ARCTIC WOLF

THE LEADER IN SECURITY OPERATIONS

UNDER RANSOM

RANSOMWARE TABLE READ EXERCISE

The Table Read

This exercise will review a sample ransomware event. As we read through the scenario, please consider the following points for discussion.

- What did this fictional company do well during this incident?
- Where did they falter in their response?
- When could they have responded differently or been better prepared?
- How is your organization more - or less - equipped to handle this situation?
- Could your organization benefit from a table-top exercise?

Company Overview

Company Name: Sidekicks

Industry: Retail and Manufacturing (shoes)

Revenue: $7M last quarter; $80K per day

Stores: 38 retails stores in Europe

Manufacturing: South Korea and China

Casting – Who plays a role in ransomware?

- IT Helpdesk
- IT Manager
- Operations Manager

Casting – Who else plays a role in ransomware?

- IT Helpdesk
- IT Manager
- Operations Manager
- CIO
- Privacy Attorney
- Cyber Insurance Representative

Casting – Who really plays a role in ransomware?

- IT Helpdesk
- IT Manager
- Operations Manager
- CIO
- Privacy Attorney
- Cyber Insurance Representative
- CEO
- CFO
- Warehouse Manager
- Director of e-Commerce
- Director of Human Resources
- VP of Marketing
- Incident Response Team Lead

Casting – IT and Beyond

ROLE	PARTICIPANT
IT Helpdesk *	1
IT Manager	2
Operations Manager	3
CIO	4
Privacy Attorney	5
Insurance Representative **	6
CEO	7
CFO	8
Warehouse Manager ***	9
Director of e-Commerce **	6 (or 12)
Director of Human Resources *	1 (or 11)
VP of Marketing ***	9 (or 13)
Incident Response Team Leader	10

*** characters can be played be the same individual if needed**

The Script

Company Background

Characters

Act 1 – Discovery

Act 2 – Impact

Act 3 – Response

Act 4 – Recovery

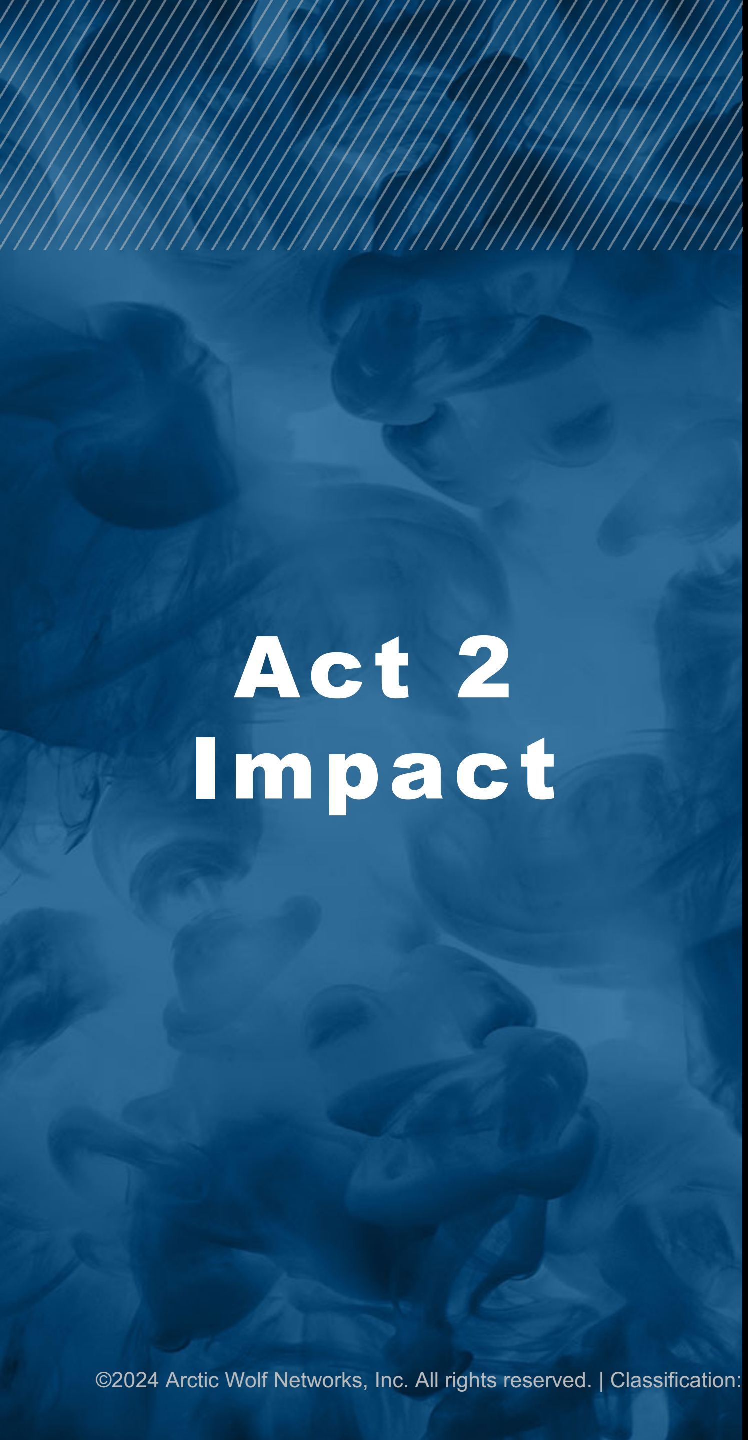
Appendices

Act 1 Discovery

Table Read Act 1

Act 1 Discussion Points

- What should have been done differently?
- What action should be taken on laptops or systems infected with ransomware?
- Does your organization have clear guidelines for when and how to report a security incident?
- How has lack of 24x7 monitoring impacted your organization?

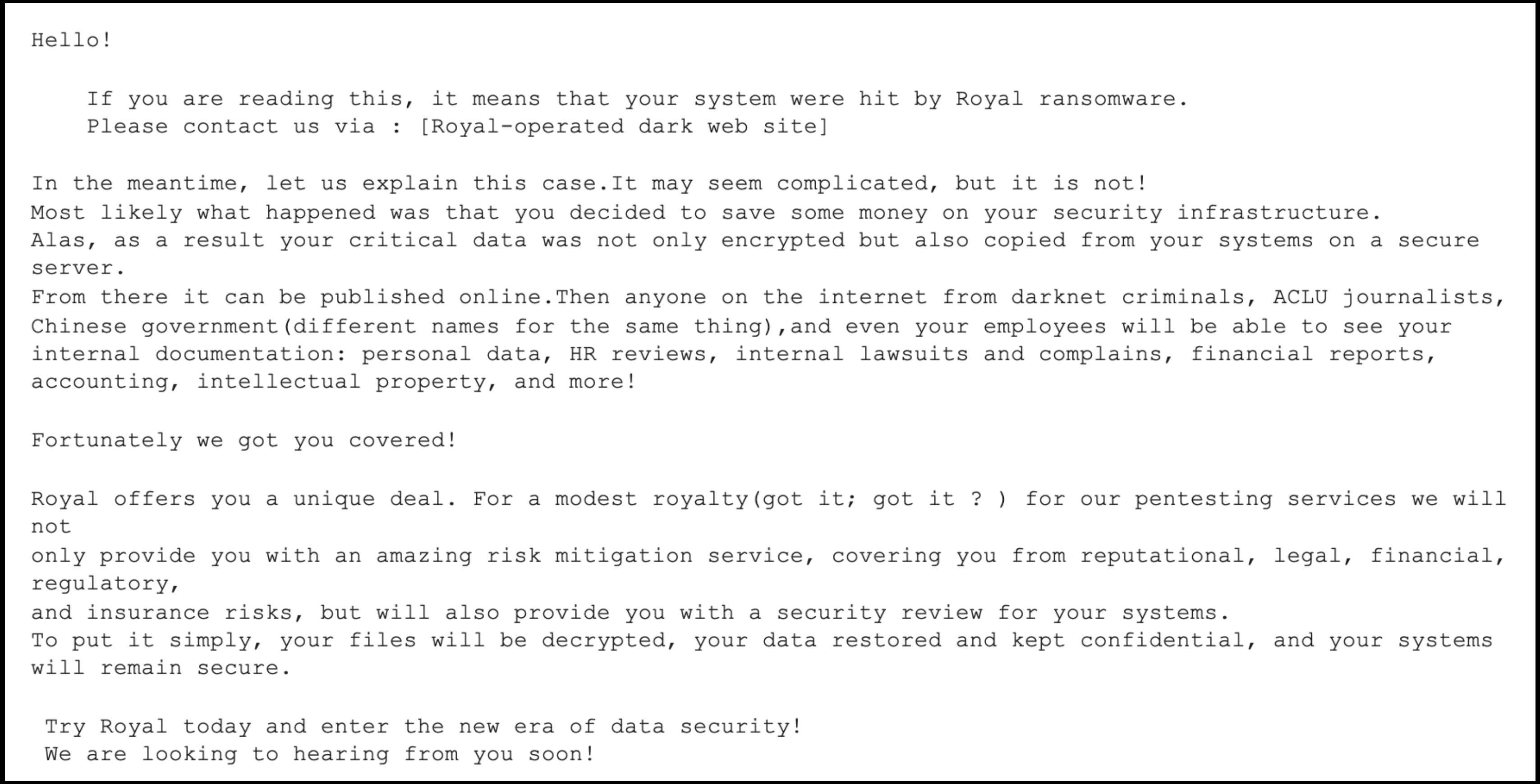


Act 2 Impact

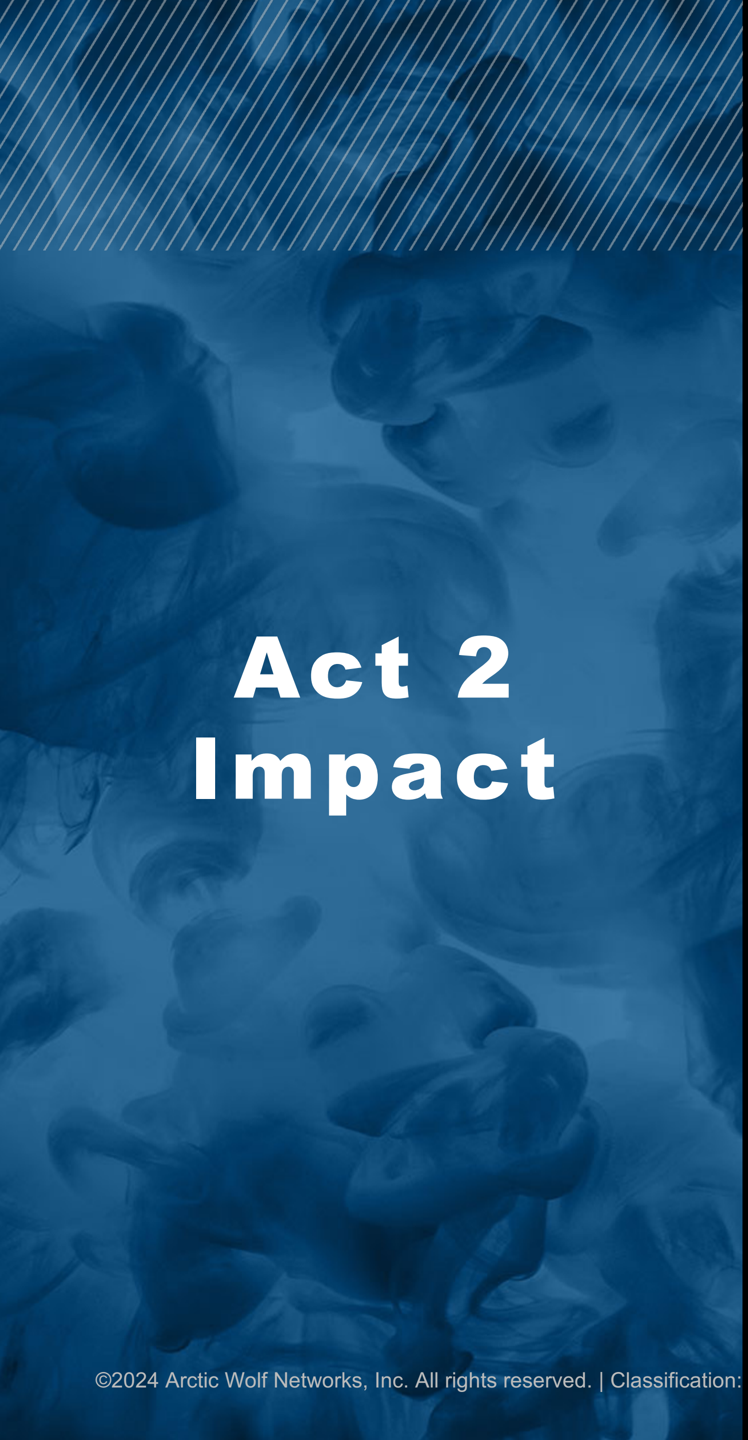
Table Read Act 2

Act 2 Impact

Table Read Act 2
Review Ransom Note – Appendix A



```
Hello!

    If you are reading this, it means that your system were hit by Royal ransomware.
    Please contact us via : [Royal-operated dark web site]

In the meantime, let us explain this case.It may seem complicated, but it is not!
Most likely what happened was that you decided to save some money on your security infrastructure.
Alas, as a result your critical data was not only encrypted but also copied from your systems on a secure
server.
From there it can be published online.Then anyone on the internet from darknet criminals, ACLU journalists,
Chinese government(different names for the same thing),and even your employees will be able to see your
internal documentation: personal data, HR reviews, internal lawsuits and complains, financial reports,
accounting, intellectual property, and more!

Fortunately we got you covered!

Royal offers you a unique deal. For a modest royalty(got it; got it ? ) for our pentesting services we will
not
only provide you with an amazing risk mitigation service, covering you from reputational, legal, financial,
regulatory,
and insurance risks, but will also provide you with a security review for your systems.
To put it simply, your files will be decrypted, your data restored and kept confidential, and your systems
will remain secure.

 Try Royal today and enter the new era of data security!
 We are looking to hearing from you soon!
```



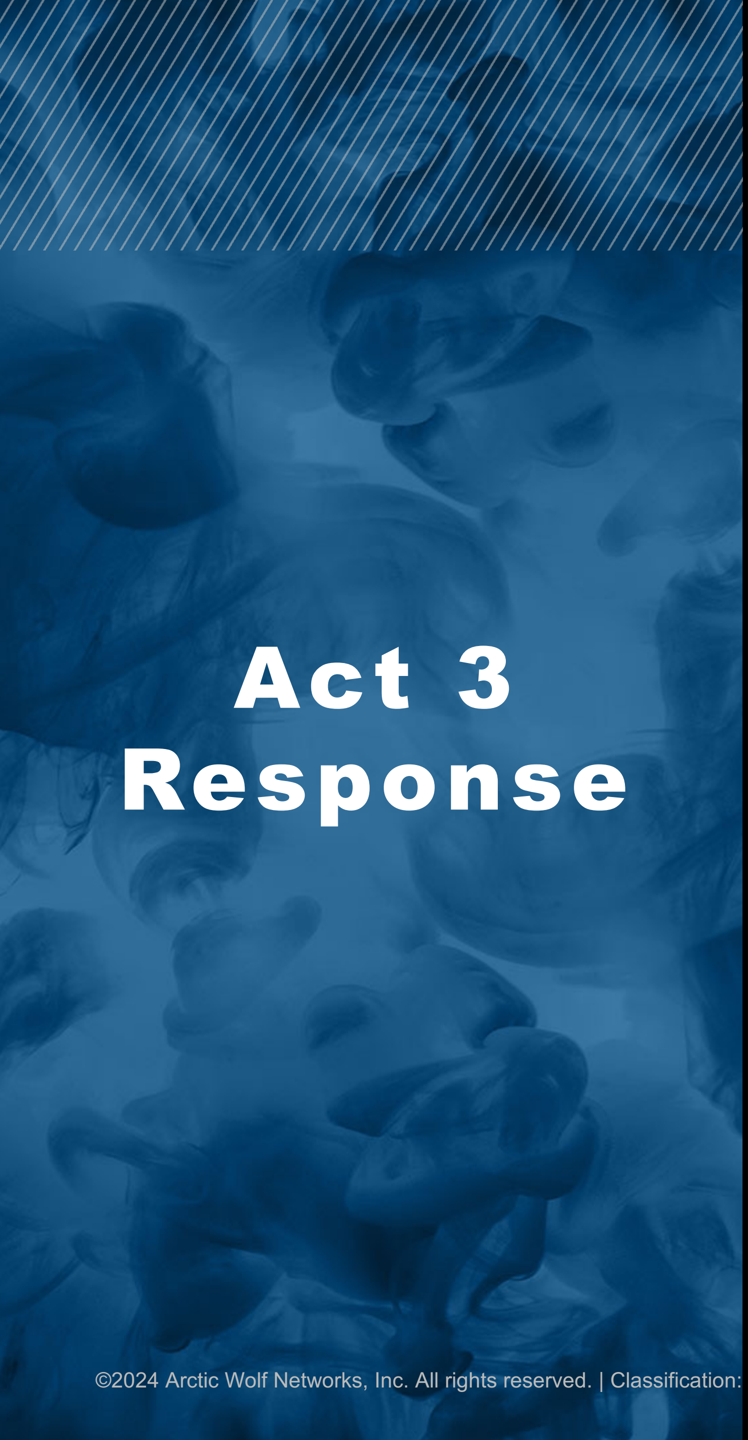
Act 2 Impact

Table Read Act 2

Review Ransom Note

Act 2 Discussion Points

- What solutions would have help this go smoother?
- How could having an IR retainer help speed up the process?
- How does your company ensure knowledge is shared and transitioned?
- Do most companies have documented, emergency procedures for retail and remote locations?

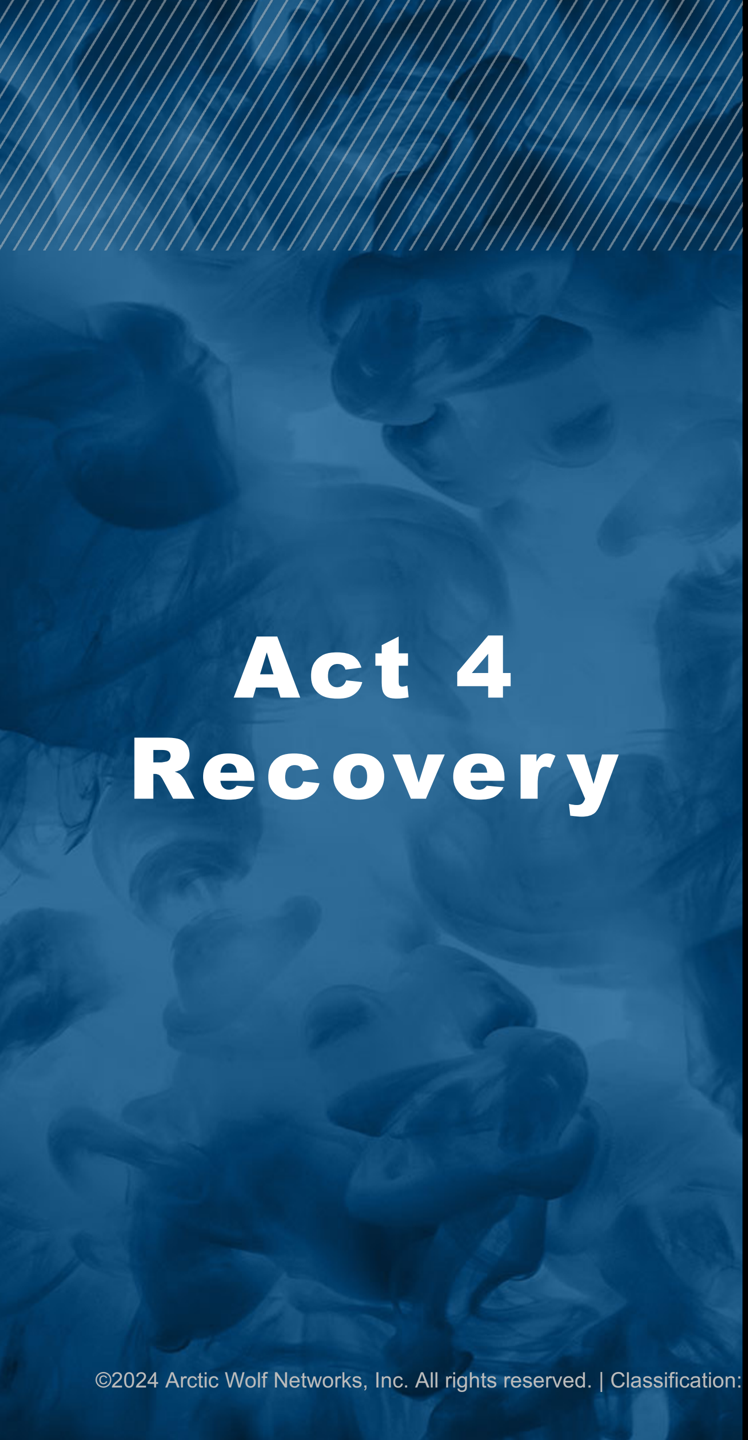


Act 3 Response

Table Read Act 3

Act 3 Discussion Points

- What other processes or procedures should the company have considered to get the online orders processed in the near term?
- How and when should service interruptions be communicated to customers?
- Are the variable terms of cyber insurance well understood by most organizations?
- What would have made the inventory system recovery faster?



Act 4 Recovery

Table Read Act 4

Act 4 Discussion Points

- Did this company overlook anything when weighing the option of paying the ransom?
- How long do you have to consider the decision to pay a ransom?
- Has annual compliance training been enough for our organization?
- How is the post-mortem process handled in your organizations?

The Outcome

Company Name: Sidekicks

Attack: Ransomware via phishing

Total Outage: Four days (Saturday – Tuesday)

Revenue Lost: $120,000

Ransom Payment: $0

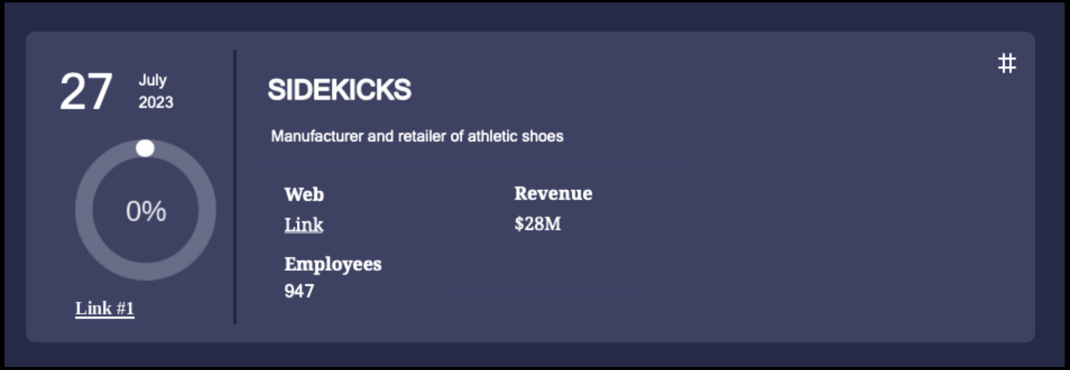
Actions Taken Post-Event:

- Reviewed recommendations of IR team.
- Deployed MDR solution.
- Updated documentation. System recovery plans, back up procedures, incident response plans, etc.

Other Lessons Learned:

- An IR retainer can save valuable time.
- Understand your cyber insurance policy.

Attacker's commonly make "brag" posts on the dark web.



27 July 2023

0%

Link #1

SIDEKICKS

Manufacturer and retailer of athletic shoes

Web
Link

Revenue
$28M

Employees
947

#