Q4 November 2024

Ransomware Trends & Future Prevention

Rick Vanover

Veeam Product Strategy

RICKATRON

Veeam is
purpose-built
for powering
data resilience

Quote of the Year

From VeeamON 2024

Words to live by

William Siegel, CEO Coveware by Veeam

- *"I can tell in the first 15 minutes of a conversation how well or how poorly an incident response is going to progress just based on how prepared an organization presents themselves during the initial phone call."*

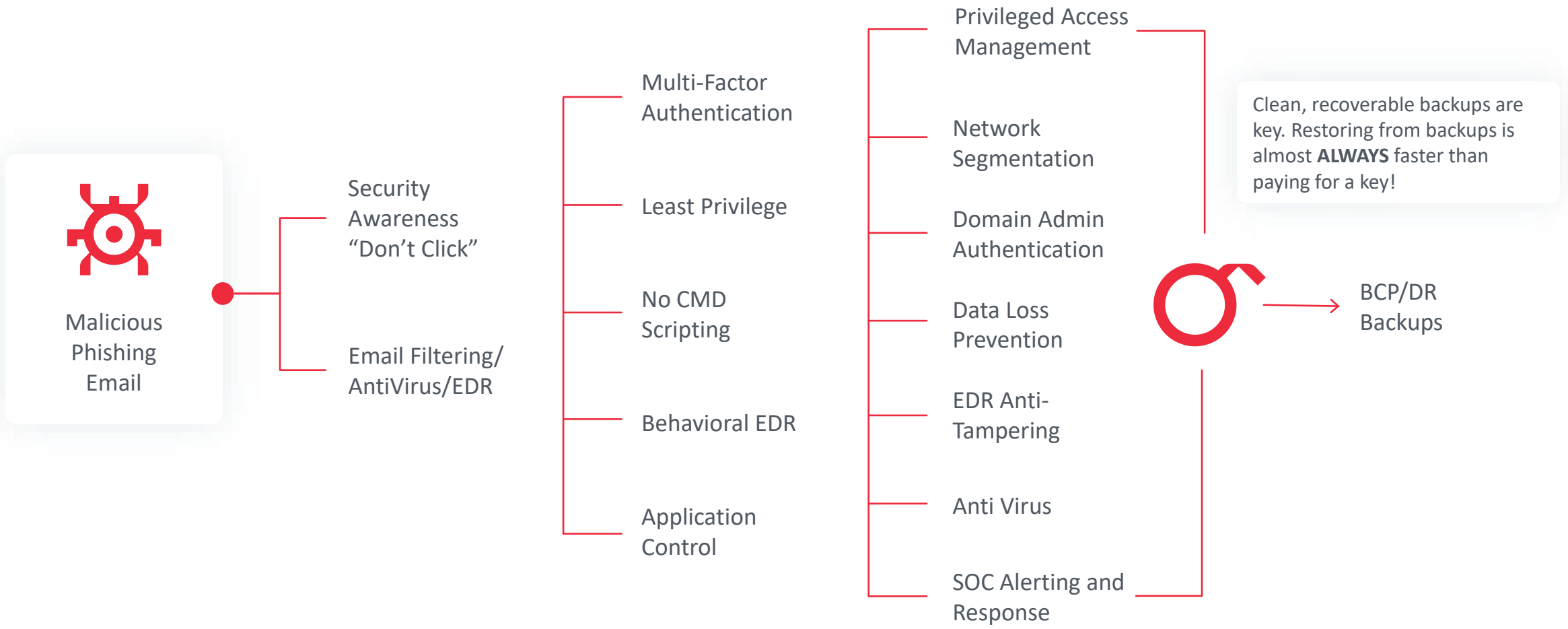
- **Summarized quote from general session"**

Q2 2024
Top 10 Threat Actors

- Based on percentage of cases in Q2 2024
- Groups such as Akira and Black Basta continued to hold a comparable market without a noticeable shift in techniques and behaviors
- Suggesting that not all ransomware brands have opened their doors to displaced affiliates
- Sharp rise in the frequency of Lone Wolf “unaffiliated” extortion attacks

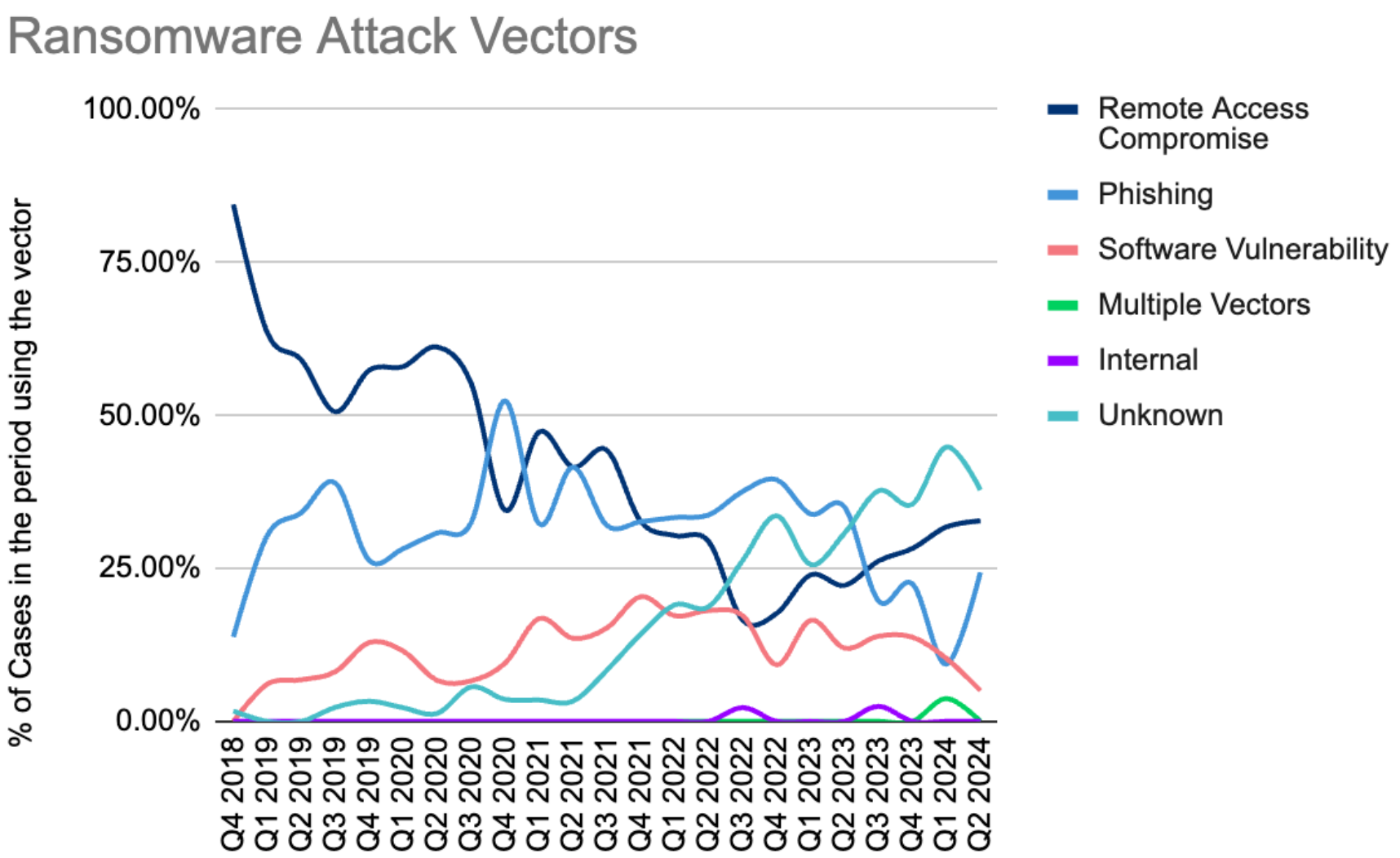
Family Name	% of Cases	Previous Rank
Akira	11%	-
”Lone Wolves”	10%	Unranked
Black Basta	8%	-1
BlackSuit	8%	+1
Lockbit 3.0	7%	-2
Medusa	7%	-1
BianLian	5%	Unranked
Inc Ransom	5%	-1
Phobos	4%	-2
Qilin	3%	Unranked

Compounding Failures in the Cyber “Kill Chain”

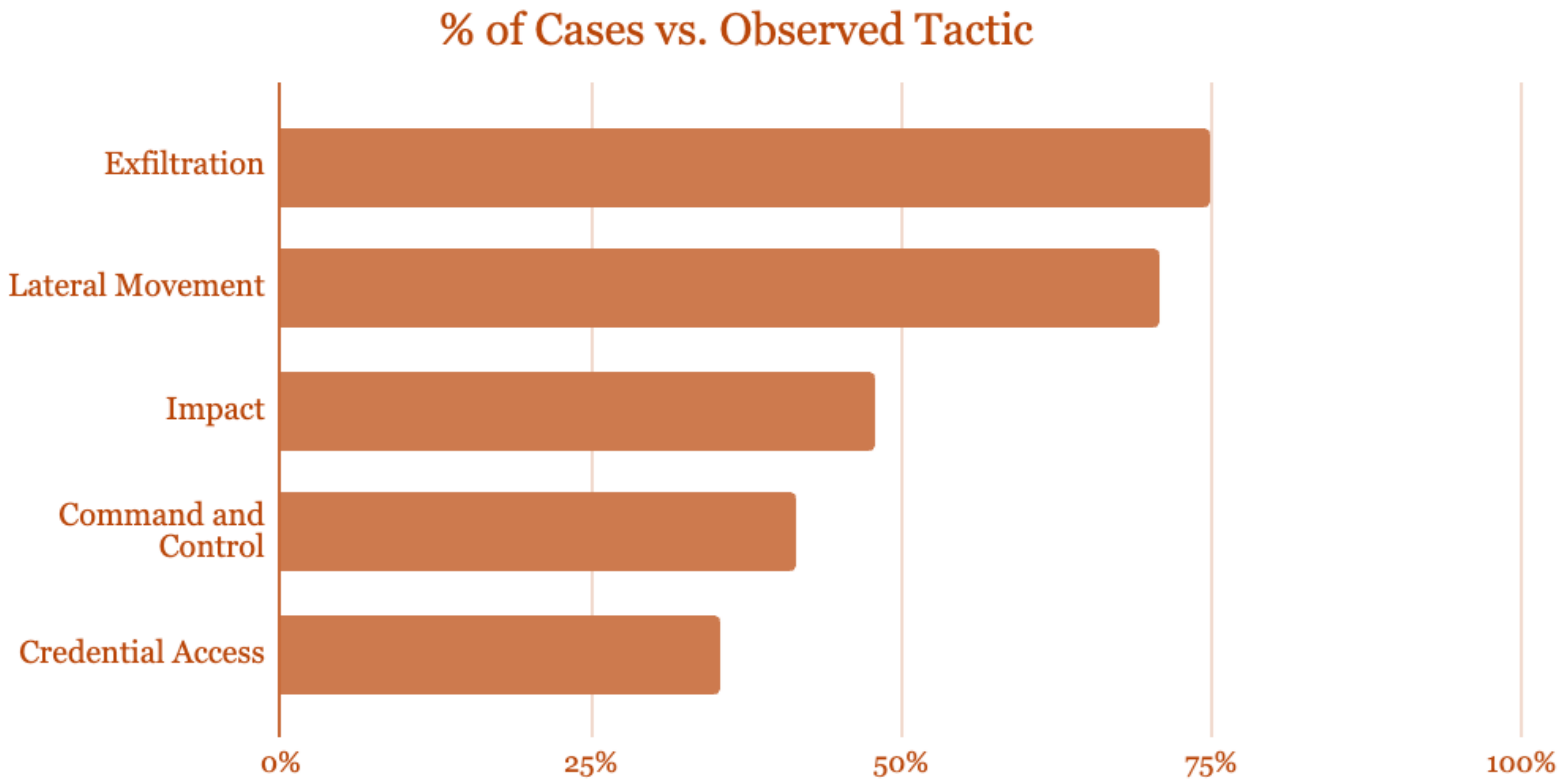


Q2 2024
Initial Access

Purpose:
The adversary is trying to get into your network.



Q2 2024
The Top 5 MITRE Tactics Observed



Common Incident Response Lifecycle

1. How do we **know what to do** when it happens?
2. How do we **identify when** it happens?
3. How do we **stop it** from spreading?
4. How do we **eliminate it** from our environment?
5. How do we **remediate** any impacts and **restore** our operations?
6. How do we **learn** from it?

Current Observations from Tech Support

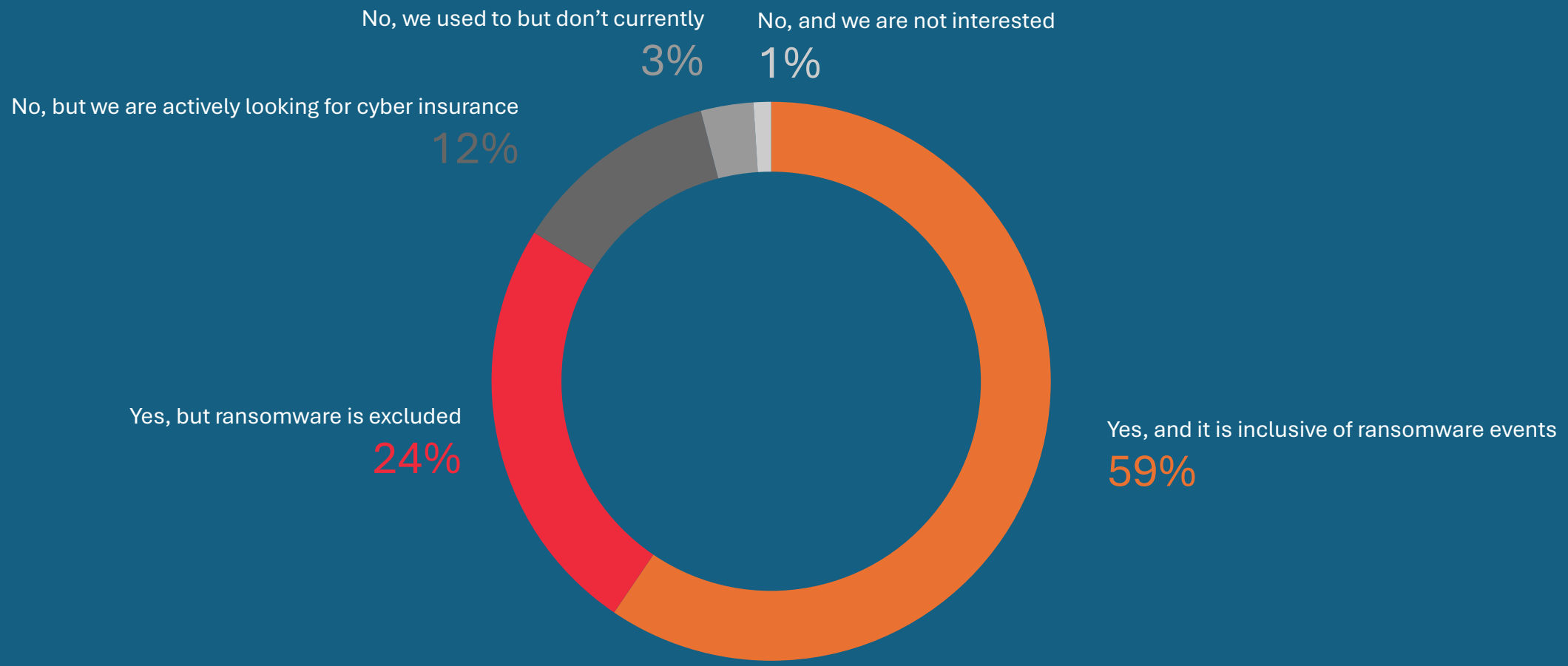
Rogue Deleting of files from threats

- EDR/Security Software “Interference”

Direct targeting of Backups

Do you currently have cyber insurance?

Does your organization currently have a cyber insurance policy?



What is some of the most valuable data to a threat actor?

A Cyber Insurance Policy!

5. Aggregate sublimit of liability for all **Cyber Extortion Loss** under **INSURING AGREEMENTS** I.G.:	USD $1,000,000
6. Aggregate sublimit of liability for all **Data Protection Loss** and **Business Interruption Loss** under **INSURING AGREEMENTS** I.H. and I.I.:	USD $1,000,000
7. First Party Business Interruption Sublimits of Liability:	
(1) **Hourly sublimit**:	USD $250,000
(2) **Forensic Expense sublimit**:	USD $250,000
(3) **Dependent Business Interruption sublimit**:	USD $250,000

The above sublimits of liability are part of, and not in addition to, the overall **Policy Aggregate Limit of Liability.**

This Endorsement is attached to and forms a part of Policy Number [redacted]
[redacted] Insurance Company, Inc. referred to in this endorsement as either the "Insurer" or the "Underwriters"

FIRST PARTY COMPUTER SECURITY COVERAGE ENDORSEMENT

This endorsement modifies insurance provided under the following:

[redacted] RESPONSE SELECT

In consideration of the premium charged for this Policy, it is hereby understood and agreed that:

1. Item 3.A. of the Declarations is amended to add the following:

5. Aggregate sublimit of liability for all **Cyber Extortion Loss** under **INSURING AGREEMENTS** I.G.:	USD $1,000,000
6. Aggregate sublimit of liability for all **Data Protection Loss** and **Business Interruption Loss** under **INSURING AGREEMENTS** I.H. and I.I.:	USD $1,000,000
7. First Party Business Interruption Sublimits of Liability:	
(1) **Hourly sublimit**:	USD $250,000
(2) **Forensic Expense sublimit**:	USD $250,000
(3) **Dependent Business Interruption sublimit**:	USD $250,000

The above sublimits of liability are part of, and not in addition to, the overall **Policy Aggregate Limit of Liability.**

2. Item 3.A.1. of the Declarations is amended to include **INSURING AGREEMENTS** I.G. (**Cyber Extortion**), I.H. (**First Party Data Protection**) and I.I. (**First Party Network Business Interruption**) within the **Policy Aggregate Limit of Liability** set forth therein.

3. Item 4. of the Declarations is amended to add the following:

F. **INSURING AGREEMENTS** I.G.: Each **Extortion Threat** Retention	USD $2,500
G. **INSURING AGREEMENTS** I.H.: Each **Security Breach** Retention	USD $2,500
H. **INSURING AGREEMENTS** I.I.: Each **Security Breach** Retention	
(1) Income Loss:	USD $2,500
(2) Extra Expense:	USD $2,500
I. **INSURING AGREEMENTS** I.I.: **Waiting Period**	10 Hours

4. Clause **I. INSURING AGREEMENTS**, is amended to add the following:

G. **Cyber Extortion**

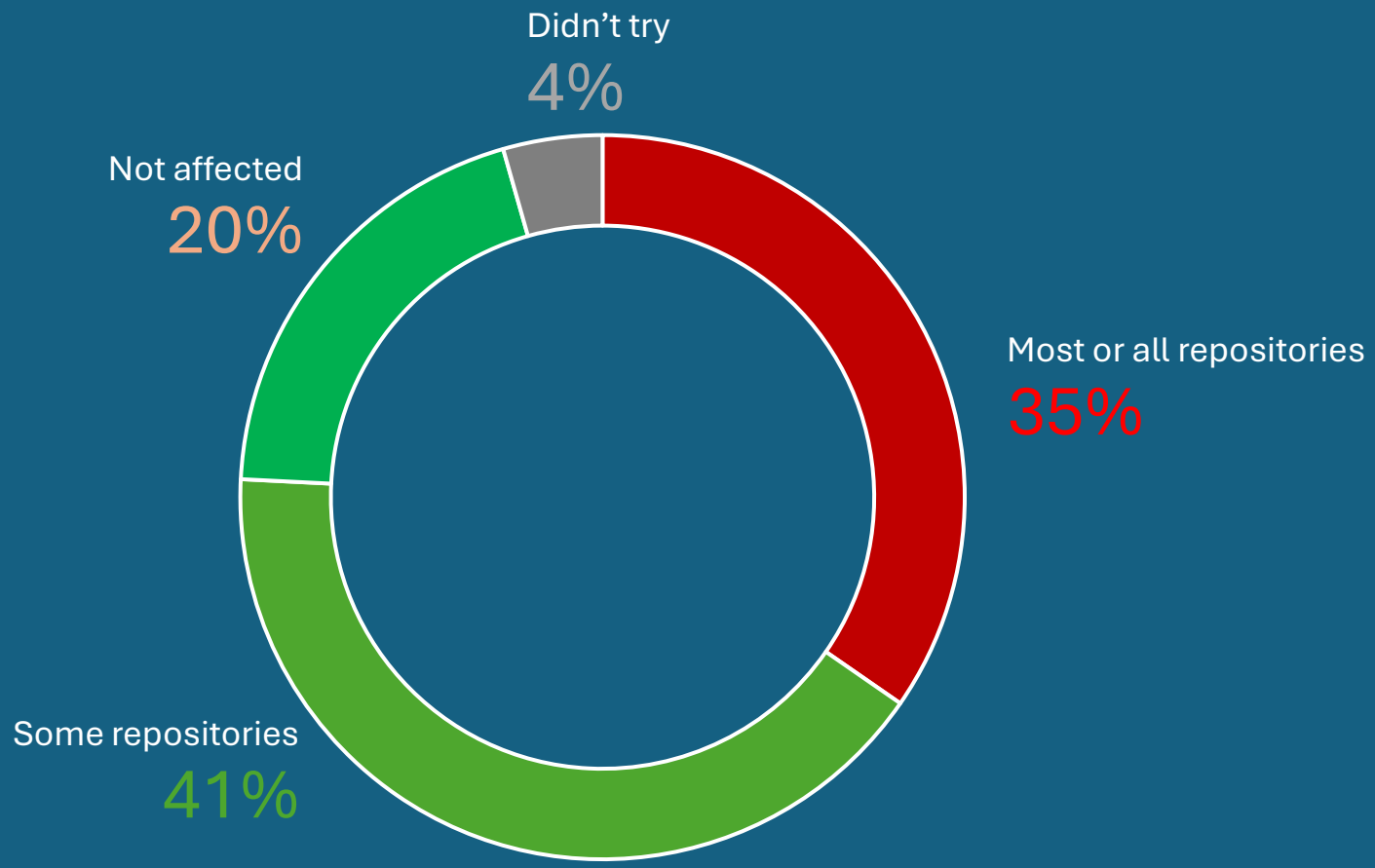
To indemnify the **Named Insured** for:

Cyber Extortion Loss, in excess of the **Retention**, incurred by the **Insured Organization** as a direct result of an **Extortion Threat** first made against the **Insured Organization** during the **Policy Period** by a person, other than the **Insured Organization's** directors, officers, principals, trustees, governors, **Managers**, members, management committee members, members of the management board, partners, or any

The Attack

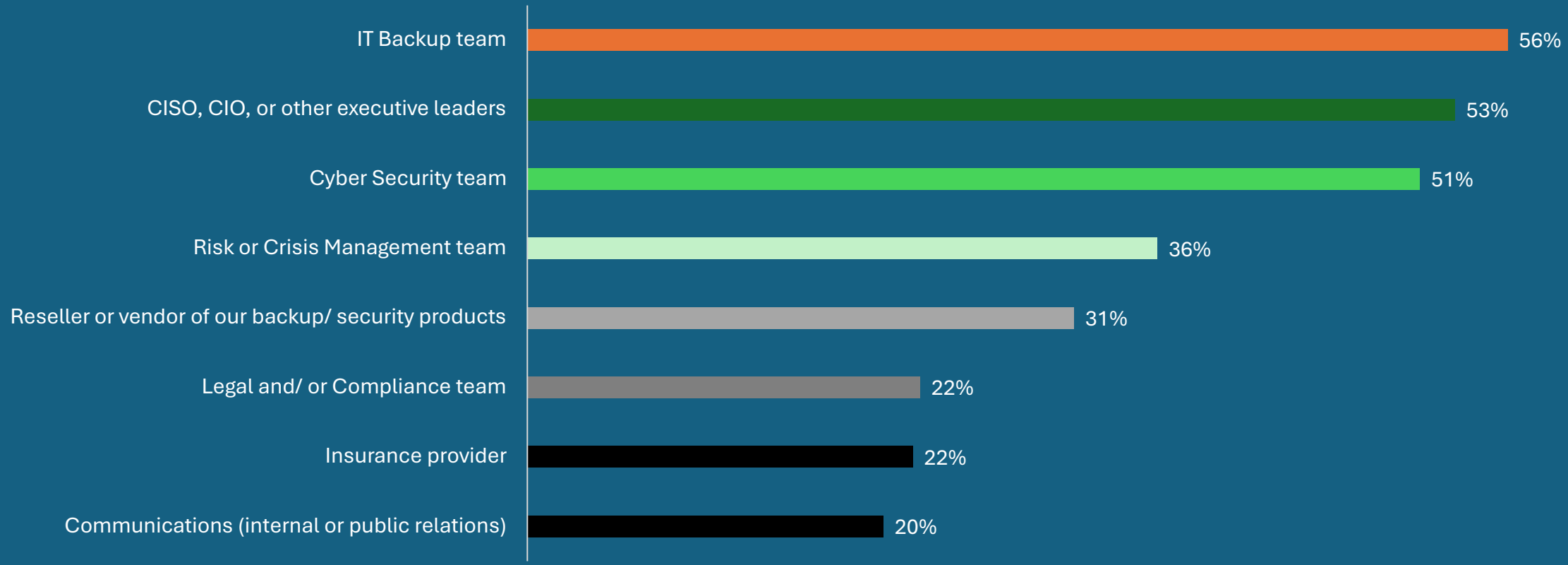
Backup repositories were targeted in 96% of attacks

Did the threat actor attempt to modify/ delete backup repositories as part of the ransomware attack?



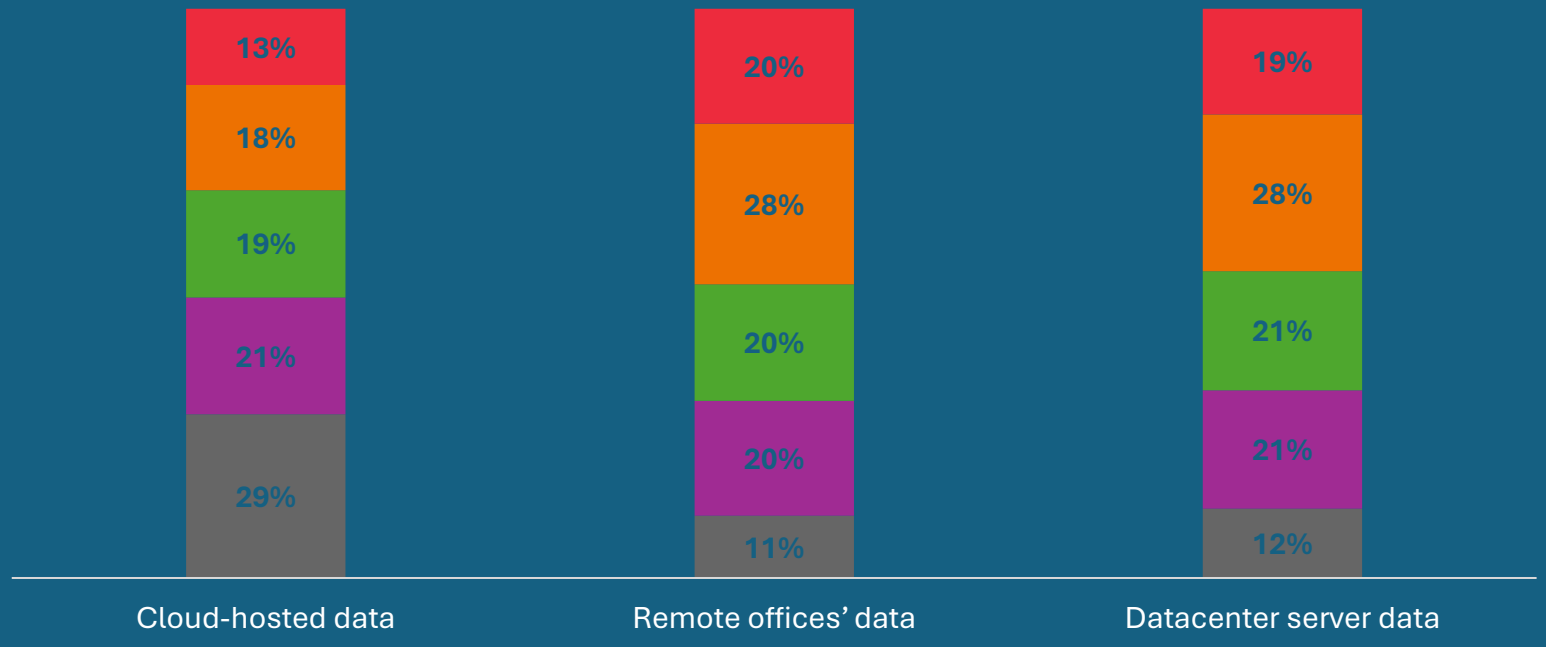
Which teams do you engage first?

When a cyberattack happens in your organization, which teams are among the first to be actively engaged?



All environments are equally vulnerable

How widespread was the ransomware infection
with regard to the amount of data impacted across the following in your organization?



What now?

Q4 November 2024

Ransomware Trends & Future Prevention

Rick Vanover

Veeam Product Strategy

RICKATRON

Veeam is purpose-built for powering data resilience

Quote of the Year

From VeeamON 2024

Words to live by

William Siegel, CEO Coveware by Veeam

"I can tell in the first 15 minutes of a conversation how well or how poorly an incident response is going to progress just based on how prepared an organization presents themselves during the initial phone call."

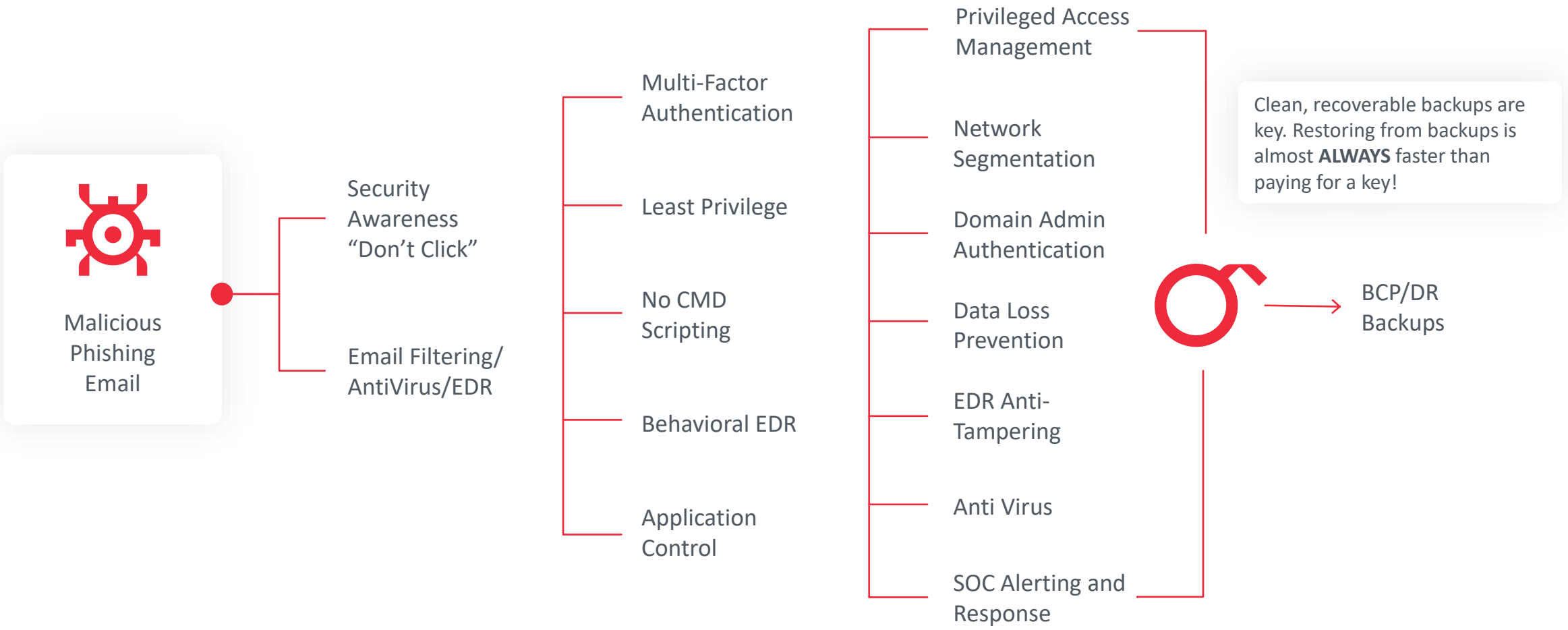
Summarized quote from general session"

Q2 2024
Top 10 Threat Actors

- Based on percentage of cases in Q2 2024
- Groups such as Akira and Black Basta continued to hold a comparable market without a noticeable shift in techniques and behaviors
- Suggesting that not all ransomware brands have opened their doors to displaced affiliates
- Sharp rise in the frequency of Lone Wolf “unaffiliated” extortion attacks

Family Name	% of Cases	Previous Rank
Akira	11%	-
”Lone Wolves”	10%	Unranked
Black Basta	8%	-1
BlackSuit	8%	+1
Lockbit 3.0	7%	-2
Medusa	7%	-1
BianLian	5%	Unranked
Inc Ransom	5%	-1
Phobos	4%	-2
Qilin	3%	Unranked

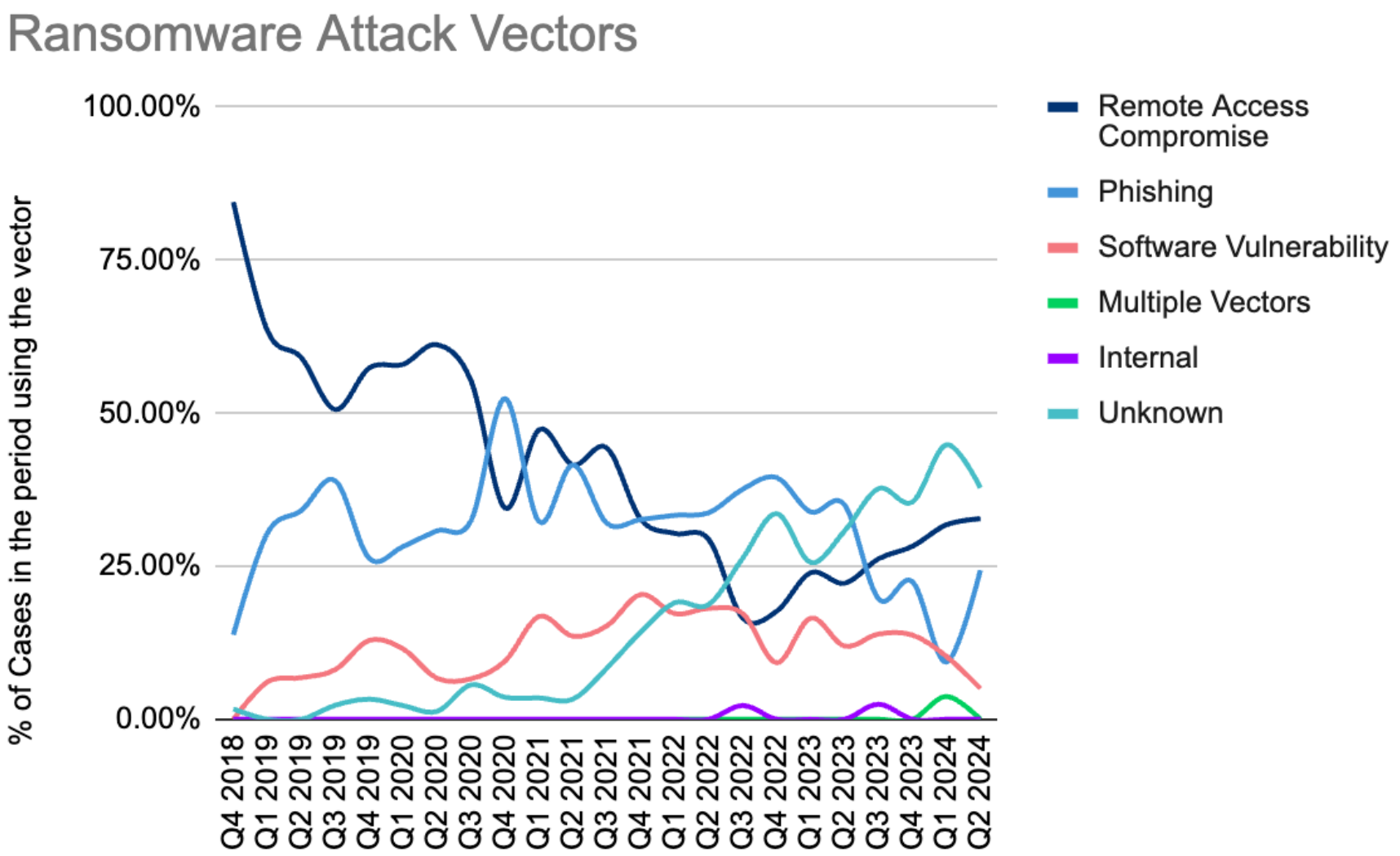
Compounding Failures in the Cyber “Kill Chain”



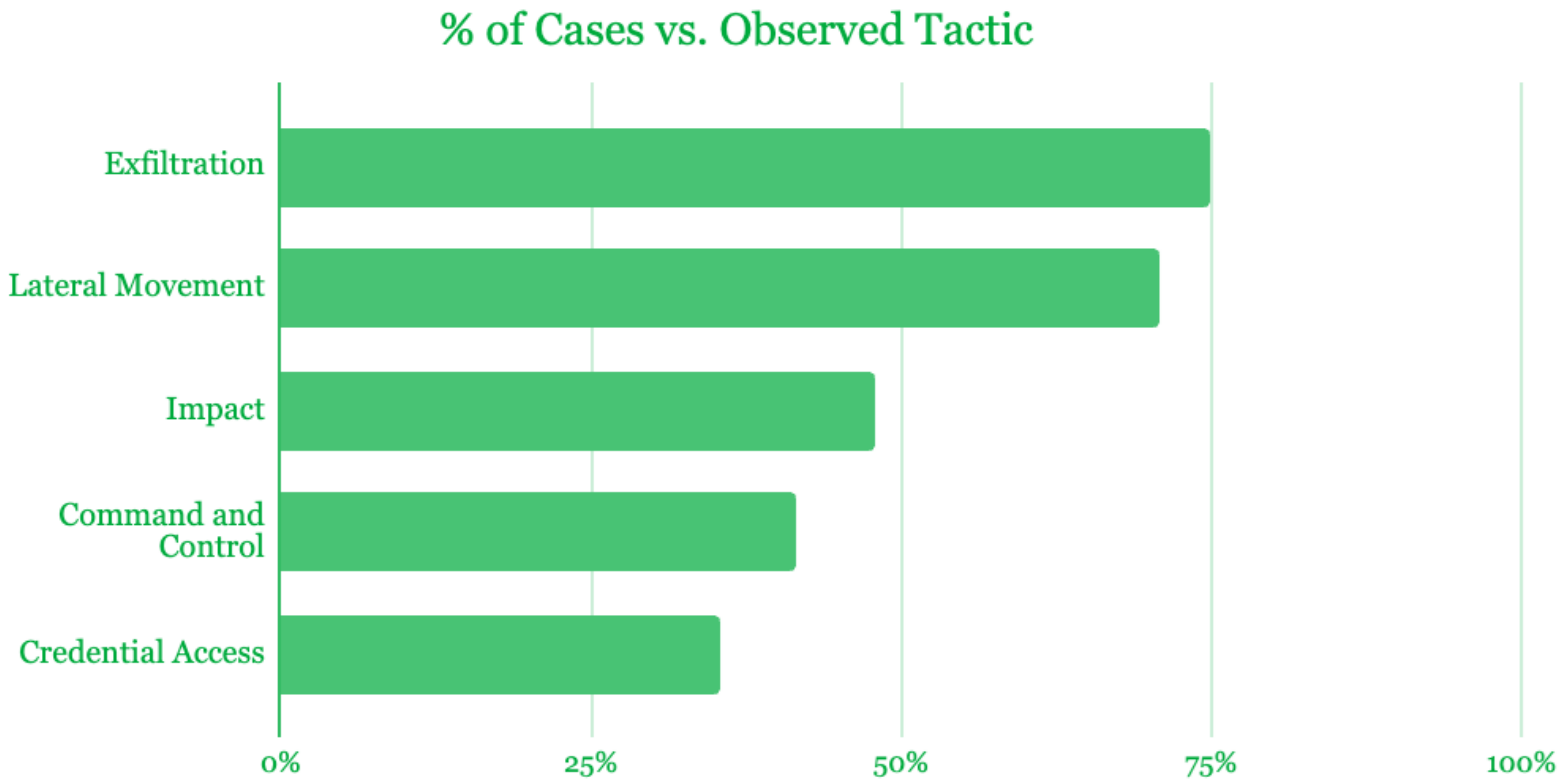
Q2 2024
Initial Access

Purpose:

The adversary is trying to get into your network.



Q2 2024
The Top 5 MITRE Tactics Observed



2024 Trends

Law Enforcement Takedowns and Downstream Effects

Payment Bans and New Regulations

Phantom Attacks and Data Hostage Trading

Increasing Velocity of Critical Vulnerability Exploitation

Continued VMWare ESXi Targeted Attacks and Impact

Aggressive Persistence and Nuclear Options for Eradication

Common Incident Response Lifecycle

1. How do we **know what to do** when it happens?
2. How do we **identify when** it happens?
3. How do we **stop it** from spreading?
4. How do we **eliminate it** from our environment?
5. How do we **remediate** any impacts and **restore** our operations?
6. How do we **learn** from it?

Current Observations from Tech Support

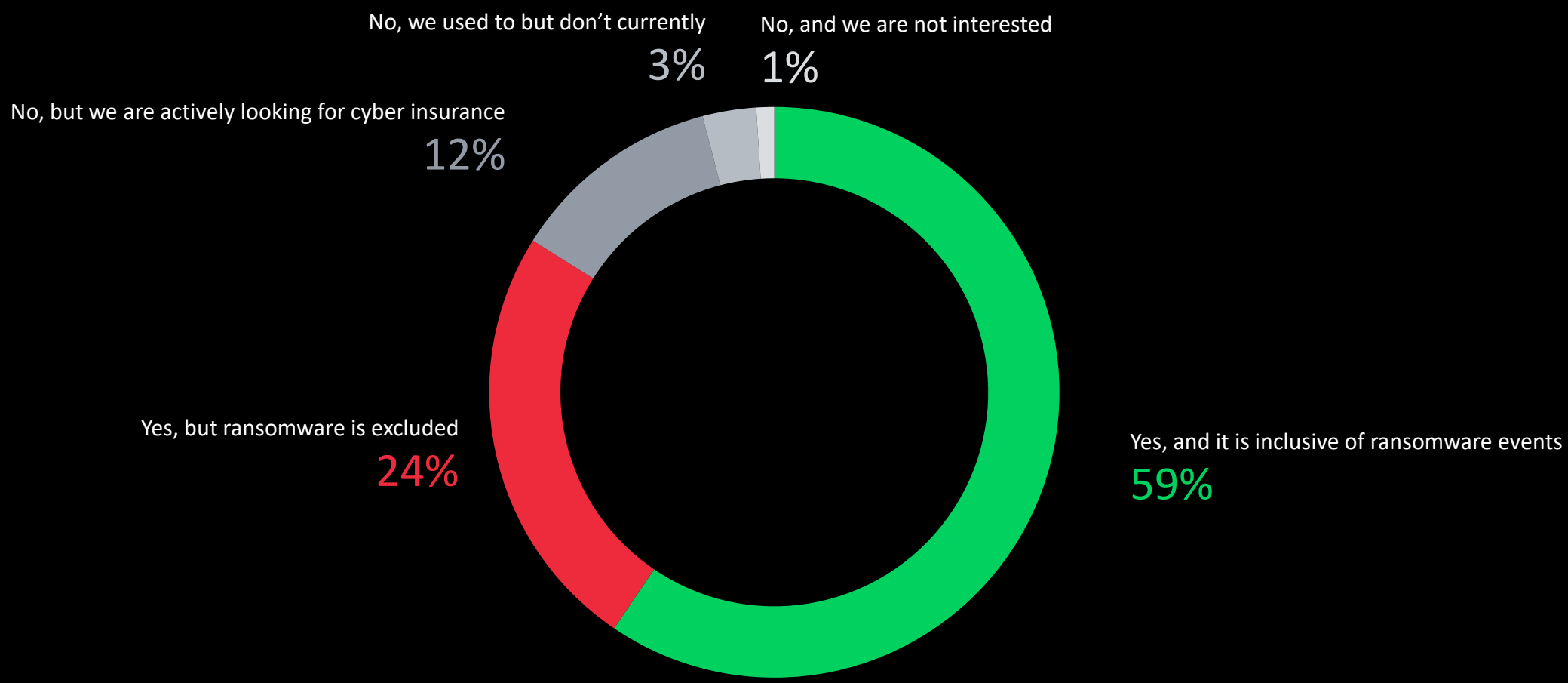
Rogue Deleting of files from threats

EDR/Security Software “Interference”

Direct targeting of Backups

Do you currently have cyber insurance?

Does your organization currently have a cyber insurance policy?



What is some of the most valuable data to a threat actor?

A Cyber Insurance Policy!

5. Aggregate sublimit of liability for all **Cyber Extortion Loss** under **INSURING AGREEMENTS** I.G.:	USD $1,000,000
6. Aggregate sublimit of liability for all **Data Protection Loss** and **Business Interruption Loss** under **INSURING AGREEMENTS** I.H. and I.I.:	USD $1,000,000
7. First Party Business Interruption Sublimits of Liability:	
(1) **Hourly sublimit**:	USD $250,000
(2) **Forensic Expense sublimit**:	USD $250,000
(3) **Dependent Business Interruption sublimit**:	USD $250,000

The above sublimits of liability are part of, and not in addition to, the overall **Policy Aggregate Limit of Liability.**

This Endorsement is attached to and forms a part of Policy Number [redacted]
[redacted] Insurance Company, Inc. referred to in this endorsement as either the "Insurer" or the "Underwriters"

FIRST PARTY COMPUTER SECURITY COVERAGE ENDORSEMENT

This endorsement modifies insurance provided under the following:

[redacted] RESPONSE SELECT

In consideration of the premium charged for this Policy, it is hereby understood and agreed that:

1. Item 3.A. of the Declarations is amended to add the following:

5. Aggregate sublimit of liability for all **Cyber Extortion Loss** under **INSURING AGREEMENTS** I.G.:	USD $1,000,000
6. Aggregate sublimit of liability for all **Data Protection Loss** and **Business Interruption Loss** under **INSURING AGREEMENTS** I.H. and I.I.:	USD $1,000,000
7. First Party Business Interruption Sublimits of Liability:	
(1) **Hourly sublimit**:	USD $250,000
(2) **Forensic Expense sublimit**:	USD $250,000
(3) **Dependent Business Interruption sublimit**:	USD $250,000

The above sublimits of liability are part of, and not in addition to, the overall **Policy Aggregate Limit of Liability.**

2. Item 3.A.1. of the Declarations is amended to include **INSURING AGREEMENTS** I.G. (**Cyber Extortion**), I.H. (**First Party Data Protection**) and I.I. (**First Party Network Business Interruption**) within the **Policy Aggregate Limit of Liability** set forth therein.

3. Item 4. of the Declarations is amended to add the following:

F. **INSURING AGREEMENTS** I.G.: Each **Extortion Threat** Retention	USD $2,500
G. **INSURING AGREEMENTS** I.H.: Each **Security Breach** Retention	USD $2,500
H. **INSURING AGREEMENTS** I.I.: Each **Security Breach** Retention	
(1) Income Loss:	USD $2,500
(2) Extra Expense:	USD $2,500
I. **INSURING AGREEMENTS** I.I.: **Waiting Period**	10 Hours

4. Clause **I. INSURING AGREEMENTS**, is amended to add the following:

G. **Cyber Extortion**

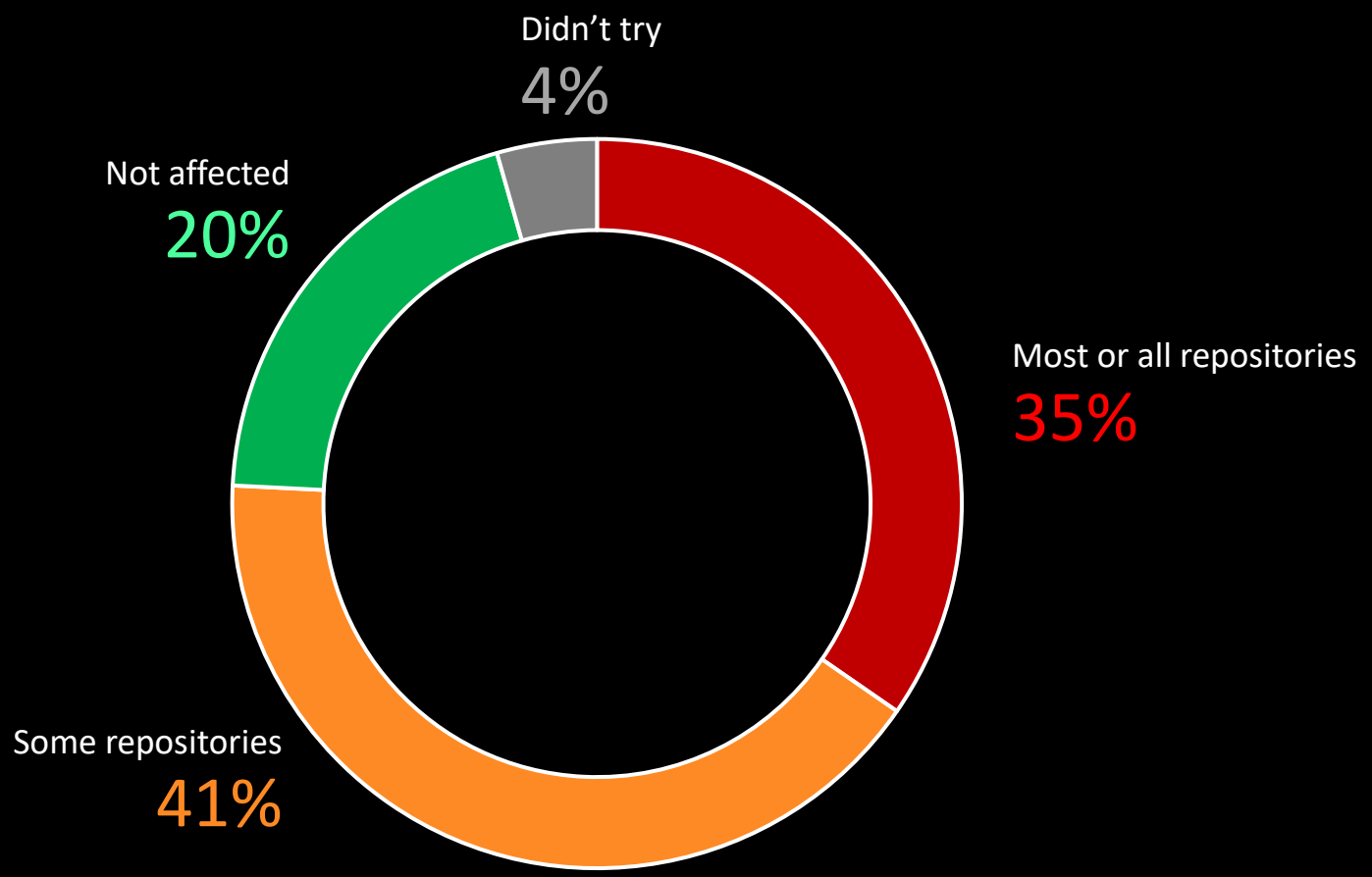
To indemnify the **Named Insured** for:

Cyber Extortion Loss, in excess of the **Retention**, incurred by the **Insured Organization** as a direct result of an **Extortion Threat** first made against the **Insured Organization** during the **Policy Period** by a person, other than the **Insured Organization's** directors, officers, principals, trustees, governors, **Managers**, members, management committee members, members of the management board, partners, or any

The Attack

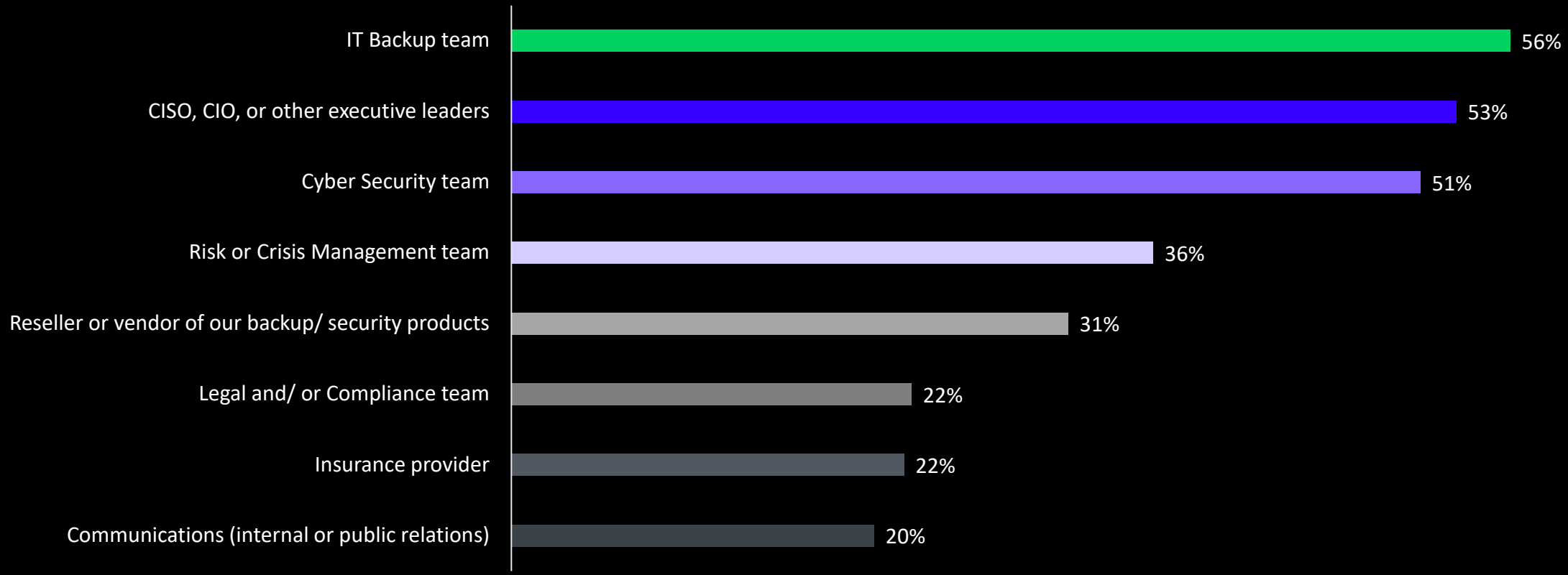
Backup repositories were targeted in 96% of attacks

Did the threat actor attempt to modify/ delete backup repositories as part of the ransomware attack?



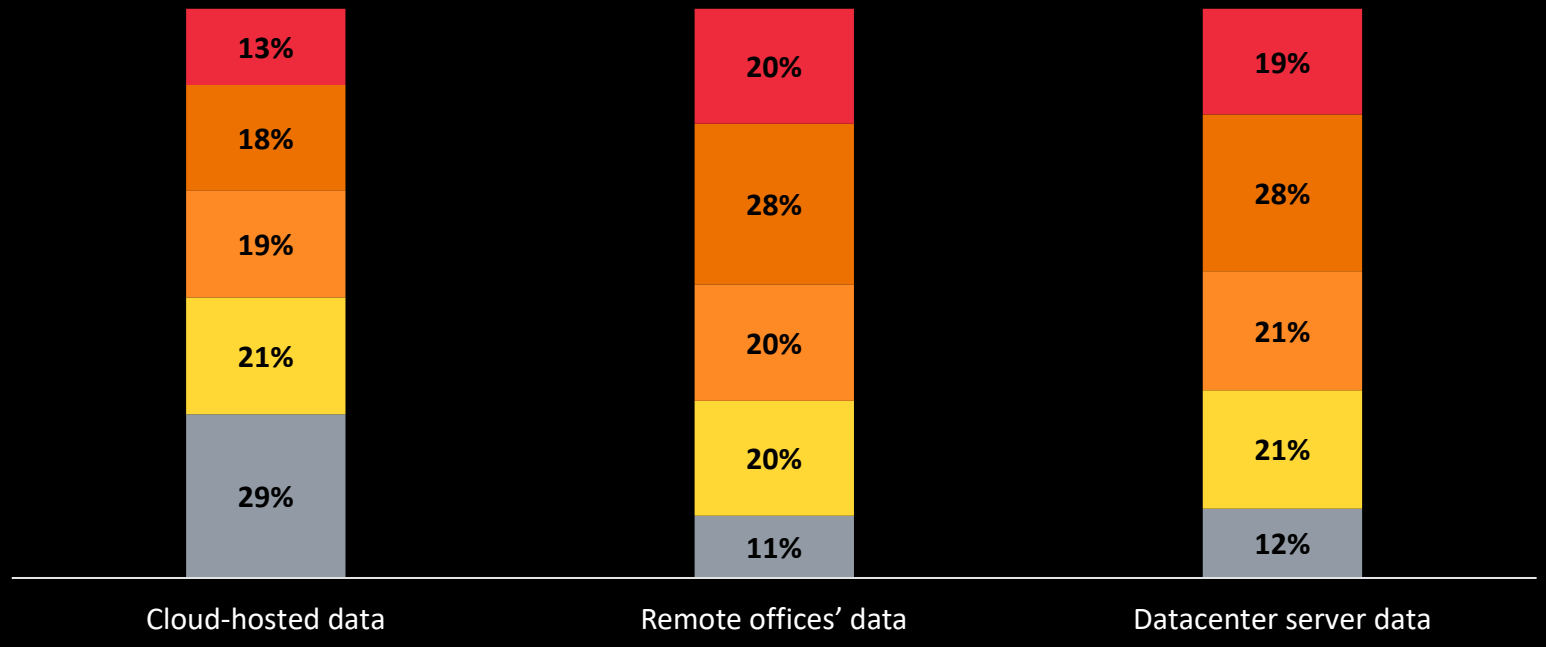
Which teams do you engage first?

When a cyberattack happens in your organization, which teams are among the first to be actively engaged?



All environments are equally vulnerable

How widespread was the ransomware infection
with regard to the amount of data impacted across the following in your organization?



What now?