



Cybersecurity and Pandemic

Cybersec and Risk Management as Business Differentiators



What is a pandemic?



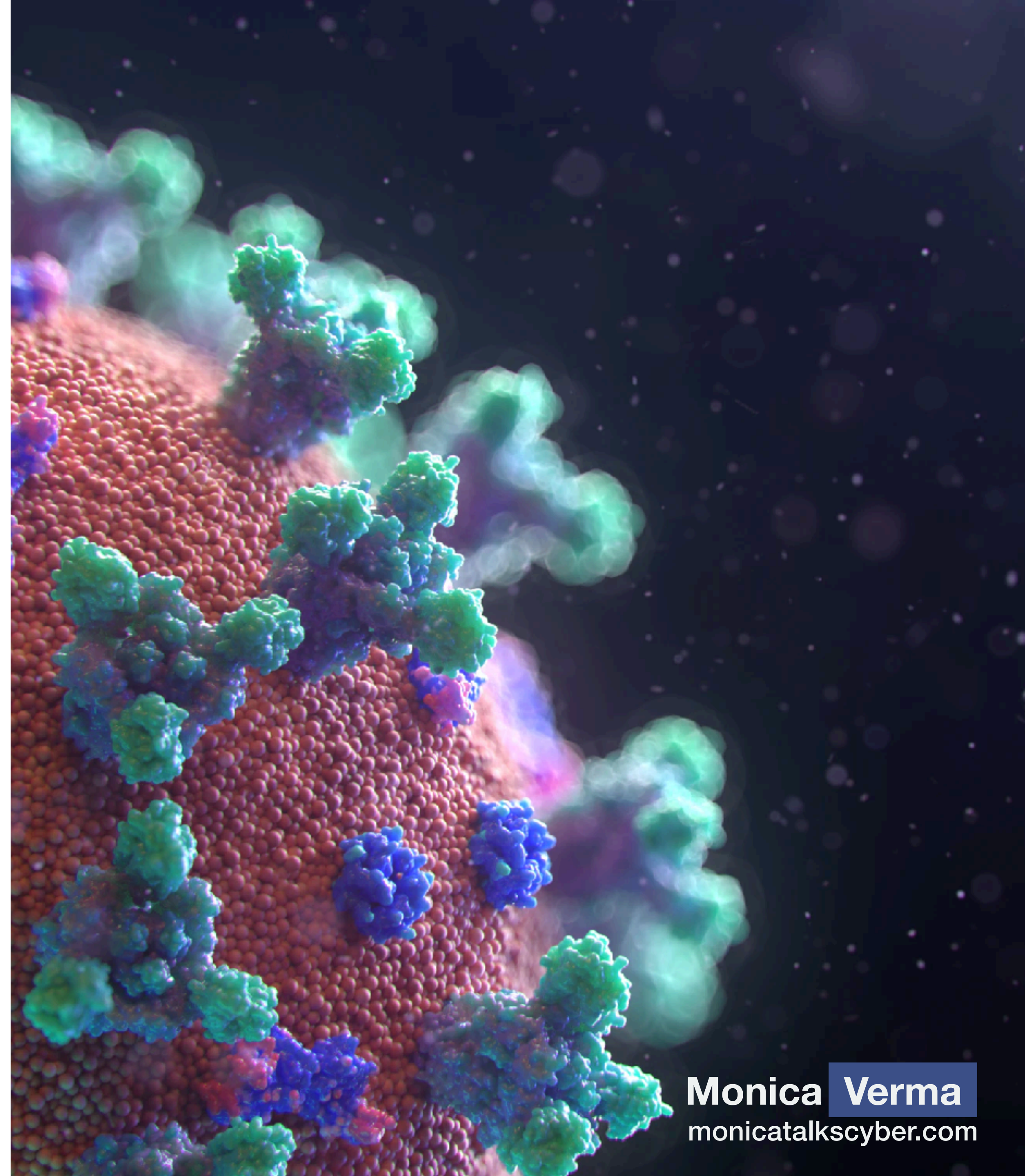
Global Outbreak World Crisis





Pandemic

A few challenges





Globalization Interconnection Lack of Immunity Unknowns



Cybersecurity

Similarities to a Pandemic



Globalization Interconnection Lack of Immunity Unknowns



The Cybersecurity and Infrastructure Security Agency (CISA) has

- a) received multiple reports of**
- b) advanced persistent threat (APT) actors**
- c) actively exploiting trust relationships in information technology (IT) service provider networks**
- d) around the world**—such as managed service providers (MSPs) and cloud service providers (CSPs)—has increased in recent years.

2018 CISA, Department of Homeland Security



APT10 Cloud Hopper

Cloud Hopper - 2017

“APT10 has recently unleashed a sustained campaign against MSPs. The compromise of MSP networks has provided broad and unprecedented access to MSP customer networks.”

“PwC UK and BAE Systems assess APT10 as highly likely to be a China-based threat actor.”

PwC, Operation Cloud Hopper



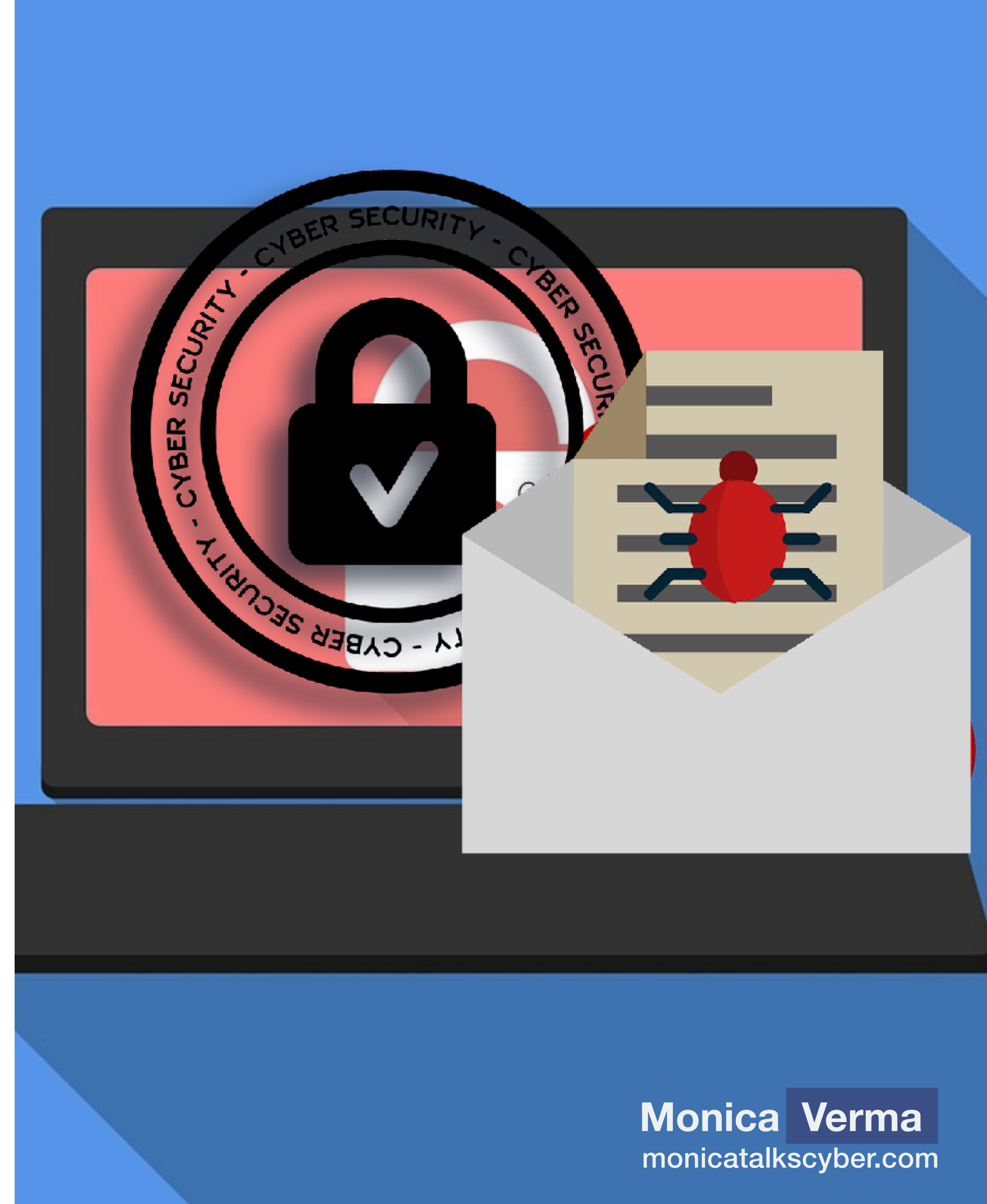


Advanced Phishing Campaign

WIPRO - 2019

“We detected a potentially abnormal activity in a few employee accounts on our network due to an advanced phishing campaign. Upon learning of the incident, we promptly began an investigation, identified the affected users and took remedial steps to contain and mitigate any potential impact,”

Wipro 2019





Maze Ransomware

Cognizant MSP Attack - 2020

“Cognizant can confirm that a security incident involving our internal systems, and causing service disruptions for some of our clients, is the result of a Maze ransomware attack,”

Cognizant, 2020





Globalization Interconnection Lack of Immunity Unknowns



**Adapt
Adjust
Build resilience
Understand
technological disruptors**





One of the best defenses against
cybersecurity threats is
Cyber Resilience.

— Monica Verma





1. Building Immunity Resilience



Cyber Resilience



1. Cyber Resilience

Cybersecurity + Business Resilience

Anticipate Chaos! Be Prepared!

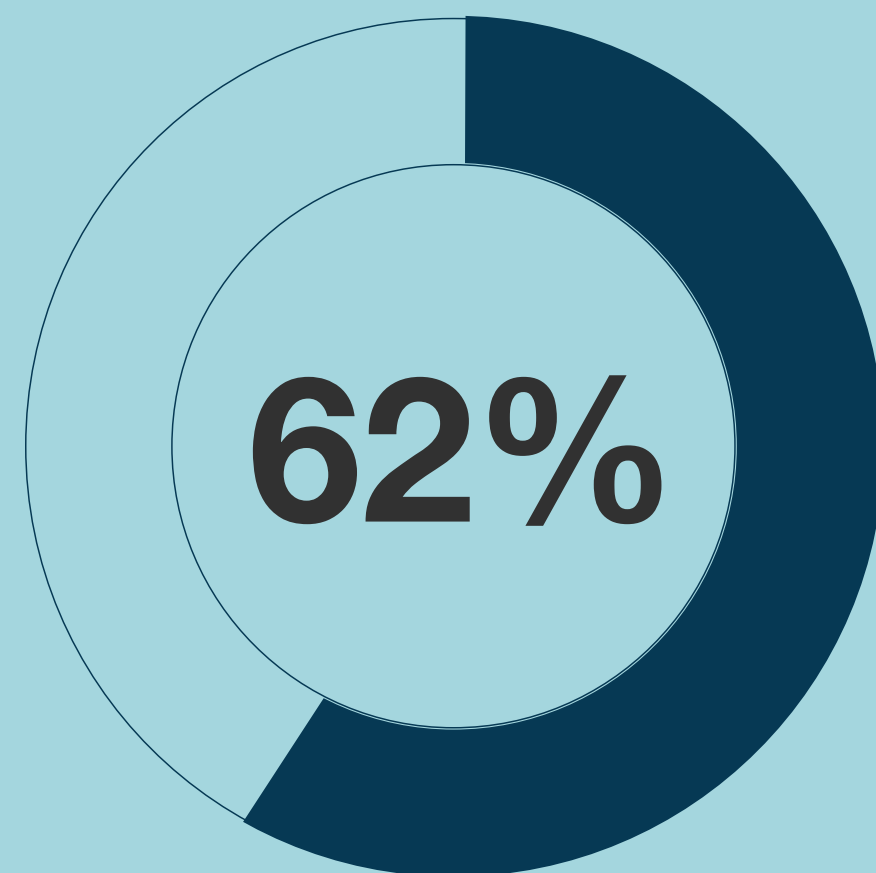
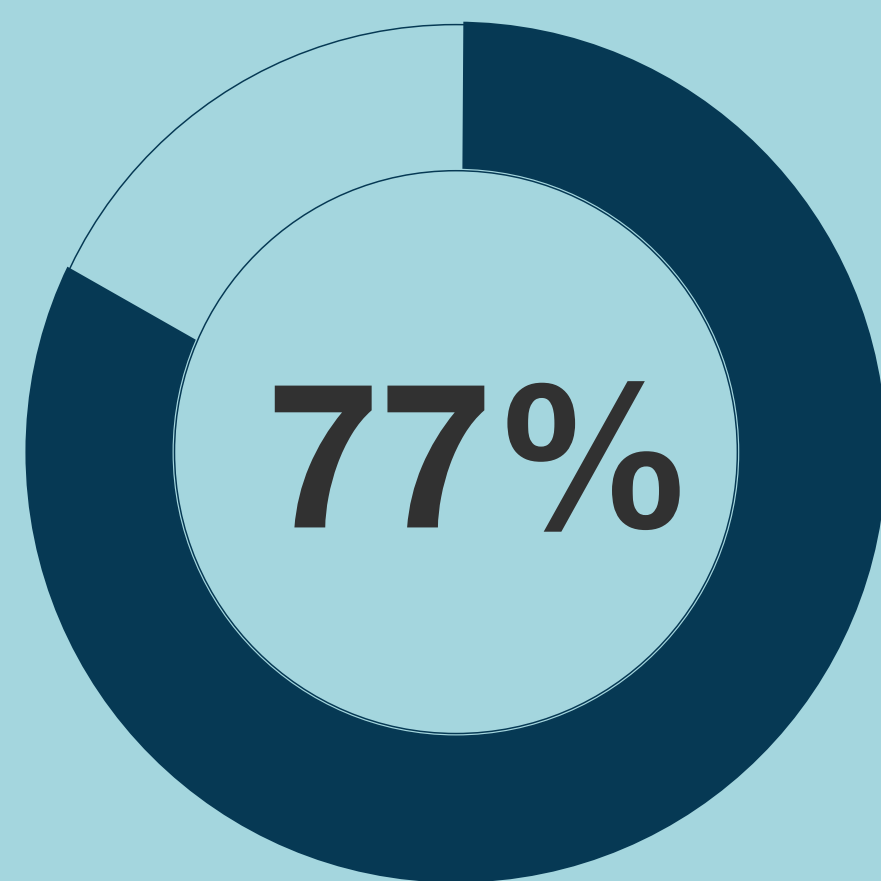
Critical to understand the threat landscape and the cybersecurity risks you face

Resilience happens when you are better able to detect, contain, respond to and adapt to cyber attacks, whilst continuing normal business operations.





1. Cyber Resilience



Source: IBM Study

77 percent of firms surveyed lack proper cyber resilience plans

Only 44 percent of respondents believe their organizations' leaders recognize that enterprise risks affects cyber resilience

62 percent of respondents say risk assessment is a critical element to cyber resilience plans



Cyber Resilience

Anticipate Chaos!
Be Prepared!



2. Risk Quantification

Understanding the Exposure



Risk Quantification



2. Risk Quantification

Financial estimation of a cyber risk impact including financial, business and reputational impact, in order to

- a) understand risk exposure
- b) ensure right security investment at right time





The risk I took was calculated,
.....but man, I am bad at math.



**Cyber Risk
Management:
A part of
Enterprise Risk
Management**

**Clear and Well-
Defined Risk
Appetite and
Tolerances**

**The True Cost
of a Cyber
Incident**

**Right
Expertise.

Right
Competency.**



Categorization
Key Scenarios
and Key Cyber
Risks

Threat Factor
Capability and
Motivation

Monetary Loss
(Range of)
Amount of loss
with ca. 90%
certainty

Subjective BUT
numeric
(amount or
range)



3. Testing and Verification



3. Testing and Verification

Testing BCP, cyber resilience plans, security incident and crisis management plans

Verify - Treat all accesses as unauthorized unless and until identified, authorized and verified.

Verifications policies independent of working from office or from home.





4. Increase Visibility Constant and Consistent



Business Differentiator Key Elements





Differentiator

Something that differentiates!
Gives you competitive edge!



Not just a matter of if and
when, but

how long?
how much impact?
how to contain?
how to invest?
how to continue?
how to adapt?
how to predict?

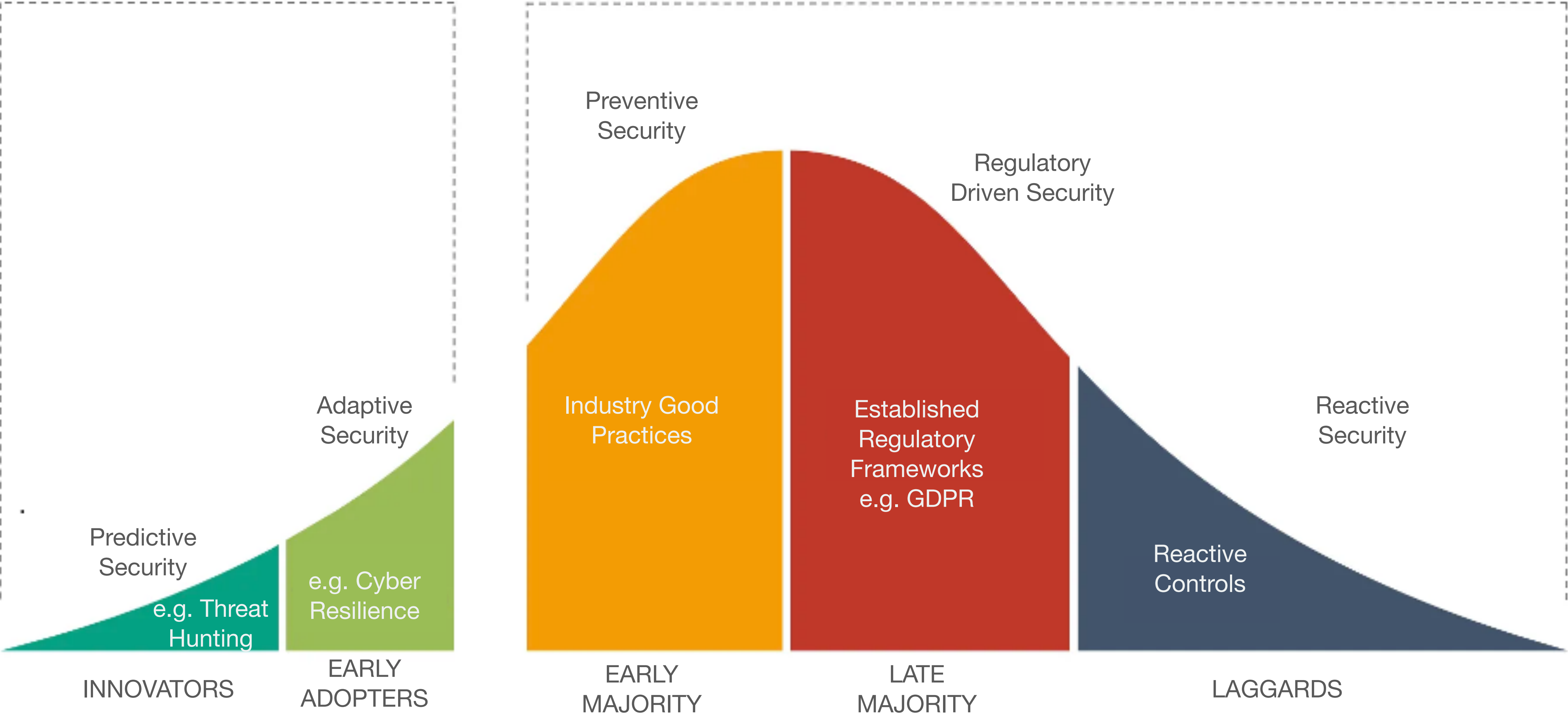




EARLY MARKET

THE CHASM

MAINSTREAM MARKET



©Monica Verma May 2020 Adapted From The Technology Adoption Lifecycle



Next Steps

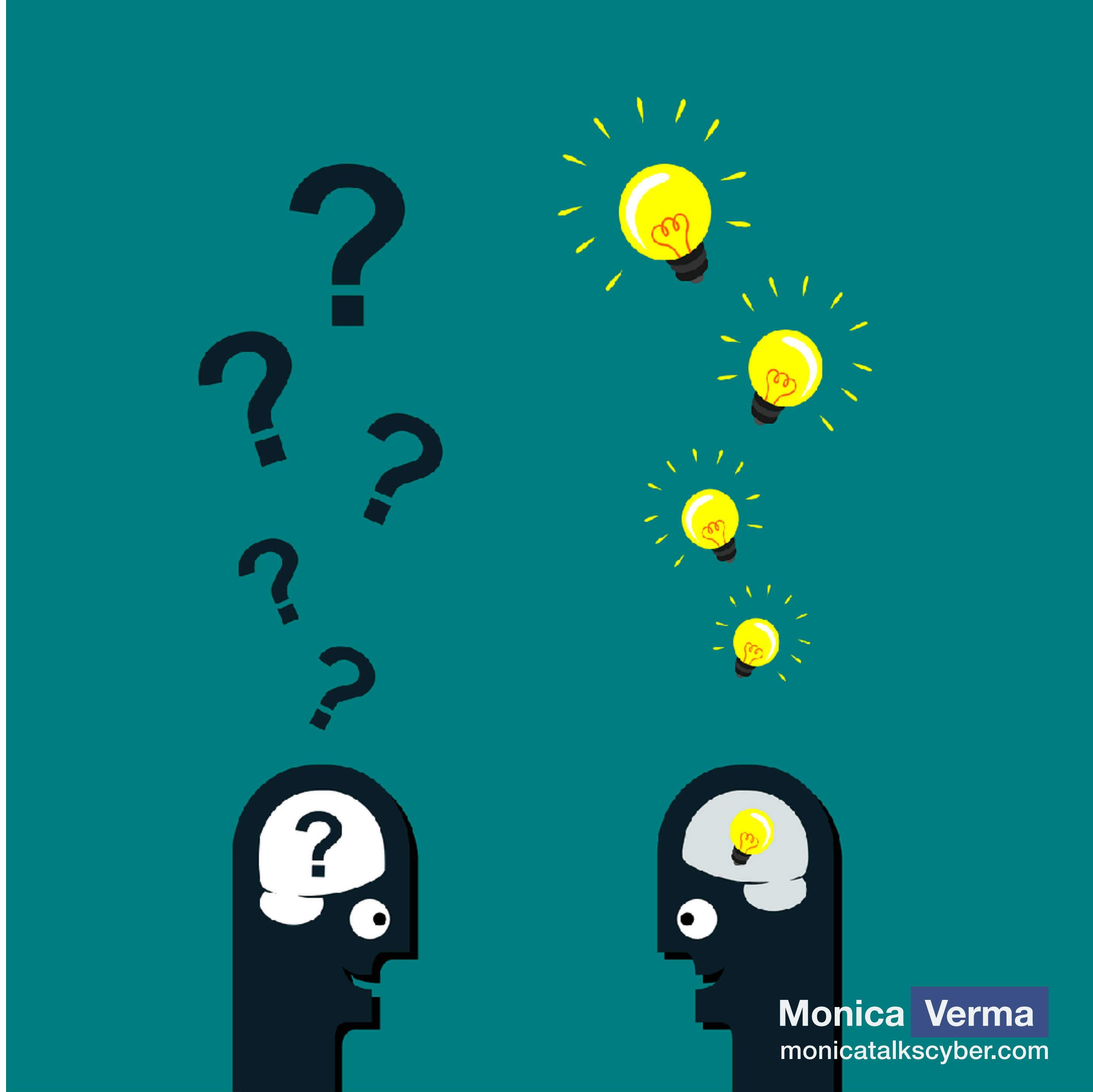
Linking to Risk Assessment (RoS analyse) to select a position in curve?

What type of business should be in which part of the curve?

What kind of typical vulnerabilities will hit businesses in the different phases?

What business benefits are associated with being a specific position in the curve?

What type of investment is required for the different phases?





MONICA VERMA

THE BLOG ON ALL THINGS CYBER

Speaker, CISO, 2019-OSPA Winner, Board
Member CSA & Women In Cybersecurity





“In today’s digital landscape, cyber risk is not only an enterprise risk but also a systemic risk.”

Monica Verma, Chief Information Security Officer (CISO)
Board Member, Cloud Security Alliance Norway