ERIE® Business Products

Cyber Suite Claims Scenarios

Note: this document is intended for informational purposes only and does not modify or invalidate any of the provisions, exclusions, terms or conditions of the policy and endorsements.

The examples may have multiple coverage exposures and implications; note that a deductible applies to the total costs.

Contractor Scenarios

1. An attacker caused significant damage, infecting the system with malware and erasing all information at an **electrical contractor**. Though cyber security was installed, a hacker was able to access a remote server, log in and set up as a system administrator. Once in control, the intruder turned off the antivirus and anti-malware programs, stopped all backups, installed ransomware and removed hard drive partitions, effectively erasing all information on the system. Evidence showed the attacker had been there for months. The contractor did not pay the thief but did pay the breach notifications that went out to all the individuals whose data was exposed. The company also paid for credit monitoring services for affected employees, as well as forensic IT services, system and data restoration and remediation. Downtime to restore systems and data cost the company further potential income.
   Total Cost: $32,750 under Computer Attack (for System Restoration and Data Restoration) + Data Breach Response Expenses (for Forensic IT Review, Notification to Affected Individuals and Services to Affected Individuals/credit monitoring services). Ransom not paid.

2. A phishing scheme delivered a ransomware virus to a **drywall contractor**, damaging systems and stalling business. A drywall contractor fell prey to phishing, a common scheme using emails that appear to be from a trusted sender to trick the user into clicking on a virus-carrying link or disclosing confidential information. The owner unwittingly gave cyber thieves access to the business's systems. The attackers installed ransomware, which infected systems and held data hostage, and demanded payment from the company. The contractor did not pay the ransom but did pay a sizeable amount to restore operations. The damaged customer database had to be rekeyed from paper files. A server and computer had to be rebuilt. Business was down for a week while damage was remediated, causing the contractor to lose a contract and other business income.
   Total Cost: $15,000 under Computer Attack (for System Restoration and Loss of Business). Ransom not paid.

3. An HR employee's email account, containing sensitive employee and client data, was breached. An unknown third party used a phishing email scheme to deceive an HR employee for a small commercial **landscaper**. The tactic—which fooled the employee into thinking the email was from a legitimate source—allowed outsiders to gain the employee's email log-in credentials. For several days, attackers

accessed the email account along with all the information stored there. This included personal data for all employees and sensitive materials for some customers. The commercial landscaper notified all affected individuals regarding the data breach and offered services to address potential fraud. The landscaper faced the threat of litigation, which caused the business to incur legal expenses. Also, the breach damaged the landscaper's image, harming the trust of both employees and customers.
Total Cost: $11,150 under Data Breach Response Expenses (for Legal Review, Notification to Affected Individuals, Services to Affected Individuals and Reputational Harm) + Privacy Incident Liability (for defense)

Landlord/Property Management/Real Estate Scenarios

1. An **apartment building's management company** had to scramble when the webhost company that processed their rental applications suffered a cyber attack. By contacting their cyber insurance carrier, they discovered that the cyber criminal stole applicants' personally identifying information and sent emails to them demanding $100 in exchange for deleting their information. The apartment building's management company's claims adjuster introduced the insured to legal counsel, who determined that there was a data breach and helped them quickly recover from it. The insured's cyber policy covered the cost of legal counsel, notification to affected individuals and regulators and credit monitoring as well as identity recovery case management.
   Total Cost: $47,121 under Data Breach Response Expenses (for Legal Review: $3,984, Notification to Affected Individuals: $40,892 and Services to Affected Individuals/credit monitoring & case management: $2,245)

2. Data thieves hacked into the database of an **apartment leasing company**. The company's database contained personal information on about 100 tenants and another 275 applicants. Information included Social Security numbers, employment and credit information.
   Total Cost: $17,850 under Data Breach Response Expenses (for Legal Review, IT Forensic Review and Notification to Affected Individuals)

3. The **real estate** business received a ransomware email demanding payment to gain access to the company's files. The manager called her external IT vendor they confirmed it was a ransomware variant and that the system had been locked. The insured got approval from Claims to pay the ransom, in bitcoin, about $8,700. The attacker provided 5 different decryption keys and the IT vendor decrypted the system successfully getting the insured back online. The ransomware also took the system down and system restoration had to be performed. Coverage provided for the costs associated with the cyber extortion expense and system restoration expenses.
   Total Cost: $14,258 under Cyber Extortion (for extortion payment: $8,000) + Computer Attack (for System Restoration: $6,258)

4. At a **rental property** office, a box of rental applications with the name, address and Social Security numbers of 2,600 individuals was stolen from an apartment building office.

Total Cost: $91,000 under Data Breach Response Expenses (for Notification to Affected Individuals and Services to Affected Individuals)

Manufacturing Scenarios

1. The **metal manufacturing facility**'s computer systems were attacked by ransomware that gained access to the system through a phishing email. The ransomware encrypted the data filed and demanded a ransom of 60 Bitcoin ($240K) for decryption. The insured did not pay the ransom. Four months of data had to be recreated by temporary employees. A total of 10 virtual servers, 5 physical servers and 50 workstations were affected.
   Total Cost: $47,139 under Computer Attack (for Data Restoration, System Restoration and Loss of Business)

2. A hacker gained access to the **manufacturing office** insured's computer system via a desktop and got administrative privileges in order to encrypt the insured's data. Proprietary data was lost. IT forensics showed the event occurred in less than two hours. The hacker was able to delete the external back up associated with the server. The entire facility was taken offline while a remote scan was performed. Affected machines had their hardware replaced and backups were restored from a remote site and data had to be recreated.
   Total Cost: $41,938 under Computer Attack (for Data Re-Creation and Loss of Business due to the computer attack)

3. A ransomware attack at a **machine parts and components manufacturer** seized the manufacturer's system and a payment was demanded for release. Employees and vendors are the biggest cyber security weakness for small and mid-sized businesses. In this case, no remote access was detected so it is believed that an employee inadvertently downloaded the ransomware virus while browsing the web. Their lack of security awareness and unsafe online habits opened the door to a ransom demand. The attack brought the manufacturer's system and operations down, halting production. No ransom was paid, but the attack was still costly. An IT provider had to rebuild two servers and five workstations from scratch, which included reloading the operating system and reinstalling all software and other functions.
   Total Cost: $22,000 under Computer Attack (for Data Restoration, Data Re-Creation, System Restoration and Loss of Business). Ransom not paid.

4. The owner of a **wine and oak barrel manufacturer** was having computer issues and hired an external IT consultant to assist. One morning, the insured noticed the computer was glitching, so he attempted to reboot the computer. When the computer restarted, a ransomware message showed up the screen. The insured called the IT consultant, and the ransomware was identified. The IT consultant was able to determine that the server was impacted and advised the insured to shut down all company workstations, including warehouse, office and remote employees. After an investigation, it was determined that only the servers had been impacted and the workstations were not. The insured was referred to a notification legal expert to determine if the insured needed to notify any affected

individuals. Through the claims process, they were also able to work with an IT service provider to get the decryption key for the insured.
Total Cost: $9,197 under Computer Attack (for System Restoration: $405) + Cyber Extortion (for negotiator/investigator: $2,710 and extortion payment: $3,000) + Data Breach Response Expenses (for Legal Review: $3,082)

5. The insured, a **manufacturer**, discovered that their main server was encrypted with ransomware. The insured identified that no other workstations or servers, other than the main server C-Drive, had been affected. The C-Drive stored the insured's applications which ran to operate the business. The insured was unsure how the ransomware got onto the drive, but it was believed that someone clicked on a malicious pop up. There was no personal information stored on the affected server and the backup files were encrypted. The insured utilized the services of an approved vendor to assist the insured. The ransomware was successfully paid, and the decryption tool was able to decrypt the data. The computer attack was discovered during the policy period and was reported within 60 days of discovery.
Total Cost: $8,810 under Cyber Extortion (for extortion payment: $5,000 + negotiator/investigator: $3,810)

6. The insured, a **manufacturer,** discovered that his internet service was not working over a weekend and called his IT firm. He discovered a few days later that all his systems were encrypted and received a ransom note. The insured immediately determined they would not pay the ransom. The first attack was on the off-site backups. The insured only had a backup from QuickBooks on his desktop, where personally identifying information for their employees (SSNs, etc.) was stored and password protected. Once claims reviewed the situation, it was determined that the ransom would not be paid; however, breach counsel was engaged, and 154 notifications were sent to affected individuals.
Total Cost: $22,965 under Data Breach Response Expenses (for Legal Review: $10,679 and Notification to Affected Individuals: $797) + Computer Attack (for System Restoration: $5,295 and Data Recreation: $1,244) + Cyber Extortion (for negotiator/investigator: $4,950)
7. A cyber criminal used stolen credentials to infiltrate a **machine shop**'s server and encrypted files with a ransomware virus. A ransom demand of $50,000 in Bitcoin was made. The business owner was introduced to a ransomware specialist and an attorney specializing in cyber and privacy incidents. The insured's team negotiated the ransom down by half, and successfully obtained the decryption keys. A digital forensics investigator and systems remediation team investigated and determined that no data breach had occurred. The system was restored to full functioning, but the business suffered a business interruption.
Total Cost: $183,500 under Computer Attack (for Data Restoration, System Restoration and Loss of Business) + Data Breach Response Expenses (for Legal Review and Forensic IT Review) + Cyber Extortion (for extortion payment/negotiator but ransom not paid)

Restaurant Scenarios

1. The insured was informed by his **restaurant** manager that their POS computer system went down. They contacted the IT provider, who confirmed the POS software system had been infected with ransomware, pushing ransomware down to many customers' local system, including the insured's. The

insured has an office server used to store the POS information, and several terminals; however they use an independent company to take the credit card payments. The insured's POS provider was infected with the ransomware, resulting in local encryption. The insured restored their system and opted for new hardware. HSB provided coverage for the expenses incurred for the system restoration and loss of business income**.**
Total Cost: $38,106 under for Computer Attack (for System Restoration: $13,106 and Loss of Business: $25,000)

2. While reviewing the most recent bank statement, the bookkeeper for a **restaurant** with four locations noticed an unusual payment to a vendor she did not recognize. The bank confirmed that the payment was made and was unable to recover the funds. After reviewing emails, the insured was able to identify a phishing email that led another employee to reveal bank account information, which the cyber criminal used to initiate the fraudulent funds transfer.
Total Cost: $43,200 under Misdirected Payment Fraud (for direct financial loss/reimbursement for fraudulent funds transfer)

3. The **restaurant** fell victim to a targeted email phishing scam, resulting in the misdirection of funds. The insured received several emails that appeared to be from customers, requesting a change in banking information. Believing the requests were legitimate, the insured changed the bank information, and transferred money to unauthorized accounts. The incident occurred within the accounts payable department of the corporate office and affected six locations. A statement from the insured's IT provider, confirmed that there was no unauthorized access to the insured's system.
4. **Total Cost: $28,329 under Misdirected Payment Fraud (for direct financial loss of wrongful transfer costs)**

5. The **restaurant** chain's server, backup server and 20 workstations were encrypted from a ransom attack. The insured contacted their IT provider to assist in ransom negotiations. The insured paid the ransom in exchange for decryption keys. The insured's IT provider was assisting with both data and system restoration efforts. The Cyber Suite endorsement provided coverage for the expenses incurred for the ransom, data and system restoration.
Total Cost: $42,973 under Cyber Extortion (for the extortion payment: $20,417) + Computer Attack (for System Restoration: $3,299 and Loss of Business: $19,257)

Retail Scenarios

1. Identity thieves used card skimmers at a **gas station** to steal bank account numbers with PIN codes from 550 customers. The thieves then created false debit cards, using the stolen information at ATMs to drain funds from client accounts.
Total Cost: $19,250 under Data Breach Response Expenses (for Notification to Affected Individuals and Services to Affected Individuals)

2. When ransomware infected servers at a chain of **gas stations and convenience stores**, over 200 devices at 16 locations were impacted. However, because the insured's IT Director had read the cyber insurance company's advisories on what to do if his system was infected by ransomware, he knew what to do. Rather than pay the ransom demand of $250,000, he opted to wipe the devices, reinstall software and restore data from recent backups. Because the insured had backups that were not affected by the infection, his business was only interrupted for a short time. The insured paid the following costs and was reimbursed by cyber policy, less its deductible.
   Total Cost: $89,924 under Data Breach Response Expenses (for Legal Review: $14,926 and Forensic IT Review: $25,000) + Computer Attack (for System Restoration: $19,178, Data Restoration: $30,307 and Loss of Business: $513)

3. A keylogger originating from the **retaile**r's host captured customer credit card data. An online equipment retailer's server was breached by a keylogger, which captures information typed into the computer. This occurred three times over the course of several months and, with each new breach, customers' credit card numbers were captured. The retailer's server was also corrupted each time and needed to be fully replaced. Finally, IT forensics found the keylogger originated from the retailer's hosting provider but by then 16,000 credit cards had been exposed. Three separate notifications were sent to affected individuals, one for each breach. In total, 315,500 people and 31 attorney generals had to be alerted, all at the retailer's expense. The retailer also paid a high price to restore its data and systems and suffered greatly from loss of business and a damaged reputation.
   Total Cost: $207,500 under Computer Attack (System Restoration, Data Restoration and Loss of Business) + Data Breach Response Expenses (for Forensic IT Review, Notification to Affected Individuals and Reputational Harm)

4. A **retailer**'s eCommerce provider suffered a security breach, exposing thousands of credit cards. When an eCommerce vendor experienced a data breach, all its clients, including this online equipment retailer and the retailer's clients, were put at risk. Thousands of credit card numbers were exposed and, while the eCommerce provider was at fault, the breach of customer data—and trust—negatively impacted the retailer's business. Fortunately, the retailer's contract with the eCommerce provider included data breach response. So, the costs to notify affected individuals and provide services to address potential fraud were paid by the eCommerce provider. Without this contract provision, the retailer would have been stuck with these expenses. Still, the retailer reviewed its potential legal obligations for which it incurred legal expenses.
   Total Cost: $5,000 under Data Breach Response Expenses (for Legal Review)

5. The employee of a **retailer** received an email appearing to come from her company's owner, asking for employee information. She replied asking why he needed it but gave him the information. Later in the day, the insured felt that something wasn't right, so she reached out to the owner and asked if he emailed her, and he responded in the negative. She had provided information to an unknown third party that may have included the Personally Identifiable Information of the insured's 150 employees.
   Total Costs: $6,020 under Data Breach Response Expenses (for Legal Review: $4,774, Notification to Affected Individuals $286, and Services to Affected Individuals: $960)

6. A **retailer**'s bank notified the insured after discovering fraudulent credit card transactions on their website. The Insured investigated and found that their website had been affected. The insured's bank could not assist in the notification of the affected individuals, but the this insured carried Cyber Suite insurance; breach counsel was offered to the insured and those expenses as well as the notification to the affected individuals was covered under this endorsement.
   Total Costs: $17,251 under Data Breach Response Expenses (for Legal Review: $5,000, Notification to Affected Individuals: $11,234 and Services to Affected Individuals/credit monitoring & case management: $1,017)

7. The insured **furniture store** had a trojan downloaded to one of their workstations which then infected the server. The insured immediately contacted their IT company to mitigate the issue. The infected machine was wiped clean, and the IT firm restored the server from their backup. The only loss incurred was for their IT company to assist with the remediation and recovery of the network from backups.
   Total Cost: $5,650 under Computer Attack (for System Restoration)
8. A **retailer** experienced a data breach, which exposed all their customers' credit card numbers. Upon review by a Payment Card Industry (PCI) forensic investigator, it was determined that the retailer was not compliant with PCI security standards. As a result, the credit card company levied fines and penalties against the retailer for noncompliance and required that they pay for a PCI investigation. Coverage was provided for the fines and penalties as well as the PCI assessment.
   Total Costs $44,541 under Data Breach Response Expenses (including PCI Assessments, Fines and Penalties)

9. A small online **retailer** had their privacy policy listed on their website. Even though the small business never had a security incident or data breach, one of their savvy customers who was also a lawyer sued the retailer claiming that their treatment of his personal information violated the retailer's own privacy policy.
   Total Cost: $32,360 under Privacy Incident Liability (for defense and settlement, after deductible)

10. A ring of methamphetamine addicts was scavenging through specific dumpsters located outside of a **retail store** for credit card information, transaction and account statements. None of the information was shredded. The identity theft ring included a computer security technician and an internet service provider (ISP) employee. When discovered, the insured was responsible for giving notification to potential affected individuals.
    Total Cost: $11,230 under Data Breach Response Expenses (for Legal Review and Notification to Affected Individuals)

Services And Other Miscellaneous Business Scenarios

1. A burglar broke into an **accountant**'s office and stole a computer with the tax records of clients. The insured's clients were in four states and he needed assistance meeting the various state law

notification requirements. Clients were urged to contact their banks and place alerts on their credit files.

Total Cost: $28,000 under Data Breach Response Expenses (for Notification to Affected Individuals and Services to Affected Individuals)

2. When a burglar broke into an **accountant**'s office and stole a computer with client tax records, after consulting with the insurance company, the accountant offered a reward for assisting in finding the burglar. A few weeks later, the burglar boasted about the score in a public forum and a third party reported the heist to police. The report led to the arrest and conviction of the perpetrator and coverage reimbursed the accountant for the reward payment he had offered to bring the criminal to justice.

   Additional Cost: $15,000 under Data Response Expenses' Reward Payments, having a separate <u>per policy period</u> sublimit)

3. Ransomware infected 25 computers and business servers of a, **ag produce shipper**. Attackers exploited a common Windows web utility to upload ransom malware and gain remote control of a single computer within the business. The infection then spread to 25 computers as well as the business's servers, crashing systems and bringing production to a halt. Once in control, the brazen attackers stepped up the ransom threats culminating in calling one of the owners directly. The owners refused to pay, and normal business operations ceased for nine days while systems were restored. The business paid multiple IT vendor specialists to recover or re-create data and restore systems so they could return to normal operations. Owners also paid to expedite delivery of replacement computer hardware that could not be fixed.
   Total Cost: $62,000 under Computer Attack (for Data Restoration, Data Re-Creation, System Restoration, and Loss of Business)

4. The **amusement park**'s computer systems were infected by ransomware. The criminals left a ransom note requesting the insured to click on a link to solicit the ransom demand. The insured reported that no personally identifying information was stored on the infected computer systems. The insured engaged an outside professional IT firm to assist in restoring the computer systems. The insured was unable to conduct business for 8 days and incurred lost income. The systems were restored. Cyber Suite assisted in system restoration, loss of income and ransom payment costs.
   Total Costs: $61,237 under Cyber Extortion (for extortion payment: $10,000) + Computer Attack (for Loss of Business: $49,850 and System Restoration: $1,387)

5. At an **auto dealership**, an unknown actor stole approximately 20 deal jackets containing the Personal Identifying Information of customers from a dealership. The insured provided breach notifications and credit monitoring services to affected individuals. Two customers subsequently made legal demands as a result of this breach.

   Total Cost: $20,013 under Data Breach Response Expenses (for Notification to Affected Individuals and Services to Affected Individuals) + Privacy Incident Liability (for legal defense and settlement costs)

6. An **auto repair shop** received a few emails with new payment instructions that appeared to come from one of their vendors. The emails appeared to come directly from the vendor, so the insured was not suspicious. The insured transferred $10,000 according to the new instructions but it was later determined that the vendor's email had been compromised and criminals had been sending the fraudulent emails. The insured attempted to recover the money on their own but could not, so reported it to their insurance carrier as the insured carried Cyber Suite coverage. The incident was also reported to the police.

   Total Cost: $9,500 under Misdirected Payment Fraud (for direct financial loss/wrongful transfer costs)

7. One member of a group of **dry cleaners** was completely shut down by a ransomware attack. The cyber criminals demanded $150,000 to decrypt the system. Following negotiation and evaluation of the decryption keys, the ransomware specialist determined that the decryption keys provided by the cyber criminals would not be effective in unlocking the encrypted files. The insured was able to move its operations to a partner organization, where it manually restored its files and was able to avoid an extended business interruption. Legal counsel, in consultation with IT forensics examiners and the ransomware expert, were able to determine that no data was stolen, and no data breach occurred.
   Total Cost: $96,700 under Computer Attack (for System Restoration) + Cyber Extortion (for extortion payment) + Data Breach Response Expenses (for Legal Review and Forensic IT Review)

8. All 27 employees in a **financial consulting firm** received a phishing email. Unfortunately, one of them clicked on the malicious link and entered her login credentials, allowing the cyber criminal to take over her email account and access personally identifying and confidential information of several of the firm's clients. When the insured called their cyber insurance carrier, their claims adjuster introduced the insured to a digital forensics firm that determined what happened and legal counsel who advised them to notify and arrange for credit monitoring and case management services for the affected individuals. The insured paid the following expenses to manage the incident and help the individuals whose information had been breached. Their Cyber Suite covered $50,000 and the insured ended up paying an additional $12,000.
   Total Cost: $50,000 under Data Breach Response Expenses (for Legal Review $19,188, Forensic IT Review: $19,285, Notification to Affected Individuals: $7,694 and Services to Affected Individuals/credit monitoring: $3,833)

9. An employee of a **financial investment firm** installed peer-to-peer file sharing software on a company computer. Identity thieves manipulated the software to access the records of clients on the computer system. After consultation with an attorney, the insured learned that he was obligated to notify the clients of the breach. Additionally, it was determined that the insured would need to hire an outside firm to help restore the computer system to its pre-attack functionality.
   Total Cost: $50,000 under Data Breach Response Expenses (for Notification to Affected Individuals and Services to Affected Individuals) + Computer Attack (for System Restoration)

10. The **financial savings and loan institution** insured discovered that one of their employee's email account had been hacked and that emails and funds were being forwarded to an unknown account. The funds were recovered but the information of 292 individuals in multiple states was compromised. The insured utilized a notification vendor, a public relations firm and forensic IT services.
    Total Cost: $46,335 under Data Breach Response Expenses (for Forensic IT Review, Notification to Affected Individuals, Services to Affected Individuals, Public Relations and Regulatory Fines and Penalties)

11. A successful phishing attack at a **hotel chain** released malware into the insured's system. A malicious actor also telephonically procured verification codes from one of the insured's employee to access their online bank account through social engineering. This resulted in thousands fraudulently transferred to various accounts. The malware interfered with access to the insured's accounts while multiple banks wires were completed. An IT service provider turned on malware protection services and wiped the system clean.
    Total Cost: $19,180 under Computer Attack (for System Restoration) + Misdirected Payment Fraud (for reimbursement of direct financial loss)

12. A **medical office** of a dentist used a managed service provider (MSP) to handle its information technology. When the MSP suffered a ransomware attack, the dental office was not able to access any of its data—it couldn't schedule patients, confirm appointments, conduct billing or file insurance claims. The office was forced to shut down operations until the ransomware was remediated, and the MSP's system restored. The insured filed a claim and was introduced to legal counsel and a digital forensics investigator to determine if any patient or employee personal or health information was compromised, which requires notification to affected individuals and, often, government regulators. The investigation determined that patient data was stolen, which necessitated notification to 235 affected individuals, the state's attorney general and federal regulators. The insured's policy covered that cost as well as engagement of credit monitoring services for the affected patients.
    Total Costs: $70,000 under Data Breach Response Expenses (for Forensic IT Review, Legal Review, Notification to Affected Individuals and Services To Affected Individuals) + Computer Attack (for Systems Restoration and Loss of Business)

13. Three external back-up hard drives with private personal records for 300 patients were stolen from a locked **medical office** of physicians. Notifications were sent to affected individuals advising them to place a fraud alert with credit bureaus and to monitor their credit reports and other financial statements.
    Total Cost: $10,500 under Data Breach Response Expenses (for Notification to Affected Individuals and Services to Affected Individuals)

14. A laptop was stolen from the **medical office** of a primary care physician. The stolen computer contained information on 255 former and current patients, including their names, dates of birth, Social Security numbers, medical records, and payment information.
    Total Cost: $9,744 under Data Breach Response Expenses (for Forensic IT Review and Notification to Affected Individuals)

15. The **medical office** insured's systems were infected with ransomware that accessed the system through a compromised administrator password. The systems had to be restored over a 19-day period.
    Total Cost: $50,000 under Computer Attack (for System Restoration and Loss of Business)

16. A disgruntled employee used a card skimming device to steal bank account numbers with PIN codes from 550 clients at a **medical office**, a **veterinarian office**. The employee sold the stolen information to cyber criminals, who then created false debit cards, using the stolen information at ATMs to drain funds from client accounts.
    Total Cost: $19,300 under Data Breach Response Expenses (for Notification to Affected Individuals and Services to Affected Individuals)

17. The **professional services** insured unknowingly received a fraudulent payment invoice. The instructions to pay the invoice were followed, resulting in a misdirected payment fraud. The insured discussed the incident with their IT service provider and there was no breach of personally identifying or sensitive information. This incident occurred during the policy period and was reported within 60 days. This wrongful transfer event was covered.
    Total Cost: $7,508 under Misdirected Payment Fraud (for direct financial loss/wrongful transferred funds)

18. It began with a phishing email at this **professional's office**. A Cyber Suite insured's employee clicked on a linked in a phishing email that downloaded ransomware onto her machine. It quickly spread to other networked devices. No ransom was demanded, but the entire system was encrypted. The insured's Cyber Suite policy covered the cost to restore the system and data from backups.
    Total Cost: $5,600 under Computer Attack (for System Restoration: $2,900 and Data Restoration: $2,700)

19. The insured, a **professional technical services company**, reported an issue with their Microsoft Exchange server during the process of migrating from a physical Microsoft Exchange server to a cloud-based email server. After the migration, the insured was locked out of their system. The claim's investigation concluded that that the insured's system was infected with Ramsey ransomware. The insured paid the ransom and then continued with system restoration. The insured was not able to operate for about 3.5 weeks.
    Total Cost: $52,000 under Cyber Extortion (for extortion payment of: $10,000) + Computer Attack (for System Restoration: $42,000)

20. At a **professional office**, hackers exploited a Cyber Suite insured's inadequately secured Remote Desktop Protocol to launch a ransomware attack on its computer systems. The insured's server and eight workstations were all encrypted. The insured's Cyber Suite coverage provided for the cost of legal advice, the ransom payment and services of a ransom negotiator, a digital forensics and incident response firm to decrypt the systems, determine whether any personally identifying information was compromised and ensure that functions returned to normal, and the data was restored. The digital forensics investigation determined that there was no data compromise.

Total Cost: $16,972 under Cyber Extortion (for the extortion payment and negotiator/investigator: $9,288) + Data Breach Response Expenses (for Forensic IT Review and Legal Review: $7,684)

21. At a **religious institution**, a church treasurer was working one night when he discovered a "Readme" message that popped up on his laptop. He viewed the message, and this caused the files to encrypt. The insured was required to disconnect their VPN and computer system after they confirmed this information to their IT Consultant. The IT consultant discovered that the insured's computer system was hit with a virus. It was likely that the criminals could have been in their church's systems for days. They did not engage with the threat actor's ransom demand. The affected data was backed up into a cloud-based environment. The insured was able to restore most of their backup data but lost about a week of data. The restoration process lasted about a week. The insured engaged legal counsel and forensic IT firm. The insured suspected that the old files that were encrypted included some Personally Identifiable Information (PII). Cyber Suite provided reimbursement for the costs associated with restoring the insureds system, less the deductible.
    Total Cost: $8,308 under Computer Attack (for System Restoration). Ransom not paid.

22. The insured, a **religious organization,** was notified by the their 3rd party cloud provider that there was a breach of their systems. Breach counsel was engaged, and it was determined notifications would be required for some donors to the organization based on their location. The Cyber Suite endorsement provided for the costs associated with the legal review and notification to those affected individuals.
    Total Cost: $2,339 under Data Breach Response Expenses (for Legal Review: $1,380 and Notification to Affected Individuals: $1,559)

23. The **school** insured's systems were infected with ransomware. The system was infected by their IT consultant service who had failed to install a virus patch that allowed the ransomware into the network. They hired a service to remediate their system, restore backups, and reconfigure the network.
    Total Cost: $24,636 under Computer Attack (for Data Restoration and System Restoration)

24. Burglars used crowbars to break into a storage space leased by a Cyber Suite insured. The small private **school** used the space to store filing cabinets that held personal information of former students and payment information. The insured's Cyber Suite policy covered its cost to retain an attorney who helped determine the extent of the insured's responsibility to notify potentially affected individuals, notification costs and credit monitoring and related services for affected individuals.
    Total Cost: $2,518 under Data Breach Response Expenses (for Legal Review: $514, Notification to Affected Individuals: $1,472 and Services to Affected Individuals/credit monitoring & case management: $532)

25. The insured **seafood company** found that their system was infected with ransomware. They were down for 8 hours while IT services brought in a new server and restored the system and data from backups.

Total Cost: $19,938 under Computer Attack (for System Restoration, Data Restoration and Loss of Business)

26. A hacker gained access to one of the usernames and passwords to a website hosted by the **service provider insured** for one of their clients. Multiple files and databases were modified by the hacker. More than 600,000 patient records were compromised. The records all contained personally identifying information and personal health information. An outside IT firm assisted in the restoration of the data and computer systems as well as conducting a forensic analysis. An attorney was also hired to assist with the notification process.
    Total Cost: $100,000 under Data Breach Response Expenses (for Legal Review, Forensic IT Review and Notification to Affected Individuals) + Computer Attack (for Data Restoration and System Restoration)

27. Twelve computers crashed in conjunction with a ransomware attack at a **truck stop operation**. The ransomware was delivered by an email attachment that was opened. All files were encrypted, and $15,000 ransom was demanded to release their data. The main server and 14 desktops were impacted. Two months of data was permanently lost. The ransom was negotiated down with the help of a negotiator and paid.
    Total Cost: $7,200 under Cyber Extortion ($4,200 for extortion payment and negotiator costs) + Computer Attack ($3,000 for Data Restoration)

Wholesaler/Distributor Scenarios

1. Through an automated process, ransomware was able to seize a **wholesaler**'s extensive computer system. After 2,000 automated log-in attempts, a remote brute force attack succeeded in guessing the company's login credentials, which allowed hackers to access and infect the wholesaler's system with ransomware. The attackers took control of six physical servers, 35 virtual servers and 90 workstations, demanding a ransom be paid for their release. The wholesaler refused to pay, and system backups the wholesaler had in place helped to lessen the blow. But given the size of the infrastructure, remediation efforts were extensive and costly. Lost business income added up as it took time to restore data and systems, and to re-create any data that couldn't be recovered.
    Total Cost: $79,100 under Computer Attack (for Data Restoration, Data Re-Creation, System Restoration, and Loss of Business)

2. A **wholesaler** insured's systems and applications started to malfunction. After contacting the IT service provider, the insured learned that their systems were infected with a malware, including an encryption virus which made the data inaccessible. The business was able to continue without using their systems. The attack was discovered during the policy period and was reported with 60 days of discovery.
    Total Cost: $4,609 under Computer Attack (for System Restoration: $4,131 and Data Restoration: $478)

Trucking Scenarios

1. A **transportation** contractor was hacked by a former employee, whose passwords had not been changed upon termination. The insured's computer system began to act erratically, crucial software programs were unavailable and large amounts of data appeared to have been deleted. An outside IT firm was hired to recover electronic data and input other records only available in paper form. In addition, the IT firm reinstalled software, re-configured the insured's servers and repaired other damage to the insured's computer system. The insured also had to replace various pieces of cargo tracking software that had been damaged or destroyed. Separately, the insured suffered a business income over the course of several days while systems issues were being addressed. The insured also hired a public relations firm to help it communicate with its customers about the incident.
   Total Cost: $33,850 under Computer Attack (for Data Restoration, Data Re-Creation, Systems Restoration, Loss of Business, and Public Relations expenses)

2. The insured, who was the owner of a **trucking company**, discovered that their files was encrypted with a Ransomware virus. They decided to pay the ransom to regain access to the encrypted files, however, the decryption key code contained backdoors and allowed remote attackers to enter the insured's systems. An IT Forensic expert was hired to research and determine how much damage was done. She found that an unknown third party had access to the insured's systems as well as access to all their employee and customer personal information. Notification was immediately provided to the affected individuals.
   Total Cost: $5,800 under Computer Attack (for Systems Restoration), Cyber Extortion (for the extortion payment/negotiator expenses) + Data Breach Response Expenses (for Legal Review, IT Forensic Review and Notification to Affected Individuals)

Generic (Any Business Type)

1. While trying to balance the books, **a business** owner received a strange pop-up on his laptop. A ransomware virus locked the system until the extortion demand was paid. After consulting with the insurance carrier, the insured decided to pay the $600 to unlock the system.

   Total Cost: $2,400 under Cyber Extortion (for extortion payment) + Computer Attack (for Systems Restoration)

2. A **small business** owner experienced a computer attack that corrupted data and caused the company's laptops to stop functioning properly. The insured hired a system restoration firm to remove the malware and reinstall software however the firm determined it would be more cost effective to simply replace the insured's three laptops. Coverage paid for the initial data and system restoration work, as well as the new laptops after it was determined that it would reduce the amount of the loss.

   Total Cost: $11,259 under Computer Attack (for Data Restoration, System Restoration which included new laptops to reduce amount of loss/bricking)

3. When a **Cyber Suite insured**'s computer system were infected with ransomware, they filed a claim. The insured's Cyber Suite coverage provided for the cost of a ransom negotiator, paid the ransom and covered the cost for a digital forensics incident response firm to decrypt the data and investigate whether any personally identifying information was compromised. The Insured's systems were infected with a ransomware virus.
   Total Cost: $7,765 under Cyber Extortion (for negotiator/investigator: $165 and extortion payment: $7,100) + Computer Attack (for Data Restoration: $500)

4. Hackers gained access to a **Cyber Suite insured**'s system and initiated a ransomware attack that encrypted their data across the entire network. The insured's Cyber Suite policy covered the cost of the ransom paid, approved in advance, decrypting the data and restoring the system to its prior level of functioning. An investigation by a digital forensics and incident response firm determined that no personally identifying information had been breached.
   Total Cost: $5,600 under Computer Attack (for System Restoration: $2,900 and Data Restoration: $2,700)

5. A **business** experienced a cyber-attack that involved compromise of its servers. After hacking into the system, criminals used the contacts from the business system to launch a ransomware attack against every email address in the insured system's contacts. Several of the contacts filed lawsuits claiming that they failed to properly secure the insured's system. Coverage was provided for the costs of hiring lawyers and to settle cases.

   Total Cost: $14,000 under Network Security Liability (for legal defense and settlement costs)

6. A **business** posted a picture of a local celebrity on their website. The insured noticed increased business attributed to this change. However, a letter was received from the celebrity's lawyer demanding that the picture be taken down. The lawyer also argued that their client's reputation may have been harmed by the association to this insured's product. The business owner hired an attorney to respond to the demand letter.

   Total Cost: $7,000 under Electronic Media Liability (for legal defense and settlement costs)

7. An employee in the finance department of a **business** received an email that looked like it was from the company's CFO directing that employee to send a wire for an overdue vendor invoice. Later that day after the employee sent the wire, he bumped into the CFO in the hallway and mentioned he sent the payment. The CFO said he never sent any such request. The employee checked the email and noticed that the CFO's name was spelled slightly incorrectly. The company had been duped by a fraudster that made an outside email look like it came from the CFO. The coverage reimbursed the amount of the wire transfer.
   Total Cost: $9,500 under Misdirected Payment Fraud (for direct financial loss/reimbursement of the funds transferred)
8. A hacker found his way into a **company**'s computer system and changed the banking instructions on several employees' payroll deduction accounts, mapping the payroll deductions to his bank account.

Within a few weeks after several employees complained they did not get their pay, the company investigated and realized they had been hacked. The coverage reimbursed the amount of the diverted funds.

Total Cost: $17,500 under Computer Fraud (for direct financial loss/reimbursement of diverted funds)

9. A website hosted by a **Cyber Suite insured** was accessed by a bad actor using a compromised username and password. After gaining access to the website, the bad actor used stolen credentials to install malware and access client data. The Cyber Suite policy covered the costs of legal advice and hiring a digital forensic incident response firm to investigate whether any personally identifying information was compromised. After determining that a data breach occurred, the insured opted to notify affected individuals without reimbursement under the Cyber Suite policy.
   Total Cost: $100,000 under Data Breach Response Expenses (for Legal Review: $59,424, Forensic IT Review: $40,576, but Notification to Affected Individuals: None)

10. The "computer attack" was discovered by **the insured** while monitoring traffic on their network/firewall. Excessive traffic caused them to further investigate and during that investigation, they discovered that user accounts had been created on their servers and that files on one or more computers on their network were being actively deleted as they watched. The insured disconnected all their systems from the internet at that time and corrected their systems.
    Total Cost: $80,264 under Computer Attack (for System Restoration and Data Restoration)

11. A **small business** owner clicked on an email attachment that looked legitimate. However, the attachment contained malware (commonly referred to as a computer virus) and within a short period of time, the malware spread throughout the owner's computer system causing damage to the company's network. As a result, an outside firm was called in to restore the computer system to its pre-attack functionality. Upon completing the restoration, the firm discovered that the insured was using an outdated operating system. The firm advised the insured to upgrade to a more current operating system that has regular patch updates. The insured did just that and insurance covered $1,000 of the total cost, since the coverage allows for up to 10% of the remediation cost.
    Total Cost: $10,000 under Computer Attack (for System Restoration and $1,000 towards Future Loss Avoidance coverage)

12. A **small business** owner experienced a data breach and provided the necessary notification to affected individuals. The breach was also reported in local media outlets. Over the next three weeks, the owner noticed a decrease in business income as word spread of the breach.
    Total Cost: $19,360 under Data Breach Response Expenses (for Notifications Expenses and Reputational Harm Coverage was provided for the loss of business income for the 30 days following the data breach notification)

13. A **small business** owner received an exorbitant bill from their telephone service provider. It was later determined that a hacker infiltrated the insured's telecommunications system to automatically make outgoing phone calls to expensive 900 numbers which the hacker also controlled. Coverage was provided to reimburse the insured for the fraudulent phone calls.
    Total Costs: $22,963 under Telecommunications Fraud (for the direct financial loss)