CLAIM SCENARIO

RANSOMWARE | Wholesale Trade

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 beverage distributor 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 $17,500 paid in Bitcoin within 24 hours to release their data files.

575 customer records including company name, address, phone and bank details were encrypted. The distributor called their insurance company's cyber response team, who responded by assigning a "breach coach," which is covered as part of the distributor'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	$18,775
Forensic investigation costs to locate malware, analyze damage, ensure containment and calculate loss	$22,500
Legal fees	$34,100
NOTIFICATION COSTS	$2,225
BUSINESS INTERRUPTION	$278,552
DATA RECOVERY Costs associated with replacing lost or corrupted data	$31,235
EXTORTION/RANSOMWARE Ransom payment	$104,000
BRICKING Damage to computer and hardware systems	$39,900
TOTAL POTENTIAL CLAIM	$531,287

RESOLUTION

While the business maintained regular back-ups online, the hackers also encrypted these files leaving the distributor 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 distributor.

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

CLAIM SCENARIO

OUTDATED SOFTWARE | Wholesale Trade

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Hackers penetrated an art supply wholesaler's network from a vulnerability in an outdated software application. 355 company names, emails, credit card information and banking details were compromised.

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

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

POTENTIAL IMPACT

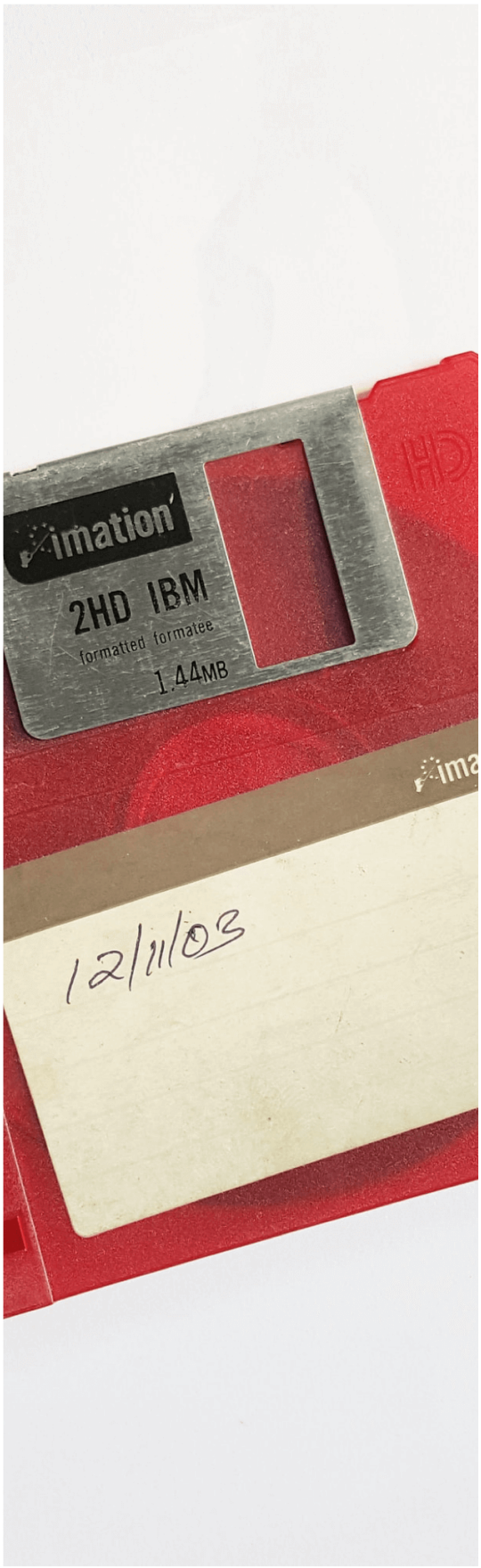
INCIDENT RESPONSE	
Forensic investigation costs to isolate vulnerability, analyze damage, ensure containment and calculate loss	$6,000
Identity theft and credit monitoring services	$1,278
Incident response fees	$5,000
Public relations fees to minimize reputational impact	$6,000
Call center set up and operation to field inquiries	$5,000
NOTIFICATION COSTS	$575
DATA RECOVERY Costs associated with replacing lost or corrupted data	$6,500
REGULATORY	
Legal expenses arising from regulatory investigation due to mismanagement of private information	$7,100
Legal expenses and settlement costs for claims	$4,960
Business interruption	$7,872
TOTAL POTENTIAL CLAIM	$50,285

RESOLUTION

The wholesaler'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 wholesaler had up-to-date cyber defenses including firewalls, intrusion detection software, and encrypted databases.

Concurrently, officials worked with local media to notify affected customers 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 | Wholesale Trade

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 food products distributor'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 distributor discovered that unauthorized payments were made totaling $340,688, they immediately contacted their bank to freeze the funds and notified their cyber insurance carrier. Together, they were able to recover $310,000 of the unauthorized transactions.

POTENTIAL IMPACT

INCIDENT RESPONSE	
Forensic investigation costs to locate the breach, analyze damage, and ensure containment	$8,730
Legal fees	$6,025
FUNDS TRANSFER FRAUD Transferred funds not recovered	$30,688
TOTAL POTENTIAL CLAIM	$45,443

RESOLUTION

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

As the distributor 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 | Wholesale Trade

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 geothermal heating/cooling distributor lost their laptop. An Excel file on the computer contained company records of 920 customers including the company names, emails, credit card information and banking details.

Once the loss was realized, the distributor 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	$7,375
Legal fees	$11,000
Public relations fees to minimize reputational impact	$8,000
NOTIFICATION COSTS	$900
DATA RECOVERY Costs associated with replacing lost or corrupted data	$8,800
REGULATORY Settlement fine	$17,968
Patient liability settlements	$33,607
TOTAL POTENTIAL CLAIM	$87,650

RESOLUTION

The breach coach assigned a forensics team, provided by the insurance company, to determine the potential exposure of the customer information. It was determined that the customer records were, in fact, compromised. The customers 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 customers.

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 | Wholesale Trade

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 appliance distributor was hacked by a former employee, whose user credentials were not deleted when they were terminated. The employee sold 2,050 customer records on the dark web including company names, emails, credit card information and banking details.

The distributor 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 distributor in managing their actual and reputational damage.

POTENTIAL IMPACT

INCIDENT RESPONSE	
Forensic investigation costs to analyze damage and ensure containment	$9,200
Identity theft and credit monitoring services	$5,904
Legal fees	$12,720
Public relations fees to minimize reputational impact	$9,430
Call center set up and operation to field inquiries	$7,200
NOTIFICATION COSTS	$1,450
DATA RECOVERY Costs associated with replacing lost or corrupted data	$9,600
TOTAL POTENTIAL CLAIM	$55,504

RESOLUTION

The forensic team quickly identified the breach and worked with the distributor's IT department to initiate repairs. The breach coach guided the distributor to hire a call center to quickly inform affected customers, 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 distributor, 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 distributor were minimized.