial of Service (DoS) mitigation services, but will understand the cost of the organization being unable to serve customers due to a DoS Attack.

2. The underwriting process can help organizations identify cybersecurity gaps and opportunities for improvement. In the same way property insurance has helped create safer buildings, cyber insurance can help create safer cybersecurity practices and policies. During the underwriting process, an organization must be able to adequately describe and maintain its administrative, technical, and physical controls (*i.e.,* its cyber hygiene profile). The insurers provide a third-party assessment of that profile and can then assist in identifying areas of improvement or adjustment that may help to bring down insurance costs.

3. In addition to providing the traditional risk transfer function, many cyber insurance policies bring supplemental value through the inclusion of risk mitigation tools, as well as significant incident response assistance following a cyber incident. Such assistance can be essential, particularly for smaller organizations that lack experience with or the manpower to respond to these issues, when faced with reputational damage or regulatory enforcement. With respect to regulatory enforcement, organizations face heightened scrutiny in both the EU and the U.S. From an EU perspective, the proposed GDPR will also add to the value proposition of cyber insurance due to the high level of fines allowed for in the legislation. A regulatory fine of 4% of global turnover could

[13] RIMS, the risk management society, *Cyber Survey* (May 2015).
[14] http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

cripple a company and is arguably a risk too big for the balance sheet of small- to medium-sized enterprises to carry. The prospect of such a fine should give companies a compelling reason to move into the cyber risk market. Additionally, in the U.S., the SEC recently announced it will be increasing its focus on investment advisors to ensure they have appropriate procedures in place to keep customers' information private, following a cyber attack in 2013.[15]

Where and How to Begin

As with any risk, the first step in determining whether or not to purchase insurance is to evaluate the potential risk exposure. What kind of information does the organization have (*i.e.,* credit card numbers and passwords, health records, trade secrets, patents, *etc.*)? What are the potential ramifications to the organization if this information is compromised or exposed (reputational damage, regulatory actions, litigation, inability to continue operations, repairs to network, *etc.*)? What steps (if any!) has the company taken to protect this information?

There are a number of framework and assessment tools that have been developed to help aggregate and determine the risk posture and level of risk an organization is managing. The United States government has publicly released two tools, discussed below, that are useful for businesses assessing cyber risks and cybersecurity risk management. These tools help an organization determine the level of risk it is managing and identify steps to meet those risks.

The first tool, released in 2014 by the National Institute for Standards and Technology (NIST), is the Framework for Improving Critical Infrastructure Cybersecurity (or NIST Cybersecurity Framework), which is a voluntary framework, based on existing standards, guidelines and practices, to help reduce cyber risks. While intended for critical infrastructure, the Cybersecurity Framework can be used by any organization.[16]

In 2015, the Federal Financial Institutions Examination Council (FFIEC) released its Cybersecurity Assessment Tool (Assessment). This tool is intended to help institutions identify their risks and determine their cybersecurity preparedness in a repeatable, measurable way. To do so, the Assessment allows an organization to analyze its Inherent Risk Profile (based on factors like technology and connection types and delivery channels) and its Cybersecurity Maturity (based on compliance with a series of declarative statements regarding cybersecurity risk). Although the Assessment was created for financial institutions, aspects of it – particularly its approach to matching risk profile to cybersecurity maturity – may be useful across other sectors as well.[17]

The NIST and FFIEC framework categories have been mapped against each other and provide as comprehensive a roadmap as exists to cyber maturity. Together with pre-

[15] http://www.reuters.com/article/us-sec-cybersecurity-idUSKBN0TT25D20151210.
[16] National Institute for Standards and Technology (NIST) Information Technology Portal.
[17] Federal Financial Institutions Examination Council (FFIEC) Cyber Assessment Tool. While the FFIEC Cyber Assessment Tool was designed specifically for banks, other organizations may also find it useful.

assessment underwriting tools, following these guides enhances the chances of receiving an offer of insurance for greater limits at less premium cost. See the NIST/FFIEC map here.[18]

These protocols are also helpful when negotiating coverage for residual risk after loss. Once a breach has occurred and remediation techniques have been applied, it is unwise to assume risk has been eliminated; but the character of the remediation may be rigorous enough to improve the organization's over-all cyber hygiene profile.

Tip: If your company increases its cyber maturity through application of the NIST/FFIEC frameworks, request re-underwriting based upon the new risk profile.

How Much Insurance Should be Purchased?

While there is some information on how much cyber insurance different sized organizations purchase, most numbers are proprietary and cannot be used to create an accurate picture of any one sector.[19] The top ten U.S. banks purchase between $0-$400MM+ of specific cyber insurance. Some organizations choose to integrate cyber insurance into existing policies, while others use a combination of incorporation and cyber specific policies to outsource risk. Ranking risk is an internal process, too, although agreement that cyber risk is a high priority is consistent throughout the private sector and government.[20] While there is some regulatory guidance, much of the determination is dependent upon an organization's risk appetite. This space is still developing, and currently there is no authoritative schematic for cyber insurance purchasing.[21]

What Coverage is Available?

As data breaches or cyber attacks can cause different types of losses, both to the organization itself (first-party or direct losses) and/or to its customers (third-party loss), it is important that purchasers obtain coverage for both types of loss. Below are examples of the first and third-party coverages available.

First-Party Coverage:

- **Crisis Management & Identity Theft Response:** Expenses for communications to notify affected customers, provide credit monitoring services, conduct forensic investigations, and for expenses incurred in retaining a crisis management or public relations firm for the purpose of protecting/restoring the organization's reputation.

[18] http://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_App_B_Map_to_NIST_CSF_June_2015_PDF4.pdf
[19] http://databreachinsurancequote.com/cyber-insurance/cyber-insurance-data-breach-insurance-premiums/http://www.marketwatch.com/story/cybersecurity-insurance-weighing-the-costs-and-the-risks-2015-03-25?page=2.
[20] http://csis.org/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf
http://www.economistinsights.com/technology-innovation/analysis/measuring-cost-cybercrime/custom.

[21] http://www.dhs.gov/publication/cybersecurity-insurance-reports.

- **Cyber Extortion:** Expenses to pay ransom or investigate a threat to release, divulge, disseminate, destroy, steal, or use confidential information; introduce malicious code into a computer system; corrupt, damage, or destroy a computer system, or restrict or hinder access to a computer system.

- **Data Asset Protection:** Recovery of your costs and expenses incurred to restore, recreate, or regain access to any software or electronic data from back-ups or from originals, or to gather, assemble, and recreate such software or electronic data from other sources to the level or condition in which it existed immediately prior to its alteration, corruption, destruction, deletion, or damage.

- **Network Business Interruption:** Reimbursement for loss of income and/or extra expense resulting from an interruption or suspension of systems.

Third-Party Coverage:

- **Network Security Liability:** Covers claims from third parties arising from a breach in network security or transmission of malware/viruses to third-party computers and systems.

- **Privacy Liability:** Covers claims from third parties as a result of a failure to properly handle, manage, store, or otherwise protect personally-identifiable information, confidential corporate information, and unintentional violation of privacy regulations.

Are These Exposures Already Covered Under Existing Policies?

Unfortunately, there are many gaps in coverage provided by traditional insurance products where the policy will not cover loss or costs associated with a data breach or liability claims made by third parties resulting from a data breach. In addition to the gaps already present in traditional products, due to recent loss developments and evolving case law, Insurers are now adding cyber-specific exclusions to traditional insurance products.[22]

For example, a typical commercial general liability (CGL) policy would likely include coverage for personal and advertising injury resulting from the publication of material that violates a person's right of privacy. This would seem to cover costs associated with claims by third parties for privacy liability as described above. However, many CGL insurers have now added exclusions specifically removing coverage for the disclosure of personal or confidential information. The exclusion essentially negates the personal and advertising injury coverage and purchasers should read their CGL and Umbrella forms carefully to determine whether this exclusion has been added.

Below are some additional examples of gaps in traditional coverage:

[22] http://www.law360.com/articles/529464/coming-to-a-cgl-policy-near-you-data-breach-exclusions.

- **Directors and Officers (D&O):** Many D&O policies contain a standard privacy exclusion that would negate coverage for D&O's faced with lawsuits alleging privacy violations.
- **Errors and Omissions (E&O):** Even broadly worded E&O policies remain tied to "professional services" and often further tied to a requirement that there be an act of negligence.
- **Property:** Courts have consistently held that data is not "property"— "direct physical loss" requirement not satisfied.
- **Crime:** Requires intent and only covers money, securities, and tangible property.
- **Kidnap and Ransom (K&R):** One may not have coverage without specific amendment for "cyber-extortion."

Tip: Work with a broker or insurance agent to analyze gaps in current traditional coverage and available cyber insurance coverage.

The Underwriting Process - Get Your Data House In Order *Before* Seeking Coverage

Prior to placing coverage, the insurer will engage in an underwriting process. Companies can do a lot to shore up their information security policies and practices to increase the availability of coverage and reduce the cost of coverage.

Even before seeking cyber coverage and engaging in the underwriting process, businesses should work to get their data house in order. During the process, underwriters will ask for information related to the cyber security maturity of a business. The answers and the level of comfort the business can provide will greatly impact the amount of coverage available and the terms and cost of the coverage. Below are some of the general categories of information that insurers typically ask for before offering coverage:

Dedicated Information Security Resources: Underwriters will want to know whether the company has a Chief Information Officer (CIO) or a Chief Information Security Officer (CISO) and whether that individual has other responsibilities outside of information security. They are typically interested in the amount of resources a company spends on information security and the number of employees dedicated to information security.

Information Security Policies and Procedures: Underwriters will want information related to policies and procedures. It is important to have a comprehensive written information security program that covers the technical, administrative, and physical measures taken to protect data. They will also want to know the cyber security maturity of an organization and whether the organization follows national cyber

standards, such as the NIST Cybersecurity Framework, FFIEC Cybersecurity Assessment Tool, and ISO standards.

Employee Education: With the increase in targeted phishing campaigns and user errors resulting in security breaches, underwriters are looking to insurance applicants to provide security awareness programs for employees and may specifically ask whether the organization conducts regular phishing tests on employees and what the consequences are to employees who repeatedly fail the tests.

Incident Response Planning: The underwriters will want to know whether the business has a formal incident response plan in place and will also inquire regarding regular testing, through tabletops or simulation exercises.

Security Measures: Underwriters are typically interested in data retention, network segmentation, data classification, log monitoring, penetration testing, patch management, and business interruption planning. They will also want to know whether the business has an encryption strategy and the technologies used to encrypt or otherwise protect sensitive data.

Vendor Management: As many recent data breaches have occurred through third-party relationships, underwriters are concerned with third-party vendor management. It will be important to describe whether the business has a formal third-party management process, due diligence, and ongoing oversight performed on third parties, and the contractual obligations required of third parties.[23]

Board Oversight: Underwriters will also likely ask how frequently cyber security risk issues are reported to the Board and whether there is Board-level approval or oversight of the information security program.

Keep in mind that the underwriting process and communications with your insurance broker and/or agent are not privileged communications and could be discoverable in litigation, so it is important to think about what you put in writing to your underwriters, brokers, or agent. In addition, information security measures and security risks are often sensitive, and the organization may feel more comfortable providing verbal answers to underwriter questions. Underwriters are generally amenable to a verbal question and answer session to discuss the security posture of the organization. It is best to receive a list of questions from the underwriters prior to the discussion so the organization can appropriately prepare and make sure the correct individuals are present to respond to the questions.

What to be Aware of when Shopping for a Cyber Policy?

I. Policy Construction – Insuring Agreements

[23] For additional information related to Supply Chain Cyber Assurance, including suggested contract clauses with third parties, please see Appendix B.

When is coverage triggered?

The insuring agreement in a CGL policy reads something like the following:

"With respect to Claims firm made against an Insured during the Policy Period, the Insurer shall pay all Loss in excess of the applicable Retention that the insured is legally obligated to pay resulting from a *Claim* alleging or relating to any cyber event."

The definition of Claim in a standard CGL policy is usually defined as:
"A written demand for money, services, non-monetary relief, or injunctive relief, or a lawsuit or regulatory action."

Under a standard CGL, the policy is triggered when a Claim is first made against the Insured (in the form of a demand letter, lawsuit, or other document) that their product, service, or property has caused a third party some type of harm, loss, or damage. In the context of a slip and fall scenario, this is straightforward. A customer comes in, slips on a wet floor and breaks a leg. The customer notifies the company in writing of the incident and demands their medical bills be paid or threatens further action or litigation. The organization notifies its insurer and the Policy is triggered.

In the context of a data breach, the issue of when the policy is triggered is much less straightforward. Often, a third party or customer will likely not know their information has been breached until the company notifies them. Only *after* the organization notifies the customer, does it receive an actual demand or lawsuit constituting a Claim that would trigger the Policy. Unfortunately, the costs incurred by the company to notify customers or third parties of the data breach, which typically include legal costs, credit monitoring services, postage, *etc.*, may not be covered as the Insurer is likely to say those costs were incurred before a Claim (as defined in the policy) was made and thus coverage under the Policy had not yet been triggered. Additionally, costs to conduct forensic investigations into how a breach occurred, expenses of providing credit monitoring services, or public relations expenses may also not be covered to the extent those costs were incurred before coverage was triggered.[24]

Contrasted with the way a data breach typically works, the standard liability policy wording would cover only those costs incurred after a Claim was made, leaving the insured organization to pay for many costs associated with a cyber breach they may have thought were covered.

Tip: To resolve this situation, look closely at how the policy is constructed, especially the insuring agreement. The element of time is critical to ensuring coverage is triggered appropriately. A policy requiring a "Claim" to be made before coverage applies may not be in line with the expectations of the insured. Rather, a policy that is triggered upon the

[24] http://insurancethoughtleadership.com/tag/columbia-casualty-company-vs-cottage-health-system/.

"discovery" of a data breach may be more appropriate to cyber risks. Additionally, an all-risk construction (where all losses are covered, except those which are specifically excluded) is preferable to peril-specific coverage (where only the specifically listed perils or causes of loss are covered).

Tip: Only buy coverage you need. If multiple insuring agreements are used in an "off-the-shelf" policy, discuss customizing a product that covers your company's risks, while not paying for unnecessary coverage.

When is notice to the insurers required?

Notice is another issue that must be considered when looking at how a cyber policy is constructed. Typically, notice to the insurers is required at a very early stage of potential breach identification, and consent from the insurers is often required for many expenditures following a breach, including retaining breach vendors, incurring breach notification costs, and settling any claims. As noted above, if a policy is not structured properly, there could be no opportunity to provide the carrier "notice" of a Claim before significant costs are incurred. It is important to ensure compliance with these requirements are met as it could result in loss of coverage.

Tip: Include key notification requirements in the incident response plan and pinpoint a key stakeholder to make sure those notification obligations are appropriately satisfied.

How are breach counsel and vendors selected?

In the critical moments of responding to a potential data breach, the last thing an organization should be worried about is whether their insurance provider will approve their selected breach counsel and forensics firm. Typically, cyber insurance policies require underwriter approval of the use of breach vendors. It is prudent to select these vendors in advance of a breach and get any contractual and conflict measures resolved with these vendors prior to a breach, but it is also important to make sure your insurance provider approves of the use of the vendors. The vendors are typically written into the organization's incident response plans, and the response plans should also trigger a notification to the insurance companies of a potential claim and notify them of the use of breach vendors.

Tip: Include selected breach counsel and vendors (*e.g.*, forensics firm, public relations, crisis management firms, *etc*.) in the incident response plan. Discuss your selected breach vendors with the insurers prior to policy purchase to ensure they will approve the use of those vendors if there is an incident. Remember to include a step in your incident response plan to notify the insurers of the use of the vendors after a breach.

II. Key Exclusions/Sublimits

Below are several key exclusions to be mindful of when examining a cyber insurance policy.

Portable electronic device exclusion

If the device leading to a cyber breach is portable, many policies could exclude coverage completely for any resulting loss.

Tip: Request removal of the exclusion from the policy. If insurer will not remove, request an exception to the exclusion, to cover losses involving portable devices if the data is encrypted.[25]

Intentional acts exclusion

Again, the gap here is best outlined in a scenario that contrasts different types of insurance products, namely a liability product against a crime product. A crime or fidelity policy generally covers first-party loss to the Insured even where such loss is caused by the Insured, while liability policies generally provide for damages or losses the Insured causes to a third party. Most cyber insurance policies do not adequately provide for both first-party and third-party loss.

For example, liability policies typically exclude coverage for damages or losses intentionally caused by an Insured. Thus, if an employee accidentally caused a cyber breach, the resulting loss would be covered (either under a general liability or umbrella policy that does not exclude cyber perils or under a stand-alone cyber policy). However, if a different employee caused the exact same cyber breach *intentionally*, the resulting loss would be denied under a general liability policy if this exclusion is present.

Tip: Request that exclusion apply only to the company's highest ranking directors or officers. This is especially important as many IT experts agree that one of the biggest cyber threats to companies today is their own employees.[26] In addition, make sure the exclusion applies only after a finding of intentionality has been fully adjudicated on the merits in a court of law. Often if a claim of intentionality is settled, insurers may claim there is no coverage for the claimed intentional act.

Nation/state, terrorism, cyber terrorism exclusions/acts of God

Similar to the previous scenario, where coverage was precluded simply based on whether the breach was caused intentionally or unintentionally, nation/state and terrorism, as well as Acts of God exclusions, can result in coverage being precluded simply based on who or what caused the breach to occur. For example, if a terrorist attack resulted in an explosion at an organization's facility or a tornado caused massive damage to an organization's power source, the resulting losses may not be covered under a standard cyber policy.

[25] www.irmi.com/online/insurance-glossary/terms/l/laptop-exclusion.aspx.

[26] www.cio.com/article/2872517/data-breach/6-biggest-business-security-risks-and-how-you-can-fight-back.html.

Fundamentally, companies expect cyber insurance to cover their losses whenever a cyber breach happens, regardless of who caused it or why.[27]

Tip: Limit Nation/State exclusions to those recognized by the U.S. Government or United Nations. Clearly define Act of Terrorism or Cyber Terrorism and limit any exclusion so it only applies where the U.S. Government officially declares an incident as an act of Terrorism or Cyber Terrorism. Review "Acts of God" exclusions carefully in Cyber policies, negotiate to limit exclusions as much as possible. Discuss and clarify with brokers/insurers whether certain elements of loss *(i.e.*, actual damaged property, loss of use of network, extra costs associated with restoring network connectivity, *etc.*) would be better covered under Property or Cyber policy, explicitly stating where coverage applies.

Negligent computer security exclusion
Some policies exclude coverage if data is unencrypted or if the Insured has failed to appropriately install software updates or security patches.

Tip: Review policy terms to see if/when data is to be encrypted and what duties exist to install updates, security patches or take other security measures to protect confidential information.[28]

Sublimits
Many policies also have sublimits that may apply for things such as breach notification costs, forensic expenses, credit monitoring costs, business or network interruption, and extra expense. In addition, business or network interruption coverage may have a larger deductible or include a time element component (*i.e.*, business or network must be down for a certain number of hours before business interruption coverage will be triggered).

Tip: Request removal of sublimits from the policy. If sublimits cannot be removed, negotiate highest sublimit possible for least associated cost.

Post-breach services
Some insurers are starting to partner with cybersecurity specialists to assist customers who experience a cyber breach with forensic investigations, proactive incident response strategies, and training, as they realize the benefit both to the customer and themselves in responding as quickly and efficiently as possible to a cyber breach to keep resulting costs, claims, and damages as low as possible.[29]

Tip: Companies should examine the services offered and negotiate coverage for services the Insurer may offer. (Consequently, there should be no reason why an Insurer should

[27] http://www.weil.com/~/media/files/pdfs/cyber_security_alert2_jan2015_v31.pdf.
[28] See http://insurancethoughtleadership.com/tag/columbia-casualty-company-vs-cottage-health-system/.
[29] http://www.insurancejournal.com/uncategorized/2015/04/16/364661.htm.

refuse to pay for such costs once a cyber breach occurs.) By working together with their customers, Insurers will gain valuable loss information and further establish cyber insurance as a viable product that offers real benefit to customers.

Vicarious liability/vendors
Many standard Cyber policies exclude coverage for data an organization has entrusted to a third-party vendor that is breached.

Tip: Institute and maintain thorough vendor network review requirements when employing third parties to handle confidential, sensitive, or personally identifiable information. Ensure all third-party vendors with which business is conducted maintain Cyber insurance policies of their own.

III. Other Policy Considerations

Carefully review the terms of your policy. If you do not understand what something means, that often means it is not clear and could lead to coverage denial or litigation over the terms. It is important to understand the terms of the policy, and underwriters will typically explain their position, so just ask. Below are some other items to consider while reviewing the terms of your policy:

Insider threats. Does your coverage include incidents of insider malfeasance?

Data on unencrypted devices or BYOD. Some policies do not cover devices that are unencrypted or non-company-owned devices.

Information maintained and stored by third parties. Understand whether your policy will extend coverage if there is a breach at one of the organization's vendors.

Costs to replace, upgrade, update, improve, or maintain a computer system. Often, coverage is not available to replace or upgrade systems that have vulnerabilities, and the coverage only provides replacement costs for the existing infrastructure.

Coverage for potential regulatory investigations and fines. Ensure that any potential regulatory investigation is covered. As more government agencies become involved in cyber issues, it is important to make sure you are not leaving any gaps in coverage. For example, an organization should make clear in its policy that investigations by the SEC related to cyber issues are covered, even though SEC securities-related issues are typically excluded.

Damages to corporate clients. Often cyber coverage extends only to individual consumers and not to third-party corporate clients. It is important to understand whether your other insurance coverage would kick in for these damages.

Territorial limits. Some coverage is limited only to incidents that occur in the United States, and an organization may need additional coverage depending on where data is stored.

Credit monitoring costs. Cyber insurance policies typically provide for the offering of one year of credit monitoring to affected consumers, but some state attorneys general have announced that two years is expected.

Conclusion

As insurers attempt to gather enough frequency and severity data to move to an actuarial model for cyber insurance, it is essential that companies seek cyber insurance with coverage sufficiently high and broad and present themselves to a potential insurer in the best possible cyber risk management posture.

Companies with a proactive approach to cybersecurity will take the time to examine their networks, cybersecurity practices, train their employees, maintain rigorous self and vendor testing, and promptly remediate issues.

Appendix A

GLOSSARY

CIAO: Critical Infrastructure Assurance Office.

Cyberattack: Includes a wide range of technical and social methods to pursue an ultimate goal – the propagation, extraction, denial, or manipulation of information.

Cybercrime: Includes a wide swath of activities that affect both the individual citizen directly (*e.g.*, identity theft) and corporations (*e.g.*, the theft of intellectual property).

Cyber insurance: An insurance market covering first- and third-party risk relating to cybersecurity.

Cyber risk: Any risks that emanate from the use of electronic data and its transmission, including technology tools such as the internet and telecommunications networks.

Cyber terrorism: Criminal acts that involve the use of electronic means.

Claim: The process by which the insured activates a policy.

Data confidentiality: The protection of communications or stored data against interception and reading by unauthorized persons. The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

Data integrity: The confirmation that data which has been sent, received, or stored are complete and unchanged. The property that data has not been altered or destroyed in an unauthorized manner.

Deductible: The amount of a claim the insured is responsible for, before the insurance company will start paying its share of costs.

Disaster recovery: The process of restoring a system to full operation after an interruption in service, including equipment repair/replacement and file recovery/restoration.

Exclusion: Those risks excluded from an insurance policy.

Exposure: The potential loss to an area due to the occurrence of an adverse event.

Gap analysis: A comparison that identifies the difference between the actual and the expected/specified system status.

Impact analysis: The identification of critical business processes, and the potential damage or loss that may be caused to the organization resulting from a disruption to those processes. Business impact analysis identifies: the form the loss or damage will take; how that degree of damage or loss is likely to escalate with time following an incident; the minimum staffing, facilities, and services needed to enable business processes to continue

to operate at a minimally acceptable level; and the time for full recovery of the business processes.

Insurance carrier: The company holding and supporting the insurance policy purchased from it. The company issues and upholds the risk associated with an insurance policy

Insurance policy: The document defining what risks or perils are insured along with exclusions

Insured: The party having taken out or likely to acquire or renew an insurance product

Liability: The state of being legally obliged and responsible under the terms of a policy

Mitigation: Limitation of any negative consequence of a particular event.

Monitor and review: A process for measuring the efficiency and effectiveness of the organization's Risk Management processes is the establishment of an ongoing monitor and review process. This process makes sure that the specified management action plans remain relevant and updated. This process also implements control activities, including re-evaluation of the scope and compliance with decisions.

Premium: The fee paid by the insured to the insurer for assuming the risk

Risk assessment: A scientific and technologically-based process consisting of three steps, risk identification, risk analysis, and risk evaluation.

Risk avoidance: Decision not to become involved in, or action to withdraw from, a risk situation.

Risk management: The process, distinct from risk assessment, of weighing policy alternatives in consultation with interested parties, considering risk assessments and other legitimate factors, and selecting appropriate prevention and control options.

Risk optimization: A process, related to a risk, to minimize the negative and to maximize the positive consequences and their respective probabilities. Risk optimization depends upon risk criteria, including costs and legal requirements.

Risk perception: Way in which a stakeholder views a risk, based on a set of values or concerns. Risk perception depends on the stakeholder's needs, issues, and knowledge. Risk perception can differ from objective data.

Risk reduction: Actions taken to lessen the probability, negative consequences, or both, associated with a risk.

Risk retention: Acceptance of the burden of loss, or benefit of gain, from a particular risk. Risk retention includes the acceptance of risks that have not been identified. Risk retention does not include treatments involving insurance, or transfer by other means.

Risk transfer: Sharing with another party the burden of loss or benefit of gain, for a risk. Legal or statutory requirements can limit, prohibit, or mandate the transfer of certain risks. Risk transfer can be carried out through insurance or other agreements. Risk transfer can create new risks or modify existing risk.

Risk treatment: Process of selecting and implementing measures to modify risk. Risk treatment measures can include avoiding, optimizing, transferring, or retaining risk

Security: All aspects related to defining, achieving, and maintaining data confidentiality, integrity, availability, accountability, authenticity, and reliability. A product, system, or service is considered to be secure to the extent that its users can rely on the expectation that it functions (or will function) in the intended way.

Threat: Any circumstance or event with the potential to adversely impact an asset through unauthorized access, destruction, disclosure, modification of data, and/or denial of service.

Vulnerability: The existence of a weakness, design, or implementation error that can lead to an unexpected, undesirable event compromising the security of the computer system, network, application, or protocol involved.

Appendix B

Supply Chain Cyber Assurance – Procurement Requirements

Introduction

To give some practical detail with regards to assessments of a supplier, enclosed is specific language and steps to take with your organization to determine if a supplier is in line with your company's guidelines. These model procurement policies are recommended to be in place when companies purchase software and hardware. Companies that implement these procurement policies should find themselves more insurable in the market, both in terms of the dollar amount of the insurance and scope of coverage.

This document serves as a minimal set of requirements for any supplier providing network-connectable software, systems, or devices as part of a contractual bid to [FULL NAME OF ORGANIZATION]. A description of the required methods by which features and functions of network-connectable devices are expected to be evaluated at the product level and tested for known vulnerabilities and software security weaknesses, while also establishing a minimum set of verification activities intended to reduce the likelihood of exploitable weaknesses that could be vectors of zero-day exploits that may affect the device, are articulated throughout this document. While this document serves as a minimal set of requirements, [FULL NAME OF ORGANIZATION] expects that suppliers will remain conscious of the dynamic nature of cybersecurity and provide incremental improvements as needed, which [FULL NAME OF ORGANIZATION] shall consider for inclusion in future versions of this document. Suppliers shall be required to provide [FULL NAME OF ORGANIZATION] with any and all requested artifacts as evidence that the supplier is in compliance with stated requirements.

Scope

These requirements apply to (but are not limited to) the following:

- Application software
- Embedded software
- Firmware
- Drivers
- Middleware
- Operating Systems

The requirements in this document are derived from various industry standards, guidelines, and other documents, including, but not limited to:

- IEC 62443
- ISO 27001

FSSCC Classification: TLP - White

- NIST SP 800-53
- NIST SP 800-82
- DHS Cyber Security Procurement Language for Control Systems
- ISA EDSA
- FIPS 140-2
- Common Criteria Smartcard IC Platform Protection Profile
- Mayo Clinic Technology and Security Requirements Procurement Language
- UL 2900

The requirements in this document apply to devices, software, or software services that will be referred to as "product" throughout this document. The product can be connected to a network (public or private) and may be used as part of a system. These requirements are applicable to products that contain software where unauthorized access or operation, either intentional or through misuse, of the product can impact safety, privacy, loss of data, and compromise operational risks.

Requirements

The requirements portion of this section will be broken out into the following components:

1. **Product Development Specification and Policy**
2. **Security Program**
3. **System Protection and Access Control**
4. **Product Testing and Verification**
5. **Deployment and Maintenance**

1. The word "shall" precedes all requirements to indicate that they are normative.
   Product Development Specification and Policy - Supplier shall represent and warrant that it has established and implements security standards and processes that must be adhered to during all equipment and product development activities, with such security standards being designed to address potential security incidents, product vulnerability to unauthorized access, loss of functions, malware intrusion, or any other compromise to confidentiality, integrity, or availability. Supplier shall represent that its security standards practices include testing procedures and tools designed to ensure the security and non-vulnerability of all products and equipment. Supplier shall warrant that it will, for all products and equipment, implement fail-safe features that protect the product's critical functionality, even when the product's security has been compromised. Supplier shall provide [FULL NAME OF ORGANIZATION] with a written copy of its Development Security Standards upon request and shall allow [ORGANIZATION NAME] personnel, or a third party identified by [FULL NAME OF ORGANIZATION], to view and assess the standards. Supplier represents and warrants that, with respect to all of its Products (as applicable), it meets and complies with all cybersecurity guidelines and similar requirements and

standards promulgated by any applicable regulatory body, where present. Supplier can provide a third-party assessment of organization's product development as a validation of the process employed.

2. **Security Program** - Supplier shall represent and warrant that it has developed and continues to maintain a comprehensive written security program that contains administrative, technical, and physical safeguards to ensure the confidentiality, integrity, and availability of all of [FULL NAME OF ORGANIZATION]'s systems and data. Supplier represents and warrants that all audits and reports, produced as part of its written security program and all reports required to be produced or made available to [ORGANIZATION NAME] are able to be exported and delivered in electronic format. The supplier's written security program shall include, but not be limited to:
    a. Identifying and assessing reasonably foreseeable internal and external risks to the availability, security, confidentiality, and/or integrity of any and all supplier products, systems, servers, equipment, software, electronic, paper or other records. The written security policy shall include means of evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such supplied product(s)' vulnerability and risks, including but not limited to:
        i. Ongoing employee (including temporary and contract employee) training;
        ii. Employee compliance with policies and procedures; and
        iii. Means for testing for, detecting, and preventing security system failures on an ongoing basis.
    b. Regular monitoring to ensure that the written security policy is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of [FULL NAME OF ORGANIZATION]'s systems and data, or any compromise in confidentiality, integrity, or availability of [FULL NAME OF ORGANIZATION]'s systems and data.
    c. Reviewing the scope of the security measures at least annually or whenever there is a material change in business practices that may reasonably implicate the security or integrity of supplier's products containing or which may access or be used to access [FULL NAME OF ORGANIZATION]'s networks, systems, and data, or compromise the confidentiality, integrity, or availability of [FULL NAME OF ORGANIZATION]'s systems and data.
    d. Documenting responsive actions taken in connection with any incident involving a breach of security, and mandatory post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of [FULL NAME OF ORGANIZATION].
    e. Supplier can provide a third-party assessment of organization's security program as a validation of the process employed.
3. **System Protection and Access Control** - Supplier shall demonstrate that [FULL NAME OF ORGANIZATION]'s systems and [FULL NAME OF ORGANIZATION]'s data are

protected by appropriate network security controls that prevent unauthorized access by providing [FULL NAME OF ORGANIZATION] with network diagrams of supplier's environment used to provide products, equipment, maintenance, and services to [FULL NAME OF ORGANIZATION].

a. **Supplier infrastructure** - Supplier shall warrant that an incident response mechanism is in place for unauthorized access to or disclosure of technology and assets on the supplier's infrastructure. Supplier shall have an approved C-level process for notification to [FULL NAME OF ORGANIZATION] of unauthorized access or disclosure of technology and assets on the supplier infrastructure that may impact business operations of products and services delivered to [FULL NAME OF ORGANIZATION].
b. **Supplier shall provide [FULL NAME OF ORGANIZATION] with a standard operating procedure for securing supplier's technology assets with independent evaluation and assessment where applicable and a management audit of said standard operating procedure annually**.
c. Communications between Supplier and [FULL NAME OF ORGANIZATION] shall be performed with a secure mechanism. Supplier shall provide operating procedures for the secure mechanism to ensure that there is no unauthorized access or disclosure of technology and assets.
d. All supplier products and services that have the capability to perform remote system maintenance, software upgrades, troubleshooting, and diagnostics shall provide technical documentation on these capabilities, which shall have the following at a minimum:
    i. Strong authentication mechanisms for access to products and services.
    ii. Mechanism to perform any remote software downloads are:
        i. Validated as an uncompromised supplier deliverable;
        ii. Validated as an unaltered supplier deliverable;
        iii. Validated that only that action is performed; and
        iv. Validated that it does not provide access to any other systems except for the purpose of updating the software to a supplier deliverable.
    iii. Ability to prevent the introduction of any unwanted activity unauthorized by the supplier.
e. Supplier agrees that no external access to its internal networks and systems, will be permitted unless strong authentication and encryption is used for such access. Supplier represents and warrants that all internet and network communications will be encrypted and authenticated. Any necessary external communications for purposes of service or maintenance functions to be performed by supplier will be encrypted and will utilize multi-factor authentication to access any and all devices, equipment, and/or applications. Supplier shall maintain an access control list for all access to the internal network from an external network and supplier agrees that any of its servers

exposed to the internet that contain [FULL NAME OF ORGANIZATION] data or access [FULL NAME OF ORGANIZATION] systems run on a hardened operation system.

4. **Product Testing and Verification** - Supplier shall perform a vulnerability assessment for any or all products that will be provided to [FULL NAME OF ORGANIZATION] as part of a contractual agreement, including scanning and penetration testing by a tester of [FULL NAME OF ORGANIZATION]'s choosing (or a tester selected by supplier and approved by [FULL NAME OF ORGANIZATION]) or, in [FULL NAME OF ORGANIZATION]'s discretion, [FULL NAME OF ORGANIZATION] personnel may perform such vulnerability assessment, all at no cost to [FULL NAME OF ORGANIZATION]. Supplier represents and warrants that it performs security testing and validation for all of its products, and that all security testing performed by supplier covers all issues noted in the "SANS/CWE Top 25" and "OWASP Top 10" documentation, and shall include a vulnerability scan encompassing all ports and protocols. Supplier shall provide [FULL NAME OF ORGANIZATION] with a test plan for all tests performed for review and approval by [FULL NAME OF ORGANIZATION]. The testing shall include, but not be limited to:
    a. **Communication Robustness Testing** – This shall include, at a minimum, communication protocol fuzz testing to determine the ability to properly handle malformed and invalid messages for all identified communication protocols in the supplier product, as well as data resource exhaustion tests (*i.e*., aka "load testing" and "DoS testing"). Communication robustness testing shall be performed using tools that are approved by [FULL NAME OF ORGANIZATION], and that produce machine-readable data.
    b. **Software Composition Analysis** – This shall include, at a minimum, an analysis of all compiled code found in the supplier product and shall identify all third-party open source components, and shall, at a minimum, identify all known vulnerabilities found in the Common Vulnerabilities and Exposures (CVE™) in publicly-available databases. Software composition analysis shall be performed using tools that are approved by [FULL NAME OF ORGANIZATION], and that produce machine-readable data.
    c. **Static Source Code Analysis** – This shall include, at a minimum, an analysis of all available source code found in the supplier product and shall identify weaknesses enumerated by Common Weakness Enumeration (CWE™). Static source code analysis shall be performed using tools that are approved by [FULL NAME OF ORGANIZATION] and that produce machine-readable data. All CWE Top 25 and OWASP Top 10 issues that have not been remediated must be clearly documented as an exception.
    d. **Dynamic Runtime Analysis** – This shall include, at a minimum, an analysis of how the supplier-provided software behaves during operation and whether such behavior introduces potential security vulnerabilities that could negatively impact confidentiality, integrity, and availability.

e. **Known Malware Analysis** – This shall include, at a minimum, a scan of supplier-provided software to determine if any known malware exists in the supplier-provided software and a risk assessment on mitigation controls or value of risk.
f. **Bill of Materials** – The supplier shall provide [FULL NAME OF ORGANIZATION] a bill of materials that clearly identifies all known third-party software components contained in the supplier product. This shall be provided in a machine-readable format.
g. **Validation of Security Measures** – This shall ensure that all security measures described in the product's design documentation are properly implemented and mitigate the risks associated with use of the component or device.
h. **Third-Party Penetration Test** – The supplier shall provide [FULL NAME OF ORGANIZATION] with the results of a penetration test performed by a third-party penetration tester. [FULL NAME OF ORGANIZATION] may, at its discretion, recommend a penetration tester of its choosing. The third-party penetration test shall, at a minimum, but not limited to, determine the following:
    i. All ports and interfaces that the product has enabled and disabled for all configurations.
    ii. All services that are external to the product for all configurations of the product. The test shall determine operational, service, test, and non-functional services of the product.
    iii. Measures implemented to prevent denial of service attacks on all ports, interfaces, and services.
    iv. That all ports, interfaces, and services are documented and that there exists no undocumented port, interface, or service.
    v. All ports, interfaces, and services that require authentication shall meet the requirements of the authentication section in the companion standard for the product ecosystem.
    vi. Probing for vulnerabilities in the product and providing conceptual exploits to attack the vulnerability.
    vii. Software and hardware weaknesses that are identified in the product that are in "SANS WE Top 25" and "OWASP Top 10" and/or otherwise negatively impact confidentiality, availability, and integrity of the supplier's product.
i. **Risk Assessment** – The supplier shall provide [FULL NAME OF ORGANIZATION] with a threat model and subsequent risk assessment that includes, at a minimum, but not limited to:
    i. Risk criteria used to evaluate the significance of risk, including the level at which risk becomes acceptable;
    ii. Risk identification, including (but not limited to) all known vulnerabilities identified through testing and all software weaknesses per "SANS WE Top 25" and "OWASP Top 10" publicly available lists;

iii. Risk analysis, including consideration of the causes and sources of the risks and their consequences;
iv. Risk evaluation, comparing the level of risk found during the analysis process with the established risk criteria to determine the acceptability of the risks; and
v. Additional risk control measures shall be implemented to address all known vulnerabilities and software weaknesses that have been determined to present an unacceptable level of risk.

5. **Deployment and Maintenance** – Supplier shall provide [FULL NAME OF ORGANIZATION] with detailed installation, deployment, and configuration instructions, and, at the request of [FULL NAME OF ORGANIZATION], assistance in installation, deployment, and configuration that supplier warrants meets the expected security context resulting from meeting the requirements in this document. All supplied software products shall be authenticated through code signing. Supplier shall provide [FULL NAME OF ORGANIZATION] with a stated lifecycle of supplied product and shall provide [FULL NAME OF ORGANIZATION] with a maintenance plan that addresses both current and legacy products provided to [FULL NAME OF ORGANIZATION]. Supplier shall provide, at a minimum, but not be limited to, the following:
    a. **Ongoing Vulnerability Assessment** – Supplier shall periodically apply all previously listed vulnerability assessment testing to the supplied products at a frequency of no less than once annually, and report any newly discovered vulnerabilities to [FULL NAME OF ORGANIZATION] within 15 days of being discovered.
    b. **Patch Management and Deployment** – Supplier shall design all products with the ability to apply patches when needed and shall provide [FULL NAME OF ORGANIZATION] with the patch management plan. Supplier shall provide [FULL NAME OF ORGANIZATION] with tested, verified, and validated patches in a timely manner, to not exceed 90 days for any vulnerabilities found in "SANS WE Top 25" and "OWASP Top 10", or any vulnerabilities deemed critical by [FULL NAME OF ORGANIZATION]. All patches and provided updates shall be authenticated through code signing.
    c. **Updates to Bill of Materials** – Supplier shall provide [FULL NAME OF ORGANIZATION] with an updated bill of materials per the previously-stated requirement for any changes resulting from product updates, patches, *etc*.
    d. **End of Life** – Supplier shall provide [FULL NAME OF ORGANIZATION] with a disposition plan for all software that has reached the supplier-stated end of life. This plan shall include, at a minimum, but not be limited to:
        i. Uninstallation instructions;
        ii. Removing of confidential information (*e.g.*, data and keys);
        iii. Transition plan to updated version of supplier product; and
        iv. Supplier warrants that expected security context remains intact.

6. **Security Incidents and Responses** – Any and all security issues (or potential security issues) associated with any Product or any of supplier's, networks, systems, or services ("Security Incident"), whether identified by supplier, or another entity or customer of Supplier, shall be reported by supplier within thirty (30) days of the issue identification.
    a. The notification shall include supplier's intended Security Incident mitigation and response plan, along with the timeframe during which mitigation will occur.
    b. Supplier will implement and maintain a process to document, report, and track identified and/or reported Security Incidents.
    c. In the case of a suspected or confirmed Security Incident, the supplier will take all such actions as may be necessary to assist [FULL NAME OF ORGANIZATION] and its delegates in an investigation of the Security Incident in order to determine the nature and impact of the Security Incident upon [FULL NAME OF ORGANIZATION], its facilities and affiliates, and will work with [FULL NAME OF ORGANIZATION] to mitigate any adverse impact.
    d. In the event that supplier fails to respond or take action to mitigate the Security Incident (regardless of how or by whom the Security Incident arose or was identified), supplier shall:
        i. indemnify and hold harmless [FULL NAME OF ORGANIZATION] from and against any and all damage, fines, penalties, harm, liability, costs, suites, actions, claims, or losses that arise from or are related to the Security Incident.

        ii. be responsible for any and all costs and expenses incurred by [FULL NAME OF ORGANIZATION] in its mitigation of the Security Incident and any resulting damages or issues, and
        iii. pay [FULL NAME OF ORGANIZATION] a penalty in the amount of __% of the total purchase price of all Products purchased by [FULL NAME OF ORGANIZATION] under this Agreement. In the event that [FULL NAME OF ORGANIZATION] (or supplier) modifies or alters any product to address or mitigate a Security Incident, such action shall not serve to negate or amend the warranty associated with the product, or negate or reduce supplier's obligations hereunder.
7. **Accountability and Responsibilities** – Business relationships between entities that have electronic access to the other's systems should define their relationship and responsibilities to create accountability and responsibilities for each party, as well as limit liability via written agreements.
   Further, such relationships should agree upon a defined level of cyber security for them all, and a trusted third party to inspect and audit each connected entity for the good of all contracted and connected parties.