

D.

Webinar | Expert Industry Panel

# Cyber Liability Insurance Q&A

What Brokers Need to Know

---

Transcript



**Heidi Strommen**

President,  
Primary Hospitality Programs



**Haley Cagle**

Cyber Liability Product  
Manager, Primary Hospitality



**Host - Ritchie Vener**

Chief Growth Officer

**Distinguished.**

Ritchie Vener:

Hello, everyone, and thank you for joining us for our webinar, "Cyber Liability Insurance Q&A: What Brokers Need to Know." My name is Ritchie Vener, and I'm the Chief Growth Officer at Distinguished Programs. I'm very excited to be leading the discussion today with members of our Cyber Liability program. We pride ourselves on having the experience, flexibility, and depth of expertise to help brokers get their deals done, and this team really exemplifies that.

After today's webinar, we'll send all registrants a copy of the slides, the webinar recording, and a PDF with the questions and answers from today's session. If anyone has a question during the presentation, please use the Q&A button on the bottom of your screen. If we don't get to it live, those questions will still be answered in the follow-up materials that we'll send out.

Distinguished Programs is a leading national insurance program manager with a growing number of specialized insurance programs. These include real estate, community associations, hotels, restaurants, cyber liability, fine art and collectibles, inland marine, executive lines, crisis management, surety bonds, marine cargo, transactional risk, and environmental and construction professional insurance.

I'm very excited about today's session, given the increasing importance to businesses across so many industries for cyber liability. During this 30-minute session, we will learn about the latest enhancements to our Cyber Liability Insurance program and how these updates are essential in today's digital environment. Are you ready to grow your book of business with Distinguished? Let's get started.

Joining us today are Heidi Strommen and Haley Cagle. Heidi is the President of our Primary Hospitality program and is well-known in the industry. She oversees the overall strategy and management of our Distinguished Primary Programs for restaurants, hotels, and cyber. Heidi joined Distinguished in April 2019 with our acquisition of ProHost USA, a program administrator specializing in restaurants where she served as president. She has an extensive background in building programs for restaurants and related risks. She's also a past president of Target Markets Program Administrators Association and is currently on their advisory board. She's authored numerous articles about insuring restaurant exposures for various industry magazines, including Risk & Insurance, Insurance Journal, Agent and Broker, and Rough Notes. Heidi earned a BA in Government from Cornell and an MBA from Metropolitan State University.

Also joining us today is Haley Cagle. Haley joined Distinguished in January 2022 as our Cyber Liability Product Manager. She previously worked under a program administrator for Lloyd's of London and has been in the professional liability insurance industry as a wholesale surplus lines broker and underwriter for 14 years. She specializes in cyber, tech, and miscellaneous E&O exposures and now focuses solely on cyber. She earned her Cyber Professional Liability Practitioner designation, which she adds to her RPLU and ASLI designations.

Let's jump right in. I'm going to start with you, Haley. What is Cyber Liability Insurance?

**Distinguished.**

Haley Cagle: Cyber Liability Insurance is a top-of-business insurance designed to help protect organizations from the financial impact of cyber attacks, data breaches, and other cyber-related incidents.

It typically combines both first-party coverage, which addresses direct losses separate from the business, and third-party coverage, which helps respond to claims, lawsuits, or liabilities involving customers, vendors, or other affected parties.

Coverage can also include expenses such as breach response and notification costs, public relations support, legal fees, forensic investigations, and data restoration. So more than just helping a business recover after an incident, cyber liability insurance is designed to help minimize the long-term financial, operational, and reputational consequences of a cyber event.

Ritchie Vener: Can you discuss some of today's cyber threats that impact business?

Haley Cagle: Today's cyber threats come in many forms and continue to evolve as we make more technological advances. Some of the most common risks businesses face today are phishing and social engineering schemes, where cyber criminals use deceptive emails, messages, or tactics to trick employees into revealing sensitive information or transferring funds.

Organizations are also increasingly vulnerable to cyberattacks that can disrupt their operations, compromise their data, and impact their business continuity. Another growing concern in this area is cyber extortion and ransomware attacks, which these terms are sometimes used interchangeably, in which attackers encrypt or steal data and demand payment in exchange for restoring access or preventing the release of sensitive information.

Additionally, the rise of contactless technology in digital payment systems, which we see a lot more in the hospitality industry with these contactless payment systems, has created even more new opportunities for cyber criminals to exploit these vulnerabilities, and it makes strong cybersecurity measures and risk management practices more important than ever.

Ritchie Vener: Heidi, how risky is it for businesses to self-insure for cyber? I know that quite a few do that.

Heidi Strommen: Yeah, you're right, Ritchie. A lot of self-insurance is occurring among a variety of businesses right now, and how risky is it? In my opinion, it's pretty crazy, and it's also unnecessary because there are very affordable and comprehensive insurance policies available to cover this exposure, and there's just really no reason to self-insure.

Heidi Strommen: The financial impact of a cyber incident can be significant, making cyber liability insurance an important consideration for businesses of all sizes. The average cost of a data breach globally reached \$4.88 million in 2024, a 10% increase from the prior year.

For businesses in the hospitality industry, the average cost of a breach rose to \$3.86 million, highlighting the substantial financial exposure organizations face when sensitive data is compromised. The risk is also widespread. In the past year, 90% of global organizations reported experiencing a cyberattack, demonstrating that cyber threats are no longer a matter of if, but when.

Businesses that choose to self-insure these costs must absorb them directly, including expenses related to incident response, legal defense, regulatory compliance, data recovery, and reputational damage.

To be honest, brokers who represent cyber as a non-essential optional coverage when you're meeting with your clients are really doing a disservice. It's incumbent upon us in this industry to help educate our clients about the exposure that they have in this area.

Ritchie Vener: Distinguished has been really working hard to make sure that we've got a great program here. Can you tell us, Heidi, we recently introduced several enhancements to our Cyber Liability Insurance program. Can you give us a high-level overview of what's new before we dive into the details?

Heidi Strommen: We are really excited to talk about several enhancements that make our Cyber Liability Insurance program more accessible and efficient for brokers and their clients. We've expanded eligibility to include art galleries, museums, and contractors, building on our established appetite for hotels, restaurants, and community associations. We've also streamlined the quoting process by enabling brokers to receive instant quotes through the Broker Connect Portal, making it faster and easier to secure coverage. In addition, we are updating our policy form to further strengthen the program.

Ritchie Vener: Haley, can you dive into some case studies for each eligible industry and maybe share examples of cyber risks that restaurants face today to start off?

Haley Cagle: I love doing the case studies. It's often the thing that kind of sells the product. When you actually hear a real-world example, it really helps you understand what's going on out there. We'll start with restaurants.

Haley Cagle: Restaurants are increasingly relying on technology, particularly their point-of-sale systems, which can make them really attractive for cybercriminals.

A notable example occurred in 2023, when the BlackCat ransomware group breached the Aloha POS platform, which is used by thousands of restaurants nationwide. The attack disrupted operations and exposed payment credentials, and this just highlights how a single cyber event can impact revenue, customer trust, and day-to-day business functions.

Ritchie Vener: How about some examples from the hotel industry?

Haley Cagle: We have plenty examples for hotels too. Hotels continue to be a prime target because they handle large volumes of guest and payment information.

In 2024, Omni Hotels & Resorts experienced a cyber attack that caused a significant IT outage. It disrupted reservations, room access, and payment processing. In that same year, a breach involving the Otelier platform exposed guest information associated with major hotel brands.

Additionally, Marriott reported a social engineering incident in which hackers obtained approximately 20 gigabytes of data from a single property.

Ritchie Vener: Let's talk about a couple of lines where it might not be top of mind for people that this is where cyber attacks can happen. How do cyber threats impact museums and art galleries?

Haley Cagle: Places where you wouldn't even really expect it, such as museums and art galleries. They depend on digital systems to manage collections, exhibits, and donor information, and their day-to-day operations.

In 2023, a ransomware attack on Gallery System disrupted the eMuseum platform. This affected online access to collections and internal systems at institutions across the country. And that same year, Walters Art Museum experienced a data breach that exposed sensitive personal and health-related information.

Ritchie Vener: How about cyber risks for community associations that we should be aware of?

Haley Cagle: Community associations are increasingly being targeted by financial fraud and social engineering schemes.

A real-life example for community associations, it happened in Florida, and this was a condominium association where fraudsters used a spoofed email to redirect a \$105,000 payment into their own account.

Haley Cagle: Incidents like this really demonstrate how a seemingly simple email can result in a substantial financial loss and operational challenges for associations and their management teams.

Ritchie Vener: Cyber risk isn't always the first thing people think about with contractors. Why is it important to this industry?

Haley Cagle: According to the 2024 Construction Cybersecurity Report, more than 70% of contracting firms have been impacted by cyberattacks.

Contractors rely heavily on their digital systems for project management, accounting, vendor payments, payroll, and their communications.

A real-life example for contractors, they had a spoofed email request that appeared to come from a legitimate vendor, and it resulted in another six-figure payment being sent to a fraudulent account. Incidents like this demonstrate how a seemingly routine email exchange can lead to significant financial losses, project delays, and operational disruptions.

Ritchie Vener: Those are great examples, Haley.

Heidi, one of the enhancements you mentioned was a new policy form. What are some of the key enhancements brokers should know about?

Heidi Strommen: We're very excited to be introducing this new policy form in the next month or so. We're updating our policy form to the latest Beazley Breach Response 5.0 form, which includes several new coverages and enhancements that reflect how cyber risks continue to evolve. Some of the new insuring agreements include computer bricking loss, which helps cover the cost of replacing computers that become unusable due to software or firmware corruption, and reputation loss, which can help cover lost income when a cyber event leads to negative media attention and impacts a business's revenue.

We've also added invoice manipulation coverage for situations involving fraudulent invoices or payment instructions, and cryptojacking coverage for unauthorized use of computer systems to mine cryptocurrency, and proof of loss expenses coverage, which can help insureds bring in outside experts to document and support a claim.

There are also some important enhancements to existing coverages. For example, our cyber extortion loss coverage now gives policyholders more flexibility when responding to a ransomware event, and it specifically covers the cost of consulting with legal counsel to determine whether a ransom payment can be made in compliance with applicable laws. We've also clarified our subsidiary coverage wording so that if a subsidiary is sold during the policy period, coverage continues to apply to covered incidents that occurred before the sale.

Ritchie Vener: Haley, I'm going to go back to one of our important features, the ability for brokers to get an instant quote. How can they do that?

Haley Cagle: Brokers can submit new Cyber business online and receive an instant quote for eligible risks, all in one place and at their own time.

Our Broker Connect Portal allows you to upload supporting documents, such as loss runs, for quicker underwriting reviews. Once a quote is ready, brokers can request to bind new business directly through the platform.

The Broker Connect Portal makes ongoing policy management easier by allowing users to electronically sign applications and submit endorsement requests online. What we're really looking to do is just help make the process easier and faster for everybody.

Ritchie Vener: Heidi, what are the coverages that our Cyber Liability Program offers?

Heidi Strommen: Our coverage includes breach response costs such as customer notifications and access to legal, forensic, public relations, and crisis management services following a cyber event.

I want to add that one area that's sometimes underestimated in terms of what it can cost someone who has decided to self-insure, perhaps someone who has bought an inferior policy, is the cost associated with these notifications and compliance requirements that even if there was no actual damage done to your customers, you still have to follow all of these rules, and to do that as a business owner on your own can be quite overwhelming.

We're very proud of the breach response coverages that are included in our program, and we feel that it's truly industry-leading.

The policy also provides protection for cyber extortion and ransomware-related expenses, as well as business interruption losses. The program includes data and network liability coverage, regulatory defense costs and penalties, and payment card liability and associated expenses.

Businesses are also protected against media liability exposures and certain types of fraud, including funds transfer fraud, telephone fraud, and fraudulent instruction schemes. The policy includes a criminal reward benefit which can help support efforts to identify and apprehend those responsible for a cybercrime.

Ritchie Vener: That's quite a comprehensive list. What doesn't Distinguished's Cyber Liability Insurance Program cover?

Heidi Strommen: While our program is designed to provide broad protection, there are some important limitations, and many of these are common in the marketplace

.

The policy does not cover cyberattacks carried out by nation-states or terrorist groups, which are typically excluded under standard cyber coverage. It also does not cover post-breach upgrades or system improvements, meaning costs to enhance or modernize systems after an incident wouldn't be included.

The program does not respond to losses related to intellectual property theft, such as the loss of proprietary ideas or trade secrets. It also excludes long-term reputational damage or projected future income loss, which can be difficult to quantify and directly attribute to a specific cyber event. The policy remains focused on providing strong financial protection for the immediate and direct impacts of a covered cyber incident.

Ritchie Vener: Haley, how much does cyber liability insurance cost?

Haley Cagle: It can vary so much by industry to industry, what they're looking at here, so let's just go into it a little deeper.

The cost of cyber liability insurance varies a lot. It depends on the risk profile of the business, and we're looking at several key factors when determining pricing. So some of the biggest factors include the size and how much revenue they're taking in, because larger organizations really do have a big data exposure and operational complexity as well.

The industry risk profile also plays a major role. Some sectors are facing much higher cyber threat activities than others. Pricing is also influenced by a company's network security protocols and their overall cyber hygiene, as well as the history of cyber claims or any prior incidents. Then, depending on what limits and deductibles you take, that also affects the cost. Higher limits generally lead to higher premiums.

Finally, underwriters consider the type of data a business stores. So are you storing credit card information or Social Security numbers? Are you storing sensitive personal data? The more sensitive the data, the greater the potential exposure, and all that can affect pricing.

Ritchie Vener: That all makes sense. Can we write in all states?

Haley Cagle: Yes. We are available in all 50 states.

Ritchie Vener: Heidi, who is our carrier partner?

Heidi Strommen: Our carrier partner is Beazley, recognized worldwide as a leader in cyber coverage. We offer a proprietary rating structure that is available exclusively for Distinguished clients.

Ritchie Vener: Haley, what can we do to help brokers successfully sell cyber liability to clients?

Haley Cagle: I think one of the most effective ways is to start by highlighting the average cost of the data breach. Once they see the actual process they have to go through and what an average data breach actually costs, it helps them understand more readily the financial exposure they're facing.

It's important to walk through what actually happens during a data breach. That includes notification requirements, forensic investigations, legal response, and reputational management. Many businesses underestimate how complex and costly these steps can be in real time. And a lot of these businesses don't have the staff to do this on their own.

Lastly, using real-life cyber examples, which I talked about a little bit earlier, helps bring the conversation to life. When clients see how similar businesses have been disrupted or financially impacted, it becomes much easier for them to understand why cyber liability coverage isn't optional. Nowadays, it really is just a critical part of their overall risk management strategy.

Ritchie Vener: Heidi, why should brokers choose Distinguished's Cyber Liability Program?

Heidi Strommen: We've made it easy to get a quick quote. Our investment in the Broker Connect Portal Cyber product has really been designed to ease brokers through that process; it doesn't take up much of your time, and most submissions will receive an instant quote if you use the portal.

Second, our program offers strong first and third-party coverage addressing both direct financial losses from a cyber event and liability claims that may follow. It also includes media liability protection, which helps address risks tied to digital content, online communications, and reputational exposure.

The program provides higher limits than many of our competitors. We offer up to \$5 million, depending on the class, along with cyber extortion coverage to help protect against ransomware and other extortion threats. In addition, notification expenses are covered outside of the liability limits, an important coverage note. It helps to ensure clients have access to necessary resources without eroding their core coverage.

One of the key differentiators is access to 24/7 crisis response support, giving insureds immediate help from experts who can assist with containment, recovery, and next steps after an incident.

Finally, the program is designed to fit seamlessly alongside other Distinguished offerings, making it a strong option for industries like art galleries, museums, hotels, restaurants, community associations, and contractors.

Ritchie Vener: Haley, who should a broker contact if they have additional questions and how should they contact?

Haley Cagle: If you have additional questions, you can feel free to reach out to me at [hcagle@distinguished.com](mailto:hcagle@distinguished.com) or give me a call at (212) 297-3146. We also have a general cyber inbox you can reach out to: [cyber@distinguished.com](mailto:cyber@distinguished.com).

We are happy to help you. If you have any questions about getting started with the Broker Portal or any general cyber questions, feel free to contact me.

Ritchie Vener: We also got some questions that were sent in ahead of time in response to our emails inviting people. Do small businesses really need cyber liability insurance?

Heidi Strommen: Absolutely. Small businesses need cyber coverage. Cyber criminals don't distinguish between large corporations and small businesses. In many cases, small businesses are actually seen as easier targets because they have fewer cybersecurity resources or fewer formal protections in place.

It's more difficult for a small business to absorb the costs associated with responding to a cyberattack. You can make a very strong case to your small-business clients that they should carry cyber insurance.

Ritchie Vener: I just want to put an exclamation point, how do I submit business?

Haley Cagle: You can get an instant quote through our Broker Connect Portal. You have to be registered with Distinguished to get started. If you have any questions along the way, just feel free to reach out to us.

Ritchie Vener: I see that we're running out of time. We will send all registrants a copy of the slides, the webinar recording, and a PDF with the questions and answers from today's session, including the questions that were submitted in the chat during the webinar.

If you enjoyed today's webinar, stay up to date on our latest events by following us on social media. We post about the insurance market insights and industry news, and you'll learn about our latest free webinars, eBooks, and case studies.

I'd like to thank everyone who joined us today for the webinar, and to our panelists, Heidi Strommen and Haley Cagle, for sharing their valuable insights. We hope you found this information helpful and that you now have a clear understanding of the latest enhancements in our Cyber Liability Program, giving you the tools to better support your clients.

Remember, our underwriters will be available to answer any follow-up questions. Thank you for joining us today, and we'll see you at the next webinar. Bye, everybody.

# Cyber Liability Insurance

Below are additional attendee questions we could not address during the session.

---

## **Q: What limits are available?**

A: We currently offer Cyber Liability limits up to \$5M.

## **Q: How do I submit business?**

A: Get an instant quote through the [Broker Connect Portal](#). Please note, you must be registered with Distinguished to submit business with us. If you have any questions along the way, feel free to reach out.

## **Q: What are the best practices for managing cyber risks associated with third-party vendors that may not maintain strong cybersecurity protocols?**

A: Third-party vendors can create major cyber exposure if they don't have strong security practices in place. The best approach is for insureds to carefully vet vendors, require cybersecurity standards in contracts, and make sure vendors carry their own Cyber Liability coverage.

## **Q: Who is the carrier?**

A: Beazley is our carrier partner, a leader in Cyber coverage. We offer a proprietary rating structure offered exclusively for Distinguished clients.

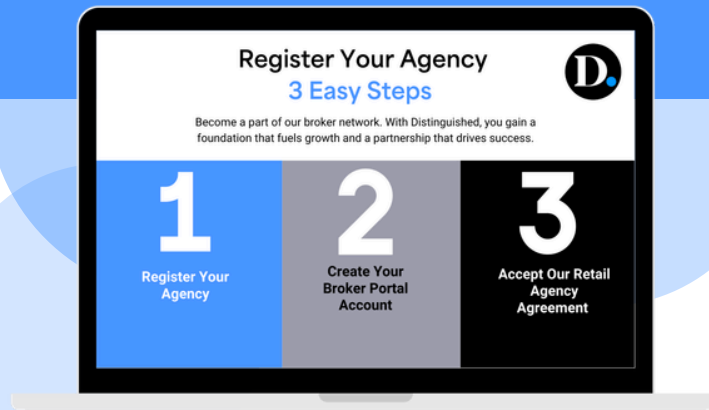
## **Q: What limit of insurance do you recommend for the average insured? Is a \$1M limit still sufficient?**

A: Recommended coverage limits depend on the insured's specific risk profile and exposures. We offer Cyber Liability limits up to \$5M to help support a range of client needs.

## **Q: Do small businesses need Cyber Liability coverage?**

A: Yes, they do. Cybercriminals typically don't distinguish between large corporations and small businesses. In many cases, small businesses are actually seen as easier targets because they may have fewer cybersecurity resources or less formal protections in place. It is also more difficult for a small business to absorb the costs associated with responding to a cyberattack.

# How to Register Your Agency



1.

Go to

[www.distinguished.com/site/brokers/](http://www.distinguished.com/site/brokers/)

2.

Click on

'Launch Broker Portal'

3.

Login to quote, bind and issue  
in real time

[Register Now](#)

## Distinguished benefits you can count on.



**WORLD-CLASS  
EXPERTS**



**UNMATCHED  
SOLUTION**



**PROGRAM  
STABILITY**

This document is for informational purposes only and reflects the opinions of the authors. It may include references to laws, regulations, court decisions, reports, charts, market trends, claims or claim outcomes. These references are for general discussion and do not constitute legal, financial, insurance, or professional advice. Readers should not rely on this document as a substitute for legal counsel, regulatory guidance, independent research, or advice from a licensed insurance broker. The authors and publishers make no warranties regarding the accuracy, completeness, or applicability of the information presented. Any actions taken based on this content are at the sole discretion and risk of the reader. This document may include general insurance policy information. This information does not provide a complete description of coverage terms, conditions, and limits, nor does it purport to restate, explain, or interpret any insurance policy or terms therein. Only the actual policy contains a complete description of all provisions of the coverage. The policy described may not be available in all States. Nothing herein is intended to confirm what should be included in a comprehensive risk mitigation plan. Any recommendations or lists contained herein are illustrative and are not intended to be exhaustive.

For more information, visit [www.distinguished.com](http://www.distinguished.com)

CA License # 0D06551

