CLAIM SCENARIO

RANSOMWARE | Construction

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 commercial construction company 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 $24,000 paid in Bitcoin within 48 hours to release their data files.

750 customer records including company name, address and banking information were encrypted. The company called their insurance company's cyber response team, who responded by assigning a "breach coach," which is covered as part of the company'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	$3,500
Forensic investigation costs to locate malware, analyze damage, ensure containment and calculate loss	$5,400
Legal fees	$4,250
NOTIFICATION COSTS	$850
BUSINESS INTERRUPTION	$13,656
DATA RECOVERY Costs associated with replacing lost or corrupted data	$4,403
EXTORTION/RANSOMWARE Ransom payment	$24,000
BRICKING Damage to computer and hardware systems	$5,750
TOTAL POTENTIAL CLAIM	$61,809

RESOLUTION

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

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

CLAIM SCENARIO

OUTDATED SOFTWARE | Construction

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Hackers penetrated a residential construction company's network from a vulnerability in an outdated software application. 750 name, address, phone and credit card information were compromised.

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

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

POTENTIAL IMPACT

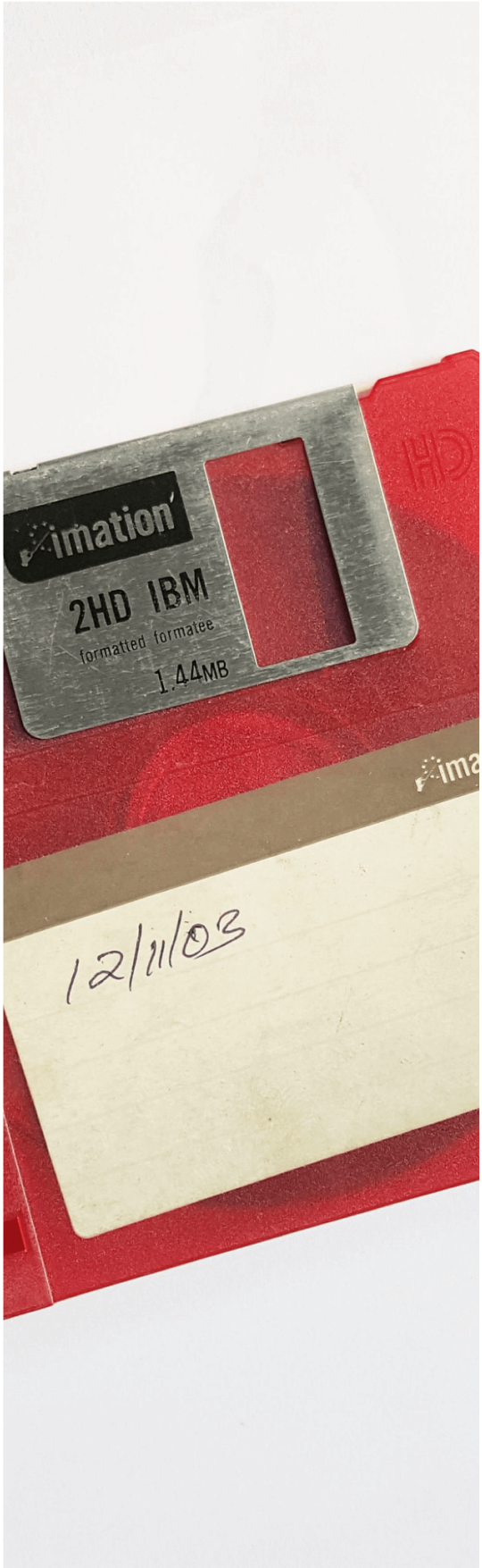
INCIDENT RESPONSE	
Forensic investigation costs to isolate vulnerability, analyze damage, ensure containment and calculate loss	$24,470
Identity theft and credit monitoring services	$13,860
Incident response fees	$16,050
Public relations fees to minimize reputational impact	$18,500
Call center set up and operation to field inquiries	$15,400
NOTIFICATION COSTS	$1,800
DATA RECOVERY Costs associated with replacing lost or corrupted data	$22,850
REGULATORY	
Legal expenses arising from regulatory investigation due to mismanagement of private information	$54,700
Legal expenses and settlement costs for claims	$193,080
Business interruption	$210,815
TOTAL POTENTIAL CLAIM	$571,525

RESOLUTION

The construction company'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 construction company 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 | Construction

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 slate installation contractor'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 contractor discovered that unauthorized payments were made totaling $270,000, they immediately contacted their bank to freeze the funds and notified their cyber insurance carrier. Together, they were able to recover $238,600 of the unauthorized transactions.

POTENTIAL IMPACT

INCIDENT RESPONSE	
Forensic investigation costs to locate the breach, analyze damage, and ensure containment	$8,625
Legal fees	$6,570
FUNDS TRANSFER FRAUD Transferred funds not recovered	$31,400
TOTAL POTENTIAL CLAIM	$46,595

RESOLUTION

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

As the contractor 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 | Construction

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 crane rental company lost their laptop. An Excel file on the computer contained company records of 1,400 customers including the company names, employee names, emails, credit card information and banking details .

Once the loss was realized, the company 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	$7,900
Legal fees	$12,740
Public relations fees to minimize reputational impact	$10,000
NOTIFICATION COSTS	$1,200
DATA RECOVERY Costs associated with replacing lost or corrupted data	$9,460
REGULATORY Settlement fine	$18,075
Patient liability settlements	$31,060
TOTAL POTENTIAL CLAIM	$90,435

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 | Construction

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 flooring contracting company was hacked by a former employee, whose user credentials were not deleted when they were terminated. The employee sold 1,950 customer records on the dark web including company names, emails, credit card information and banking details.

The company 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 company 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	$5,616
Legal fees	$12,600
Public relations fees to minimize reputational impact	$9,350
Call center set up and operation to field inquiries	$7,100
NOTIFICATION COSTS	$1,380
DATA RECOVERY Costs associated with replacing lost or corrupted data	$9,520
TOTAL POTENTIAL CLAIM	$54,766

RESOLUTION

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