CLAIM SCENARIO

RANSOMWARE | Manufacturing

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 textile manufacturer 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 $47,700 paid in Bitcoin within 48 hours to release their data files.

3,100 customer records including company name, address, credit card details and banking information were encrypted. The manufacturer called their insurance company's cyber response team, who responded by assigning a "breach coach," which is covered as part of the manufacturer'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	$18,460
Forensic investigation costs to locate malware, analyze damage, ensure containment and calculate loss	$25,090
Legal fees	$25,240
NOTIFICATION COSTS	$3,620
BUSINESS INTERRUPTION	$423,884
DATA RECOVERY Costs associated with replacing lost or corrupted data	$30,075
EXTORTION/RANSOMWARE Ransom payment	$150,000
BRICKING Damage to computer and hardware systems	$28,800
TOTAL POTENTIAL CLAIM	$705,169

RESOLUTION

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

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

CLAIM SCENARIO

OUTDATED SOFTWARE | Manufacturing

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Hackers penetrated a candle manufacturer's network from a vulnerability in an outdated software application. 800 company names, emails, credit card information and banking details were compromised.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

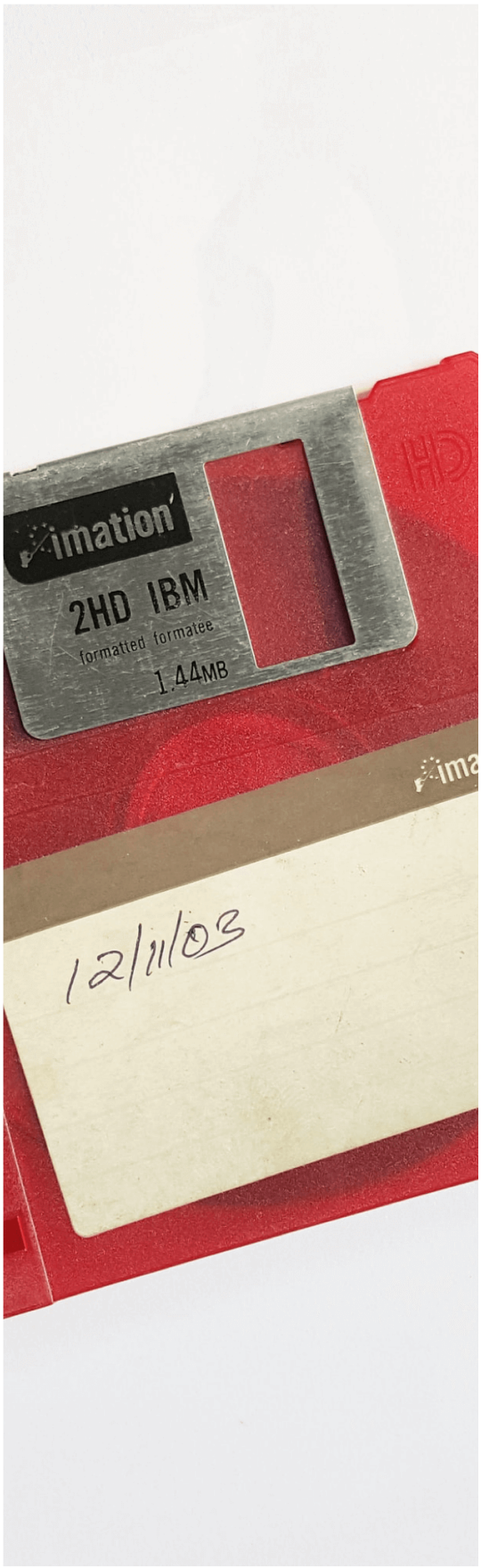
INCIDENT RESPONSE	
Forensic investigation costs to isolate vulnerability, analyze damage, ensure containment and calculate loss	$6,755
Identity theft and credit monitoring services	$2,900
Incident response fees	$6,350
Public relations fees to minimize reputational impact	$6,000
Call center set up and operation to field inquiries	$5,500
NOTIFICATION COSTS	$825
DATA RECOVERY Costs associated with replacing lost or corrupted data	$7,925
REGULATORY	
Legal expenses arising from regulatory investigation due to mismanagement of private information	$11,300
Legal expenses and settlement costs for claims	$8,200
Business interruption	$19,982
TOTAL POTENTIAL CLAIM	$75,757

RESOLUTION

The manufacturer'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 manufacturer 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 | Manufacturing

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 engine parts manufacturer'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 manufacturer discovered that unauthorized payments were made totaling $960,000, they immediately contacted their bank to freeze the funds and notified their cyber insurance carrier. Together, they were able to recover $833,000 of the unauthorized transactions.

POTENTIAL IMPACT

INCIDENT RESPONSE	
Forensic investigation costs to locate the breach, analyze damage, and ensure containment	$12,200
Legal fees	$10,050
FUNDS TRANSFER FRAUD Transferred funds not recovered	$127,000
TOTAL POTENTIAL CLAIM	$149,250

RESOLUTION

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

As the manufacturer 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 | Manufacturing

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 luggage manufacturer lost their laptop. An Excel file on the computer contained company records of 2,500 customers including the company names, emails, credit card information and banking details.

Once the loss was realized, the manufacturer 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	$9,750
Legal fees	$15,080
Public relations fees to minimize reputational impact	$12,220
NOTIFICATION COSTS	$1,370
DATA RECOVERY Costs associated with replacing lost or corrupted data	$11,750
REGULATORY Settlement fine	$20,075
Patient liability settlements	$42,900
TOTAL POTENTIAL CLAIM	$113,145

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 | Manufacturing

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 furnace manufacturer was hacked by a former employee, whose user credentials were not deleted when they were terminated. The employee sold 1,600 customer records on the dark web including company names, emails, credit card information and banking details.

The manufacturer 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 manufacturer in managing their actual and reputational damage.

POTENTIAL IMPACT

INCIDENT RESPONSE	
Forensic investigation costs to analyze damage and ensure containment	$8,500
Identity theft and credit monitoring services	$5,760
Legal fees	$11,000
Public relations fees to minimize reputational impact	$8,900
Call center set up and operation to field inquiries	$6,750
NOTIFICATION COSTS	$1,250
DATA RECOVERY Costs associated with replacing lost or corrupted data	$8,900
TOTAL POTENTIAL CLAIM	$51,060

RESOLUTION

The forensic team quickly identified the breach and worked with the manufacturer's IT department to initiate repairs. The breach coach guided the manufacturer 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 manufacturer, 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 manufacturer were minimized.