Name: _____ Date: _____ Score: _____

Ransomware Attacks & Business Recovery

Payload execution, cryptographic file encryption, offline backups, containment procedures, and disaster recovery.

RANSOMWARE ATTACKS LEARNING OVERVIEW

SECURED
DATA ENCRYPTION
256-bit AES Standard

COMPLIANT
GLOBAL STANDARDS
GDPR & CCPA Frameworks

ZERO-TRUST
ACCESS POLICY
Multi-Factor Authentication

Welcome! This activity packet guides you through ransomware attacks and business recovery. You will explore payload execution, file encryption, offline backups, threat containment, cryptocurrency payments, and disaster recovery plans.

WORKSHEET CHECKPOINTS

- [ ] **Part 1-4:** Master cybersecurity and threat prevention.
- [ ] **Part 5-7:** Solve crossword & word search puzzles.
- [ ] **Part 8-9:** Solve case studies & cipher challenge.
- [ ] **Part 10:** Review basic & advanced FAQ pages.
- [ ] **Part 11:** Explore 10 interesting real-world facts.

Open the VPN.com Cybersecurity Guide

URL: https://www.vpn.com/cybersecurity/ransomware-attack/

Your Ransomware Recovery Learning Roadmap

- Differentiate between Trojan, ransomware, and spyware payloads.
- Analyze malicious files inside secure sandboxed environments.
- Formulate rapid network isolation and containment procedures.

RANSOMWARE ATTACKS GUIDE INSTRUCTIONS

Answer the multiple choice and true/false questions, complete the fill-in-the-blank sentences using the word bank, match definitions, and solve the crossword and word search puzzles. Apply your knowledge to ransomware recovery.

RANSOMWARE ATTACKS & DISASTER RECOVERY (INTRODUCTION)

Ransomware payloads cryptographically lock system storage, demanding cryptocurrency payouts for decryption keys. Mitigating this threat involves network isolation rules, sandboxed malware analysis, and robust air-gapped cold backups.

READ EACH CHECKPOINT CAREFULLY AND SELECT OR WRITE THE CORRECT RESPONSE.

Checkpoint 1: Multiple Choice Challenge

1 What is the primary mechanism of a ransomware attack?

- ◯ A. Cryptographic encryption of user files to deny system access
- ◯ B. Injecting malicious SQL commands into form fields
- ◯ C. Sniffing network packets on a public Wi-Fi connection
- ◯ D. Forging email headers to bypass SPF validation

2 What is an offline (cold) backup?

- ◯ A. A storage copy disconnected from the network to protect it from malware propagation
- ◯ B. A backup stored on the primary web server hard drive
- ◯ C. A temporary cache of system registry logs
- ◯ D. An administrative tool used to reset user passwords

3 How should security teams isolate infected systems during a ransomware attack?

- ◯ A. Disconnect network cables and disable wireless interfaces immediately
- ◯ B. Upgrade the antivirus signatures database
- ◯ C. Shut down the primary DNS server
- ◯ D. Rename the compromised file extensions

4 Why do security agencies advise against paying ransomware demands?

- ◯ A. Paying funds encourages attackers and does not guarantee decryption key delivery
- ◯ B. It automatically invalidates all corporate insurance policies
- ◯ C. It triggers an immediate audit by the registrar
- ◯ D. It corrupts the remaining system backup files

5 What is a disaster recovery plan (DRP)?

- ◯ A. A structured process to restore operations and data after system compromise
- ◯ B. A firewall configuration mapping inbound network ports
- ◯ C. A database schema listing user administrative privileges
- ◯ D. An email authentication protocol rejecting spoofed domains

Checkpoint 2: True or False Challenge

6 Question 6

Ransomware payloads can easily propagate to online backups connected to the network.

◯ True ◯ False

7 Question 7

Paying the cryptocurrency ransom guarantees that files will be decrypted successfully.

◯ True ◯ False

8 Question 8

Disconnecting network connections stops the spread of ransomware to adjacent systems.

◯ True ◯ False

9 Question 9

Symmetric cryptography is never used by ransomware to encrypt system storage.

◯ True ◯ False

10 Question 10

Regularly testing data restoration procedures is a critical part of disaster recovery.

◯ True ◯ False

Checkpoint 3: Key Term Insertion

Read each sentence below and fill in the blank with the correct term from the Word Bank.

1. Denying access to local files uses cryptographic _____.
2. The active malicious code executed on a system is the _____.
3. Disconnected offsite storage copies represent a secure _____.
4. Stopping malware from spreading requires endpoint network _____.
5. The cryptocurrency payment demanded by cybercriminals is the _____.
6. Restoring operational data files represents disaster _____.

VOCABULARY WORD BANK

ENCRYPTION	PAYLOAD	COLDBACKUP	ISOLATION
RANSOM	RECOVERY		

Write your answers here:

1.
2.
3.
4.
5.
6.

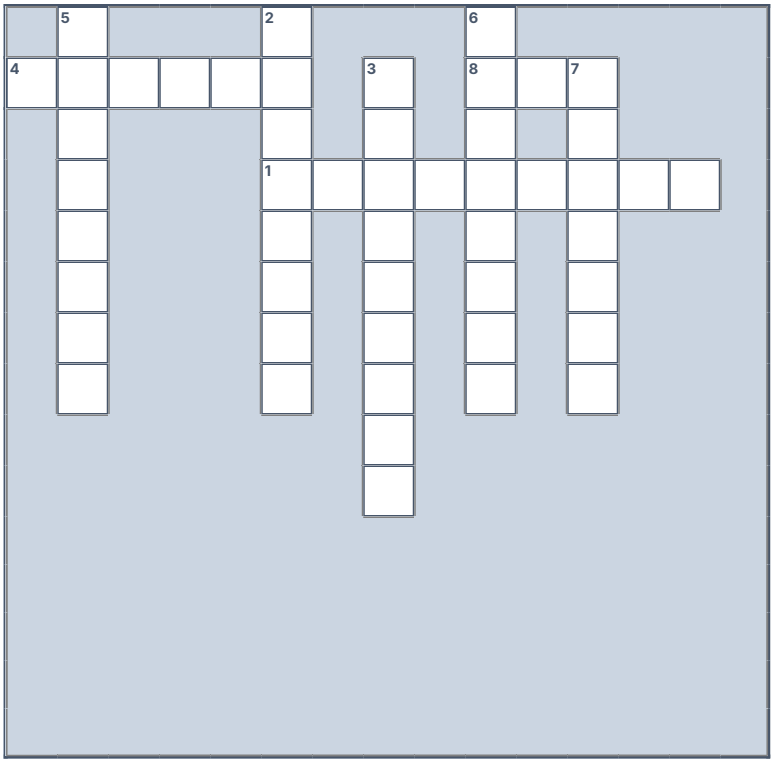
Checkpoint 4: Security Concept Match

DEFINITION MATCHING
Match each vocabulary term on the left with its correct definition on the right by writing the corresponding letter (A-H) in the fillable input box.

ENCRYPTION	**A** Locking files cryptographically. (A)
PAYLOAD	**B** Executing malicious software. (B)
COLDBACKUP	**C** Disconnected offline copy. (C)
ISOLATION	**D** Disconnecting infected network systems. (D)
RANSOM	**E** Cryptographic key payout request. (E)
RECOVERY	**F** Restoring database from backup. (F)
DISASTER	**G** Major system disruption event. (G)
TROJAN	**H** Malicious file disguised as clean. (H)

Checkpoint 5: Crossword Puzzle

Solve the crossword puzzle by typing letters into the active white boxes. The numbers correspond to the clues below.



ACROSS

1. Process of wrapping data packets inside other packets (9)

4. Remote server that routes traffic and hides your IP (6)

8. Internet Service Provider, logs traffic unless encrypted (3)

DOWN

2. Rules determining how data is sent and encrypted (8)

3. Rate of data transfer across a path (9)

5. Blocking site access based on location (8)

6. Security system that monitors and blocks traffic (8)

7. State of being free from tracking or surveillance (7)

Checkpoint 5 Alternative: Accessible Crossword Clues

Screen-reader and keyboard users can type the crossword answers directly in the text fields below.

ACROSS CLUES

1 Across: Cryptographically locking local files to deny user access. (10 letters):

4 Across: The active malicious code executed on a targeted host. (7 letters):

8 Across: Offline storage copy disconnected from the corporate subnet. (10 letters):

DOWN CLUES

2 Down: Disconnecting infected systems from the local network. (9 letters):

3 Down: Cryptocurrency payment demanded for decryption keys. (6 letters):

5 Down: Restoring database files and operational states from backups. (8 letters):

6 Down: Significant operational disruption caused by network attacks. (8 letters):

7 Down: Malicious payload disguised as clean, legitimate software. (6 letters):

Checkpoint 6: Hidden Word Search

Find the 8 key vocabulary terms hidden in the grid below. Words can be horizontal, vertical, or diagonal.

G	D	R	G	O	P	M	P	L	V	O	D	D	T	Z
Z	Y	R	G	M	R	A	Z	X	S	V	W	X	R	I
H	U	R	E	V	K	J	I	A	Q	V	N	F	O	S
U	K	E	A	C	F	T	O	E	Z	E	B	U	J	W
J	D	N	U	N	O	P	A	Y	L	O	A	D	A	Y
I	J	C	S	A	S	V	U	Z	T	Q	A	C	N	F
B	L	R	U	G	G	O	E	Y	L	H	A	V	D	R
U	G	Y	H	Q	E	Q	M	R	P	O	W	T	B	A
L	B	P	K	V	A	Y	R	E	Y	M	H	R	P	S
I	A	T	D	I	S	A	S	T	E	R	K	F	X	U
C	H	I	F	C	O	L	D	B	A	C	K	U	P	K
I	H	O	Z	U	I	S	O	L	A	T	I	O	N	B
A	N	N	E	L	M	V	D	Q	X	U	L	A	Z	G
X	A	I	N	W	E	F	P	J	B	V	A	J	N	G
G	V	I	Q	L	X	J	H	Q	U	M	L	Q	E	R

VOCABULARY WORD LIST

ENCRYPTION	PAYLOAD	COLDBACKUP	ISOLATION
RANSOM	RECOVERY	DISASTER	TROJAN

Checkpoint 6 Alternative: Accessible Vocabulary Matching

Match each of the 8 vocabulary terms from the Word Search to its correct definition by writing the letter (A-H) in the blank space.

VOCABULARY TERMS

A. ENCRYPTION
B. PAYLOAD
C. COLDBACKUP
D. ISOLATION
E. RANSOM
F. RECOVERY
G. DISASTER
H. TROJAN

DEFINITIONS & MATCH FIELDS

1. Locking files cryptographically.
2. Executing malicious software.
3. Disconnected offline copy.
4. Disconnecting infected network systems.
5. Cryptographic key payout request.
6. Restoring database from backup.
7. Major system disruption event.
8. Malicious file disguised as clean.

Checkpoint 7: Scrambled Word Challenge

Unscramble the letters below to reveal key cybersecurity concepts and terms. Write your answers in the input boxes provided.

1. N O I T P Y R C N E

2. D A O L Y A P

3. P U K C A B D L O C

4. N O I T A L O S I

5. M O S N A R

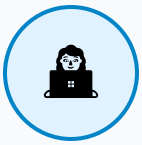
6. Y R E V O C E R

7. R E T S A S I D

8. N A J O R T

Checkpoint 8: Cybersecurity Case Studies

Apply the concepts you have learned to solve the real-world scenarios below.



CASE STUDY 1: ENTERPRISE RANSOMWARE PAYLOAD CONTAINMENT

Scenario: A corporate local area network has been breached by active ransomware. Key file servers have begun showing file extensions with .locked.

Discussion Question: Detail the containment steps, and outline the data recovery protocol.

CASE STUDY 2: EVALUATING OFFLINE BACKUP ARCHITECTURES

Scenario: An enterprise wants to design a data backup strategy that guarantees backups cannot be compromised even if the primary local network is completely hijacked by ransomware.

Discussion Question: Design a secure offline backup storage vault system.

Final Challenge: Decrypting the Cipher

A cybersecurity professional protects network assets from online threat actors. Use the Letter-to-Number key below to decrypt the message by writing the matching letters in the blank spaces.

LETTER-TO-NUMBER ENCRYPTION KEY

A=1	B=2	C=3	D=4	E=5	F=6	G=7	H=8	I=9	J=10	K=11	L=12	M=13
N=14	O=15	P=16	Q=17	R=18	S=19	T=20	U=21	V=22	W=23	X=24	Y=25	Z=26

18	5	19	20	15	18	5		5	14	3	18	25	16	20	5	4			
4	1	20	1		19	25	19	20	5	13		6	18	15	13				
3	15	12	4		2	1	3	11	21	16									

Decoded cybersecurity message:

_____

TIP: EACH NUMBER REPRESENTS THE POSITION OF THAT LETTER IN THE ALPHABET (E.G. 1 = A, 2 = B, 26 = Z).

Checkpoint 10: Basic Cybersecurity FAQs (Part A)

Review common questions and answers regarding online threat mitigation.

Q1: What is ransomware?

Ransomware is malicious software designed to block access to computer systems or files until a ransom sum is paid.

Q2: How does ransomware spread?

Via email phishing attachments, unpatched software vulnerabilities, and compromised remote access systems.

Q3: Why is payment requested in cryptocurrency?

Cryptocurrencies like Bitcoin offer relative anonymity, making it difficult for law enforcement to track the funds.

Q4: Does antivirus block ransomware?

Yes, but signature-based antivirus can fail against newly created zero-day ransomware payloads.

Q5: What is an air-gapped backup?

A backup copy that has no physical or logical connection to the primary network, protecting it from spread.

Checkpoint 10: Basic Cybersecurity FAQs (Part B)

Review common questions and answers regarding online threat mitigation.

Q6: What is double extortion?

When attackers not only encrypt files but also steal sensitive data to threaten public leaks if unpaid.

Q7: What is a decryptor?

A software utility containing the cryptographic key needed to restore locked files to plaintext.

Q8: How do you detect ransomware early?

By monitoring file systems for sudden, massive file modification and renaming activity.

Q9: What is the role of insurance?

Cyber insurance can help cover recovery costs, but many policies now restrict or forbid paying ransom demands.

Q10: Should I reboot an infected system?

No, rebooting can destroy volatile memory evidence; isolate it from the network instead.

Checkpoint 11: Advanced Security FAQs (Part A)

Explore advanced technical aspects of security frameworks, malware analysis, and data compliance.

Q1: How does ransomware use asymmetric encryption?

It uses a public key embedded in the malware to encrypt files, requiring the attacker's private key to decrypt them.

Q2: Why is symmetric encryption also used?

Symmetric encryption (like AES) is fast and can lock huge databases in minutes, while asymmetric keys secure the AES key.

Q3: What is logical segmentation?

Dividing networks into isolated zones, preventing malware from propagating laterally from workstation nodes to core servers.

Q4: What is WORM storage?

Write-Once, Read-Many media, which prevents backup data from being edited, overwritten, or deleted by ransomware payloads.

Q5: What are shadow copies?

Local backup snapshots created by Windows; ransomware typically deletes these first using administrative tools.

Checkpoint 11: Advanced Security FAQs (Part B)

Explore advanced technical aspects of security frameworks, malware analysis, and data compliance.

Q6: How does credential theft enable ransomware?

Attackers buy leaked admin logins to sign in via remote desktops, manually executing ransomware across the network.

Q7: What is dry-run restoration testing?

Regularly restoring backup databases to isolated test environments to verify that restoration speed and data integrity meet disaster metrics.

Q8: How does endpoint detection (EDR) stop ransomware?

By analyzing process behavior (e.g., rapid encryption) and instantly suspending the rogue application.

Q9: What is a ransomware-as-a-service (RaaS) model?

A franchise model where malware developers lease ransomware builders to affiliates in exchange for a percentage of payouts.

Q10: How does unpatched RDP trigger ransomware?

Exposed, unpatched Remote Desktop Protocol gateways allow attackers to brute-force logins and manually launch malware.

Part 11: 10 Real-World Cybersecurity Facts & Insights

Review real-world facts regarding security breaches, defense mechanisms, and compliance standards.

1. SECURITY INSIGHT

Over 70% of ransomware attacks target historical shadow copies first to prevent local system restoration.

2. SECURITY INSIGHT

Symmetric AES-256 keys are typically used to encrypt file payloads, which are then locked using public RSA keys.

3. SECURITY INSIGHT

The average downtime for an enterprise experiencing a successful ransomware attack exceeds 20 business days.

4. SECURITY INSIGHT

Paying a ransom does not guarantee decryption, with only 60% of paying victims recovering all their data assets.

5. SECURITY INSIGHT

Disaster recovery plans (DRP) must define a Target Recovery Time Objective (RTO) and Recovery Point Objective (RPO).

6. SECURITY INSIGHT

WORM storage backup volumes prevent any modification of stored records even if administrative accounts are compromised.

7. SECURITY INSIGHT

Ransomware developers utilize advanced obfuscation techniques to bypass traditional signature-based antivirus scanners.

8. SECURITY INSIGHT

Micro-segmentation isolates server nodes, stopping ransomware from spreading beyond the initial entry workstation.

9. SECURITY INSIGHT

Remote Desktop Protocol (RDP) exploits account for over 50% of initial entry vectors in corporate ransomware cases.

10. SECURITY INSIGHT

Air-gapped backup networks are logically disconnected from local subnets except during scheduled daily write windows.

Technical References & Sources

The study guide and interactive puzzles are compiled from global NIST, OWASP, and data privacy compliance standards.

SCHOLARLY & INDUSTRY REFERENCES

[1] CISA. (2025). Cybersecurity Alerts & Advisories. Retrieved from https://www.cisa.gov/news-events/cybersecurity-advisories

[2] GDPR. (2024). General Data Protection Regulation (GDPR) Official Text. Retrieved from https://gdpr-info.eu/

[3] NIST. (2024). Special Publication 800-53: Security and Privacy Controls. Retrieved from https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

[4] NIST. (2023). Special Publication 800-61: Computer Security Incident Handling Guide. Retrieved from https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final

[5] NIST. (2023). Special Publication 800-88: Guidelines for Media Sanitization. Retrieved from https://csrc.nist.gov/publications/detail/sp/800-88/rev-1/final

[6] IETF. (2021). RFC 8446: Transport Layer Security (TLS) 1.3 Specification. Retrieved from https://datatracker.ietf.org/doc/rfc8446/

[7] IETF. (2022). RFC 7519: JSON Web Token (JWT) Specification. Retrieved from https://datatracker.ietf.org/doc/rfc7519/

[8] Center for Internet Security (CIS). (2024). Critical Security Controls. Retrieved from https://www.cisecurity.org/controls/cis-controls-list

[9] OWASP. (2024). Top 10 Web Application Security Risks. Retrieved from https://owasp.org/www-project-top-ten/

[10] OWASP. (2025). Application Security Verification Standard (ASVS). Retrieved from https://owasp.org/www-project-application-security-verification-standard/

Answer Key: Checkpoint 1 - Multiple Choice

1 Brokerage Function BROKERAGE Correct Answer: A

TEACHING NOTE

Domain brokers act as confidential negotiators representing buyers and sellers to reach fair market transactions.

Citation: ICANN Transfer Policy [Ref 1].

2 Stealth Strategy STEALTH Correct Answer: A

TEACHING NOTE

Stealth acquisition conceals corporate buyer identity to prevent sellers from inflating asking prices.

Citation: Escrow.com Protocol [Ref 7].

3 Escrow Protection ESCROW Correct Answer: A

TEACHING NOTE

Licensed third-party escrow holds funds safely until ownership transfer verification is complete.

Citation: Escrow.com Protocol [Ref 7].

4 Domain Appraisal VALUATION Correct Answer: A

TEACHING NOTE

Short 2-letter and 1-word .com domains carry extreme global brand scarcity and liquidity.

Citation: WIPO UDRP Guide [Ref 3].

5 Dispute Resolution UDRP POLICY Correct Answer: A

TEACHING NOTE

ICANN's Uniform Domain-Name Dispute-Resolution Policy (UDRP) governs administrative trademark disputes.

Citation: WIPO Dispute Rules [Ref 2].

Answer Key: Checkpoint 2 - True or False

6 Confidential NDAs NDAS

Correct Answer: True

TEACHING NOTE

Professional domain brokers operate under non-disclosure agreements to protect buyer corporate strategy.

Citation: CIS Controls [Ref 8].

7 Escrow Delivery ESCROW

Correct Answer: False

TEACHING NOTE

Escrow holding accounts disburse funds only after full domain ownership transfer is verified by the buyer.

Citation: Escrow.com Protocol [Ref 7].

8 Digital Real Estate ASSETS

Correct Answer: True

TEACHING NOTE

Short 2-letter and 3-letter .com domains function as high-value, liquid digital property assets.

Citation: NIST Guidelines [Ref 9].

9 Stealth Negotiation STRATEGY

Correct Answer: False

TEACHING NOTE

Direct corporate buyer outreach often causes sellers to inflate asking prices significantly.

Citation: WIPO UDRP Guide [Ref 3].

10 EPP Authorization EPP CODE

Correct Answer: True

TEACHING NOTE

EPP codes are unique security passcodes generated by registrars to authorize domain transfers.

Citation: IETF RFC 5730 [Ref 4].

Vocabulary Keys & Grading Rubric

Instructor Grading Rubric: Award 1 point for each correct matching (8 points total) and context term (6 points total).

CHECKPOINT 4: CONCEPT MATCH KEY

A ENCRYPTION	B PAYLOAD	C COLDBACKUP	D ISOLATION
E RANSOM	F RECOVERY	G DISASTER	H TROJAN

CHECKPOINT 3: KEY TERM KEY

1 ENCRYPTION	2 PAYLOAD	3 COLDBACKUP
4 ISOLATION	5 RANSOM	6 RECOVERY

DISCUSSION NOTES FOR INSTRUCTORS

Threat Landscape:
Verify that students understand how malware, phishing, and zero-day attacks target and disrupt network defenses.

Defense Controls:
Emphasize the deployment of network firewalls, sandbox execution, behavior scanners, and multi-factor authentication (MFA).

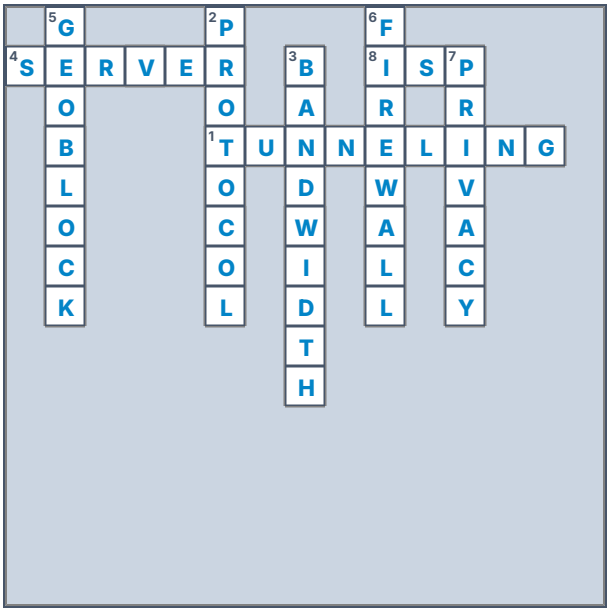
Regulatory Compliance:
Highlight user consent, data minimization, encryption at-rest and in-transit, and global frameworks like GDPR/CCPA.

Puzzles Keys & Instructor Notes

WORD SEARCH SOLUTION

G	D	R	G	O	P	M	P	L	V	O	D	D	T	Z
Z	Y	R	G	M	R	A	Z	X	S	V	W	X	R	I
H	U	R	E	V	K	J	I	A	Q	V	N	F	O	S
U	K	E	A	C	F	T	O	E	Z	E	B	U	J	W
J	D	N	U	N	O	P	A	Y	L	O	A	D	A	Y
I	J	C	S	A	S	V	U	Z	T	Q	A	C	N	F
B	L	R	U	G	G	O	E	Y	L	H	A	V	D	R
U	G	Y	H	Q	E	Q	M	R	P	O	W	T	B	A
L	B	P	K	V	A	Y	R	E	Y	M	H	R	P	S
I	A	T	D	I	S	A	S	T	E	R	K	F	X	U
C	H	I	F	C	O	L	D	B	A	C	K	U	P	K
I	H	O	Z	U	I	S	O	L	A	T	I	O	N	B
A	N	N	E	L	M	V	D	Q	X	U	L	A	Z	G
X	A	I	N	W	E	F	P	J	B	V	A	J	N	G
G	V	I	Q	L	X	J	H	Q	U	M	L	Q	E	R

CROSSWORD SOLUTION



INSTRUCTOR GUIDE FOR CROSSWORD SOLUTIONS

ACROSS CLUES

1 Across: TUNNELING Process of wrapping data packets. (3,5)

4 Across: SERVER Remote computer routing traffic. (1,0)

8 Across: ISP Internet Service Provider. (1,9)

DOWN CLUES

2 Down: PROTOCOL Rules determining data transmission. (0,5)

3 Down: BANDWIDTH Rate of data transfer. (1,7)

5 Down: GEOBLOCK Location website restriction. (0,1)

6 Down: FIREWALL Security monitor barrier. (0,9)

7 Down: PRIVACY State of freedom from tracking. (1,11)

Scrambled Words & Cipher Solution Key

Grading key for the vocabulary word unscramble activity and Secret Cipher Challenge.

WORD UNSCRAMBLE KEY

1. N O I T P Y R C N E
   ENCRYPTION

2. D A O L Y A P
   PAYLOAD

3. P U K C A B D L O C
   COLDBACKUP

4. N O I T A L O S I
   ISOLATION

5. M O S N A R
   RANSOM

6. Y R E V O C E R
   RECOVERY

7. R E T S A S I D
   DISASTER

8. N A J O R T
   TROJAN

SECRET CIPHER CHALLENGE KEY

"RESTORE ENCRYPTED DATA SYSTEM FROM COLD BACKUP"

Domain Brokerage Case Studies Solution Key

A Case Study 1: Enterprise Ransomware Payload Containment

Instructor Solution

GRADING GUIDELINE

Student answers should cover the following points:

- **Scenario Analysis:** A corporate local area network has been breached by active ransomware. Key file servers have begun showing file extensions with .locked.
- **Recommended Strategy & Solution:** Disconnect all affected servers from the local area network. Kill active administrative sessions. Restore uncompromised files from a secure, write-locked offline backup system.

B Case Study 2: Evaluating Offline Backup Architectures

Instructor Solution

GRADING GUIDELINE

Student answers should cover the following points:

- **Scenario Analysis:** An enterprise wants to design a data backup strategy that guarantees backups cannot be compromised even if the primary local network is completely hijacked by ransomware.
- **Recommended Strategy & Solution:** Implement write-once-read-many (WORM) storage. Formulate a logical air-gap by disconnecting the backup system from all networks, and enforce daily physical media rotation.