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OUTDATED SOFTWARE | Accommodation and Food Services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Hackers penetrated a local hotel's network from a vulnerability in an outdated software application. 3,000 guest names, emails and credit card information were compromised.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

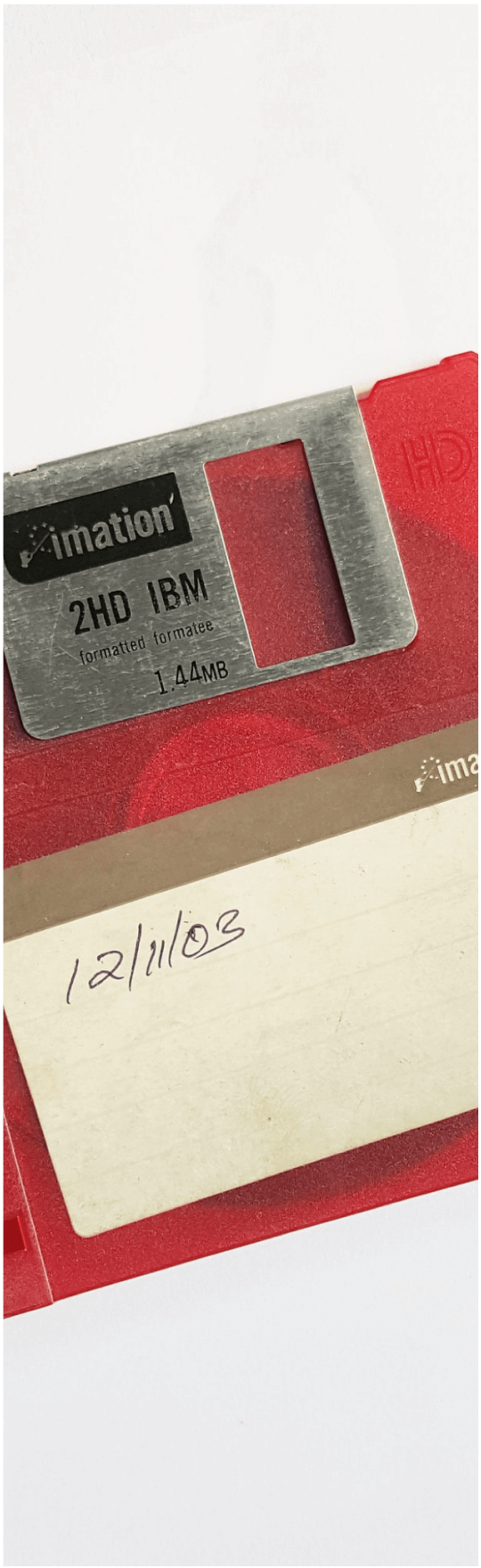
INCIDENT RESPONSE	
Forensic investigation costs to isolate vulnerability, analyze damage, ensure containment and calculate loss	$10,250
Identity theft and credit monitoring services	$8,640
Incident response fees	$8,000
Public relations fees to minimize reputational impact	$9,800
Call center set up and operation to field inquiries	$9,000
NOTIFICATION COSTS	$1,450
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	$950
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	$1,700
DATA RECOVERY Costs associated with replacing lost or corrupted data	$12,500
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.