Being Resilient. That's Live Enterprise

Security in the era of remote working

Mohit Joshi
President, Infosys

Vishal Salvi
CISO & Cybersecurity
Unit Head, Infosys

Dr. Martijn Dekker
CISO, ABN AMRO Bank

Infosys®
Navigate your next

POLL 1

What percentage of employees in your organization are working remotely today?

1. Less than 60%
2. Between 60-80%
3. Between 81-90%
4. Greater than 90%

Security in the era of remote working

Vishal Salvi
CISO & Cybersecurity Unit Head, Infosys

Infosys®
Navigate your next

Our response during the crisis – executed in three weeks!

4.5x remote access infrastructure

95% enabled to work from home

100% client approvals for WFH

 secure WFH connectivity models defined

10x hyperscaling of bandwidth

 productivity and SLA adherence measures put in place

30k desktops moved to employees' residence

 SOC operations recalibrated

Jan to March 2020 cyber threat trends

907k total COVID spam messages

48k hits on malicious URLs

737 detected malware related to COVID

522k active phishing sites as of March 20

220% increase in **spam** from Feb to March 20

260% increase in **malicious URLs** from Feb to March 20

148% increase in **ransomware** attacks

350% increase in **phishing sites** from Jan to March 2020

1. Dealing with the expanding and new threat surface
2. Protecting against data breaches and attacks on remote assets
3. Balancing security with user experience and productivity
4. Prioritizing and recalibrating governance and compliance
5. Making cybersecurity a foundation for the new digital era

1 Dealing with the expanding and new threat surface

- Overnight business enablement from 10% to 100% work from home
- New threat surface - remote access infrastructure, collaboration platforms and personal devices
- Fragility of home offices, a new target
- Lack of control on user actions
- Exception access misuse (e.g. Admin/USB)

BEST PRACTICES

- ☑ Secure VPN
- ☑ Implement 100% MFA
- ☑ Disable insecure protocols/services
- ☑ Enforce endpoint controls to prevent data leakage
- ☑ Recalibrate SOC use cases and rules
- ☑ Secure configuration and auditing of cloud environment

2 Protecting against data breaches and attacks on remote assets

- Centralized enterprise security controls rendered ineffective at the edge
- Huge spike in false positives due to new traffic pattern and user behavior
- Ineffective patch and vulnerability management due to limited bandwidth
- New methods and techniques adopted by threat actors

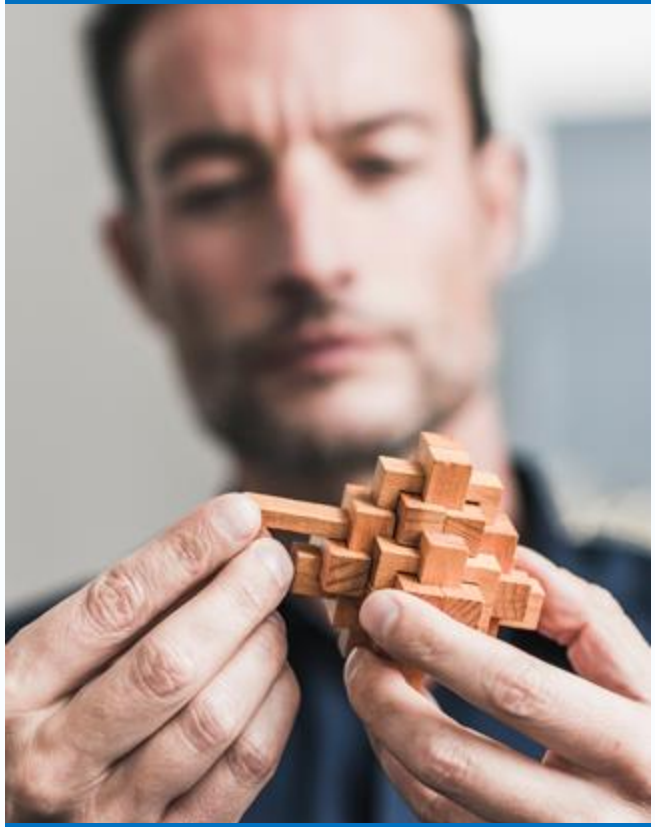
BEST PRACTICES

- ☑ Revisit and enforce usage policies
- ☑ Increase awareness on secure ways of working from home
- ☑ Implement Endpoint Detection and Response (EDR)
- ☑ Enforce zero tolerance to poor IT Hygiene (patch/vulnerability mgmt.)
- ☑ Implement endpoint data leakage controls to prevent print and screen scraping

3 Balancing security with user experience and productivity

- Too many security tools and controls may hinder productivity
- Employees overwhelmed with too many do’s and don'ts
- Balancing between user actions and central controls
- Enabling seamless access and collaboration in a zero-tolerance security environment

BEST PRACTICES



- Hyperscale user concurrency and bandwidth
- Amplify helpdesk capabilities with intelligent self-service
- Implement transparent security controls so that user experience is not impacted
- Prevent bad security behavior / decisions

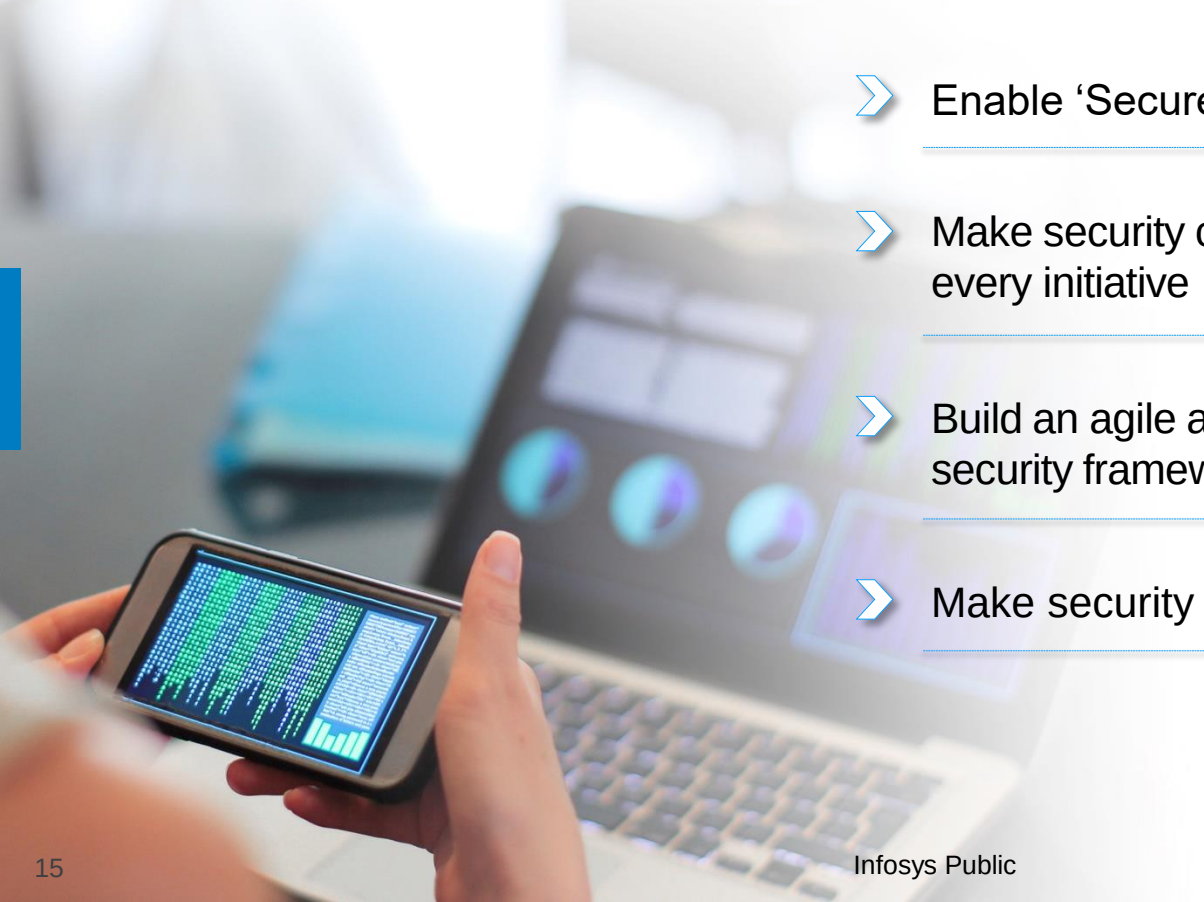
4 Prioritizing and re-calibrating governance and compliance

- Recalibrating security policies while working from home
- Taking informed decisions while making the organization resilient and agile
- Rebalancing between security and privacy
- Ensuring communication and enforcement
- Adequate documentation and user-help / FAQs

BEST PRACTICES

- ☑ Establish strong governance processes to improve visibility of cyber risks
- ☑ Ensure balance between security and privacy obligations
- ☑ Ensure compliance to legal, regulatory and contractual obligations
- ☑ Drive investments in intelligent automation
- ☑ Increase frequency of cadence and reviews
- ☑ Provide appropriate learning resources / FAQs

5 Making cybersecurity a foundation for the new digital era



- Enable ‘Secure by Design’
- Make security consideration mandatory for every initiative
- Build an agile and adaptive enterprise security framework
- Make security strategic and mainstream

BEST PRACTICES

- Make security an integral building block of every initiative and innovation
- Ensure adherence to security policies, standards and execution mandates for remote working at scale
- Focus on stabilization and implementation of best practices and industry collaborations
- Develop an agile and adaptive security architecture to face the current dynamic environment

1. Addressing new threat surface
2. Preventing attacks on remote assets
3. Balancing security with experience & productivity
4. Prioritizing governance and compliance
5. Making cybersecurity a foundation for digital

POLL 2

What is your top security focus area for facilitating remote-working?

1. Addressing new threat surface
2. Preventing attacks on remote assets
3. Balancing security with experience and productivity
4. Prioritizing governance and compliance
5. Making cybersecurity a foundation for digital

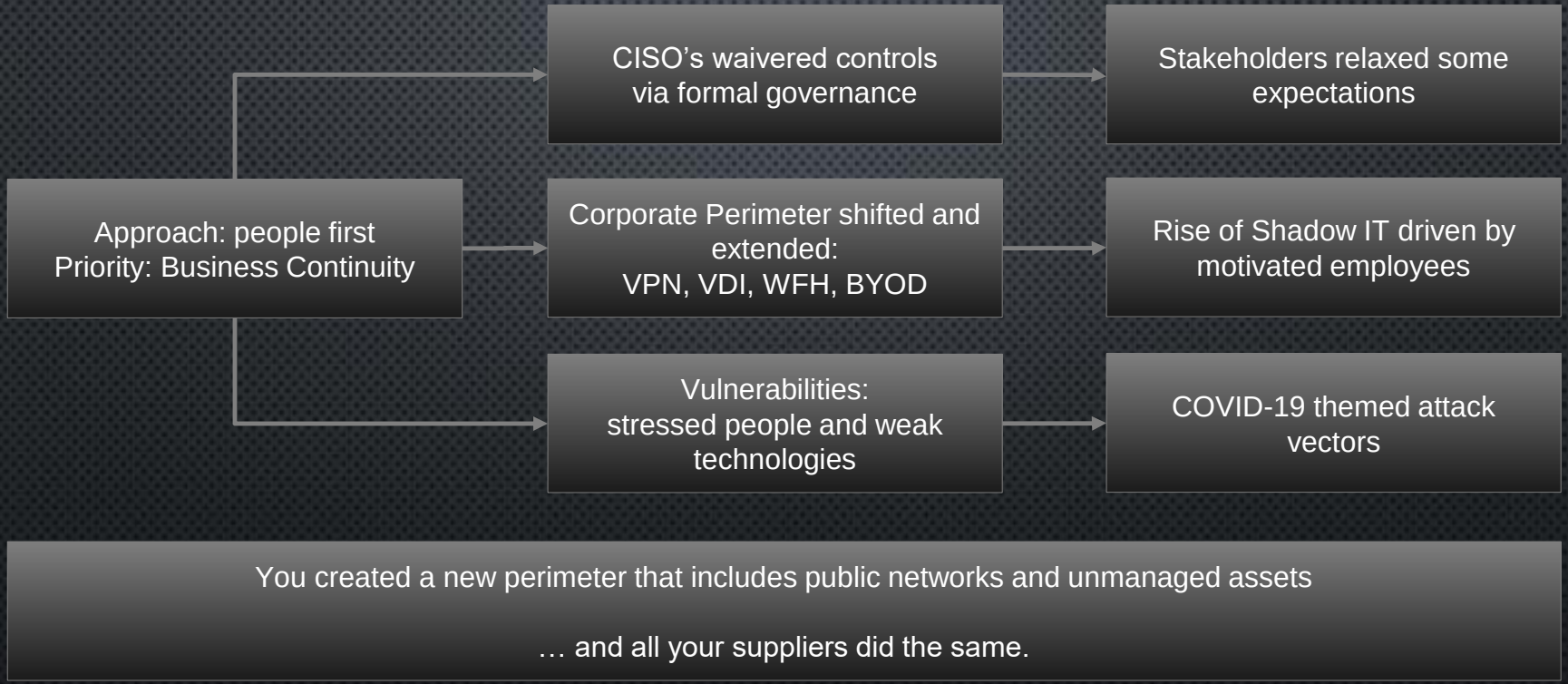
AFTER THE FIRST RESPONSE

Dr. Martijn Dekker

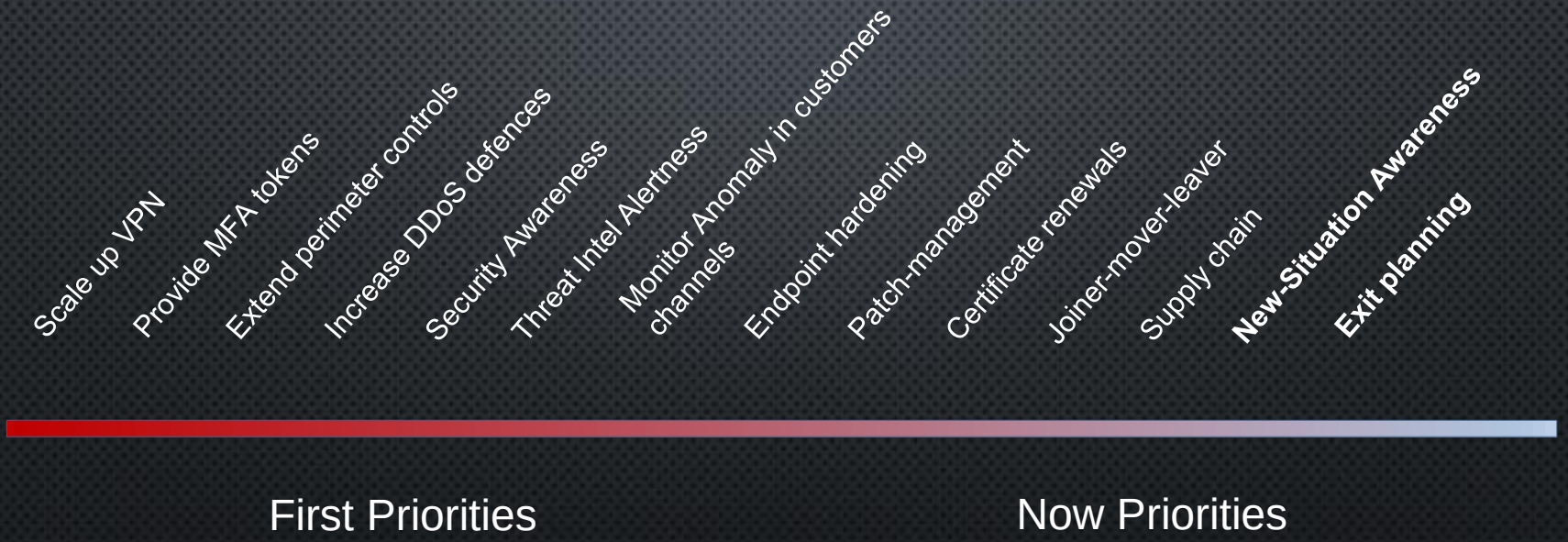
Chief Information Security Officer – ABN AMRO BANK N.V.

Visiting Professor Information Security – University of Amsterdam

PEOPLE AND BUSINESS – FIRST RESPONSE



FAST AND SLOW – NOW PRIORITIES



OLD AND NEW – NEXT PRIORITIES

Increase of
(need for) Business Agility

Openness for
change
and expectations

Accept and embrace
The new normal

REVERT AND RENEW – NEXT PRIORITIES

Information Security is a key business enabler … and now everyone knows this

Opportunity to rethink your controls

CISO's need to step up and *deliver* security *innovations*

Security Industry *forced* to improve

POLL 3

What security control would require immediate innovative approaches post-covid19 ?

1. Identity & access management
2. Secure document exchange
3. Security awareness
4. Patch- and vulnerability management
5. Security monitoring

Being Resilient. That's Live Enterprise

Security in the era of remote working

Q & A

Mohit Joshi
President, Infosys

Vishal Salvi
CISO & Cybersecurity Unit Head, Infosys

Dr. Martijn Dekker
CISO, ABN AMRO Bank

Infosys®
Navigate your next