Cybersecurity collaboration in the financial sector

Innovation and Cyber Security Conference

August 2018

South African Reserve Bank

Collaboration

South African Reserve Bank

Why?

- Obvious interconnected contagion risk but more specifically we have to make it more difficult for attackers:
  - Reduce economic incentive - just reuse methods
  - More effective response if we combine resources (together we are stronger)
  - Unable to exploit the fact that all of us has only part of the picture – unable to detect
  - Cannot abuse the fact that we fumble or are slow on response
  - Ensure they don’t migrate to the weak area … your area…

Collaboration on what?

Coordination

Prevent

Detect

Respond & Recover

CPDR^2

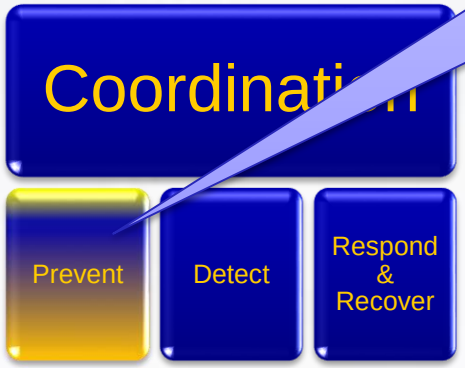
South African Reserve Bank

Collaboration on what? (Prevent)

- Ensure **Detection** and **Respond and Recover** output is formally incorporated in **Prevention** and direction setting activities – creating a learning system

Collaboration on what? (Prevent)

- Standardisation
- Risk/Status/Compliance Assessment
- Industry Vulnerability Testing



South African Reserve Bank

Collaboration on what? (Detect)

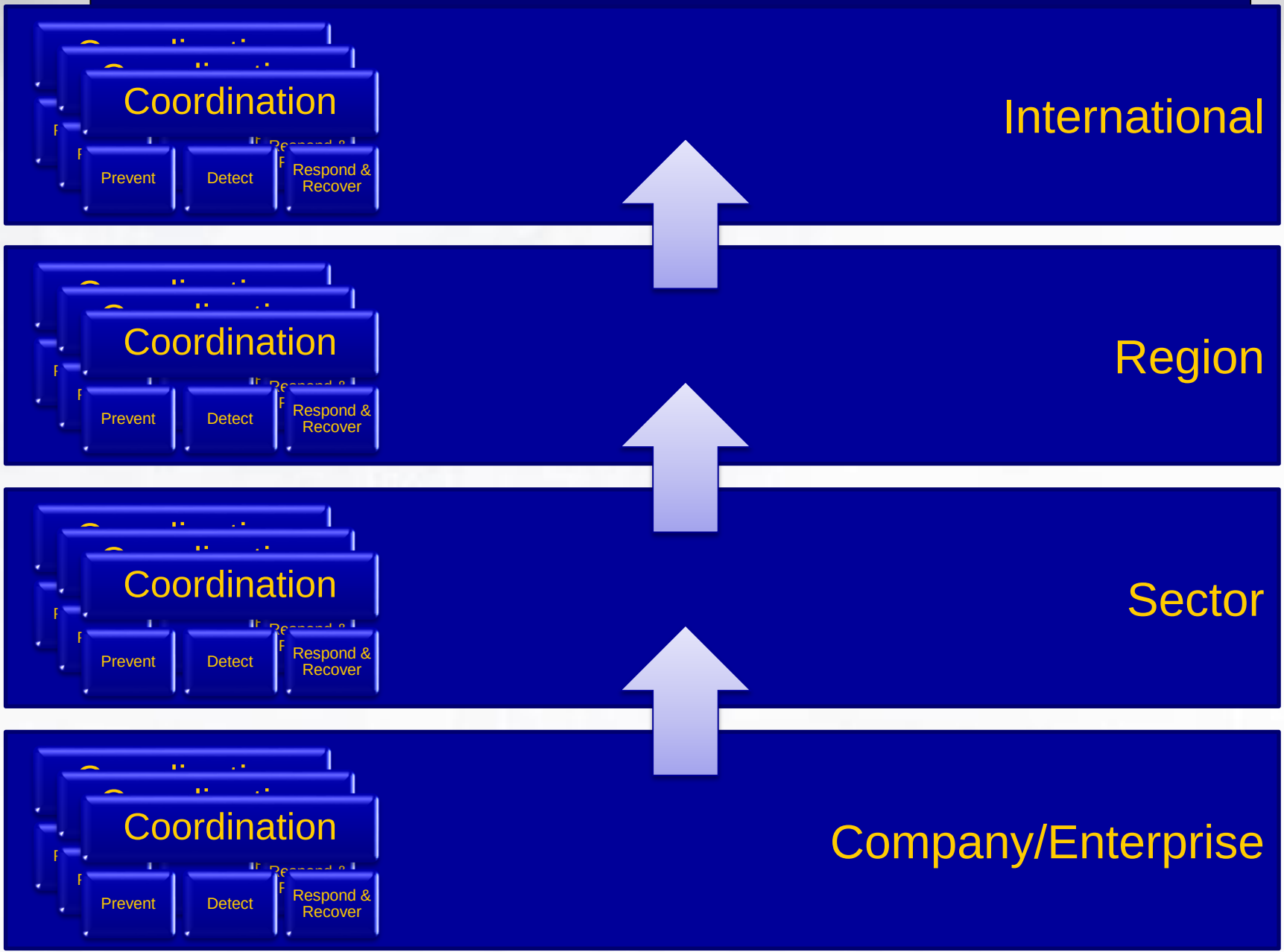
- Threat Intelligence
- Incident sharing
- Analysis (consolidation and collaboration)

South African Reserve Bank

Collaboration on what? (Respond and Recover)

- Response and recovery coordination
- Simulation Testing (Red/Blue)
- Emergency Support and Skills

Levels of Collaboration?



Bank

Depth of Collaboration (Prevent)

Shallow

Common reference framework

Integrated Measurement

Coordinated and shared implementation/ readiness testing and assistance

Deep

South African Reserve Bank

Depth of Collaboration (Detect)

Shallow

High level post fact incident sharing/ groups and lists

Selected information sharing at key points

Real time early detection technical detail and overall information sharing

Deep

South African Reserve Bank

Depth of Collaboration (Respond and Recover)

Shallow

Sharing groups and lists

Reporting defined in terms of content, timing and audience

Integrated coordination and resource sharing

Deep

South African Reserve Bank

Insights

Don’t mix PDR^2 functions/resources

Insights

Need lower layers before you can meaningfully participate

Insights

Don’t worry about the other person - do it for the greater good

Insights

Just start – depth grows with time and trust

Insights

Don’t care about domains – attackers don’t

South African Reserve Bank

Insights

Don’t shoot the messenger – cyber is tough

South African Reserve Bank

Insights

Combine formal (self organised dynamic) and formal efforts

Insights

Encourage sharing and remove roadblocks

Questions

South African Reserve Bank