Cyber Insurance Application From AIG:

To get an idea why cyber security losses are so high, lets take a look at the relatively empty effort to control cyber risks by adding qualifying policy language to the cyber security policies, which started off as completely unqualified in the early 2000's and only additional questions in the 2020's.

AIG

Cyber Insurance

Please enter the following information for the ***Applicant's*** Chief Information Security Officer (CISO), or equivalent employee, that is responsible for maintaining the ***Applicant's*** cybersecurity posture.

Name:	
Title:	
E-mail:	

*The **Insurer** may, but is under no obligation to, (1) use externally observable data about the **Applicant's** computer network, and (2) contact the **Applicant's** Chief Information Security Officer (or other person designated above) in connection with a condition or circumstance that the **Insurer** reasonably believes may result in a future event for which coverage may be afforded under the policy being applied for. The **Insurer** may continue to observe and report, as described above, during the term of any policy containing coverage issued to the **Applicant**.*

Dataprocessing

Please fill in the amount of data of each category that ***Applicant*** collects, processes, stores, or are transferred within the ***Applicant's*** environment, including records collected, processed, or stored by others for the ***Applicant***.

Unique Personally Identifiable Information (PII) records (including employees PII records):		
Unique Protected Health Information (PHI) records:	or	Not applicable
Number of unique Payment Card Information (PCI):	or	Not applicable
Number of Unique biometric identifiers:	or	Not applicable

Industry

Select in which industries ***Applicant*** operates in. Total % of revenue must be equal to 100%.

Accountants	%	Payment processing	%
Agriculture, Forestry, Mining, Fishing, and Hunting	%	Real Estate	%
Attorneys	%	Retail Trade	%
Collection Agents	%	Information, Software, and Technology (excl. payment-processing)	%
Construction	%	Telemarketing	%
Credit Bureaus	%	Employment agency, recruitment services and payrolling	%
Dining / Restaurants	%	Third party administrators	%
Education (related)	%		

Already I see some problems here. To begin with, the number of unique records for anything like health or other information is bound to change constantly and is not verifiable. It completely lacks context. What counts as a personal record? Do customer transactions count as individual records? What about biometric identifiers? Does employee photos count for that? What about if biometrics are use to authenticate to employee phones. Does that count?

There's nothing here that is verifiable or is even entirely clear in what they are looking for. Next, we see that the industry the company operates in is being inquired about. The fact is this really should not be a single insurance policy to cover so many industries, so that's a huge problem. Cyber risks are broad and highly integral, so cyber insurance for the legal sector, the retail sector, the manufacturing sector and other sectors are highly different in the risks they deal with, how

they should be administrated and what they are primarily concerned with verifying. There are common threads, but this is really a broad line of business and operational insurance

Exposure Section

a.	Does the Applicant utilize Microsoft Active Directory Domain Services ("ADDS"), whether "on prem", hosted, or in a hybrid configuration? To the avoidance of doubt: with ADDS we explicitly DO NOT refer to Azure Active Directory ("Azure AD") or Microsoft Entra ID.	Yes	No
b.	Does the Company utilize Microsoft Exchange, including in a "hybrid deployment"?	Yes	No
c.	Does the Company utilize any unsupported software (software the vendor is no longer providing security fixes for)?	Yes	No

Moving on to the next section, it's worth noting that almost all businesses utilize Microsoft's Active Directory to one degree or another, although it would not be surprising at all to learn that many do not know that is what they are using. Exchange server is also quite standard. The problem here is that these questions don't really tell you anything about state of things or configuration. This also lacks any verification, and because the question would be confusing to many people, it can't really be relied upon. Also, it is odd that they are excluding Azure AD, because that leaves a lot of businesses falling through the cracks and it makes it all the less clear. There's really no meaningful qualification here.

Next, we come to the ultimate loaded question. This issue is a bit nuanced and needs some expertise to actually sort out. By and large, of course, software that is no longer supported is not considered a good thing, but many industries still rely on it for niche applications, and it really depends on the context. There are proprietary software products that only operate certain legacy hardware. These can sometimes be run safety with mitigations. The problem is that so many companies do rely on unsupported software and how they do it has a lot of nuances to it. And again, without some more documentation and probing context, the question does not mean anything.

Lets move onto the next section…

Controls Section

Please indicate the controls within ***Applicant's*** environment. For this matter 'environment' means both the internal as well as the outsourced part of ***Applicant's*** environment. Should a response not fit 100% the Applicant's situation, please select "No" and provide additional information on the nuances where necessary either in the designated comment boxes at every page or in a separate document.

1. Backups and disaster recovery capabilities

a.	A process for creating regular backups exists (even if it is undocumented and/or ad hoc).	Yes	No
b.	Backup strategy includes regular offline backups (either onsite or offsite).	Yes	No
c.	Backups are isolated and separate from the production domain (i.e. cloud backups with MFA protection) or they are are immutable.	Yes	No
d.	A document incident response plan is in place.	Yes	No

OUCH! Why go so far out of your way to dodge an actual win. Having a meaningful backup policy in force makes a huge difference, and if you can provide actual documentation of this that proves you do backup your data off site, then you should get a discounted rate, but lets just look at how badly this is worded. First, it allows for undocumented or ad hoc plans. What the hell is with that? That makes it obviously unenforceable.

It does not distinguish between on and offsite and the way part C is required makes it unenforceable, by taking important controls and making them just suggested examples. There's nothing here that means anything. Backups are very important, but this section, if anything, makes things worse, by tacitly encouraging an undocumented or ad hoc procedure as being valid and as good as actual backups that happen for real.

2. Remote authentication (please select one answer)

Remote access to the corporate resources generally only requires a valid username and password (single factor authentication).

MFA is required and enforced for all remote access for employees to the corporate network, and all exceptions to the policy are documented.

MFA is required and enforced for all remote access (employee, vendors and 3rd party SaaS), and all exceptions to the policy are documented.

Remote access to the corporate resources is not provided at all.

MFA is one of the single most important controls for reducing losses to a cyber insurance line. It is critical that this one control be enforced on 100% of remote accounts. The problem is that organizations enforce this poorly and are often prone to dragging their feet on this. They will often fudge compliance, because people just don't have a baseline of what good cyber safety is.

In this case, there need to be a lot more specific and confirming questions, because this is so important. It's also not just about having MFA, but having strong MFA that is from a trusted provider and kept up to date. It should use secure phones or devices that the organization has control over. SMS based MFA is no longer considered secure. All MFA connections should use encryption.

There is actually quite a bit to getting this vital control correct. Clients should be offered comprehensive guidelines, compliance coaching, preferred vendors and any other guidance they need, because people will tend to get this one wrong. It must be fully audited and enforced.

This also highlights the need for specific approvals for technology products and services, to meet these criteria. MFA has a hazy definition. For example, being at a given location could be considered a factor of authentication and so could something like a biometric device, but that may or may not meet the best practices for a given case.

It's also important the MFA used be strong and phishing resistant. "Push based" MFA is worse than worthless because people often respond to it with muscle memory.

3. Password policies

a.	There's a password manager provided to all employees	Yes	No
b.	There's a policy in force against password reuse (uses unique passwords for apps in the environment)	Yes	No
c.	Service accounts (accounts used by machines - not people - for running applications and other processes) have password lengths of at least 25 characters.	Yes	No

Unfortunately, having a "password policy" does not mean much because that could just be an unenforced verbal policy. This is also focused on the wrong control, since passwords are generally not very secure for any circumstances, but things like the reuse of passwords is the kind of policy that is almost impossible to enforce.

The other glaring issue is that no auditor would ask question C without some kind of evidence or documentation. Nobody would be able to confirm this off the top of their head. If they don't have the documentation, then something that specific and weeping, would obviously need to be checked and verified.

What is also striking is how much is missing. No secure device requirements, no requirements for account lockouts or restrictions on who can log onto what or how login information is stored and transmitted.

It's also not clear what they are trying to do here. Qualify clients? Collect information? Enforce good loss controls?

It's important to note that insurance underwriting doesn't actually work very well when your clients are unable to understand what you are trying to encourage them to do and which controls should be used to get them the best rates

for the lowest risk. This is so confusing, it's not possible to even determine if these are requirements, suggestions or datapoints.

4. Monitoring & response

a.	There is a "Security Information and Event Monitoring" (SIEM) tool in place.			Yes No
b.	The environment is monitored for traffic for anomalous and potentially suspicious data transfers.			Yes No
c.	There is a "Security Operations Center" or SOC in place to monitor security incidents, internally and/or serviced by an MSSP (Managed Security Services Provider).	Yes, 24/7	Yes, but not 24/7	No
d.	There is an incident response plan documented with specific focus on Cyber incident management.			Yes No

With such subjective and non-verifiable questions, most of what it has listed for "Monitoring and Response" is not useful in telling you very much. The SIEM tool, for example, could make a difference, but almost anything would qualify for that name, without a formal definition or approval process.

The one thing that would make a huge difference is having an actual SOC center in place. If a place has a literal SOC center, a fully staffed SOC center, than that is not a small thing and that should completely change how you would go about underwriting them.

A SOC center is a fully staffed center where security professionals monitor for anomalous events, keep an eye on systems and are available to rapidly respond to problems. The question makes this seem as if it is a small thing or check box item. In fact, only a few large organizations have these, but given how unsophisticated the questions and screenings are, it's easy to see how someone might fudge the answer on this, thinking that their cloud service provider or MSP probably has one and just realizing the answer that the insurer is looking for is obvious.

5. Phishing Defense: people

a.	Security awareness training is in place, including phishing awareness training, to employees at least annually.	Yes	No
b.	Simulated phishing attacks are used to test employees' cybersecurity awareness at least annually.	Yes	No
c.	There is a documented process to report suspicious e-mails to an (internal) security team to investigate.	Yes	No

Again, this is a missed opportunity because "training" is a fuzzy statement and nothing here is fully verifiable or enforceable. What would make a big difference would be if the insurer decided to provide specific training, because proper training of a high quality can indeed make a huge difference in risk reduction.

6. Phishing Defense: technical

a.	E-mails are 'tagged' or otherwise marked as outside the organization.	Yes	No
b.	An e-mail filtering solution is in place which blocks known malicious attachments and suspicious file types, including executables.	Yes	No
c.	A web-filtering solution is in place.	Yes	No
d.	The web-filtering solution has capabilities that are effective on all organization assets, even if the asset is not on the organization's network (e.g., assets are configured to utilize cloud-based web filters or require a VPN connection to browse the internet).	Yes	No

Technical phishing defenses are very important. It is a shame they did not use telematic verification, approve vendors or work with any vendors to make this happen for real. Most organizations filling this out are going to be extremely confused by question D, which doesn't even make sense in this context. These aren't actually actionable items. A "web-filtering solution" could be almost anything.

7. Endpoint security tools

a.	The endpoint security solution includes antivirus with heuristic capabilities and/or tools with behavioural-detection and exploit-mitigation capabilities.	Yes	No
b.	There is an endpoint threat detection and response (ETDR or EDR) tool in place which does the following: indicators; identifies patterns which match known threats; automatically responds by removing or containing threats; alerts security personnel of incidents; provides forensic and analysis capabilities to allow analysts to perform threat hunting activities.	Yes	No

Ouch. Number 7 gets us nowhere, because it does not have anything beyond the need for some kind of virus or endpoint protection. The problem is that could be almost any kind of freeware or just built in operating system tools, which is much different than some of the best providers out there.

There really needs to be more effort to engage vendors and use compliance verification tools!

8. Scope of Endpoint security tools

a.	The endpoint security solution mentioned in the previous question is deployed on all workstations and laptops.	Yes	No
b.	The endpoint security solution mentioned in the previous question are deployed is deployed on all servers.	Yes	No
c.	For the endpoint security solution mentioned in the previous question, automatic updates are enabled.	Yes	No
d.	The endpoint security solution mentioned in the previous question is configured to block (vs. just notify of) suspected malicious processes/files.	Yes	No

Whoever wrote 8 has never worked in an IT environment of any size or complexity at all. It's not fair to ask if a solution is deployed at every endpoint, because there are always some in flux, just instilled or being reconfigured and many organizations have odd one-off situations. Because of this, making sure endpoint protection remains enforced is an ongoing job, so it's not unusual to keep an eye on ongoing endpoint compliance reports.

These controls are very important, but is far more complex and has many more important dimensions than this question can capture. It also really should rely on telematic reporting and enforcement.

9. Patching

a.	What is the capability to deploy the highest priority patches outside the regular periodic patching processes? (for example in the case of an in-the-wild exploitation of software for which an out-of-band patch is available)?	0-3 days	3-7 days	>7 days
b.	Are regular vulnerability scans of externally exposed environments being performed?	Yes	No	

Again, unfortunately, this doesn't get you far. It doesn't really explain what they are looking for in vulnerability scans, so most policyholders would just be left confused. Many organizations are likely to overestimate their capabilities and underestimate how long it might take them to deploy a patch in an emergency. Without testing, verification and documentation, this really does not mean anything and it can't be relied upon, because it's hard to tell if it is anything other than a subjective guess as to how long a patch would take to deploy.

10. Segmentation and protection

a.	There are network and/or host firewall rules implemented that prevent the use of external facing RDP (Remote Desktop Protocol) to log into workstations.		Yes	No
b.	There is an inventory of all service accounts (accounts used by machines - not people - for running applications and other processes.	Yes	No	We don't have any service accounts
c.	Network firewalls have been implemented on all of ***Applicant's*** locations.		Yes	No

There are a few things to note here. First, RDP is a very high risk service and absolutely should be blocked by host and firewall rules, at multiple points. RDP is used in many ransomware attacks. It is an old and mostly obsolete protocol and operates without encryption or good verification. It is possible to run it securely, but only if it is specially configured and contained for this purpose.

This is a very important control, so it should not be just one question. The settings should be confirmed and there should be more detailed explanations of what kind of blocks are required on firewalls and workstations.

Question B is silly! I can't imagine anyone who had any experience at all in the field wrote that. Every IT system does, in fact, have service accounts, but the question lacks context. Do they mean specially added service accounts? Do the ones built into Microsoft Windows count? It is entirely unclear.

The firewall question is another loaded one. Without clear definitions and technical approvals, even a rudimentary software firewall would mean that this box could be checked, and likely would.

11. Data Protection

Data is encrypted on end-user devices to safeguard data against lost devices. Example implementations include Windows Bitlocker, Apple FileVault, and Linux dm-crypt.	Yes	No

This particular control is only going to result in loss reductions in some very narrow circumstances, but it is still a good thing to have. Most would not know if they have it on or not and it really does need some more context and verifiable documentation. This is likely not going to be a yes or no question. There are certain circumstances where it is best not to encrypt data at rest, for reliability reasons, if the data is not especially sensitive.

It's just as important, however, to make sure the encryption is tied to good authentication. Some of these methods of encryption are often completely defeated by being tied to a weak password, so it's important to qualify this fully.

Outsourced Service Providers Section

Please provide the name of the third-party provider(s) you use for each of the following categories. If the ***Applicant*** does not use a third-party provider and capabilities/services or the category is not applicable to the ***Applicant's*** business operations, check N/A box for such category. If there are other third-party providers that are impactful to the ***Applicant's*** business that are not listed, use the Write-In Other(s) section.

Hosting Services	Relationship/ CRM Software	E-Commerce & Payment Services	Security Service Providers
N/A	N/A	N/A	N/A
Accenture	Aptean	Adyen B.V	Accenture
Akamai	Astute	Amazon AWS	Akamai
Amazon AWS	Atos	Apple	Atos
Atos	Deltek	Atos	Carbon Black
AT&T	eGain	BlueSnap	Cisco
CloudFlare	Gainsight	CCBill	CloudFlare
Dell	Google	EverCommerce	Comodo Group
Equinix	Infor	Fidelity National	CrowdStrike
Fujitsu	Medallia Inc	Information Services	Dell

I'm not entirely sure why they are asking this, but it may be so they can provide better notice or assessment of these vendors in case of service outage. Really, because these vendors are all so important and big in the economy, it would make sense for an organization like AIG to begin the process of examining, auditing and approving them as fully approved and compliant vendors. That is an important step to creating an ecosystem of trust. No insurers seem to be doing that, however.

Prior Claims, Circumstances & Warranties Section

1. Did the ***Applicant*** experience any of the below incidents in the past 5 years that had an impact on business operations?

a.	Ransomware	Yes	No
b.	Significant data / privacy breaches	Yes	No
c.	Other security incidents with a significant impact	Yes	No

*** If yes on any of the above questions, please provide per incident the below information:**

- Incident summary and a description of the root cause of the incident.
- The improvements made to the environment to prevent a future attack.
- If there's a forensic report available, please send us a copy.
- An (estimation) of the total loss incurred, including but not limited to fees of forensic IT, legal, PR, cost of recovery business interruption and liability etc.)

Finally, we have the questions (which continue into greater specifics) about any previous cyber incidents or claims. This makes sense, in some regard, but the way insurers apply it is not fair. It is generally used as either a reason to deny coverage or charge much higher rates. This, of course, is incentive to not be honest.

The problem is that while it might seem like being the victim of a cyber attack would increase risks, it really needs to be assessed on a case-by-case basis. Some victims of cyber crime end up becoming the most security conscious, so that effect should be accounted for.

Final Thoughts:

While this is just one of the AIG cyber applications I have seen, and they do have other versions of the coverage, but none were much better. Also, although this might seem like it is just the initial application, it's not. There isn't a whole lot more verification that goes into the process.

It is important to consider how AIG ended up where it is, with such a poorly written and high-risk line of insurance. AIG had previously sold cyber insurance with no requirements or qualifications at all, and had done so for years, making easy money with a cash and carry product that anyone could get right away from any agent by just walking in.

Of course, not all insurance can be sold so easily. Some forms of insurance require complex prequalification's, audits, inspections or other requirements. As far as that goes, many are far worse than cyber security insurance, but because it is a form of technical insurance that is based on compliance and has high potential risks, it simply isn't possible to sell cyber insurance in as blind and cash and carry a way.

It seems that AIG is addicted to the idea that this insurance can be sold with minimal qualifications, hands off assessments and relatively risk agnostic controls. The qualifications were only added in 2020, and they still seem to be unsure what they want to do with them. There really isn't any solid guidance as to which ones could be improved to reduce premiums. There's also no audit-based compliance management.

The level of absurdity for enforcement should be apparent based on the fact that no third party inspection or consultation is needed for non-technical companies. Also, the lack of requirements for documentation shows how immature the policy is. Even some of the questions don't make sense.

Because people lack context as to how important these questions are, they will likely get a "click through" mentality, clicking each one with the affirmative, knowing that is what insurers want and that it won't be verified.

Unfortunately, unless this policy is changed substantially and meaningful enforcement, compliance aid and proper assessments are made, it will continue to lose substantial amounts of money.

Next let's take a look at an application from HSB.

This one is from 2019, which is the most recent that can be found and appears to still be valid. Even if it is old, this was no more acceptable back in 2019 than it is now.

(Note that some of the general information portion of the application has been cropped out to save space, as it is not applicable to the analysis of the application.)

GROSS REVENUES: Projected Year	**NET OPERATING EXPENSES:** *(Education and Public Administration Only)* Projected Year	**GROSS REVENUES:** From Goods or Services to Customers via the Internet

DATE BUSINESS ESTABLISHED	NUMBER OF EMPLOYEES	BUSINESS DESCRIPTION

LIST ALL WEBSITE URL'S.

STOP No additional information necessary if limit requested does **not** exceed $500,000. Otherwise, please proceed.

SECTION III – GENERAL UNDERWRITING QUESTIONS AND LOSS INFORMATION

	YES	NO	N/A
1. Do you encrypt all your mobile devices *(laptops, flash drives, mobile phones, etc.)* and confidential data?			
2. Do you use up-to-date anti-virus and anti-malware protection on all of your endpoints (*desktops, laptops, servers, etc.*) and firewalls on all of your internal access points?			
3. Do you restrict employees' and external users' IT systems privileges and access to personal information on a business-need-to-know basis?			
4. Do you perform backups of business critical data on at least a weekly basis?			
5. Have you, at any time during the past 36 months, experienced a cyber incident *(hacking, intrusion, malware infection, fraud loss, breach of personal information, extortion, etc.)* that cost you more than $10,000 or experienced a lawsuit or other formal dispute *(with either a private party or*			

As with AIG, it starts off with some very vague questions that many will find difficult to understand and does not have any verification at all. This is clearly designed to be one rapidly. There is truly a lack of understanding as to how important it is to get these kind of basic business controls down an confirmed. These questions barely scratch the surface and lack context. For example, a firewall could mean almost anything, without further qualification.

Again, we see the use of a question about previous incidents, which is likely not going to be used in the most fair way and will encourage potential dishonesty.

It should be obvious to anyone that this boilerplate and generic language isn't actually going to result in any kind of reliable compliance with good rules, but it seems HSB is still stuck in the mindset that cyber risk is somehow a natural, immovable force or that the amount they are losing is somehow normal and not the result of grotesque negligence.

What is most striking, of course, is that they would give cyber insurance to anyone up to a half a million dollars without even meaningless boilerplate requirements! How is nobody in prison for this?

SECTION III – GENERAL UNDERWRITING QUESTIONS AND LOSS INFORMATION - *continued*

	YES	NO	N/A
6. Within the past 12 months, did you or one of your cloud providers experience an unplanned outage lasting longer than 2 hours? *(This does not include failure caused by an unauthorized access ("cyber attack")).* If **"Yes",** please attach details.			

STOP No additional information necessary if limit requested does **not** exceed $1,000,000. Please sign and date application. Otherwise, please proceed.

Again, we see the insistence on providing cyber insurance bellow a given limit with almost no qualifications. This added question is confusing and relatively meaningless. It seriously makes me wonder if how this is answered is even factored into the underwriting decision. It should not be, because it does not make any sense. It seems what they are getting at is some kind of an attempt to qualify those who might be prone to a technology failure.

Since this is so poorly worded, it's unlikely anyone would bother to answer yes to it, just furthering the illusion of low risk clients.

SECTION IV – DEVICES, INFORMATION AND VENDOR MANAGEMENT

1. How many of the following devices to you currently have deployed?
   - Servers: .....
   - Desktops: .....
   - Laptops: .....
   - Mobile Phones/ Devices: .....
2. How many individual people *(employees, customers, etc.)* do you currently store or maintain *(either yourself or using third parties)* information about?

   .....

	YES	NO	N/A
3. Do you process or store personal information or other confidential information for other businesses or organizations?			
4. For each vendor that processes or stores personal information for you, do you have a written agreement that makes the vendor financially responsible for the consequences of a cyber attack or data breach? *(If you do not engage any such vendors, answer **"Yes"**)*			
5. Do you require service providers to demonstrate adequate security?			

Here are some more laughably non verifiable and unenforceable questions that tell you nothing. What does number 5 even mean? How many servers do they have deployed? Does that mean virtual servers too? Servers in the cloud? If one machine is running two servers, does that count? What counts as a mobile device?

Of course, these questions are really just boilerplate language and don't tell you anything verifiable so it isn't all that important that they be accurately answered, I suppose.

SECTION V – INTERNAL POLICIES, COMPLIANCE AND PRIVACY MANAGEMENT

1. Do you have a written organization-wide privacy and security policy?
2. Do you have a document retention and destruction policy?
3. Have you implemented a *written* policy requiring:
   a) telephone confirmation *(or by means other than email)* with the payee or requestor, of the payment details before making payments *(including wire and ACH transfers)* in excess of $10,000?
   b) multiple internal parties to confirm authorization before making payments *(including wire and ACH transfers)* in excess of $10,000?
4. Does each user of your system have a separate individual account?
5. Do you have a formal process *(which includes identification, tracking, and monitoring)* in place for properly bringing servers, desktops, laptops and other digital assets into service and a formal process *(which includes removal from the network, deleting from inventory and secure wiping of sensitive data)* for properly removing those assets from service?
6. If you accept payment *(credit and debit)* cards, do you comply with Payment Card Industry Data Security Standards? *(If you do not accept payment cards, answer **"N/A"**)*
7. If you handle health information, do you comply with HIPAA and the HITECH act? *(If you do not handle health information, answer **"Yes"**)*
8. Do you have a designated Chief Information Officer or other person responsible for information and systems security?
9. Have you identified and secured personal and other highly confidential information for which you are responsible?

OUCH! A lot more hogwash of subjective, non-verifiable and generally poorly thought out security questions. A few of these are especially bad. For example, if you accept payment cards, then you are supposed to be in compliance with PCIDSS, so the answer should never be "no" to that one. What is a "formal process." In fact, most companies lack good formal processes and procedures here, even if they do have one on the books, somewhere. In many cases it's just something like "This company adheres to NIST guidelines." That doesn't mean anything without some enforcement effort.

SECTION VI – NETWORK SECURITY AND INCIDENT MANAGEMENT

	YES	NO	N/A
1. Do you update and patch critical IT-systems and applications on at least a monthly basis?			
2. Have you implemented the use of long and complex passwords or another secure account-access methodology such as multifactor identification or universal identification?			

NOOOOOO!

MFA and access control in general is the single most important control. Simply having a suggestion or mention of it in the policy language is not enough. It requires inspection, auditing, approved vendors, compliance help etc. It's a very important thing to get this one right.

This is the worst I have ever seen. The way it is worded explicitly makes it clear that it is only optional and not considered. This is so much worse than worthless.

SECTION VI – NETWORK SECURITY AND INCIDENT MANAGEMENT - *continued*

	YES	NO	N/A
3. Are all Internet-accessible systems *(for example, web-, email-servers)* segregated *(for example, within a DMZ or at a 3rd party provider)* from your trusted network?			
4. Do you use intrusion detection hardware or software or otherwise monitor your network and identify security events?			
5. Do you provide awareness training for employees in data privacy and security issues *(including legal liability issues and phishing)*?			
6. Do you delete system access, accounts and associated rights after termination of users *(including employees, temporary employees, contractors and vendors)*?			
7. Do you *(yourself or by engaging an outside vendor)* regularly scan critical systems for security vulnerabilities? These scans may include security and penetration testing.			
8. If you perform backups of business critical data on at least a weekly basis, is the backup stored offsite in a secure location? *(If you do not backup business critical data on at least a weekly basis, answer **"N/A"**)*			
9. If you perform backups of business critical data on at least a weekly basis, do you test your restore process on at least a monthly basis? *(If you do not backup business critical data on at least a weekly basis, answer **"N/A"**)*			
10. Do you have a business continuity management or disaster recovery plan in place?			
11. Do you have an incident response plan *(for cyber attacks and data breaches)* that identifies an incident response team?			
12. Do you have a process in place to review all advertising and other content prior to publication?			

Finally, we have a few more unverified, poorly worded and lacking requirements. These boilerplate questions are just security theater and may meet some requirement that policies be qualified, but it is not going to provide anything in the way of useful underwriting data or any loss controls at all.

HSB has the worst written cyber security controls I have ever seen and it's actually frightening.

The level of negligence or just idiocy that is seen in HSB's line of cyber insurance is shocking. It's clear that such as completely unqualified line of insurance is likely to attract a disproportionately high risk cliental, who prefer not to be bothered by compliance and are willing to live dangerously and pay more. This is an extremely dangerous thing. This policy language is so severely poorly written that HSB is absolutely guaranteed to hemorrhage money and continue to fund terrorism until this is completely overhauled.

What is so disturbing here is to see this kind of behavior happening in public, in broad daylight, documented and nobody can stop it. It can be assured that money will unnecessarily flow to terrorists because of this. What is more disturbing is that HSB is part of Munich RE, one of the world's largest reinsurers. Meaning, the parent company apparently thinks this

is sane and will bring that same spirit of not caring and losing money to their reinsurance treaties. Reinsurance does truly play a vital role in insurance markets and risk pricing. If Munich thinks this is at all reasonable, then we may be in some big trouble.

It's no exaggeration. Considering HSB is a company that has traditionally catered to specialized and high value industry, it's really very unsettling to see this. The worst part is just knowing those of us who have been fighting ransomware can't win because of the foolish decisions by organizations like HSB.

Next Lets Look at CNA:

(Note: Again some lines cut out because they do not pertain to what we are looking at)

This policy applies to small business broadly, which is questionable to begin with, since cyber risk is so different between different types of companies and sectors. This application is all that is required. There is no guidance as to whether the questions are enforceable requirements or just datapoints.

CONFIDENTIAL APPLICATION FOR CNA DATA BREACH AND PRIVACY EVENT EXPENSE INSURANCE - NEW HAMPSHIRE

CNA
We can show you more.®

THIS APPLICATION IS NEITHER AN OFFERING NOR A BINDER OF COVERAGE. ALSO, YOUR COMPLETION OF THIS APPLICATION DOES NOT OBLIGATE THE COMPANY TO OFFER COVERAGE TO YOU.

THE POLICY YOU ARE APPLYING FOR IS A CLAIMS MADE POLICY AND, SUBJECT TO ITS PROVISIONS, APPLIES ONLY TO ANY CLAIM BOTH FIRST MADE AGAINST THE INSURED DURING THE POLICY PERIOD AND REPORTED TO THE INSURER DURING THE POLICY PERIOD. NO COVERAGE EXISTS FOR CLAIMS FIRST MADE AFTER THE END OF THE POLICY PERIOD UNLESS, AND TO THE EXTENT, THE EXTENDED REPORTING PERIOD APPLIES.

DEFENSE COSTS, AS WELL AS ANY DAMAGES AS REFERENCED IN EACH APPLICABLE COVERAGE PART, REDUCE THE LIMIT OF LIABILITY AND ARE SUBJECT TO THE RETENTION. PLEASE REVIEW THE POLICY CAREFULLY WITH YOUR INSURANCE AGENT OR BROKER.

Company Name:_____

Company Address:_____

Agency Address:_____

After asking how much coverage is being applied for, this comes next

PLEASE DESCRIBE YOUR PLATFORM OR OUTSOURCED SERVICES VENDOR:

Financial Services and Payments		
First Data	Paypal	Other:_____

HISTORY OF CLAIMS AND COMPLAINTS:

Have you received any complaints, claims or been subject to litigation involving matters of privacy injury, identity theft, Denial of Service attacks, theft of others' information, damage to others' networks or others' ability to rely on your network or similar? Yes No

If "yes", how many in the past five years?_____

If "yes", please explain here:_____

It's a bit strange, the way it presents outsource vendors, with First Data and Paypal both listed and a small space for others. In this case, there really is neither space nor guidance to have meaningful data here.

RISK CONTROL SELF-ASSESSMENT:

1. Do you implement virus controls and filtering on all systems?
   Yes No
2. Do you check for security patches to your systems at least weekly and implement them within 30 days?
   Yes No
3. Do you replace factory default settings to ensure your information security systems are securely configured?
   Yes No
4. Do you have a way to detect unauthorized access or attempts to access sensitive information?
   Yes No
5. Do you know what sensitive or private information is in your custody along with whose info it is, where it is and how to contact individuals if their information is breached?
   Yes No
6. Do you authenticate and encrypt all remote access to your network and require all such access to be from systems at least as secure as your own? Check N/A if you do not allow remote access to your systems.
   Yes No N/A
7. Do you have a company policy governing security and acceptable use of company property?
   Yes No
8. Do you reassess security threats and upgrade your risk controls in response at least yearly?
   Yes No
9. Do you limit access to data on a need-to-know basis?
   Yes No
10. Do you outsource your information security to a firm specializing in information security or have staff responsible for and trained in information security?
    Yes No
11. Check N/A if you do not use wireless networks. On your wireless networks; do you use security at least as strong as WPA authentication and encryption?
    Yes No N/A
12. Do you control and track all changes to your network to ensure that it remains secure?
    Yes No
13. Do you have a prominently disclosed privacy policy and do you honor it?
    Yes No N/A
14. At least once a year, do you provide security awareness training for everyone who accesses your network?
    Yes No

That is it. That's all there is! No actual set in stone requirement of any real controls. Things like antivirus controls, of course, could be met with freeware controls or other substandard measures, which don't actually improve things much. Most of this is entirely subjective, such as having a need to know policy. For the most part, nothing here is enforceable or a call to action.

There isn't even a mature control for access control standards or MFA.

this fits the same pattern of companies stupidly throwing in the towel, copy pasting some boiler plate language onto their policy and idiotically saying "Well I guess it's just high loss because hackers are smart and it's high loss like that, so we won't bother with enforcement and demand the taxpayers bail us out…

Then finally, there is this additional statement, which seems to be more related to corporate values, ethics and optics than with any loss controls at all.

CNA DATA BREACH AND PRIVACY EVENT EXPENSE LIST OF PROHIBITED ACTIVITIES:

A) Activities involving: adult or "mature" content, gambling and online or interstate sales of alcohol, tobacco products, firearms or weaponry.

B) Collecting or retaining others' Social Security Numbers for any purpose other than for i) tax reporting to governmental authorities, ii) administration of benefits plans or related individual benefits, or iii) providing financial services or insurance to your clients.

C) Retaining credit card information after settlement of any related credit card transaction unless applicant encrypts it for storage or masks all but the last four digits of the credit card number.

D) In conjunction with a credit card transaction; the recording of any personally identifiable information (phone number, address etc.) other than the information appearing on the card unless: 1) the information is required for shipping, delivery, servicing or installation, 2) the transaction is for a security deposit or 3) the transaction is for a cash advance.

E) Soliciting or collecting private information on minors without consent of parent or legal guardian, including "non-public personal information."

F) Delivering unsolicited content or material to others that could be construed as "spam" or something similar (including "pop-ups").

G) Distributing or installing software or other executable files on others' computers or networks without their written permission (installs that could be construed as spyware, adware or something similar).

H) Sale of private information to others.

I accept these terms Yes No

Final Thoughts:

CNA is going to continue to do very poorly until this is changed. These vague questions must be replaced with a compressive assessment. It seems that the absolute paralyzing confusion about the risk of cyber security has caused them to not even try to qualify their policyholders or attempt to reign in losses. It's very disturbing to see this happening at major companies, who should know better.

Unfortunately, this kind of thing locks in the success of ransomware and makes the jobs of hard working cyber security professionals impossible. It's decimated the cyber security sector, because it's made ransom payments the norm while telling companies there is nothing, they can do to improve their security and not to bother. For many companies, this kind of poorly qualified cyber insurance has eaten into their risk management budgets, leaving many replacing risk mitigation with risk transfer.

It's terrible to see this happen to the world. So much terrorism funded. So many hospitals attacked. So many cyber professionals laid off.

This is exactly why!

Here is another application from CNA:

This one is for special cyber insurance for CPAs, which is interesting because the financial industry is an especially high risk sector with a great deal of highly regulated and sensitive data and a lot of formal controls.

CPA NetProtect℠ for AICPA Member Insurance Programs

Supplemental Cyber Coverage Application

1. Firm Name: _____

2. Contact: _____ E-mail: _____

History of Claims & Complaints

In the past 5 years have you received any complaints or become aware of, claims, prior incidents, circumstances, or events that could reasonably give rise to a claim involving matters of privacy injury, including but not limited to unauthorized access to non-public personal information or corporate confidential business information, identity theft, denial of service attacks, theft of information, damage to others' networks or others' ability to rely on your network or similar? . . . . . ☐ Yes ☐ No

If yes, please explain here. _____

_____

_____

CNA's Cyber Self-Assessment Primer will provide the minimum required practices for each of the following questions that you must utilize to obtain CPA NetProtect coverage. Implementing these practices will limit the possibility of having a Privacy Breach or a Network Damage claim from occurring in your firm.

1. Does your firm have a virus protection program and firewall in place? . . . . . ☐ Y ☐ N

2. Does your firm implement security software updates in a timely manner? . . . . . ☐ Y ☐ N

3. Does your firm replace all default settings to ensure your information security systems are configured secure? . . . . . ☐ Y ☐ N

4. Does your firm control access to information that resides on data storage devices such as servers, desktops, PC's, laptops and PDAs? . . . . . ☐ Y ☐ N

5. Does your firm have a password usage policy? . . . . . ☐ Y ☐ N

6. Does your firm ensure that sufficient safeguards are in place for the transmission and storage of data? . . . ☐ Y ☐ N

7. Does your firm monitor user accounts to identify and eliminate inactive users? . . . . . ☐ Y ☐ N

8. Does your firm control access to information that can be displayed, printed, and/or downloaded to external storage devices? . . . . . ☐ Y ☐ N

9. We agree to follow the minimum required practices for the questions listed above or implement them within 30 days after the effective date of your coverage using CNA's Cyber Risk Assessment Primer. . . . . ☐ Y ☐ N

A familiar pattern. Barely any questions, key controls left out entirely and no formal evaluation. These brief, largely subjective and irrelevant questions won't help. They seem to further advance the myths that there are not real and meaningful loss control measures that can be taken in cyber security.

Really, this is pathetic.

CyberChoice from the Hartford

Here is the application for CyberChoice Premier for low revenue customers, basically meaning small businesses in this case. Small businesses are some of the hardest to deal with, when it comes to cyber risks.

CYBERCHOICE PREMIER APPLICATION

(Lower Revenue)

THE HARTFORD

_____

Name of Insurance Company to which application is made

NOTICE: LIABILITY COVERAGE PARTS PROVIDE CLAIMS MADE COVERAGE. EXCEPT AS OTHERWISE SPECIFIED: COVERAGE APPLIES ONLY TO A CLAIM FIRST MADE AGAINST THE INSUREDS DURING THE POLICY PERIOD AND WHICH HAS BEEN REPORTED TO THE INSURER IN ACCORDANCE WITH THE APPLICABLE NOTICE PROVISIONS. COVERAGE IS SUBJECT TO THE INSURED'S PAYMENT OF THE APPLICABLE RETENTION. PAYMENTS OF DEFENSE COSTS ARE SUBJECT TO, AND REDUCE, THE AVAILABLE LIMIT OF LIABILITY. PLEASE READ THE POLICY CAREFULLY AND DISCUSS THE COVERAGE WITH YOUR INSURANCE AGENT OR BROKER.

MONTANA APPLICANTS ONLY: DEFENSE WITHIN LIMITS: THE AMOUNT OF MONEY AVAILABLE UNDER THE POLICY TO PAY SETTLEMENTS OR JUDGEMENTS WILL BE REDUCED AND MAY BE EXHAUSTED BY DEFENSE EXPENSES, INCLUDING BUT NOT LIMITED TO FEES PAID TO ATTORNEYS TO DEFEND YOU.

1. GENERAL INFORMATION

a) Name of Applicant Company: _____
(Together with any subsidiaries for whom this policy is intended, hereinafter, "Applicant(s).")

b) Address:

c) Nature of Business and SIC or NAIC Code:

d) Website:

2. COVERAGE REQUESTED

If Cyber coverage is not currently purchased, a dollar amount of "$0" will be assigned to current limits.

Coverage Requested	Limits Requested	Currently Purchased	Date Coverage First Purchased	Current Limits	Current Retention	Current Carrier and Premium
☐ CyberChoice Premier	$	☐Yes ☐No		$	$	

4. CYBER

a) Does an Applicant or any natural person for whom insurance is intended have any knowledge or information of any error, misstatement, misleading statement, act, omission, neglect, breach of duty or other matter that may give rise to a claim under any Cyber coverage part? ☐Yes ☐No

IT IS AGREED THAT IF ANY SUCH KNOWLEDGE OR INFORMATION EXISTS, ANY CLAIM OR LOSS BASED ON, ARISING FROM, OR IN ANY WAY RELATING THERETO SHALL BE EXCLUDED FROM COVERAGE REQUESTED.

b) If the Applicant currently purchases insurance providing any Cyber coverage, has the Applicant reported or could the Applicant have reported any facts, acts, circumstances, claims, or loss under such insurance?
☐Not Purchased ☐Yes ☐No

c) If the Applicant does not currently purchase insurance providing any Cyber coverage, has the Applicant experienced any facts, acts, circumstances, claims, or loss that would have been reported under this Cyber coverage part had it been in place?
☐N/A ☐Yes ☐No

If "YES" to any of the above, provide full details (attach a separate sheet if necessary).

Throughout questions (d) thru (l) of this section, any reference to "Applicant" shall mean the Applicant Company listed in 1(a) above and any third party on whom the Applicant currently relies, or to whom the Applicant entrusts any information.

d) Does the Applicant engage in any service or activity involving or similar to: initial offerings, mining, trading, exchanging, or storing of cryptocurrency, token, digital coin, or equivalent thereof? ☐Yes ☐No

e) How many people's non-public personal information (NPI) does the Applicant collect, store, process or otherwise handle?

☐ Under 50,000 ☐ 51,000 - 100,000 ☐ 100,001 - 1,000,000 ☐ 1,000,001 - 5,000,000 ☐ Over 5,000,000

f) Does the Applicant back-up mission critical data regularly, routinely store recent back-ups off-line and are the Applicants' backups well isolated from threats against its production systems? ☐Yes ☐No

g) How often does the Applicant implement system security updates or patches?
☐ Immediately upon availability ☐Weekly ☐Monthly ☐Yearly ☐Not at all

h) Does the Applicant use technical measures, devices or tools and techniques including: firewalls, anti-virus, and passwords/authentication? ☐Yes ☐No

Okay, so we don't actually have any qualifications of any security tools. Only that the client is in a given market and some basic demographics. It is not until we get to question F that a very vague and unenforceable question come in. This is not going to make sense to most. The whole thing is terrible and half-assed. Just look at how many vague measures are thrown together in question H. The answer is obviously "yes" if you have anything that even vaguely resembles a security control.

It's clear that the effort here was to do as little work and add as few requirements as possible. It's shocking anyone would think it ethical to approach an insurance that pays extortion in this manner.

i) Does the Applicant encrypt all electronic information that leaves its physical control (laptops, mobile devices, storage, etc.), using strong encryption and keys so that only the Applicant can decrypt it? ☐Yes ☐No

Only answer questions below if requesting Media Coverage

j) Does the Applicant have written editorial policies and a review process governing any content that the Applicant publishes both on and off line (including social media) including a formal process ensuring that the Applicant doesn't infringe another's copyright, title slogan, trademark, logo, trade name, service mark or brand? ☐N/A ☐Yes ☐No

k) Were any trademarks acquired by the Applicant in the last three years? ☐Yes ☐No
If "YES," were they screened for infringement? ☐Yes ☐No

l) Does the Applicant have a formal policy for responding to allegations that content created by the Applicant is libelous, infringing, or in violation of any other party's rights? ☐Yes ☐No

The same pattern holds true. Yet another large insurance company refuses to go about confirming that some of the most basic controls are in place. These vague, confusing, brief and unverifiable questions will simply not work to get any kind of useful results of move the needle with losses.

Look, I have been doing this for 20 years. You need to word things very carefully, making sure there is an enforceable call to action without ambiguity and with proper support to get results. Compliance enforcement in an area of risk management many feel perplexing is difficult. It requires some amount of effort. It can absolutely be done, but there must be some minimal expenditure of effort.

Failure to make any effort at all to control the problem has resulted in the largest organized crime racket of our time and is destroying the profession of cyber security, which, if enabled, can bring these problems to an end.

Insurers need to stop treating cyber professionals like the enemy and plowing into this so stupidly.

Next, a CyberRisk Application From Travelers:

Travelers is one of the largest, in terms of policies written. Their questions are slightly more detailed than others, but they're unlikely to result in any major loss reductions or provide decent data for reliable evaluation of risk.

TRAVELERS

Travelers Casualty and Surety Company of America **CyberRisk Application**

Claims-Made: The information requested in this Application is for a Claims-Made policy. If issued, the policy will apply only to claims first made during the policy period, or any applicable extended reporting period.

Defense Within Limits: The limit of liability available to pay losses will be reduced and may be completely exhausted by amounts paid as defense costs.

IMPORTANT INSTRUCTIONS

UNDERWRITING INFORMATION

DATA INVENTORY

1. Indicate whether the Applicant or a third party on the Applicant's behalf, collects, receives, processes, transmits, or maintains the following types of data as part of its business activities:
   a. Credit/Debit Card Data ☐ Yes ☐ No
      If Yes:
      i. Is the Applicant currently compliant with Payment Card Industry Data Security Standards (PCI-DSS)? ☐ Yes ☐ No
      ii. How many credit card transactions are processed or accepted for payment in a typical year? _____
      iii. What is the Applicant's reporting level? ☐ 1 ☐ 2 ☐ 3 ☐ 4
      iv. Was the Applicant's last PCI assessment conducted within the past 12 months? ☐ Yes ☐ No
   b. Medical information, other than that of the Applicant's own employees ☐ Yes ☐ No
   c. Non-employee Social Security Numbers ☐ Yes ☐ No
   d. Employee/HR Information ☐ Yes ☐ No
2. What is the approximate number of unique individuals for whom the Applicant, or a third party on the Applicant's behalf, collects, stores, or processes any amount of personal information as outlined in Question 1?
   ☐ fewer than 100,000 ☐ 100,000 – 250,000 ☐ 250,001 – 500,000 ☐ 500,001 – 1,000,000
   ☐ 1,000,001 – 2,500,000 ☐ 2,500,001 – 5,000,000 ☐ > 5,000,000
3. Indicate whether the data indicated in Question 1 is encrypted:
   a. While at rest in the Applicant's databases or on the Applicant's network ☐ Yes ☐ No ☐ N/A
   b. While in transit in electronic form ☐ Yes ☐ No ☐ N/A
   c. While on mobile devices ☐ Yes ☐ No ☐ N/A

Although Travelers does not appear as atrocious as some, already there are some problems here. For one thing, anyone who takes charge card data, should, in theory, be PCI DSS complaint. However, insurance companies ted to make a huge mistake in how they deal with PCI DSS compliance.

PCI DSS is a loss control standard used by credit card companies and merchants who process cards, along with others in the card processing ecosystem, are required to do assessments and audits to conform compliance. Insurance companies should leverage these existing loss control measures and work with PCI DSS to improve compliance, since it benefits both.

The additional questions, as per usual, lack specificity and detail. Many are ambiguous or confusing. All lack verification.

d. While on employee owned devices ☐ Yes ☐ No ☐ N/A
e. While in the care, custody, and control of a third party service provider ☐ Yes ☐ No ☐ N/A

4. Is the Applicant a Healthcare Provider, Business Associate, or Covered Entity under HIPAA? ☐ Yes ☐ No
If Yes, is the Applicant HIPAA compliant? ☐ Yes ☐ No

5. Is the Applicant subject to the General Data Protection Regulation (GDPR)? ☐ Yes ☐ No
If Yes, is the Applicant currently compliant with GDPR? ☐ Yes ☐ No
If the Applicant is subject to GDPR, and is not currently compliant, attach a description of steps being taken toward compliance.

PRIVACY CONTROLS

6. Indicate whether the Applicant currently has the following in place:
a. A Chief Privacy Officer or other individual assigned responsibility for monitoring changes in statutes and regulations related to handling and use of sensitive information ☐ Yes ☐ No
b. A publicly available privacy policy which has been reviewed by an attorney ☐ Yes ☐ No
c. Sensitive data classification and inventory procedures ☐ Yes ☐ No
d. Data retention, destruction, and recordkeeping procedures ☐ Yes ☐ No
e. Annual privacy and information security training for employees ☐ Yes ☐ No
f. Restricted access to sensitive data and systems based on job function ☐ Yes ☐ No

Although some of these questions may seem like they are useful, for the most part, they are just too subjective and fuzzy to be enforceable. These are not a reliable way of controlling or assessing risk.

NETWORK SECURITY CONTROLS

7. Indicate whether the Applicant currently has the following in place:
a. A Chief Information Security Officer or other individual assigned responsibility for privacy and security practices ☐ Yes ☐ No
b. Up-to-date, active firewall technology ☐ Yes ☐ No
c. Up-to-date, active anti-virus software on all computers, networks, and mobile devices ☐ Yes ☐ No
d. A process in place to regularly download, test, and install patches ☐ Yes ☐ No
If Yes, is this process automated? ☐ Yes ☐ No
If Yes, are critical patches installed within 30 days of release? ☐ Yes ☐ No
e. Intrusion Detection System (IDS) ☐ Yes ☐ No
f. Intrusion Prevention System (IPS) ☐ Yes ☐ No
g. Data Loss Prevention System (DLP) ☐ Yes ☐ No
h. Multi-factor authentication for administrative or privileged access ☐ Yes ☐ No ☐ N/A
i. Multi-factor authentication for remote access to the Applicant's network and other systems and programs that contain private or sensitive data in bulk ☐ Yes ☐ No ☐ N/A
j. Multi-factor authentication for remote access to email ☐ Yes ☐ No ☐ N/A
k. Remote access to the Applicant's network limited to VPN ☐ Yes ☐ No ☐ N/A
l. Backup and recovery procedures in place for all important business and customer data ☐ Yes ☐ No
If Yes, are such procedures automated? ☐ Yes ☐ No
If Yes, are such procedures tested on an annual basis? ☐ Yes ☐ No
m. Annual penetration testing ☐ Yes ☐ No
If Yes, is such testing conducted by a third party service provider? ☐ Yes ☐ No
n. Annual network security assessments ☐ Yes ☐ No
If Yes, are such assessments conducted by a third party service provider? ☐ Yes ☐ No
o. Systematic storage and monitoring of network and security logs ☐ Yes ☐ No
p. Enforced password complexity requirements ☐ Yes ☐ No
q. Procedures in place to terminate user access rights as part of the employee exit process ☐ Yes ☐ No

Some of these questions come close, but overall, it misses the mark. As with other applications, there are not clear definitions, the questions are confusing and ambiguous. There is no real enforceability. Nothing here is confirmed to have been done correctly. It's almost like informally asking. It is just as unreliable. What is frustrating is many come close. For example, having an Intrusion Prevention System could be huge, if it's a reliable and full featured one, but without asking for the make and model in use and getting some confirmation, the answer tells us nothing.

CONTENT LIABILITY CONTROLS

☐ **Communications And Media Liability Coverage is not requested.**

9. Does the Applicant have a comprehensive written program in place for managing intellectual property rights? ☐ Yes ☐ No

10. Indicate whether the Applicant has formal policies or procedures for:
    a. Avoiding the dissemination of content that infringes upon intellectual property rights ☐ Yes ☐ No
    b. Editing or removing controversial, offensive, or infringing content from material distributed or published by or on behalf of the Applicant ☐ Yes ☐ No
    c. Responding to allegations that content created, displayed, or published by the Applicant is libelous, infringing upon, or in violation of a third party's privacy rights ☐ Yes ☐ No

This is just more ineffective fluff. There's no way of verifying that a policy or procedure exists, when you don't even specify that it has to be written. And what is "comprehensive?" What does that mean?

It should be obvious to anyone that if they have a written policy or procedure, they will have no problem producing it, so why is it not required? That seems like just shoddy oversight.

BUSINESS CONTINUITY / DISASTER RECOVERY / INCIDENT RESPONSE

11. Indicate whether the Applicant has the following:
    a. A disaster recovery plan, business continuity plan, or equivalent to respond to a computer system disruption ☐ Yes ☐ No
    b. An incident response plan to respond to a network intrusion ☐ Yes ☐ No

12. Are all plans indicated above tested regularly with any critical deficiencies remediated? ☐ Yes ☐ No ☐ N/A

13. Based upon testing results, how long does it take to restore the Applicant's critical business operations following a network or systems interruption?
    ☐ Unknown ☐ 0 – 12 hours ☐ 12 – 24 hours ☐ More than 24 hours

You will need to define "regularly" and none of this should be taken at face value without some documentation. This is especially true of any testing for business restoration. It's not uncommon for the testing to be poorly done and may not reflect the actual time that it would take in a real emergency. At best, these may be estimates.

VENDOR CONTROLS

14. For vendors with access to the Applicant's computer system or confidential information, indicate whether the Applicant has the following in place:

a.	Written policies which specify appropriate vendor information security controls	☐ Yes	☐ No
b.	Periodic review of, and updates to, vendor access rights	☐ Yes	☐ No
c.	Prompt revocation of vendor access rights when access is no longer needed	☐ Yes	☐ No
d.	Logging and monitoring of vendor access to the Applicant's system	☐ Yes	☐ No
e.	A requirement that vendors carry their own Professional Liability or Cyber Liability insurance	☐ Yes	☐ No
f.	Hold harmless / indemnity clauses that benefit the Applicant in contracts with vendors	☐ Yes	☐ No

15. Indicate which of the following services are outsourced:

Data back up	☐ Yes	☐ No	☐ N/A	Payment processing	☐ Yes	☐ No	☐ N/A
Provider: _____				Provider: _____			
Data center hosting	☐ Yes	☐ No	☐ N/A	Physical security	☐ Yes	☐ No	☐ N/A
Provider: _____				Provider: _____			
IT infrastructure	☐ Yes	☐ No	☐ N/A	Software development	☐ Yes	☐ No	☐ N/A
Provider: _____				Provider: _____			
IT security	☐ Yes	☐ No	☐ N/A	Customer marketing	☐ Yes	☐ No	☐ N/A
Provider: _____				Provider: _____			
Web hosting	☐ Yes	☐ No	☐ N/A	Data processing	☐ Yes	☐ No	☐ N/A
Provider: _____				Provider: _____			

If Data center hosting or IT infrastructure is answered Yes above:

a. What is the likely impact to the organization if these services become unavailable?

_____

b. Does the Applicant have an alternative solution in the event of a failure or outage to one of these service providers?

_____

If Payment processing is answered Yes above, does the Applicant have an alternative means of processing card data in the event of an outsourced provider failure or outage? ☐ Yes ☐ No

Provide details: _____

To be perfectly honest, some of these questions are indeed very important in assessing the security of a client. However, they are simply too important to leave without some greater verification and some additional qualifications, to assure the info is correct.

These controls are simply not "Yes or No" questions. They are too important for that. Some of these requirements should be produced in writing and others need at least partial auditing or confirmation of compliance on.

A "Short Form" Version from Travelers:

Those seeking only $50,000 or less can use this much shorter application

UNDERWRITING INFORMATION

1. Indicate whether the Applicant has:
   a. Up-to-date, active firewall technology ☐ Yes ☐ No
   b. Up-to-date, active anti-virus software on all computers, networks, and mobile devices ☐ Yes ☐ No
   c. A process in place to regularly download and install patches ☐ Yes ☐ No
   d. Backup and recovery procedures in place for all important business and customer data ☐ Yes ☐ No
   e. An incident response plan to respond to a network intrusion ☐ Yes ☐ No
   f. A disaster recovery plan, business continuity plan, or equivalent to respond to a computer system disruption ☐ Yes ☐ No
   g. Controls to ensure the content of media communications and websites are lawful ☐ Yes ☐ No
   h. Procedures in place which require service providers with access to the Applicant's systems or the Applicant's confidential information to demonstrate adequate network security controls ☐ Yes ☐ No
   i. Multi-factor authentication for remote access to email and other systems and programs that contain private or sensitive data in bulk ☐ Yes ☐ No ☐ N/A
2. Is the Applicant currently compliant with Payment Card Industry Data Security Standards (PCI-DSS)? ☐ Yes ☐ No ☐ N/A
3. Is the Applicant HIPAA compliant? ☐ Yes ☐ No ☐ N/A
4. Indicate whether the Applicant encrypts private or sensitive data:
   a. While at rest in the Applicant's database or on the Applicant's network ☐ Yes ☐ No ☐ N/A
   b. While in transit in electronic form ☐ Yes ☐ No ☐ N/A
   c. While on mobile devices ☐ Yes ☐ No ☐ N/A
   d. While on employee owned devices ☐ Yes ☐ No ☐ N/A
   e. While in the care, custody, and control of a third party service provider ☐ Yes ☐ No ☐ N/A

LOSS INFORMATION

5. In the past three years, has the Applicant:
   a. Experienced: (1) a network or computer system disruption due to an intentional attack or system failure; (2) an actual or suspected data breach; or (3) a cyber extortion demand? ☐ Yes ☐ No
   b. Received any complaints, claims, or been subject to any litigation involving: Matters of data protection law, intellectual property rights, defamation, rights of privacy, identity theft, denial of service attacks, computer virus infections, theft of information, damage to third party networks, or access to the Applicant's network? ☐ Yes ☐ No
6. Is the Applicant, any Subsidiary, or any person proposed for this insurance aware of any circumstance that could give rise to a claim against them under this CyberRisk coverage? ☐ Yes ☐ No

If the Applicant answered Yes to any part of Question 5 or Question 6, attach details of each claim, complaint, allegation, or incident, including costs, losses, or damages incurred or paid, any corrective procedures to avoid such allegations in the future, and any amounts paid as loss under any insurance policy.

While the full version of Travelers cyber insurance isn't really sufficient, the short form is absolutely crazy. There's really nothing at all on here to weed out bad behavior, qualify risk or encourage lower losses. Granted it's only $50,000, but it would still be cheaper not to face such poorly controlled losses. In fact, the fact that this is so quick and easy, with no confirmation at all, does introduce the risk of insurance fraud, so there is that concern here too.

MFA Supplement from Travelers:

Because apparently, they figure out that MFA actually does matter, this supplement was added. It's unfortunate that they realized this but never went so far as to have an actual enforceable, verifiable requirement. To do that they would have been best off working with a few preferred vendors and gotten some automated auditing and enforcement in.

MULTI-FACTOR AUTHENTICATION

Multi-Factor authentication is required for all employees when accessing email through a website or cloud based service. ☐ Yes ☐ No ☐ Email is not web based

2. Multi-Factor authentication is required for all remote access to the network provided to employees, contractors, and 3rd party service providers. ☐ Yes ☐ No

3. In addition to remote access, multi-factor authentication is required for the following, including such access provided to 3rd party service providers:
   a. All internal & remote admin access to directory services (active directory, LDAP, etc.). ☐ Yes ☐ No
   b. All internal & remote admin access to network backup environments. ☐ Yes ☐ No
   c. All internal & remote admin access to network infrastructure (firewalls, routers, switches, etc.). ☐ Yes ☐ No
   d. All internal & remote admin access to the organization's endpoints/servers. ☐ Yes ☐ No
4. The signer of this form has done so with the assistance of the person in charge of IT security. ☐ Yes ☐ No

This supplement was apparently added (because they didn't know to begin with) to the Traveler's cyber insurance application when they realized that having MFA really does make a difference.

The problem is these questions don't actually make sense. MFA is not generally used for internal or local administration. If you are at the system, you don't need it. It also isn't generally going to be supported by network infrastructure. Those pieces of equipment are not part of the larger identity management ecosystem, so they can't connect to it.

Even question 2 is a bit off without more context and explanations. But I the case of question 3, more than half of it does not make any sense at all. I'd have no idea how to advise a client if they asked me should they check yes. If the answer is "they tell me I must say yes or I can't buy insurance" I'd have to tell them "Well you are as close to yes as possible. I mean some of your equipment doesn't work that way, but these questions don't even make sense so don't worry"

Unfortunately, this ridiculous trap led Travelers to do one of the most unethical things I have ever seen a company do.

Here is one article:

> **Travelers vs. ICS: Misrepresentation and Your Cyber Insurance**
>
> Imagine getting hit by a cyber-attack that ends up costing you millions of dollars and enduring a class action lawsuit served by your own clients. That's already a tough experience. Now imagine that in the middle of all that, your cyber insurance provider files to nullify your policy. Not only do you have to go through the experience without help from your insurance company, but now you're also being asked to reimburse services already rendered.
>
> …

That's what happened to a Decatur, Illinois-based electronics manufacturing services company, International Control Services (ICS).

On July 6, 2022, Travelers Insurance filed a document asking the US District Court for the Central District of Illinois to declare their insurance contract with ICS null and void. The insurer wanted to rescind its cyber policy because ICS allegedly misrepresented its use of multi-factor authentication (MFA).

…

According to the document filed by Travelers, ICS submitted a cyber policy application signed by its CEO saying that they used MFA for administrative or privileged access. However, just weeks after ICS received the policy, the Decatur-based firm was hit by a ransomware attack, prompting an investigation. Travelers found that ICS "only used MFA to protect its firewall, and did not use MFA to protect any other digital assets."

In Travelers' point of view, that proved that the statements ICS made in the application were "misrepresentations, omissions, concealment of facts, and incorrect statements" – all of which "materially affected the acceptance of the risk and/or the hazard assumed by Travelers." In layman's terms, the insurer is saying that if they had known ICS wasn't using MFA properly, they would have never approved the policy.

Now lets step back here. What Travelers did was unforgivable. It was evil. It was vile and despicable. The company Travelers has voided its right to exist and must be liquidated. This is so shocking and appalling.

Above all else, I beg those reading this NEVER DO BUSINESS WITH THIS LOATHSOME COMPANY

What Travelers did is absolutely shocking. Filled with irrational rage over their mounting losses, they decided to take it out on an innocent policyholder. ICS did nothing wrong. They had been attacked before and Traveler's failed to pay for an adequate incident response, leading to a second attack. It must be understood that the failure to properly secure the environment after the initial attack is a failure by Travelers.

ICS did nothing wrong, because, as stated, the question are unclear and don't make sense. Travelers had every opportunity to calcify the questions or attempt to check and validate compliance. But they are just being savage here because they are so stupid.

So basically, they're trying to drive ICS out of business, a company that bought insurance form them in good faith, to protect itself, only to find the insurance company turn into some kind of sociopathic villain.

Next, The Qualifying Language from a Chubb Policy:

4. Cyber and Media Controls	
Which of the following IT security controls does the Applicant have in place?	
1) Antivirus and Firewalls (Windows 7 or higher qualifies)	☐ Yes ☐ No ☐ Unknown
2) Encryption of Sensitive Data	☐ Yes ☐ No ☐ Unknown
3) Encryption of Mobile Computing Devices	☐ Yes ☐ No ☐ Unknown
4) Critical Software Patching Procedures	☐ Yes ☐ No ☐ Unknown
5) Critical Data Backup and Recovery Procedures	☐ Yes ☐ No ☐ Unknown
6) Formal Cyber Incident Response Plan	☐ Yes ☐ No ☐ Unknown
Does the Applicant accept payment card (Credit/debit card) transactions?	☐ Yes ☐ No
If Yes, is the Applicant PCI compliant? (via assessment or self-attestation)	☐ Yes ☐ No ☐ Unknown
Does the Applicant deal with protected health information as defined by HIPAA?	☐ Yes ☐ No
If Yes, is Applicant compliant with HIPAA and the HITECH Act?	☐ Yes ☐ No ☐ Unknown
Does the Applicant have operations or customers in California, or any responsibilities under the California Confidentiality of Medical Information Act?	☐ Yes ☐ No ☐ Unknown
Has the Applicant obtained legal review of its use of trademarks, including domain names?	☐ Yes ☐ No ☐ Unknown
5. Current Coverage	
Does the Applicant currently purchase Professional Liability or E&O insurance?	☐ Yes ☐ No
If Yes, what is the Retro Date? Click here to enter a date.	
Does the Applicant currently purchase Cyber or Privacy Liability insurance?	☐ Yes ☐ No
If Yes, what is the Retro Date? Click here to enter a date.	
Does the Applicant currently purchase Media Liability Insurance?	☐ Yes ☐ No
If Yes, what is the Retro Date? Click here to enter a date.	
Does the Applicant intend to purchase E&O and/or Media coverage on a separate and distinct policy? (e.g. with a separate set of limits, or with another carrier?)	☐ Yes ☐ No

Do I even need to go over why this will not work? This is just more of the same half-hearted boilerplate.

Now, it is true that some insurers are slowly evolving, offering loss control services and some are now even investing in in house services, but this goes to show how it is really just a drop in the bucket of incompetence. There is nothing on this to qualify what an actual critical data backup and recovery plan is. There is no MFA requirement. There is no audit or inspection. There is no enforcement.

Now, granted, there do seem to be some other policies from Chubb that have some additional inspection requirements, however, only a few insurers and only some policies actually bother to do more than have some check boxes to fill.

Chubb is one of the largest holders of Cyber Risk in the world.

This is why we are having massive problems. It's not that cyber losses are confounding or even especially difficult. It's just insurance companies are lying out of greed and stupidity. That is why we have the ransomware problem. This is exactly why we can't win. This is exactly why it keeps getting worse.

Finally, Let's Look At The Policy Language that can qualify up to $250 Million from Beazley:

That is a hell of a lot of money to out on the line on such a high-risk area of insurance. Lets see if they at least carefully qualified all the requirements.

General Information

Full name

Headquarters address

Business description

NAICS Code

Website URL(s)

Number of employees

1. Total revenue: Most recent fiscal year Current fiscal year (projected)

   USD

2. Do you have any revenue-generating operations outside your domiciled country? ☐ No ☐ Yes, percentage %

3. Cybersecurity point of contact (CISO/Risk Manager or equivalent role):

   First Name Last Name Job Title Email Telephone

4. Are significant changes in the nature or size of your business anticipated in the next 12 months? ☐ No ☐ Yes

Okay, so after getting some basic demographic information, here are the qualifiers:

5. Are you engaged in any of the following business activities?

   - Adult content, gambling or cannabis (containing THC) as a grower, wholesaler or medical/recreational retailer;
   - Cryptocurrency, blockchain technology, payment processing or debt collection;
   - Data processing/aggregation, storage or hosting services to third parties as a professional service (e.g., as a managed services provider (MSP) or data aggregator); or
   - Managed care or accountable care. ☐ No ☐ Yes

Records

6. How many individual records do you hold for each type of information? If a record could fall into more than one category, count it toward the most appropriate category.

   a. Payment Card Information (PCI) _____

   b. Protected Health Information (PHI) _____

   c. Biometric Information _____

   d. Personally Identifiable Information (PII) _____

Do you see the problem yet? These are not meaningful numbers because they lack context and are subject to change. They are also based on self-attestation and not subject to verification.

Now compared to some other applications, this one is a bit better, but it's still rather vague and does not go out of its way to make sure the person answering it actually knows what MFA they are looking for. In fact, it gets a little tripped up in not quite understanding how Active Directory works. But that is still a hell of a lot of risk in a field that is so dependent on compliance to not do any kind of formal audit of any kind and have no expert in cyber security risk at all involved in the writing of this.

Cybersecurity Controls

7. Do you require Multi-Factor Authentication (MFA) for remote access to your network (both cloud-hosted and on-premises, including via Virtual Private Networks (VPNs))?

   ☐ No ☐ Yes ☐ Remote access not permitted

8. Do you require MFA for access to web-based email?

   ☐ No ☐ Yes ☐ Access not permitted/no web-based email

9. What security controls do you have in place to protect Domain Administrator accounts?

   a. Do you enforce MFA for privileged accounts in Azure Active Directory (AAD) (including the members of the AAD Domain Controller administrators group)?

      ☐ No ☐ Yes ☐ We do not use AAD

   b. Are Domain Administrators permitted to connect only to domain controllers (and <u>not</u> email or connect to the internet)?

      ☐ No ☐ Yes

   c. Are Domain Administrators configured with unique, random, and long (>25 characters) passwords?

      ☐ No ☐ Yes

10. What security controls do you have in place for incoming email? Choose all that apply.

☐ Screening for malicious attachments ☐ Screening for malicious links ☐ Tagging external emails

11. How often do you conduct interactive social engineering (i.e., phishing) training?

☐ Never/not regularly ☐ Annually ☐ ≥2x per year

12. Do you regularly backup your business critical data?

☐ No ☐ At least monthly ☐ At least weekly or daily

13. Where do you backup your business critical data? Choose all that apply.

☐ Corporate network ☐ Cloud service ☐ Offline

14. If you rely on a cloud-based backup service, is it a "syncing service"? (E.g., DropBox, OneDrive, Google Drive)

☐ No ☐ Yes ☐ No cloud backups

15. How frequently do you perform a test restoration from backups?

☐ Never/not regularly ☐ Annually ☐ 2-3 times per year ☐ Quarterly or more often

16. What security solutions do you use to prevent or detect malicious activity on your network?

Security solution	Vendor
a. Endpoint Protection Platform (EPP)	
b. Endpoint Detection and Response (EDR)	
c. Managed Detection and Response (MDR)	

17. Do you have a Security Operations Center (SOC)?

☐ No ☐ Yes, working hours only ☐ Yes, 24/7

18. a. Do you have any end-of-life or end-of-support software on your network?

☐ No ☐ Don't know ☐ Yes

b. If "Yes" to a., is the software segregated on your network?

☐ No ☐ Some is, some isn't ☐ Yes

19. Are network firewalls configured to disallow inbound connections by default? ☐ No ☐ Yes

20. Do you use a hardened baseline configuration across all (or substantially all) of your devices? ☐ No ☐ Yes

21. Do you permit ordinary users local administrator rights to their devices (e.g., laptops)? ☐ No ☐ Yes

22. Do you have an incident response plan for network intrusions and malware incidents? ☐ No ☐ Yes

You get the idea…

This is just part of the application, which is about three pages. All in all, it's no less vague and has no better controls on the rest of the policy. In fact, taking on that much risk in cyber is absolutely crazy without a full evaluation by Certified Information Systems Auditors. No bank or financial institution would ever take on that kind of risk without proper compliance evaluations. There is so much missing. No questions about certain vendor products. Very little about cloud security. No requirements for any automated patch management. It's atrocious!

This really goes to show bow bad the walled off ignorance of the insurance sector was. If they knew half of what they don't know, they would not shoot themselves in the foot so badly. Nobody would do this to their own business if they knew how far off the mark they were.

None the less, this remain the most severe case of idiocy and insanity I have ever seen in business. If these idiots talked to experts even once they'd realize it would take a minimal amount of effort to turn this into a cash cow.