

CYBER INSURANCE PROPOSAL FOR WORLD GROUND CAFE, L.P.

02/16/2024



Powered by:  SAYATA

WHAT'S IN THIS DOCUMENT

Tailored cyber coverage options	page 3
FAQ	page 5
Claims scenarios	page 6
Cyber insurance glossary	page 11
Cybersecurity and regulatory glossary	page 13
Acknowledgment of rejected coverage	page 14

NEXT STEPS

1

CHOOSE COVERAGE

Select the option that best suits your coverage needs (see page 3). Quotes must be bound prior to their expiration date.

2

OPEN THE APPLICATION

Click the "Review application" link below the coverage price.

3

COMPLETE, APPROVE AND SUBMIT

Complete and approve the application. Get your policy faster by using the digital application.

*If you choose not to purchase coverage, please sign the Acknowledgement of rejected coverage form and return to your agent (see page 14).



CYBER COVERAGE OPTIONS FOR WORLD GROUND CAFE, L.P.

Select your preferred option, and click "Review application". See footer below for more details.

COST AND COVERAGE MAY CHANGE BASED ON YOUR RESPONSES TO THE APPLICATION.

	cowbell PRIME 100	BRIT	Coalition	at bay SURPLUS
VALID UNTIL	04/13/24	04/13/24	04/13/24	04/13/24
ADMISSION STATUS	Admitted	Non-Admitted	Admitted	Non-Admitted
ISSUING INSURER	Refer to quote letter	Certain Underwriters at...	Coalition Insurance...	Trisura Specialty Insurance...
AM BEST RATING Financial strength rating	A (Excellent)	A (Excellent)	A- (Excellent)	A- (Excellent)
AGGREGATE LIMIT Maximum amount paid by the insurance company for the duration of the policy	\$1,000,000	\$1,000,000	\$1,000,000	\$1,000,000
RETENTION The same as a deductible, the amount of a claim you pay	\$2,500 ¹	\$2,500 ¹	\$2,500 ¹	\$2,500 ¹
NOTIFICATION COSTS Cost to notify affected individuals after a data breach	\$1,000,000	\$1,000,000	\$1,000,000	\$1,000,000
BREACH COSTS INSIDE/OUTSIDE Will the breach costs erode the aggregate limit (inside) or are separate (outside)	Inside	Outside	Outside	Outside
BUSINESS INTERRUPTION Covers lost profits incurred due to not operating	\$1,000,000	\$1,000,000	\$1,000,000	\$1,000,000
BI WAITING PERIOD Minimum duration of business interruption before coverage starts	6 hours	8 hours	8 hours	8 hours
CONTINGENT BUSINESS INTERRUPTION Losses from an interruption in 3rd party computer services or software	\$1,000,000	\$1,000,000	\$1,000,000	\$1,000,000
DATA RECOVERY The cost of recovering lost data	\$1,000,000	\$1,000,000	\$1,000,000	\$1,000,000
EXTORTION/RANSOMWARE Covers damage and ransom payments from an attack	\$1,000,000	\$1,000,000	\$1,000,000	\$1,000,000
BRICKING When computers and electronic hardware are damaged beyond repair	\$1,000,000	\$1,000,000	\$1,000,000	\$1,000,000
NETWORK SECURITY AND PRIVACY LIABILITY Third party liability costs	\$1,000,000	\$1,000,000	\$1,000,000	\$1,000,000
PCI Covers fines or penalties imposed by banks or credit card companies	\$1,000,000	\$1,000,000	\$1,000,000	\$1,000,000
REGULATORY In case you're fined by regulators (e.g., for breaching consumer privacy)	\$1,000,000	\$1,000,000	\$1,000,000	\$1,000,000
MEDIA When your content triggers legal action against you (e.g. - libel, plagiarism)	\$1,000,000	\$1,000,000	\$1,000,000	\$1,000,000
COMPUTER FRAUD Covers funds or property stolen resulting from a hack	\$1,000,000 ¹	\$1,000,000 ¹	\$1,000,000 ¹	\$1,000,000 ¹
FUNDS TRANSFER FRAUD When a criminal deceives a bank/institution to transfer funds	\$1,000,000 ¹	\$1,000,000 ¹	\$1,000,000 ¹	\$1,000,000 ¹
SOCIAL ENGINEERING When cyber criminals deceive a business to transfer funds willingly	\$1,000,000 ¹	\$1,000,000 ¹	\$1,000,000 ¹	\$1,000,000 ¹
TOTAL	(Approximate*) \$2,885	(Approximate*) \$3,480.4	(Approximate*) \$3,885	(Approximate*) \$3,996.3
	PREMIUM \$2,500 CARRIER FEE \$0 BROKER FEE \$200 PROCESSING FEE ³ \$185	PREMIUM \$3,000 CARRIER FEE \$0 BROKER FEE \$200 PROCESSING FEE ³ \$185 SL FEES & TAXES \$95.4	PREMIUM \$3,500 CARRIER FEE \$0 BROKER FEE \$200 PROCESSING FEE ³ \$185	PREMIUM \$3,500 CARRIER FEE ⁴ \$0 BROKER FEE \$200 PROCESSING FEE ³ \$185 SL FEES & TAXES \$111.3

FIRST PARTY COVERAGE

THIRD PARTY COVERAGE

CYBER CRIME

[REVIEW APPLICATION](#)
 [REVIEW APPLICATION](#)
 [REVIEW APPLICATION](#)
 [REVIEW APPLICATION](#)

[View Sample policy / Full quote](#)
 [View Sample policy / Full quote](#)
 [View Sample policy / Full quote](#)
 [View Sample policy / Full quote](#)

1 Cyber crime **retentions** may vary. After confirming presumptions, check firm quote for full details.
 2 All cost components are estimated. After the application is completed and signed you will receive a firm quote from the carrier. Costs may change based on final application responses.
 3 Processing Fee is a client-related expense for processing quotes.
 4 At-Bay's carrier fee is for embedded security services.
 * Please review final quotes for most accurate information, as comparison data above is a simplified view and may contain inaccuracies. Retentions may vary by coverage part.



CYBER COVERAGE OPTIONS FOR WORLD GROUND CAFE, L.P.

Select your preferred option, and click "Review application". See footer below for more details.

COST AND COVERAGE MAY CHANGE BASED ON YOUR RESPONSES TO THE APPLICATION.

VALID UNTIL	04/13/24	04/13/24	04/13/24	04/13/24
ADMISSION STATUS	Non-Admitted	Non-Admitted	Admitted	Non-Admitted
ISSUING INSURER	North American Capacity, Arch...	CFC Underwriting Limited	Clear Blue Insurance...	Hudson Excess Insurance...
AM BEST RATING Financial strength rating	A+ (Superior) A- (Excellent)	A (Excellent)	A- (Excellent)	A (Excellent)
AGGREGATE LIMIT Maximum amount paid by the insurance company for the duration of the policy	\$1,000,000	\$1,000,000	\$1,000,000	\$1,000,000
RETENTION The same as a deductible, the amount of a claim you pay	\$2,500 ¹	\$2,500 ¹	\$2,500 ¹	\$2,500 ¹
NOTIFICATION COSTS Cost to notify affected individuals after a data breach	\$1,000,000	\$1,000,000	\$1,000,000	\$1,000,000
BREACH COSTS INSIDE/OUTSIDE Will the breach costs erode the aggregate limit (inside) or are separate (outside)	Outside	Outside	Outside	Outside
BUSINESS INTERRUPTION Covers lost profits incurred due to not operating	\$1,000,000	\$1,000,000	\$1,000,000	\$1,000,000
BI WAITING PERIOD Minimum duration of business interruption before coverage starts	8 hours	8 hours	8 hours	6 hours
CONTINGENT BUSINESS INTERRUPTION Losses from an interruption in 3rd party computer services or software	\$1,000,000	\$1,000,000	\$1,000,000	\$1,000,000
DATA RECOVERY The cost of recovering lost data	\$1,000,000	\$1,000,000	\$1,000,000	\$1,000,000
EXTORTION/RANSOMWARE Covers damage and ransom payments from an attack	\$1,000,000	\$1,000,000	\$1,000,000	\$1,000,000
BRICKING When computers and electronic hardware are damaged beyond repair	\$1,000,000	\$1,000,000	\$1,000,000	\$1,000,000
NETWORK SECURITY AND PRIVACY LIABILITY Third party liability costs	\$1,000,000	\$1,000,000	\$1,000,000	\$1,000,000
PCI Covers fines or penalties imposed by banks or credit card companies	\$1,000,000	\$1,000,000	\$1,000,000	\$1,000,000
REGULATORY In case you're fined by regulators (e.g., for breaching consumer privacy)	\$1,000,000	\$1,000,000	\$1,000,000	\$1,000,000
MEDIA When your content triggers legal action against you (e.g., libel, plagiarism)	\$1,000,000	\$1,000,000	\$1,000,000	\$1,000,000
COMPUTER FRAUD Covers funds or property stolen resulting from a hack	\$1,000,000 ¹	\$250,000 ¹	\$1,000,000 ¹	\$1,000,000 ¹
FUNDS TRANSFER FRAUD When a criminal deceives a bank/institution to transfer funds	\$1,000,000 ¹	\$250,000 ¹	\$1,000,000 ¹	\$1,000,000 ¹
SOCIAL ENGINEERING When cyber criminals deceive a business to transfer funds willingly	\$1,000,000 ¹	\$250,000 ¹	\$1,000,000 ¹	\$1,000,000 ¹
TOTAL	(Approximate) ² \$4,512.2	(Approximate) ² \$4,512.2	(Approximate) ² \$4,885	(Approximate) ² \$5,028.1
	PREMIUM \$4,000 CARRIER FEE \$0 BROKER FEE \$200 PROCESSING FEE ³ \$185 SL FEES & TAXES \$127.2	PREMIUM \$4,000 CARRIER FEE \$0 BROKER FEE \$200 PROCESSING FEE ³ \$185 SL FEES & TAXES \$127.2	PREMIUM \$4,500 CARRIER FEE \$0 BROKER FEE \$200 PROCESSING FEE ³ \$185	PREMIUM \$4,500 CARRIER FEE \$0 BROKER FEE \$200 PROCESSING FEE ³ \$185 SL FEES & TAXES \$143.1

FIRST PARTY COVERAGE

THIRD PARTY COVERAGE

CYBER CRIME

[REVIEW APPLICATION](#)
 [REVIEW APPLICATION](#)
 [REVIEW APPLICATION](#)
 [REVIEW APPLICATION](#)

[View Sample policy / Full quote](#)
 [View Sample policy / Full quote](#)
 [View Sample policy / Full quote](#)
 [View Sample policy / Full quote](#)

1 Cyber crime **retentions** may vary. After confirming presumptions, check firm quote for full details.
 2 All cost components are estimated. After the application is completed and signed you will receive a firm quote from the carrier. Costs may change based on final application responses.
 3 Processing Fee is a client-related expense for processing quotes.
 * Please review final quotes for most accurate information, as comparison data above is a simplified view and may contain inaccuracies. Retentions may vary by coverage part.



FAQ

WHAT IS CYBER INSURANCE?

When a breach occurs, cyber insurance covers the range of expenses that arise. These include identifying and solving the breach, recovering data, customer notifications, PR costs, possible credit monitoring expenses, legal expenses, potential fines from compliance regulators, extortion costs from ransomware, and general business interruption.

DO HACKERS REALLY BOTHER WITH ATTACKING SMALL BUSINESSES?

Yes. Hackers use technology to scan the internet for businesses with weak defenses regardless of the size of the business. A recent [Verizon report](#) notes that 43% of all cyber attacks are against small businesses. Worse, [63% of small businesses](#) had experienced a breach in the last 12 months. Any business with a computer and an internet connection is at risk - even if you don't sell anything on your website.

WHAT'S COVERED?

First-party coverage - Intends to cover damages a business suffers because of a cyber breach. This can include things like investigative services, business interruption coverage and data recovery.

Third-party coverage - Intends to cover damages if a business' customers or partners are affected by a cyber attack. This can include legal fees, settlement costs, security failures and media liabilities.

Cyber crime — Intends to cover damage due to any type of illegal activity that occurs using digital means. Examples of cybercrime are extortion/ransomware, phishing, social engineering, and wire transfer fraud.

DOESN'T MY CURRENT BUSINESS INSURANCE INCLUDE CYBER ATTACKS?

Many general business protection policies only partially cover damage from cyber events, *if at all*. As mentioned above, cyber coverage protects against the vast array of possible damages, expenses, and lost business that can occur from a cyber attack.

WHAT SHOULD I CONSIDER WHEN CHOOSING BETWEEN PURCHASING A STAND-ALONE CYBER POLICY VS. ADDING AN ENDORSEMENT TO AN EXISTING POLICY?

To be fully protected, ensure you have all coverages - first-party, third-party, and cyber crime. Further, since some cyber events can result in large expenses, confirm you have adequate sublimits for each of three above coverages.

WHY DO I NEED A "BREACH COACH"?

If your company gets hacked, you will need a breach coach to get your business back up and running fast. When a breach occurs, you need to assess and contain the damage, notify affected parties (e.g. customers and vendors), evaluate and act on the legal ramifications from agitated customers to regulatory bodies, and more. A breach coach will quickly assemble the right response team to deal with these issues. Without an expert it all falls on you, costing you time and money while adversely affecting your business. Fortunately, most insurance companies now provide a breach coach as part of a greater suite of services when you purchase stand-alone cyber insurance coverage.

DO SMALL BUSINESSES NEED CYBER INSURANCE IF THEY PRACTICE GOOD CYBER HYGIENE?

Being properly protected definitely helps. However, there is no way to fully protect against new threats. Hackers are always adapting to overcome cyber defenses with new versions of current threats or creating brand new methods of attacking businesses. Human error can also be a factor. Easy-to-hack passwords, phishing emails, or even a lost laptop also present potential entry points for a cyber criminal. Additionally, a third-party vendor could be attacked, impacting your ability to do business and exposing your data. Even if you use a third-party vendor for business services, as the data owner you may be legally responsible. A thorough cyber insurance policy is part of your overall risk management plan to ensure your business runs smoothly.

* All of the above is general information which may vary based on context. Please consult the quote or ask an agent/broker for precise definitions and details.



CLAIM SCENARIO

RANSOMWARE | Accommodation and Food Services

The following example is meant to illustrate a potential scenario you might encounter. It may not necessarily represent details of a specific claim.

SITUATION

An employee of a regional pizza franchise accidentally clicked on a malware link. The virus was downloaded onto the company server causing all data to be encrypted. The employee then received an email demanding \$115,550 paid in Bitcoin within 24 hours to release their data files.

5,000 customer records including name, address, phone and credit were encrypted. The franchise called their insurance company's cyber response team, who responded by assigning a "breach coach," which is covered as part of the franchise's stand-alone cyber policy.

The breach coach sent in a forensics team to assess the situation, including any computer or electronic hardware damage, and determine if paying the ransom was necessary. Concurrently, the insurance company confirmed coverage and assisted with opening a claim to minimize the effect of business interruption.

POTENTIAL IMPACT

INCIDENT RESPONSE	
Incident response manager ("breach coach") fees	\$22,570
Forensic investigation costs to locate malware, analyze damage, ensure containment and calculate loss	\$29,180
Legal fees	\$42,120
NOTIFICATION COSTS	
	\$3,150
BUSINESS INTERRUPTION	
	\$298,899
DATA RECOVERY	
Costs associated with replacing lost or corrupted data	\$41,775
EXTORTION/RANSOMWARE	
Ransom payment	\$121,500
BRICKING	
Damage to computer and hardware systems	\$44,030
TOTAL POTENTIAL CLAIM	\$603,224

RESOLUTION

While the business maintained regular back-ups online, the hackers also encrypted these files leaving the franchise no way to restore the data. The insurance company and breach coach agreed the fastest, best way to get the business back up and running was to pay the ransom.

The insurance company immediately paid the ransom via their pre-established Bitcoin account, releasing the records back to the franchise.

The swift assessment and payment, minimized the business interruption allowing the franchise to resume operations.





CLAIM SCENARIO

OUTDATED SOFTWARE | Accommodation and Food Services

The following example is meant to illustrate a potential scenario you might encounter. It may not necessarily represent details of a specific claim.

SITUATION

Hackers penetrated a local hotel's network from a vulnerability in an outdated software application. 3,000 guest names, emails and credit card information were compromised.

Local authorities received multiple complaints of suspicious activity, leading the hotel's IT department to discover an unauthorized user had accessed the system.

Once discovered, the hotel called their insurance carrier who immediately brought in forensic experts to initiate the hotel's IT recovery plan and notification program.

POTENTIAL IMPACT

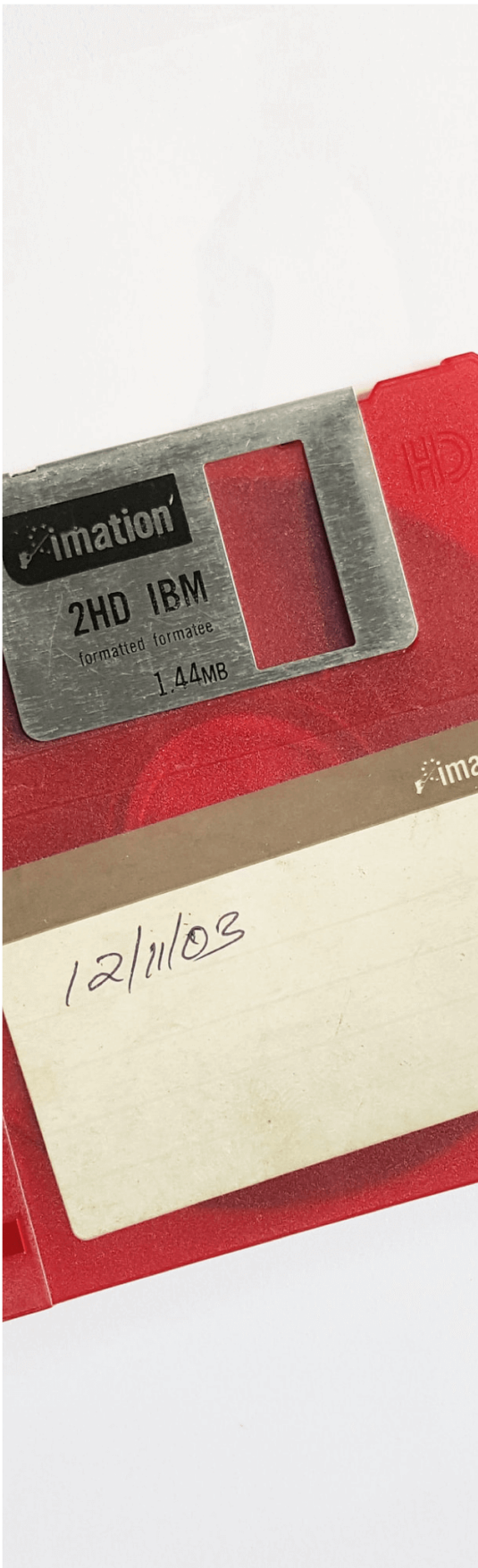
INCIDENT RESPONSE	
Forensic investigation costs to isolate vulnerability, analyze damage, ensure containment and calculate loss	\$10,250
Identity theft and credit monitoring services	\$8,640
Incident response fees	\$8,000
Public relations fees to minimize reputational impact	\$9,800
Call center set up and operation to field inquiries	\$9,000
NOTIFICATION COSTS	
DATA RECOVERY Costs associated with replacing lost or corrupted data	\$13,500
REGULATORY	
Legal expenses arising from regulatory investigation due to mismanagement of private information	\$20,070
Legal expenses and settlement costs for claims	\$14,300
Business interruption	\$30,269
TOTAL POTENTIAL CLAIM	\$251,650

RESOLUTION

The hotel's cyber policy was triggered, giving them immediate access to response services. The insurance company dispatched a forensic team who quickly isolated the unauthorized user.

A claim was started immediately to help with impending legal, consulting and media costs. The insurance company, IT team and forensic consultants ensured the hotel had up-to-date cyber defenses including firewalls, intrusion detection software, and encrypted databases.

Concurrently, officials worked with local media to notify affected guests and offer credit monitoring services, while the legal team handled the backlash from those affected. Finally, the forensic consultants helped develop a new plan that included regular updates, testing, and education of all staff to minimize future breaches.



CLAIM SCENARIO

SOCIAL ENGINEERING | Accommodation and Food Services

The following example is meant to illustrate a potential scenario you might encounter. It may not necessarily represent details of a specific claim.

SITUATION

A catering company's emails were accessed by an attacker who, posing as the General Manager, asked an employee to contact the broker's bank with instructions for funds to be transferred into the hacker's bank account.

When the company discovered that unauthorized payments were made totaling \$67,500, they immediately contacted their bank to freeze the funds and notified their cyber insurance carrier. Together, they were able to recover \$54,900 of the unauthorized transactions.

POTENTIAL IMPACT

INCIDENT RESPONSE

Forensic investigation costs to locate the breach, analyze damage, and ensure containment

\$8,875

Legal fees

\$6,000

FUNDS TRANSFER FRAUD

Transferred funds not recovered

\$12,600

TOTAL POTENTIAL CLAIM

\$27,475

RESOLUTION

The company has a stand-alone cyber policy that covers social engineering as well as provides crucial response services. Once the company notified their insurance company, an IT forensic consultant was appointed to assist the company in repairing the damage to their system as well as to prevent future attacks.

As the company has expanded cyber crime coverage under their policy, they were reimbursed for the direct financial loss, less the deductible, of the unrecovered fraudulent transfers as well as their forensic and legal costs.





CLAIM SCENARIO

LOST HARDWARE | Accommodation and Food Services

The following example is meant to illustrate a potential scenario you might encounter. It may not necessarily represent details of a specific claim.

SITUATION

An employee of A country club lost their laptop. An Excel file on the computer contained member records of 1,000 members including the guest names, emails, and credit card information.

Once the loss was realized, the country club immediately notified their insurance company who provided a “breach coach” to assess the damage and help the insured comply with regulatory and notification requirements.

POTENTIAL IMPACT

INCIDENT RESPONSE	
Forensic costs to assess and contain damage	\$7,300
Legal fees	\$11,400
Public relations fees to minimize reputational impact	\$8,000
NOTIFICATION COSTS	
DATA RECOVERY Costs associated with replacing lost or corrupted data	\$9,000
REGULATORY Settlement fine	\$16,675
Patient liability settlements	\$31,233
TOTAL POTENTIAL CLAIM	\$84,558

RESOLUTION

The breach coach assigned a forensics team, provided by the insurance company, to determine the potential exposure of the personal information. It was determined that the member personal information was, in fact, compromised. The members were immediately notified and offered credit monitoring services.

Concurrently, the breach coach engaged a public relations agency to minimize the reputational damage as well as alerted counsel to help settle legal action from members.

They were proactive in contacting the Department of Health and Human Service Office for Civil Rights and agreed upon a settlement amount as well as a corrective action plan that included employee cyber and data protection training.





CLAIM SCENARIO

FORMER OR ROGUE EMPLOYEE | Accommodation and Food Services

The following example is meant to illustrate a potential scenario you might encounter. It may not necessarily represent details of a specific claim.

SITUATION

A children's summer camp was hacked by a former employee, whose user credentials were not deleted when they were terminated. The employee sold 3,000 guest records on the dark web including guest names, emails, and credit card information.

The camp notified their insurance company immediately. The carrier provided forensic expertise, legal services, and media relations help to investigate and control the damage.

In addition, the insurance company enlisted a "breach coach" to guide the camp in managing their actual and reputational damage.

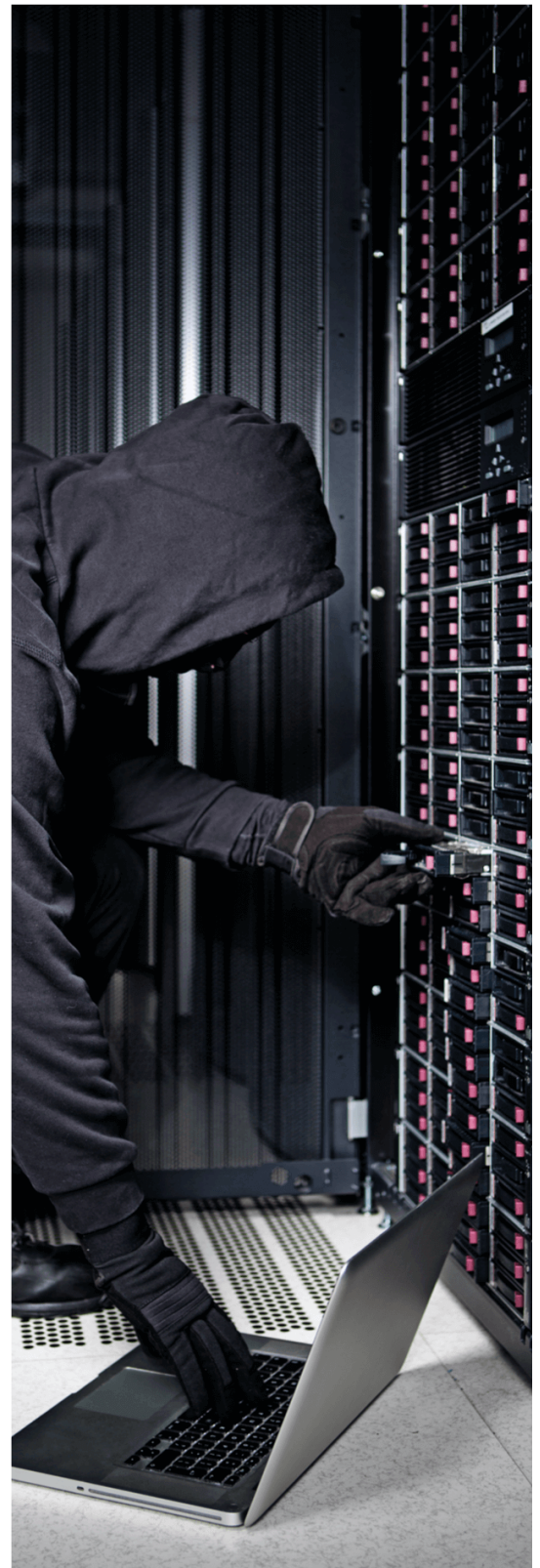
POTENTIAL IMPACT

INCIDENT RESPONSE	
Forensic investigation costs to analyze damage and ensure containment	\$10,360
Identity theft and credit monitoring services	\$10,800
Legal fees	\$15,730
Public relations fees to minimize reputational impact	\$10,000
Call center set up and operation to field inquiries	\$8,800
NOTIFICATION COSTS	
DATA RECOVERY Costs associated with replacing lost or corrupted data	\$1,700
TOTAL POTENTIAL CLAIM	\$69,890

RESOLUTION

The forensic team quickly identified the breach and worked with the camp's IT department to initiate repairs. The breach coach guided the camp to hire a call center to quickly inform affected guests, field questions, and offer identity protection and credit monitoring services to ensure trust going forward. The insurance company recommended seeking legal counsel to pursue civil action against the former employee.

Concurrently, the camp, in tandem with the media relations team, responded quickly and transparently to the media. Finally, the insurance company and forensic team recommended an updated cyber response plan that included more rigorous IT policies and procedures as well as several technological updates to improve cyber hygiene. Due to the fast response, the costs and reputational damage to the camp were minimized.





CYBER INSURANCE GLOSSARY

BUSINESS INTERRUPTION

Cyber business interruption covers the net profit earned before taxes that would have been earned had there been no interruption due to a cyber event.

BI (BUSINESS INTERRUPTION) WAITING PERIOD

A predetermined amount of time that must elapse before any loss or expenses are considered covered by business interruption insurance.

BRICKING

Covers the cost to replace computer and electronic hardware that's rendered inoperable due to failure or purposeful attacks.

COMPUTER FRAUD

Insures against theft of funds or property specifically stolen by using cyber methods to transfer money or property from the victim.

CONTINGENT BUSINESS INTERRUPTION

A contingent business interruption loss occurs when a third-party supplier or service provider experiences an interruption of service due to a cyber event and that event directly impacts the policy holder's ability to produce a product or provide a service.

CYBER CRIME

Any type of illegal activity that occurs using digital means. Examples of cybercrime are extortion/ransomware, phishing, social engineering, and wire transfer fraud.

DATA RECOVERY

Covers the costs of recovering lost data due to a breach.

DATA RESTORATION

The process of copying backup data from secondary storage and restoring it to its original or a new location. Data restoration is done to return data that has been lost, stolen or damaged.

EXTORTION/RANSOMWARE COVERAGE

Coverage for the damage done to a business due to a cyber breach or attack including possible ransom payments to release key systems and data.

FIRST PARTY CLAIM

Where a policy holder files a claim triggered by a cyber breach or other qualifying event directly with their insurance company.

FUNDS TRANSFER FRAUD

Covers the loss stemming from unauthorized instructions from a third party to a bank without the victim's knowledge.

MEDIA (LIABILITY)

Provides coverage against media-related damage such as libel, privacy invasion, copyright infringement, and plagiarism stemming from the policy holder's media activities (e.g website content, printed articles).

NOTIFICATION COSTS

Covers the cost of notifying affected individuals in the event of a data breach. Customer notification is often required by law.

PCI (PAYMENT CARD INDUSTRY)

Coverage for assessments, fines or penalties imposed by banks or credit card companies due to non-compliance with the Payment Card Industry Data Security Standard (PCI DSS).

* All of the above are general terms which may vary based on context. Please consult the quote or ask an agent/broker for precise definitions and details.



CYBER INSURANCE GLOSSARY (CONTINUED)

PRIVACY REGULATORY LIABILITY (REGULATORY)

Covers the loss a company sustains as a result of regulatory investigations and claims.

SOCIAL ENGINEERING COVERAGE

Covers unintended payments made to cybercriminals who, through deception, convinced an employee or officer of a company to transfer funds to the criminal.

THIRD PARTY CLAIM/LIABILITY CLAIM

When a third party files a claim or lawsuit against the policy holder alleging that the policy holder caused some damage to the third party due to a cyber event.

* All of the above are general terms which may vary based on context. Please consult the quote or ask an agent/broker for precise definitions and details.

CYBERSECURITY GLOSSARY

DDOS (DISTRIBUTED DENIAL OF SERVICE) ATTACK

A DDoS attack is a malicious attempt to disrupt or shut down a website by overwhelming the website with a flood of internet traffic.

MALWARE (MALICIOUS SOFTWARE)

A program designed to infiltrate a computer or computer system to steal sensitive information and/or damage a computer or computer system.

PATCH

A software change or update. A patch is often used to repair flaws or bugs in the software as well as introduce new features and capabilities.

PENETRATION TESTING (PENTESTING)

A security test where security experts mimic hackers to expose weaknesses in a computer or computer system.

PHISHING

A message from a hacker that tries to collect sensitive information from you or your business. These messages are dressed up to look like a bank, business or government entity you do business with. Phishing attacks can take place over e-mail, text messages, through social networks or via smartphone apps.

TWO-FACTOR/MULTI-FACTOR AUTHENTICATION

Two or more ways to prove your identity before being allowed access to a site, account or system. This provides an additional layer of security beyond your password.

VULNERABILITY

Any weakness in a computer or software that a hacker could exploit to cause harm.

REGULATORY GLOSSARY

CALIFORNIA CONSUMER PRIVACY ACT (CCPA)

CCPA is legislation designed to protect the privacy rights and collected information of California residents including data held by companies outside of California.

GENERAL DATA PROTECTION REGULATION (GDPR)

GDPR is a European Union (EU) law requiring all businesses, regardless of location, to protect the privacy and personal data collected about EU citizens, including the right of complete data removal.

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)

HIPAA is a federal law that provides privacy standards to protect patient medical records and other health information provided to health plans, doctors, hospitals and other health care providers.

PAYMENT CARD INDUSTRY DATA SECURITY STANDARDS (PCI DSS)

Widely accepted set of policies and procedures intended to protect cardholders against misuse of their personal information. The PCI DSS was created jointly in 2004 by four major credit-card companies: Visa, MasterCard, Discover and American Express.

RED FLAGS RULE

A federal regulation that requires financial institutions to have an official plan and process in place designed to protect consumers from identity theft.

* All of the above are general terms which may vary based on context. Please consult the quote or ask an agent/broker for precise definitions and details.



ACKNOWLEDGMENT OF REJECTED COVERAGE

This page should only be signed if the applicant decided not to purchase the insurance coverage mentioned below.

I understand and acknowledge that the following insurance policies have been offered to me and that I have decided not to purchase the coverage at this time:

CYBER LIABILITY INSURANCE

The potential financial impact of not having these important coverages has been explained to me and I realize that my rejection of these options may result in the denial of claims in the future.

Signed: _____

Company: WORLD GROUND CAFE, L.P.

Date: _____