The Executive Cyber Viewpoint

avertro
The cyber-why company

Ian Yip | Founder & CEO, Avertro

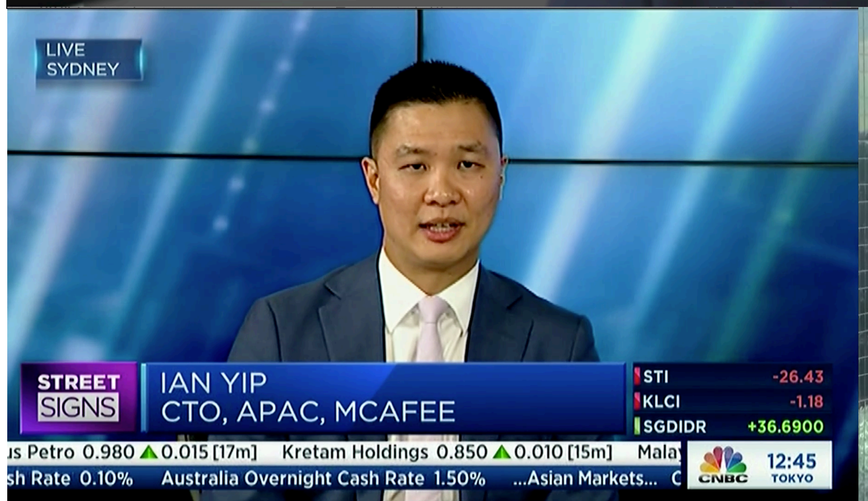
20+ years of cybersecurity experience. UNSW CSE Graduate.

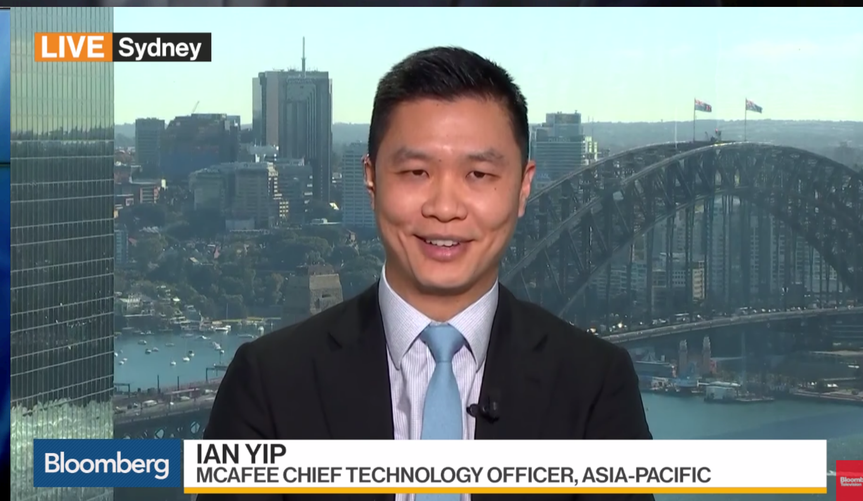
Currently also

- Advisory Board Member, UNSW Institute for Cyber Security
- Advisory Board Member, UTS Faculty of Engineering and IT

Previously

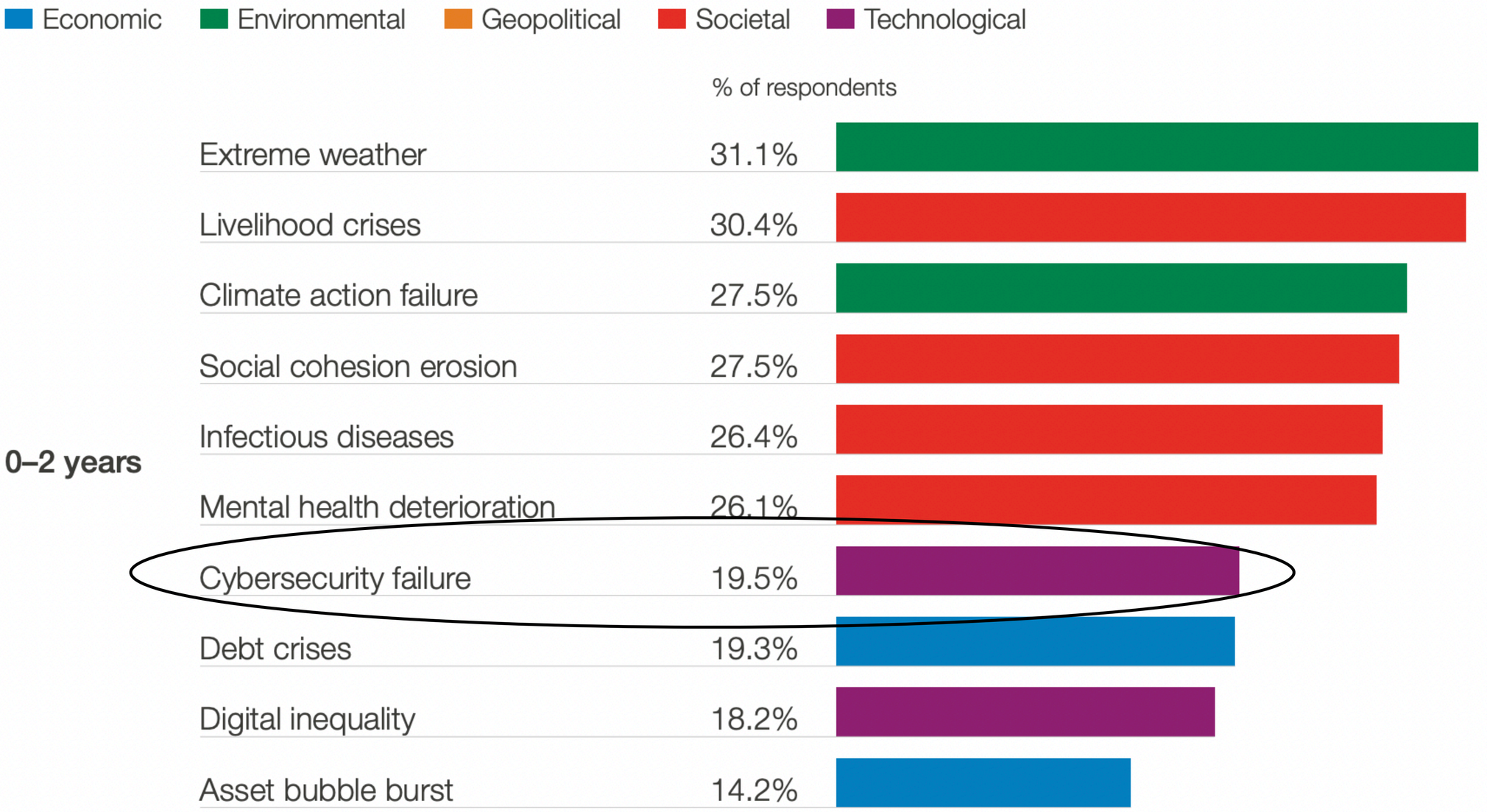
- Chief Technology Officer, APAC
- Director, Cybersecurity





Global Risks Horizon

When will risks become a critical threat to the world?



Source: World Economic Forum Global Risks Report 2022

Global cost of cybercrime (USD)

$6 Trillion	$10.5 Trillion
2021	2025

Measured as a country, cybercrime would currently be the world's third-largest economy after the U.S. and China.

By 2025, cybercrime will be exponentially larger than the damage inflicted from natural disasters in a year, and more profitable than the global trade of all major illegal drugs combined.

Source: Cybersecurity Ventures

What do cybercriminals earn annually (USD)?

$1,992,000
High earners

$900,000
Middle earners

$42,000
Low earners

Source: Dr. Mark McGuire – Into the Web of Profit study

For a price, anyone can become a cybercriminal

Product/Service	Price (USD)
SMS Spoofing	$20 / month
Custom Spyware	$200
Hacker for Hire	Starts at $200
Malware Exploit Kit	$200 - $700
Zero-Day Adobe Exploit	$30,000
Zero-Day iOS Exploit	$250,000

Source: Dr. Mark McGuire – Into the Web of Profit study

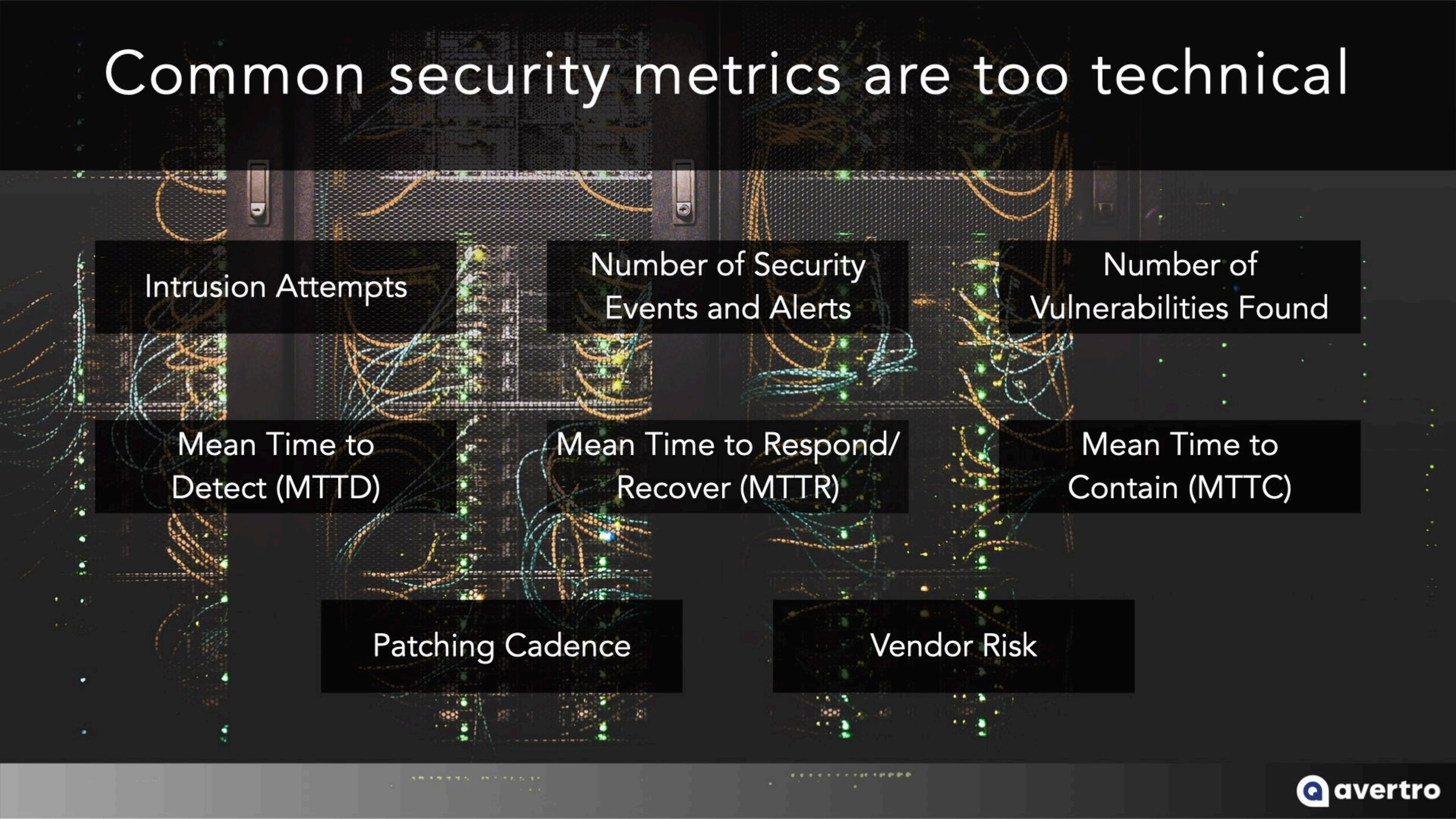
"It (the NotPetya cyber incident) cost us between $250 to $300 million. It is time to stop being naive when it comes to cybersecurity."

Jim Hagemann Snabe
Chairman, A.P. Moller Maersk

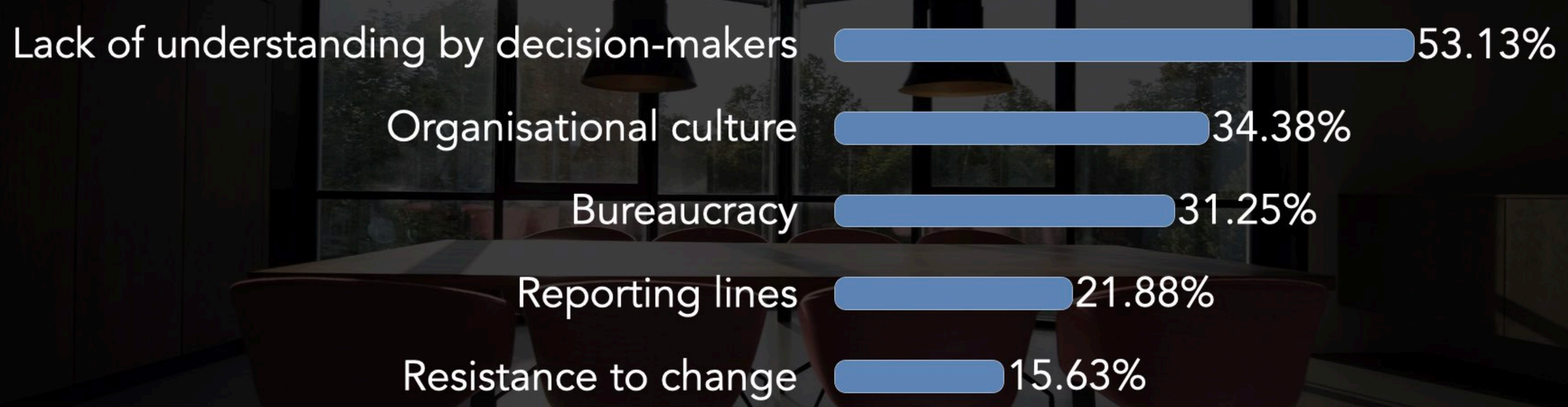
avertro


Cybersecurity is a board and executive-level issue today
But there is a communication disconnect between the cyber team and everyone else
avertro

Common security metrics are too technical



Biggest challenges when requesting funding for strategic & transformative initiatives



Source: Avertro Cyber Leadership Effectiveness Study 2021

Board & C-suite attitude towards managing cyber risk

Respondents who selected:

- Lack of understanding by decision-makers
- Organisational culture
- Bureaucracy

Source: Avertro Cyber Leadership Effectiveness Study 2021

How can we improve Cyber Leadership Effectiveness?

avertro


For boards and executives, cybersecurity
is really all about managing risk

avertro

Are these business or technical risks?

There are 500 vulnerabilities in our cloud infrastructure that need to be addressed.

Our fleet of servers in the data centre have not been patched for 3 months.

Cyber risks at the executive level are not technical

Always ask: “So what?”

There are 500 vulnerabilities in our cloud infrastructure that need to be addressed. So what?

Answer: This technical risk increases the following business risk - **Exfiltration of sensitive data** stored in our cloud resulting in regulatory fines.

Cyber risks at the executive level are not technical

Always ask: “So what?”

Our fleet of servers in the data centre have not been patched for 3 months. So what?

Answer: This technical risk increases the following business risk - **System unavailability** as a result of a malicious cyber attack resulting in the inability to process customer financial transactions.

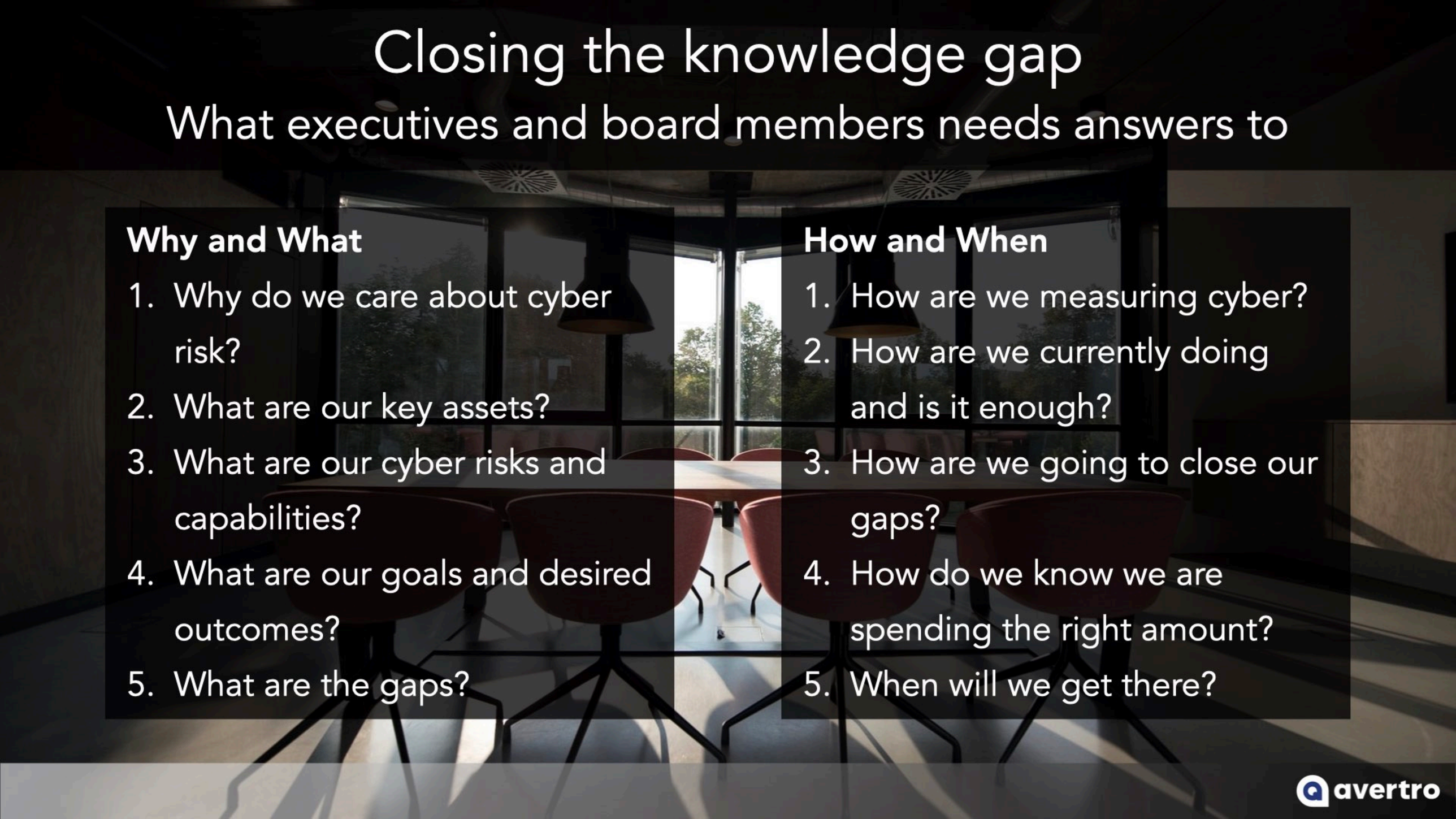
Executives and board members only care about the business risks

Data Breach Risk: Exfiltration of sensitive data stored in our cloud resulting in regulatory fines.

System Availability Risk: System unavailability as a result of a malicious cyber attack resulting in the inability to process customer financial transactions.

Closing the knowledge gap

What executives and board members needs answers to



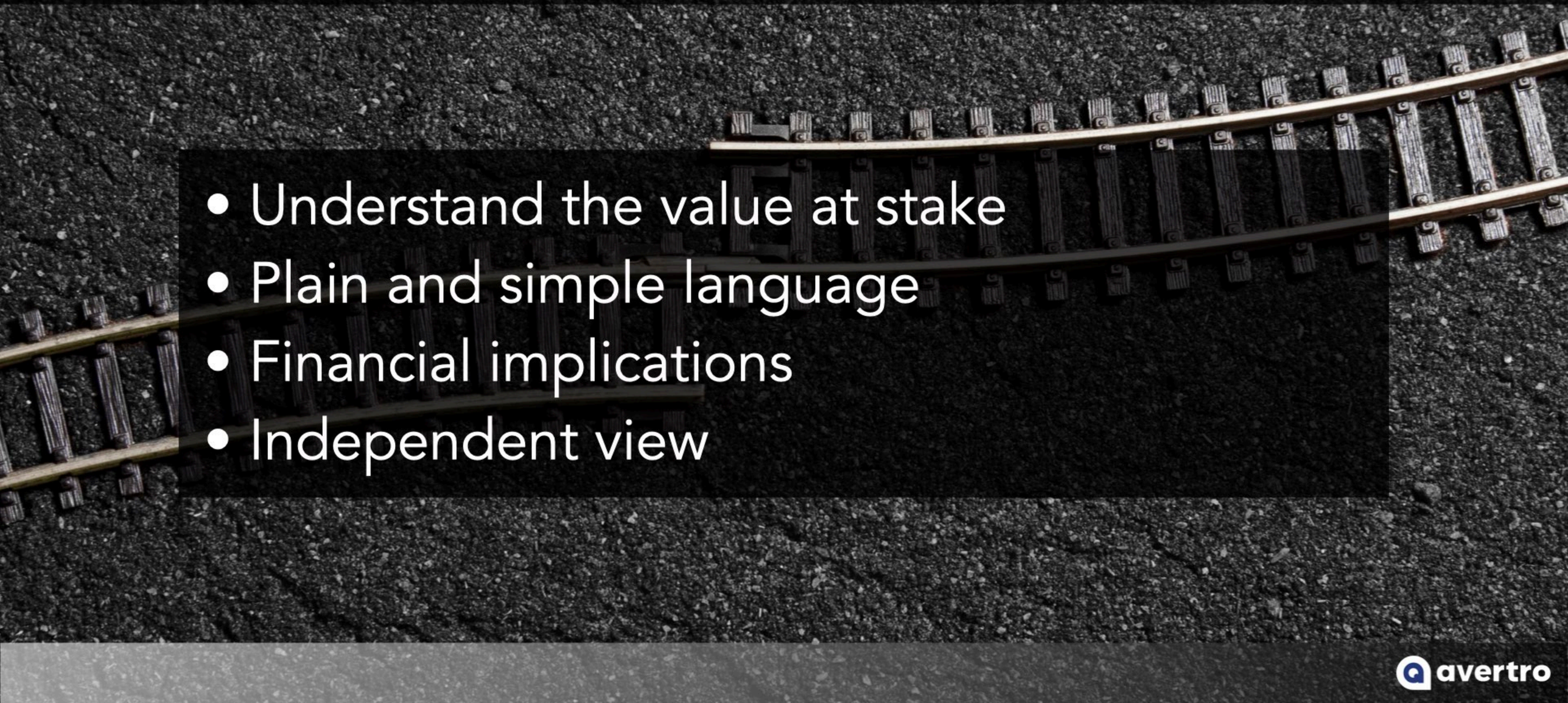
Why and What

1. Why do we care about cyber risk?
2. What are our key assets?
3. What are our cyber risks and capabilities?
4. What are our goals and desired outcomes?
5. What are the gaps?

How and When

1. How are we measuring cyber?
2. How are we currently doing and is it enough?
3. How are we going to close our gaps?
4. How do we know we are spending the right amount?
5. When will we get there?

Closing the knowledge gap



- Understand the value at stake
- Plain and simple language
- Financial implications
- Independent view

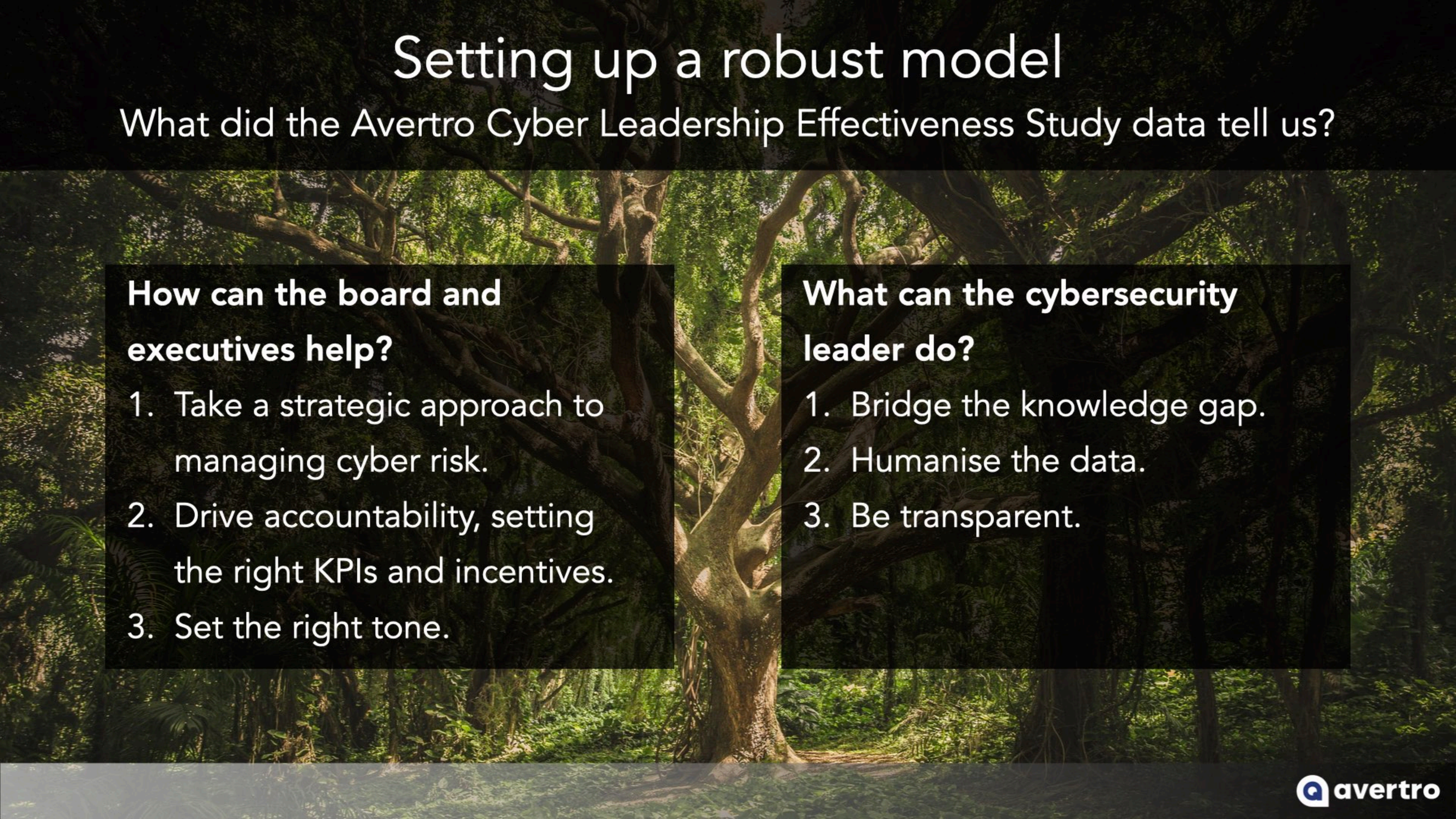
avertro


How do you better **empower** business executives to ask the **right questions** when it comes to **cybersecurity**?

avertro

Setting up a robust model

What did the Avertro Cyber Leadership Effectiveness Study data tell us?



How can the board and executives help?

1. Take a strategic approach to managing cyber risk.
2. Drive accountability, setting the right KPIs and incentives.
3. Set the right tone.

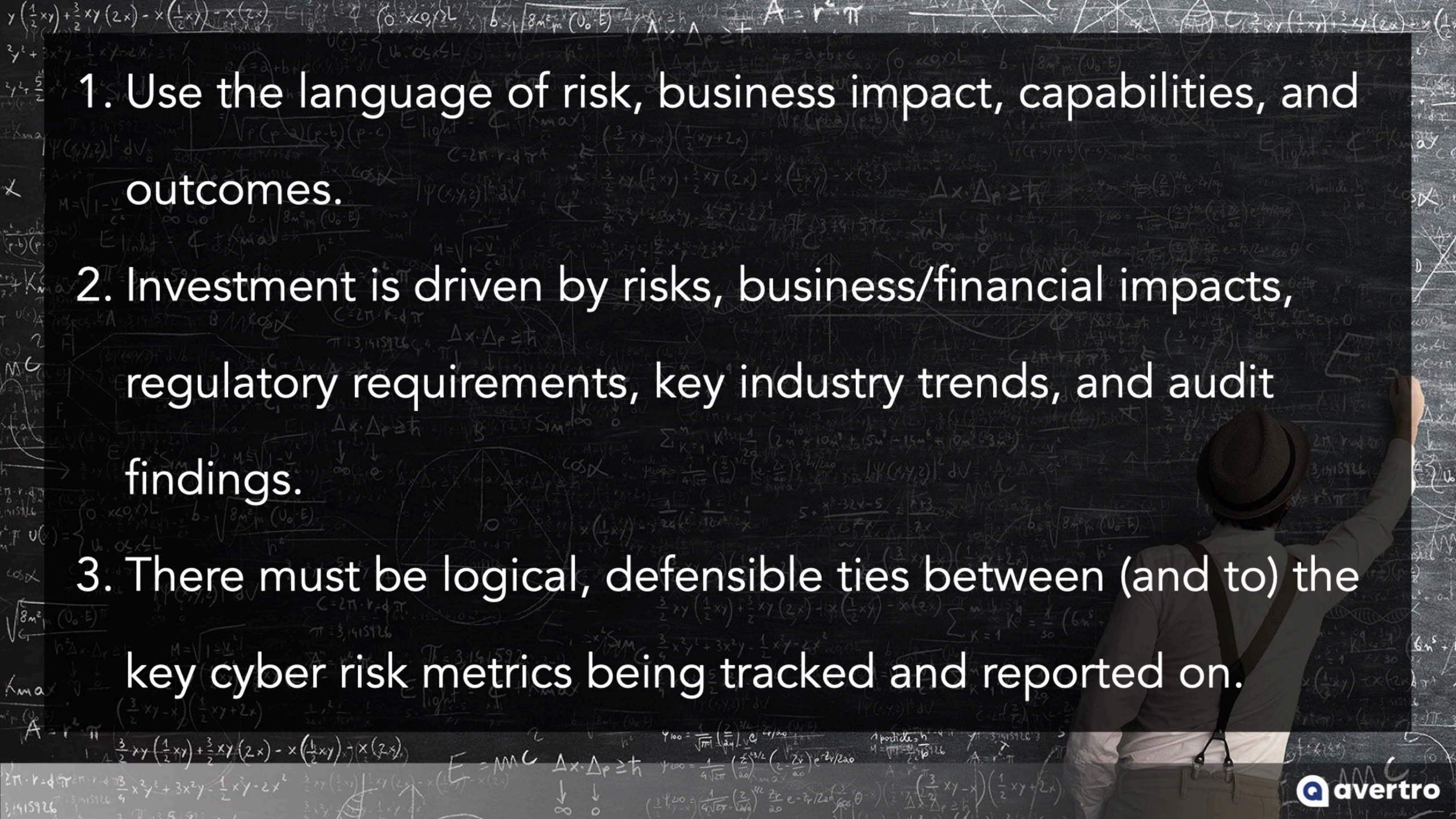
What can the cybersecurity leader do?

1. Bridge the knowledge gap.
2. Humanise the data.
3. Be transparent.

Key Takeaways

avertro

1. Use the language of risk, business impact, capabilities, and outcomes.
2. Investment is driven by risks, business/financial impacts, regulatory requirements, key industry trends, and audit findings.
3. There must be logical, defensible ties between (and to) the key cyber risk metrics being tracked and reported on.



avertro