



  
March 15-18, Orlando

# FIGHTING CYBER ATTACKS REQUIRES MORE THAN SECURITY – IT REQUIRES CYBER RESILIENCY

Patrick Potter, RSA


CONFIDENTIAL


1

## ABOUT THE SPEAKER

**Patrick Potter**  
*Digital Risk Solutions, RSA*

Patrick has spent over 30 years leading risk management programs as both a practitioner and consultant. He currently works at RSA developing digital risk solutions for organizations of all size and maturity.





2

## NOTPETYA – THE MOST DEVASTATING CYBERATTACK IN HISTORY

*It was a perfect sunny summer afternoon in Copenhagen when the world's largest shipping conglomerate began to lose its mind...*



3

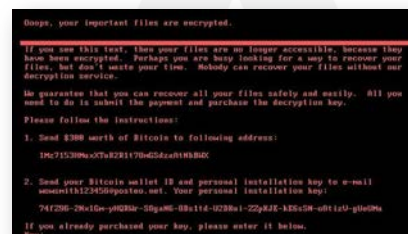


RSA

3

## NOTPETYA – THE EFFECTS

- SW vulnerability of billing software
- Minutes to compromise an organization
- Hospitals, six power companies, two airports, dozens of banks, ATM and card payment systems, transportation and more
- Circulatory system of the global economy itself, was broken
- Objective of Destruction vs. Ransom
- \$10 billion in total damages
- **Lack of Cyber Recovery Plans**



<b>\$188,000,000</b>
Swack company Mondelez (parent company of Nabisco and Cadbury)
<b>\$129,000,000</b>
British manufacturer Reckitt Benckiser (owner of Lysol and Durex condoms)
<b>\$10 billion</b>
Total damages from NotPetya, as estimated by the White House

4

RSA

4

## THE THREAT LANDSCAPE IS EVOLVING

1. Cyber attacks and data breaches
2. IT and telecom outage
3. Adverse weather/natural disaster
4. Critical infrastructure failure
5. Reputation incident
6. Regulatory changes
7. Lack of talent/key skills
8. Supply chain disruption
9. Interruption to utility supply
10. Political change

January 2019, the Business Continuity Institute (BCI)  
Horizon Scan Report for 2019

Ransomware has  
increased

# 118%




McAfee Labs Threats Report, August 2019

5

RSA

5



National Terrorism Advisory System

# Bulletin

[www.dhs.gov/advisories](http://www.dhs.gov/advisories)

January 4, 2020

### SUMMARY OF TERRORISM THREAT TO THE U.S. HOMELAND

- The United States designated Iran a "State Sponsor of Terrorism" in 1984 and since then, Iran has actively engaged in or directed an array of violent and deadly acts against the United States and its citizens globally. The United States designated Iran's Islamic Revolutionary Guard Corps (IRGC) a Foreign Terrorist Organization on April 15, 2019 for its direct involvement in terrorist plotting.

**DURATION**

This Bulletin will expire on or before **January 18, 2020** at 1:00 PM EST

#### HOW YOU CAN HELP

- Report suspicious activity to local law enforcement who are best to offer specific details on terroristic indicators.
- Report suspicious activity or information about a threat, including online activity, to fusion centers and the FBI's Field Offices – part of the Nationwide Suspicious Activity Reporting Initiative.
- Learn [how to recognize signs of pre-operational planning](#) associated with terrorism or other criminal activity.

#### BE PREPARED

- Be prepared for cyber disruptions, suspicious emails, and network delays.
- Be responsible for your personal safety. Know where emergency exits and security personnel are located. Carry emergency contact and special needs information with you.
- Implement basic cyber hygiene practices such as effecting data backups and employing multi-factor authentication. For more information visit [CISA.gov](http://CISA.gov).
- [Connect, Plan, Train, and Report](#) to prepare businesses & employees. Security tools/resources can be accessed through the DHS's [Hometown Security Campaign](#).

#### STAY INFORMED

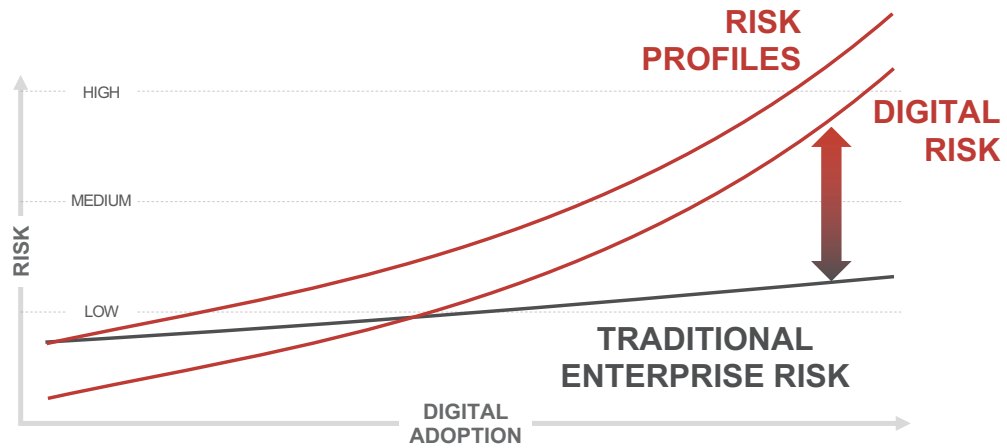
- The U.S. Government will provide additional information about any emerging threat as additional information is identified. The public is encouraged to listen to local law enforcement and public safety officials.
- We urge Americans to continue to travel, attend public events, and freely associate with others but remain vigilant and aware of surroundings.
- The Department of State issues [international travel alerts and warnings](#).
- For additional information visit [Ready](#).

6

RSA

6

## DIGITAL TRANSFORMATION INCREASES DIGITAL RISK



7 |

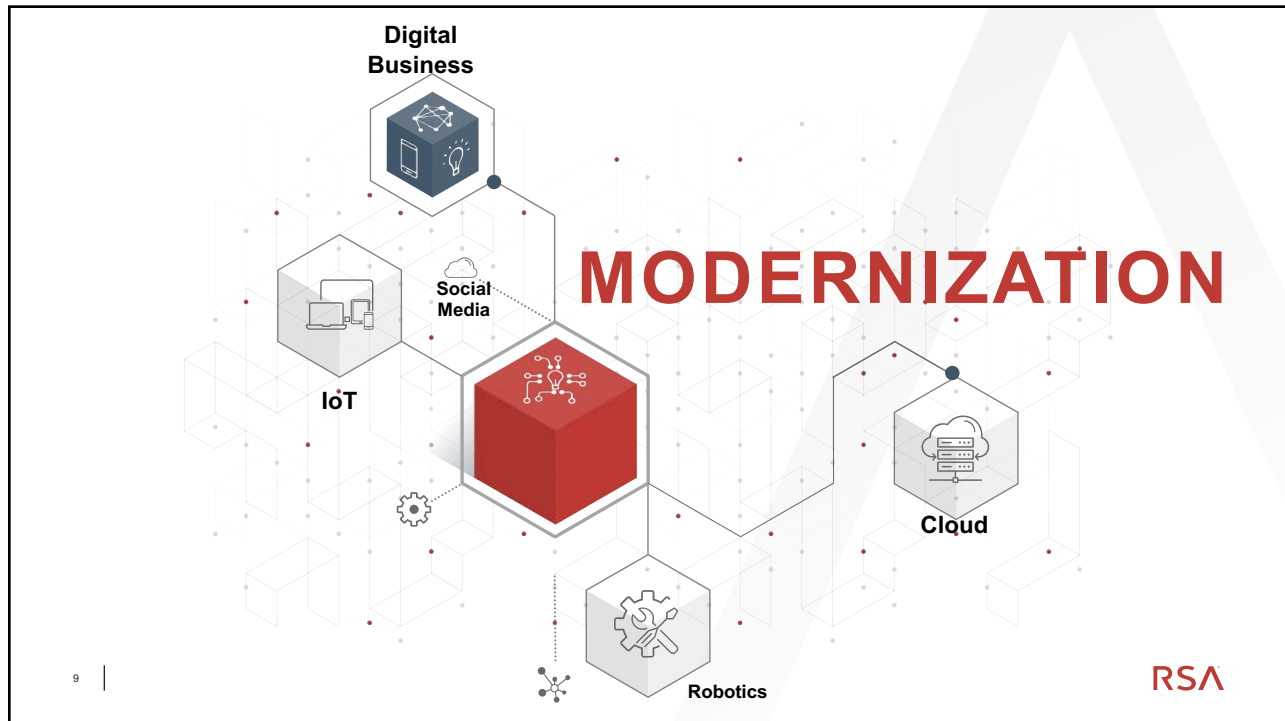
RSA

7

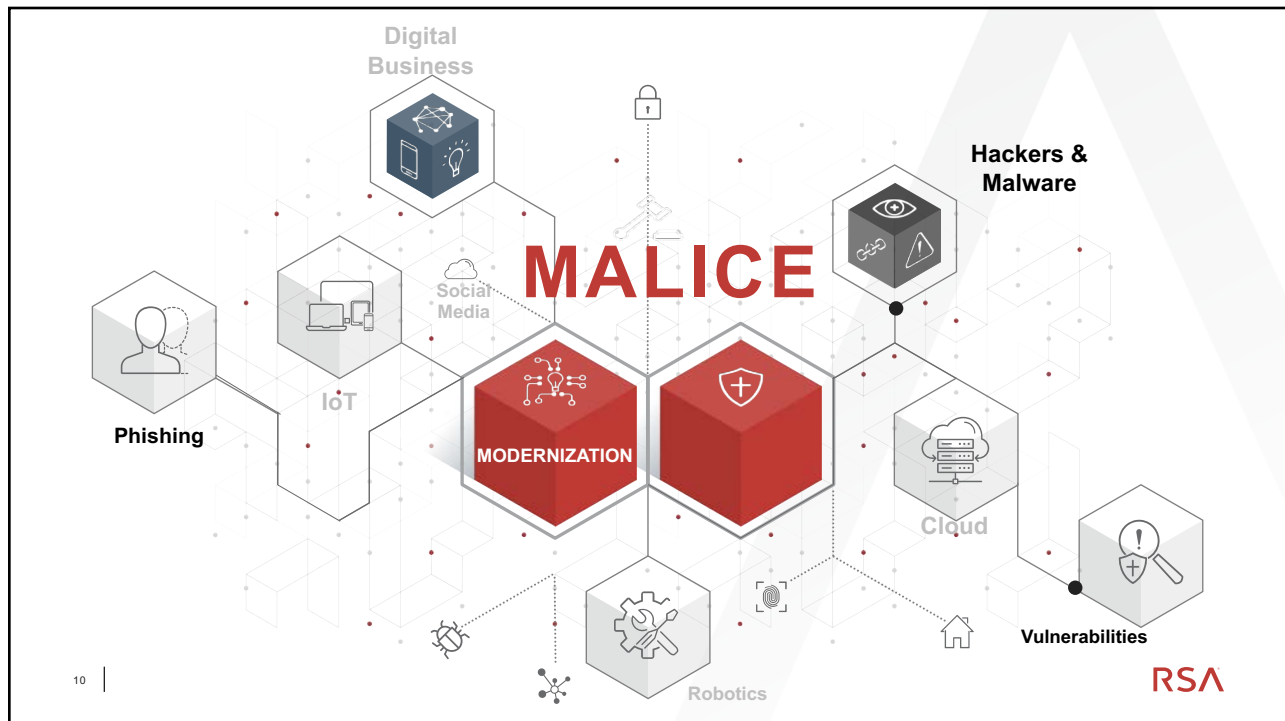
## WHAT ARE THE CHALLENGES?

RSA

8

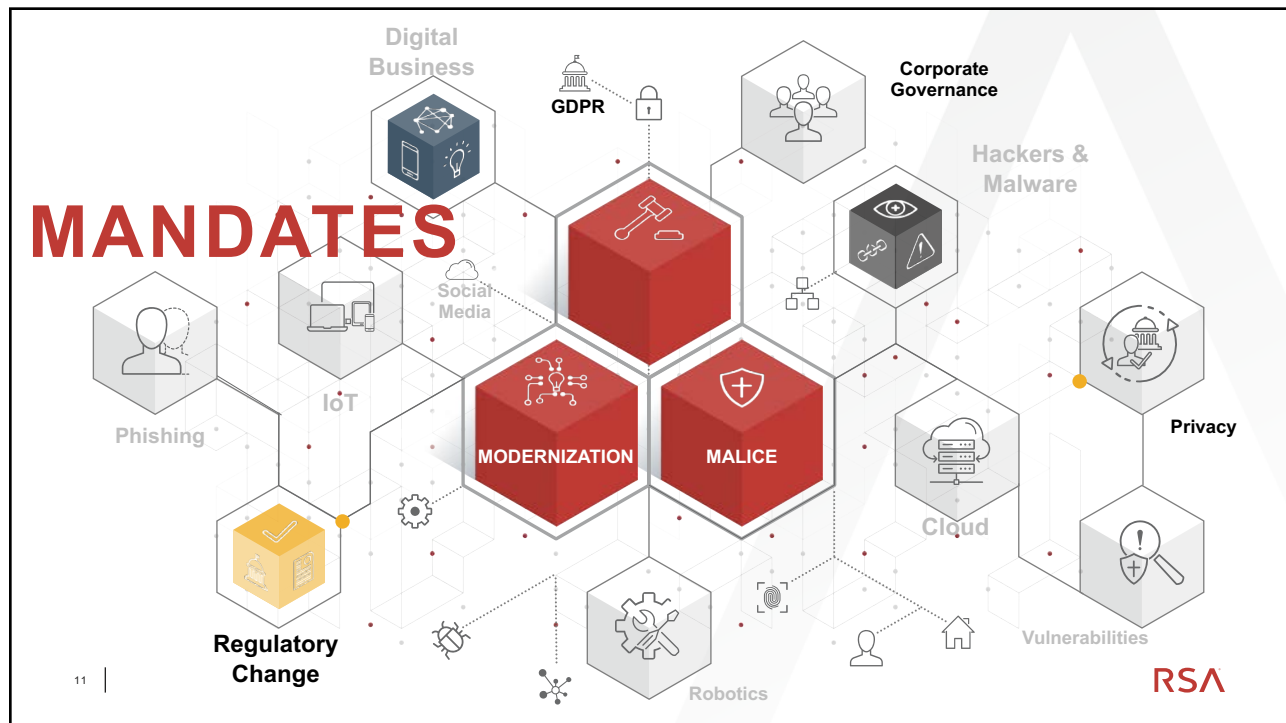


9



10

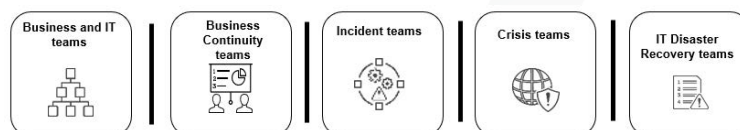




11

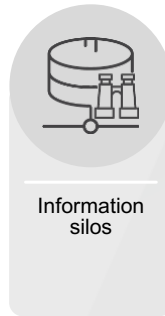
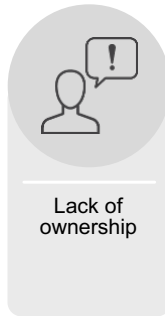
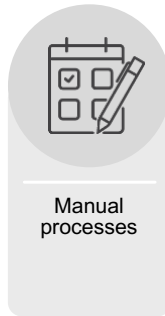
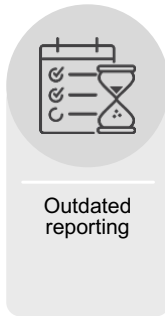
## CHALLENGES TO BUILDING BUSINESS RESILIENCY

- Organizations must be “always on” for customers, their workforce and partners
- Digital transformation is creating more complexity
- Resiliency teams are siloed with different priorities
- Teams have disconnected strategies and approaches that don’t build business resiliency
- Organizations are not building cyber resiliency



12

## TODAY'S PROCESSES...

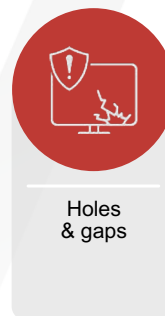
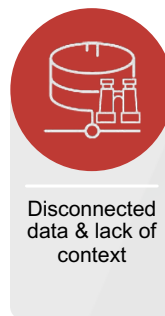
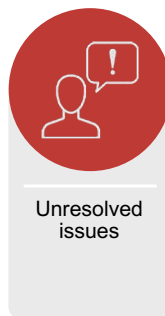


13 | CONFIDENTIAL

RSA

13

## TODAY'S PROCESSES...



14 | CONFIDENTIAL

RSA

14

To avoid being disrupted by cyberattacks and other disruptions, organizations must transform from just being “recoverable” to being resilient – and this requires a change in priority and approach.

15 |

RSA

15

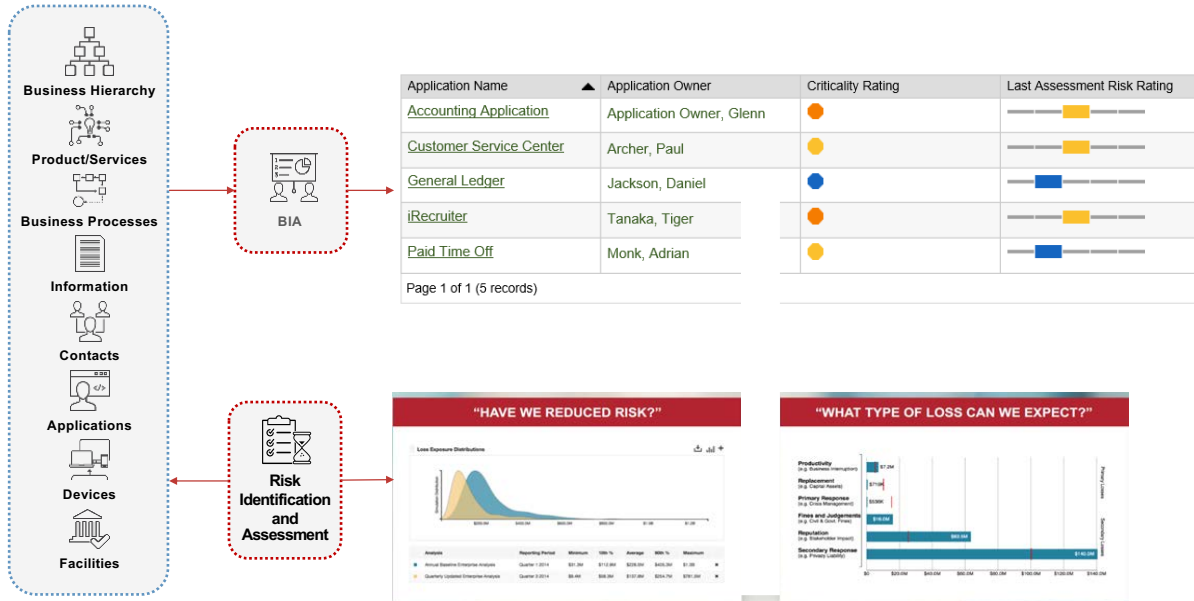
WHAT'S NEEDED TO  
**CLOSE** THE GAP?

RSA

16

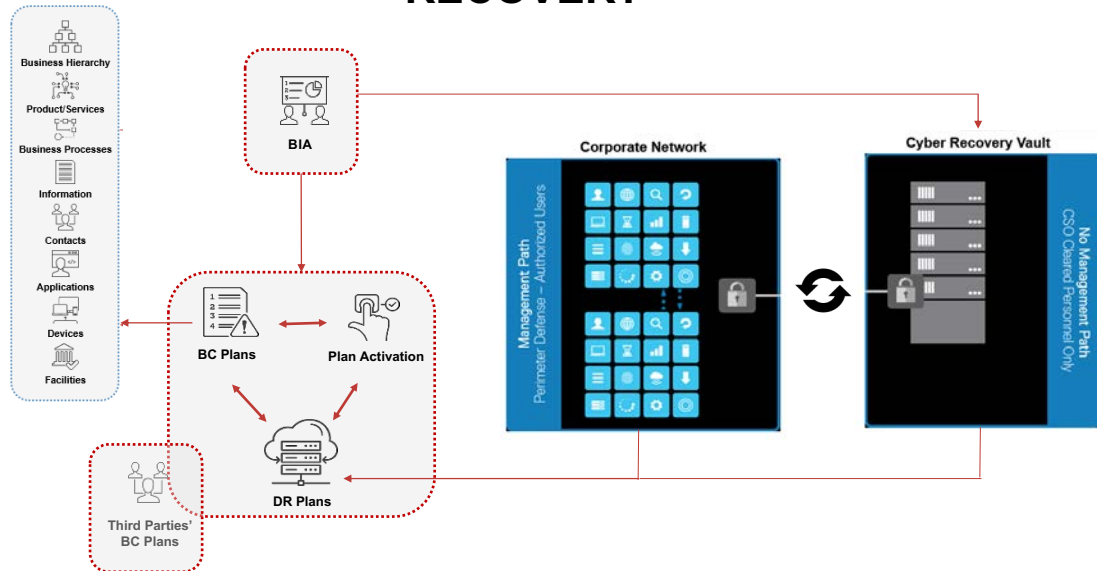


## STEP 1: DRIVE CONSISTENT PRIORITIES



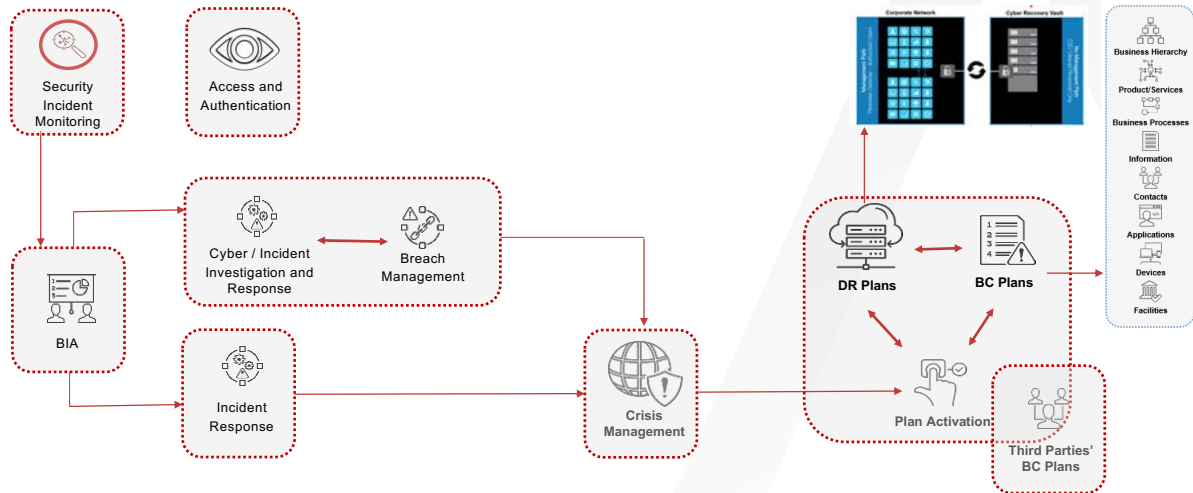
17

## STEP 2: ALIGN BUSINESS, IT DR and DATA RECOVERY



18

## STEP 3: BUILD CYBER RESILIENCY



19

RSA

19

## CYBER RESILIENCY IS MORE THAN IT DR

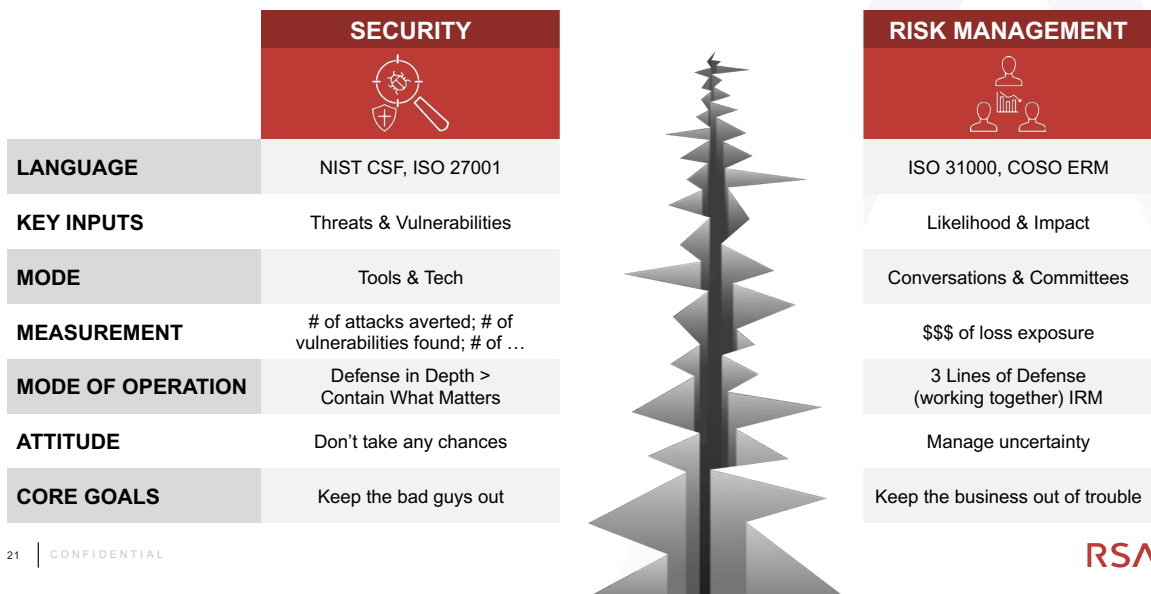
	Disaster Recovery	Cyber Resiliency
Recovery Time	❖ Close to Instant	❖ Reliable & Fast
Recovery Point	❖ Ideally Continuous	❖ 1 Day Average
Nature of Disaster	❖ Flood, Power Outage, Weather	❖ Cyber Attack, Targeted
Impact of Disaster	❖ Regional; typically contained	❖ Global; spreads quickly
Topology	❖ Connected, multiple targets	❖ Isolated, in addition to DR
Data Volume	❖ Comprehensive, All Data	❖ Selective, Includes Foundation SVCs
Recovery	❖ Standard DR (e.g. fallback)	❖ Iterative, selective recovery; part of IR

20 | CONFIDENTIAL

RSA

20

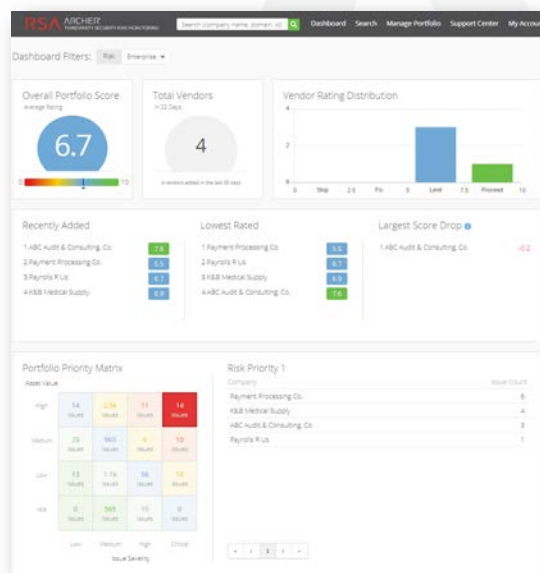
## WHY DOES THE COMBINATION OF SECURITY AND THIRD-PARTY RISK MATTER?



21

## THIRD PARTY SECURITY RISK MONITORING

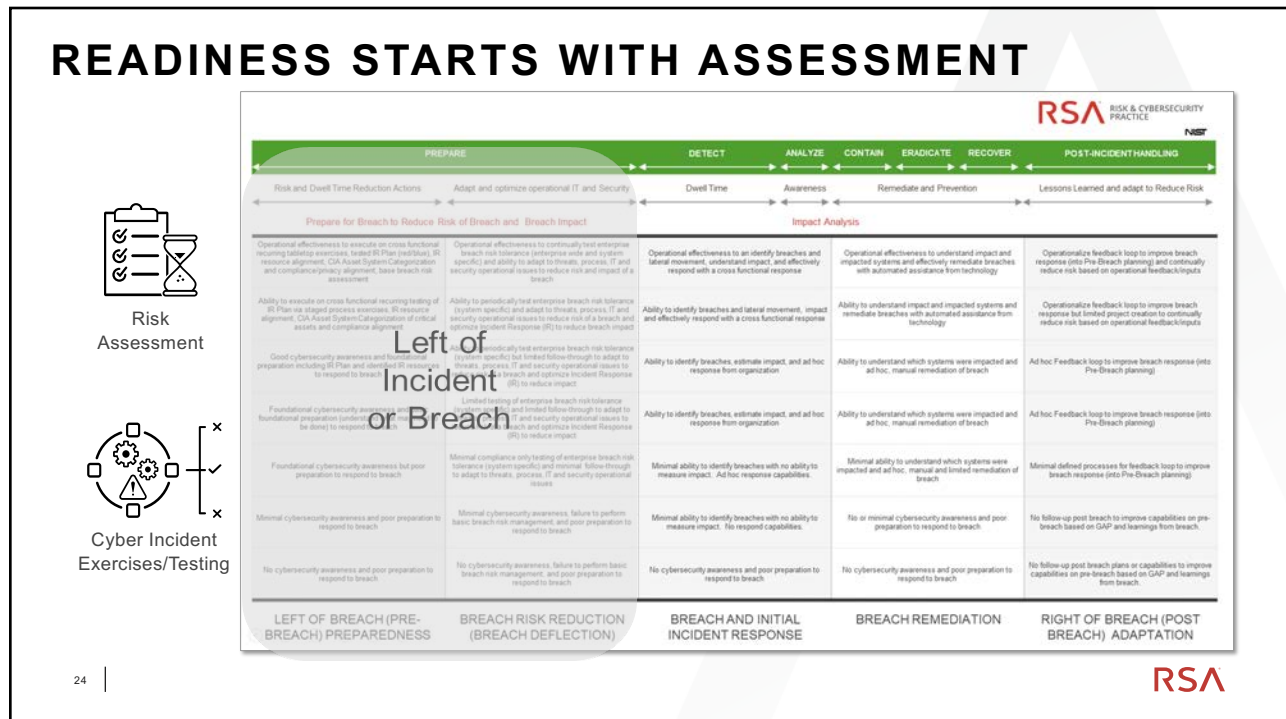
- Gain objective insight into your third-party security performance and IT landscape
- Perform third party portfolio wide diagnostics and prioritizations
- Allocate risk resources to where they are needed most - high value, low performing vendors
- Engage vendors with accurate, actionable security performance insights and corrective actions
- Continuously monitor vendor security performance
- Triage and remediate critical vulnerabilities
- Optimize use of analysts time and outside auditor resources



22

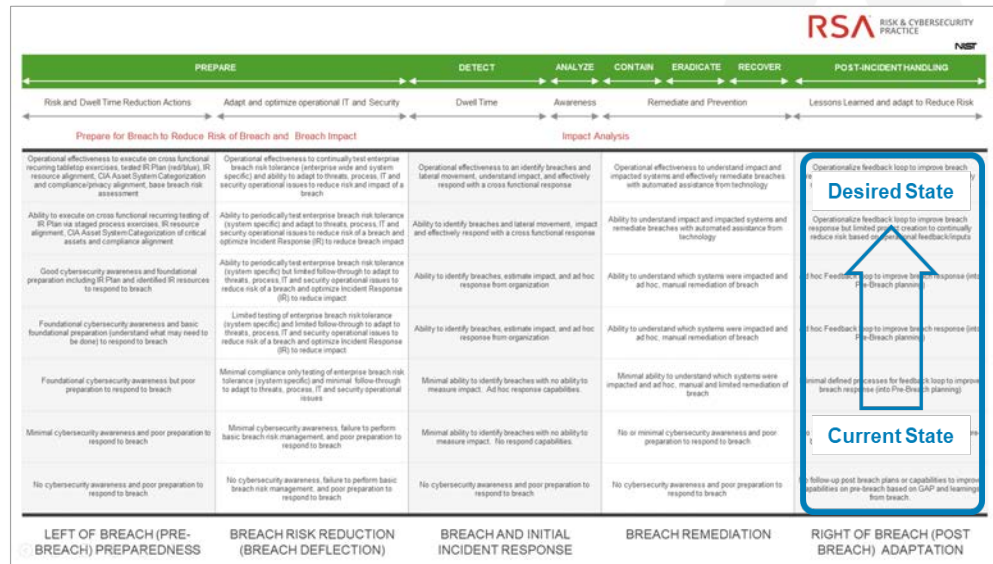


23



24

# CYBER RECOVERY AND BREACH REMEDIATION

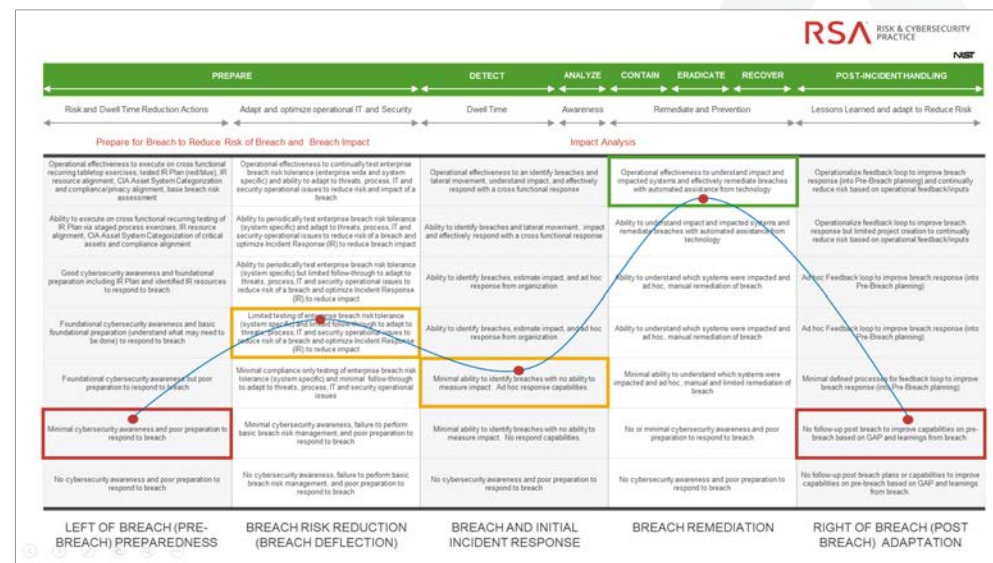


25

RSA

25

# GETTING STARTED – BASELINE AND IMPROVE



26

RSA

26

# CYBER RISK IN FINANCIAL TERMS

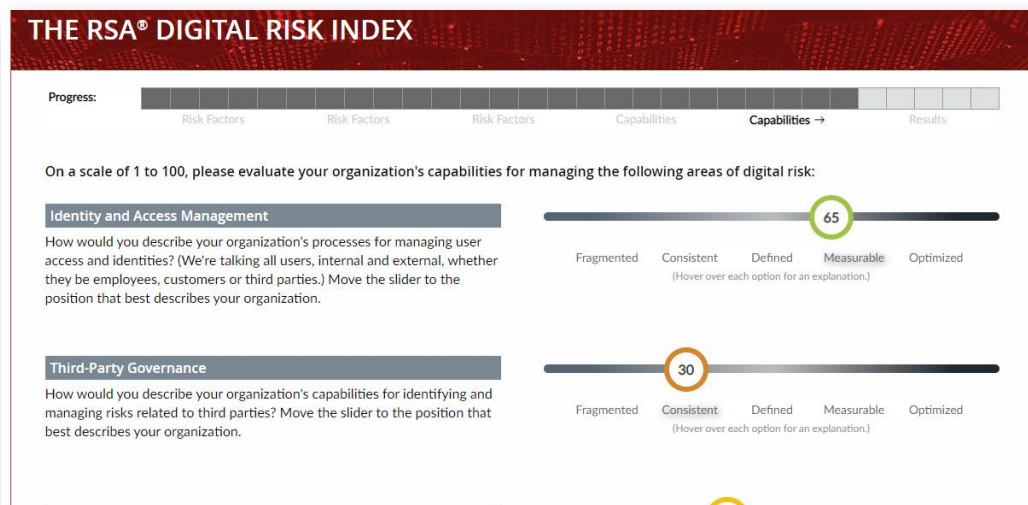


27

Private and Confidential

RSA

27



28

[RSA Digital Risk Report - Sept 2019](#)

RSA

28



## FINAL THOUGHTS

- Start at the top - Demand oversight by BoD. In organizations with BoD oversight, resiliency improves
- Coordinate across risk and security, business and IT, 3LOD
- Evaluate the maturity of your cyber resilience capabilities
- Automate to manage the governance process and lifecycle

29 |

RSA

29



RSA®

30