RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: SP01-W10

Ransomware Attack Protection & Recovery: Lessons from the Front Line

MODERATOR: **Peter Beardmore**
Director of Marketing for Digital Risk Management Solutions, RSA
@PBeardmore

PANELISTS: **Amy Blackshaw**
Director, Product Marketing
RSA
@amyblackshaw

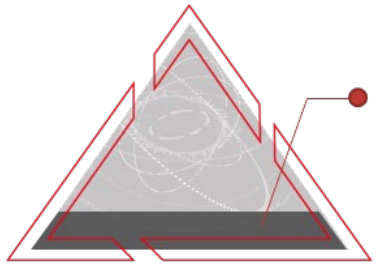
Stefan Voss
Sr. Director, Product Management
Dell
@VossmanVoss

Nick Curcuru
VP, Data & Analytics and Cybersecurity Strategist
Mastercard

Discussion Outline

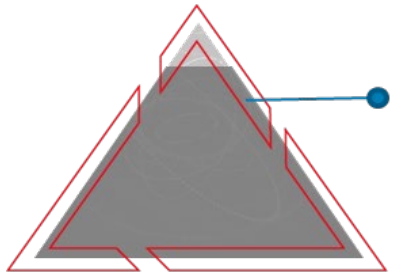
- Discuss Shifting Threats and Impacts
  - Shifting Protection Strategies
  - Shifting Vendor Requirements
- Maturation of Digital Risk Management (DRM)
  - Business Impact Analysis, Cyber Risk Measurement, Frameworks & Compliance
- Resulting Tech and Architecture Evolution
  - Risk Management, SecOps, Identity, Data Protection & Recovery
- Where to begin?

Assessing Detection & Response Capabilities



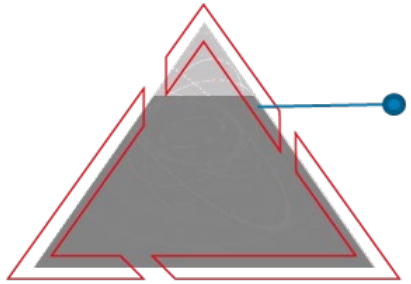
24%

Organisations satisfied with their ability to detect and investigate



92%

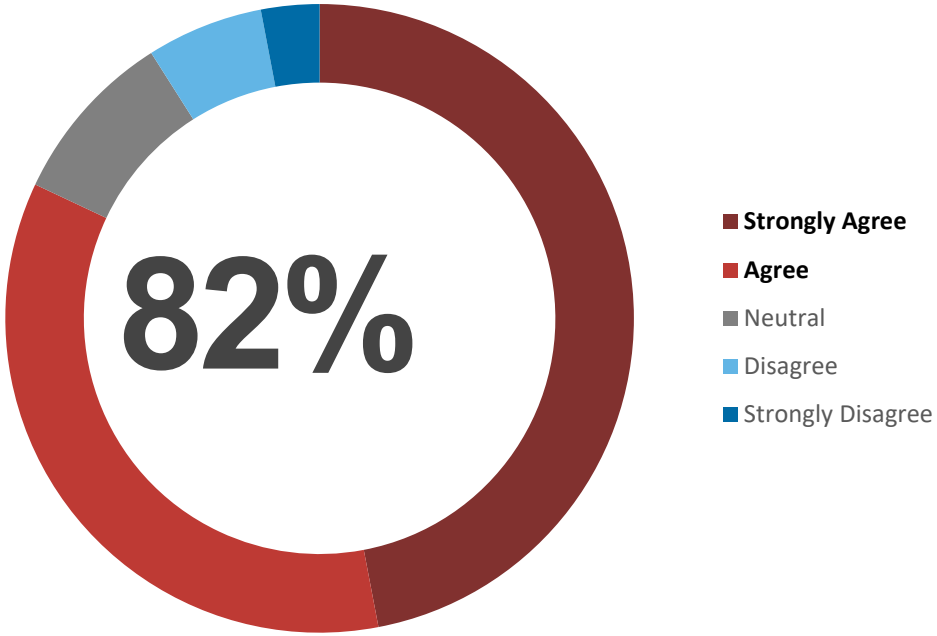
Cannot detect quickly



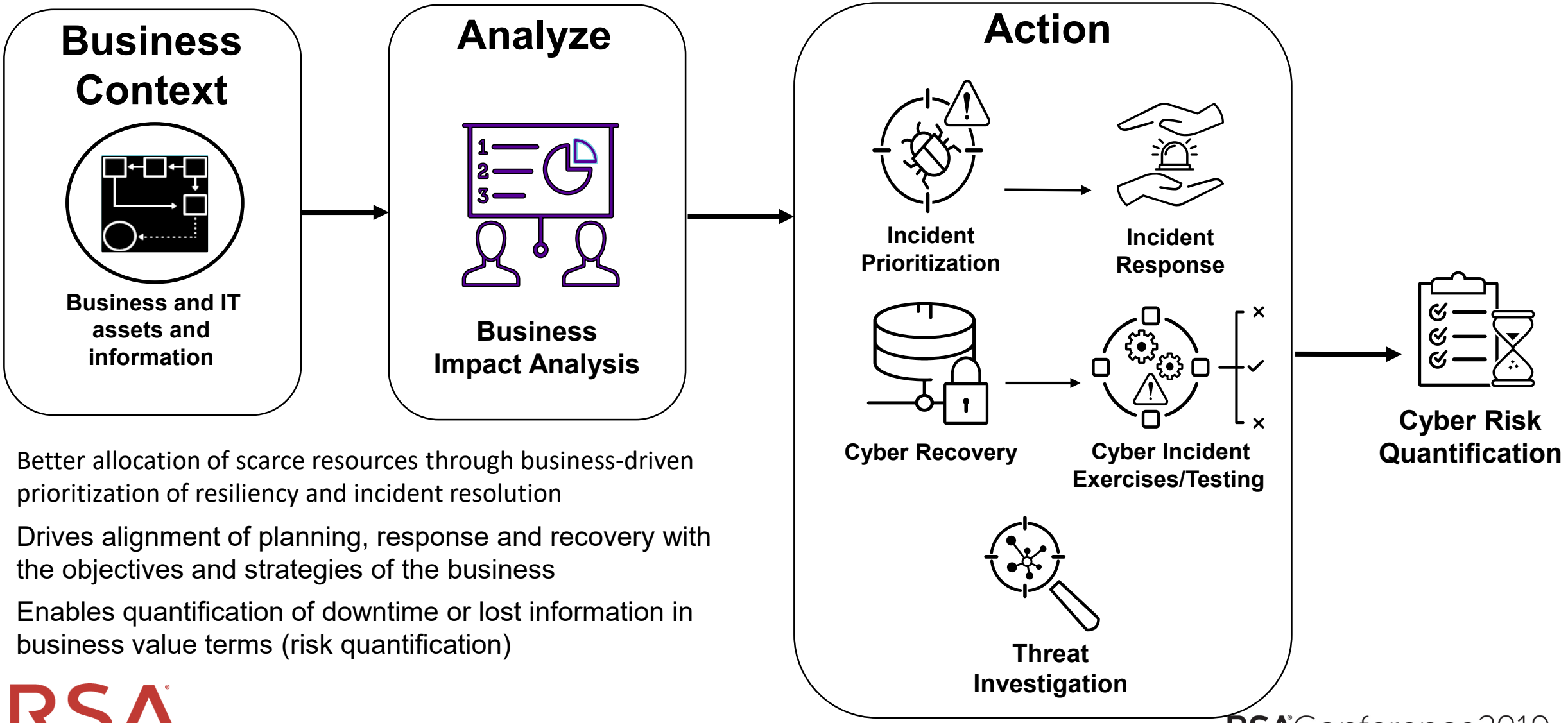
88%

Cannot investigate quickly

82% of Risk and Security professionals report that **their organizations consider security breaches as a business risk rather than just an IT risk.**

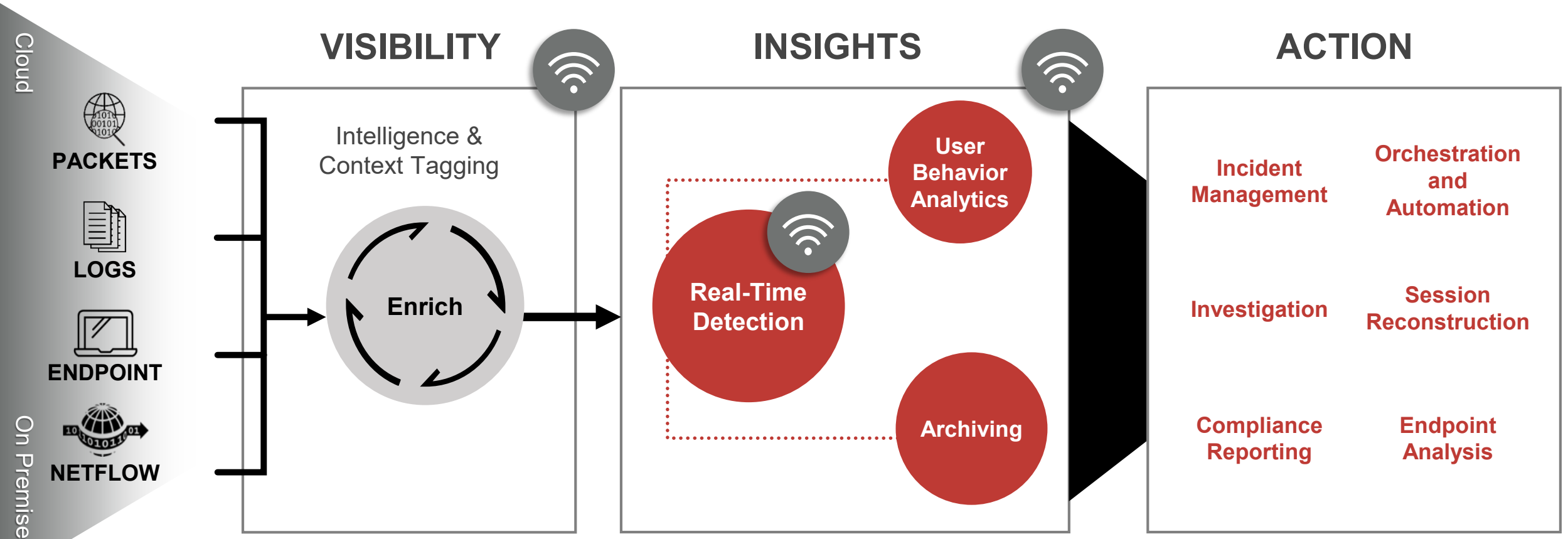


Strategy Starts with Business Impact Analysis (BIA)



- Better allocation of scarce resources through business-driven prioritization of resiliency and incident resolution
- Drives alignment of planning, response and recovery with the objectives and strategies of the business
- Enables quantification of downtime or lost information in business value terms (risk quantification)

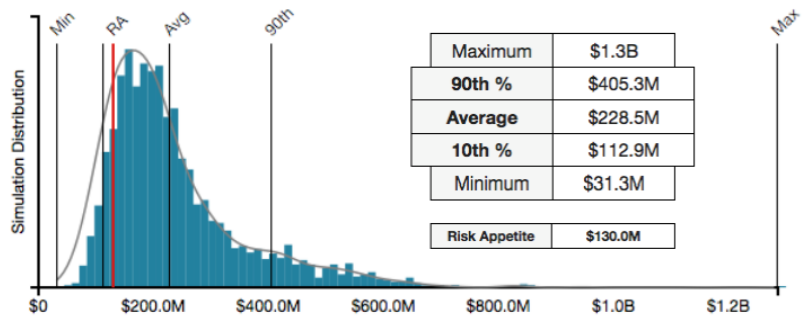
Addressing the New Requirements



Express Cyber Risk in Financial Terms

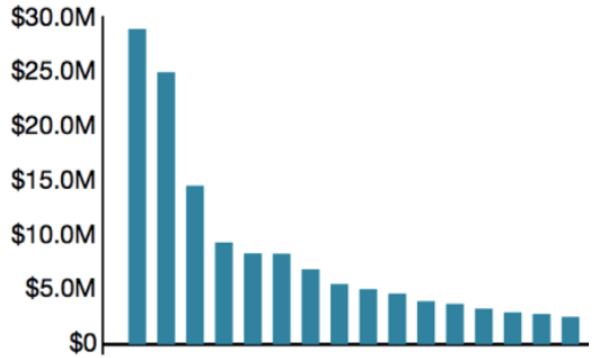
Cyber Risk Quantification

"HOW MUCH RISK DO WE HAVE?"

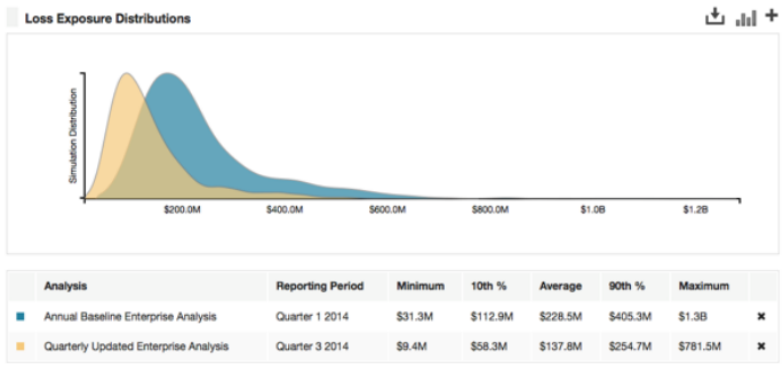


Maximum	$1.3B
90th %	$405.3M
Average	$228.5M
10th %	$112.9M
Minimum	$31.3M
Risk Appetite	$130.0M

"WHAT ARE OUR TOP RISKS?"

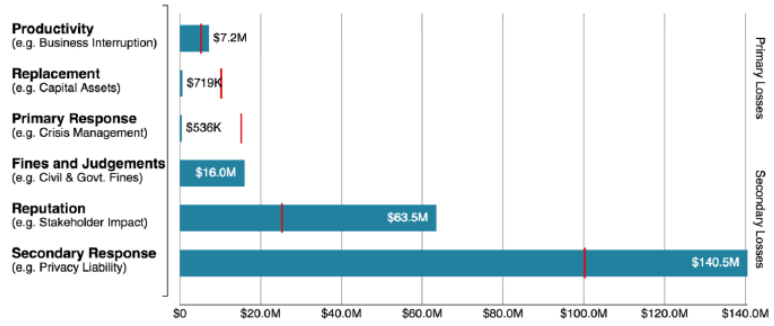


"HAVE WE REDUCED RISK?"



Analysis	Reporting Period	Minimum	10th %	Average	90th %	Maximum
Annual Baseline Enterprise Analysis	Quarter 1 2014	$31.3M	$112.9M	$228.5M	$405.3M	$1.3B
Quarterly Updated Enterprise Analysis	Quarter 3 2014	$9.4M	$58.3M	$137.8M	$254.7M	$781.5M

"WHAT TYPE OF LOSS CAN WE EXPECT?"



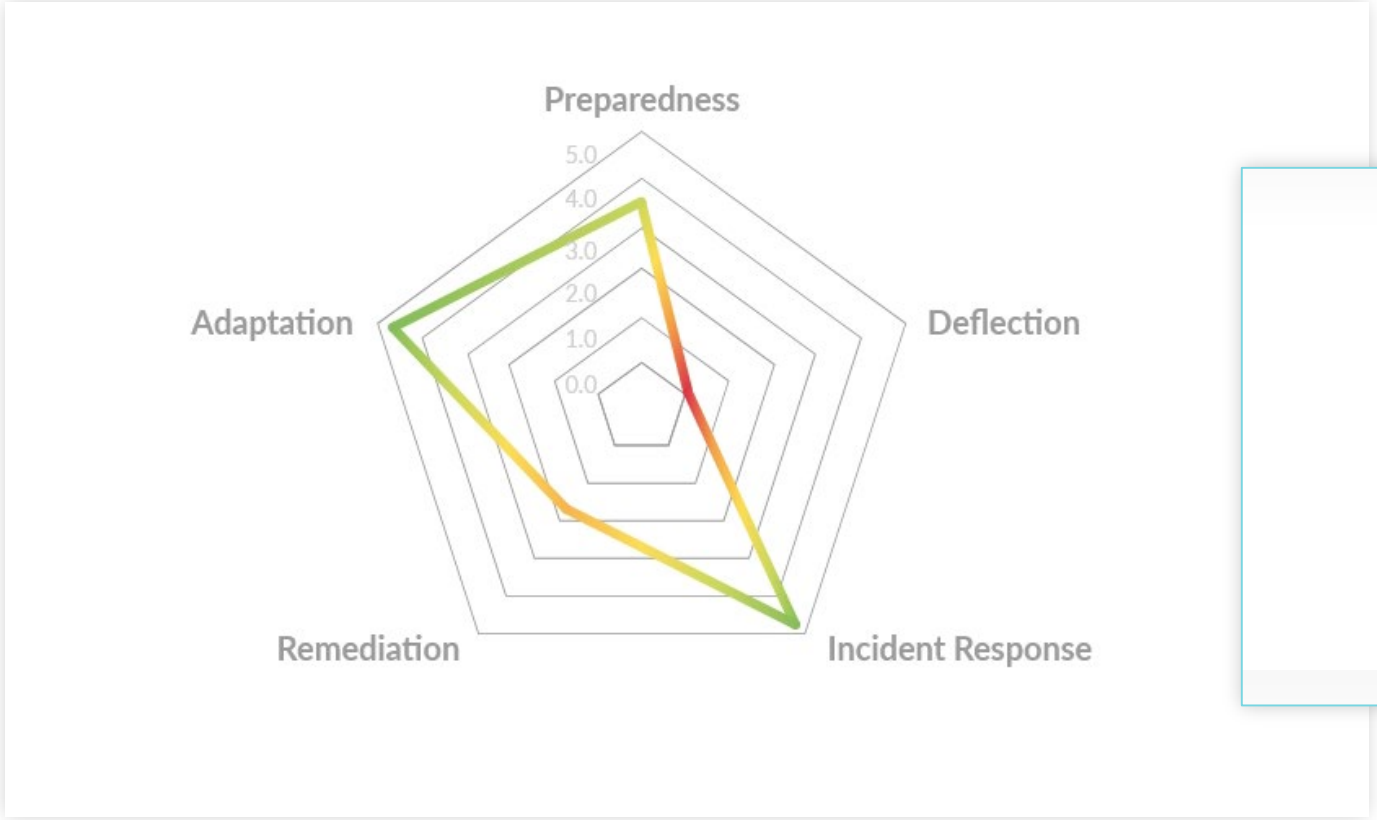
Risk Framework: Cyber Incident Risk

IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER	
BREACH PREPAREDNESS	RISK REDUCTION	INCIDENT RESPONSE	BREACH REMEDIATION	POST-BREACH ADAPTATION	
OPERATIONAL EXCELLENCE					
• Plans & resources aligned • Risks fully assessed • All assets categorized	• Continuous testing of risk tolerance • Continuous adaptation to threats, process, operational issues	• Majority of breaches identified & isolated • Advanced understanding of business impact	• Full understanding of business impact • Effective remediation of incidents • Prevention of recurrence	• Advanced feedback loop into preparedness • Good processes & tools for breach • Strong risk reduction	TOP 2
FOUNDATIONAL EFFECTIVENESS					
• Plans & resources partially aligned • Risks partially assessed • Some assets categorized	• Periodic test of risk tolerance • Good adaptation to threats, process, operational issues	• Many breaches identified & isolated • Good understanding of business impact	• Good ability to understand impact • Good ability to respond to & remediate breach	• Good feedback loop into preparedness • Regular improvement to breach response process & tools • Sound risk reduction	ABOVE avg. BELOW avg.
MINIMAL EFFECTIVENESS					
• Some alignment of resources • Some risks assessed • Some assets categorized	• Ad hoc testing of risk tolerance • Some adaptation to threats, process, operational issues	• Some ability to identify breaches • Some ability to understand impact • Ad hoc response	• Basic ability to respond to & remediate breach • Ad hoc and/or incomplete remediation	• Ad hoc feedback loop into preparedness • Some risk reduction	BOTTOM 2

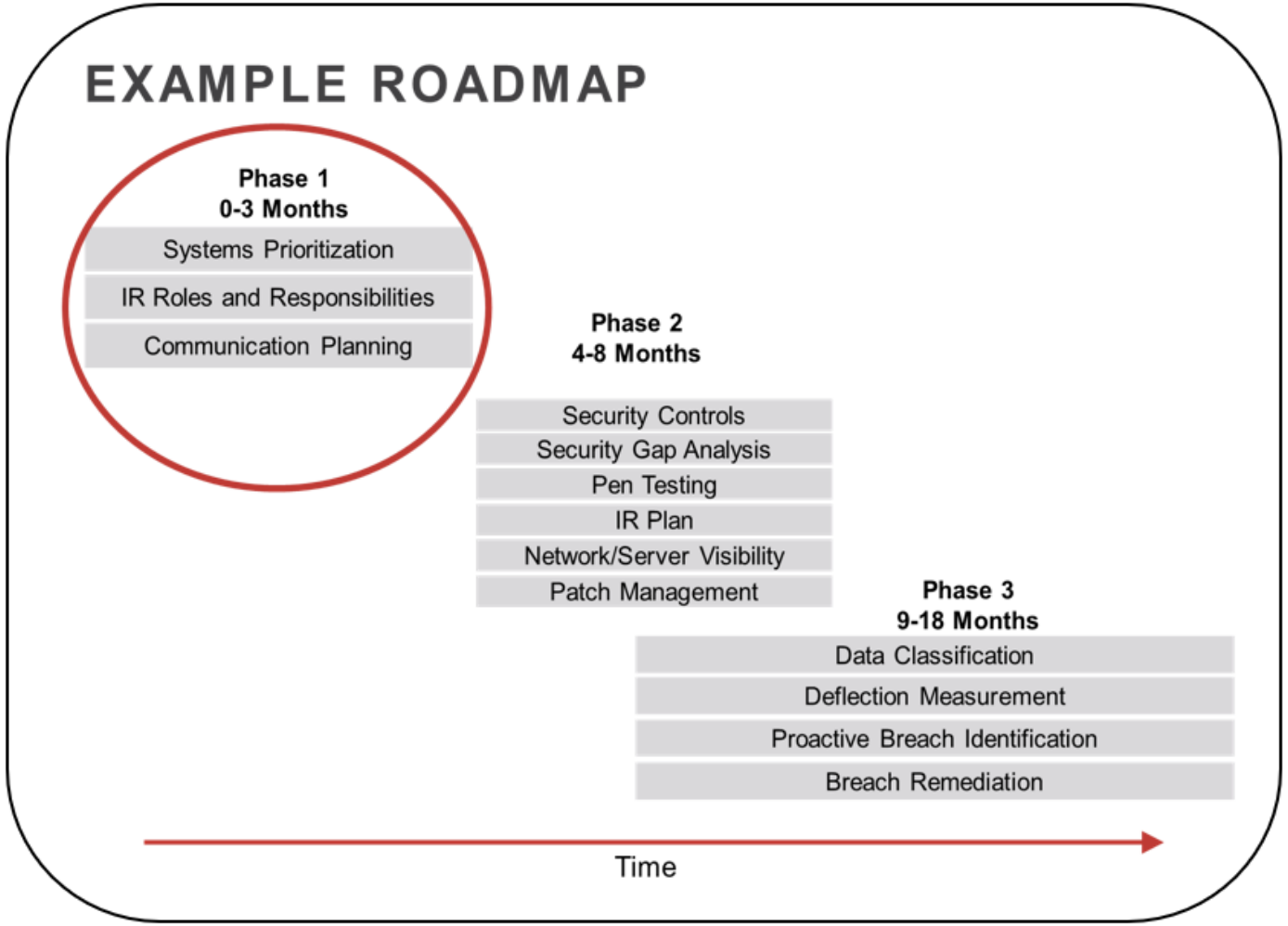
TIME

RSA

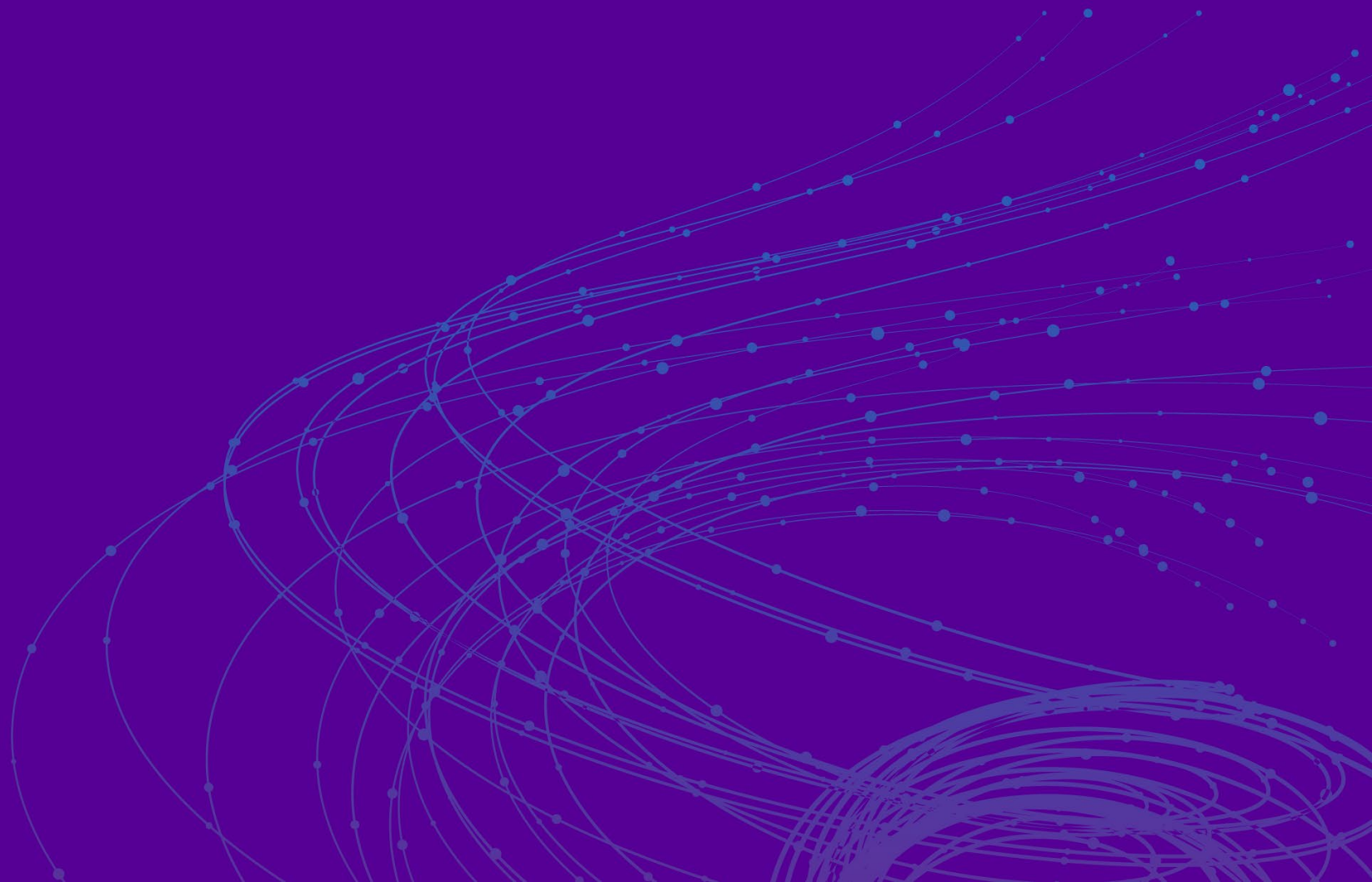
Risk Framework: Sample Outputs



Risk Framework: Sample Outputs



RSA®Conference2019



CYBERSECURITY IS YOUR BUSINESS

9 out 10

organizations are using, planning for, testing, or interested in using isolated data protection copies as a preventative measure against malware infections

60%

CISOs actively involved in data recovery planning as part of incident response

Enterprises are facing an unprecedented wave of cyber attacks and increased business risk. The time to invest in enterprise-class cyber protection and recovery tools is NOW. Don't wait! Your peers are already doing it. Find out what Dell EMC's Cyber Recovery portfolio can do to protect your business data assets.

Source:
ESG Dell EMC Isolated Recovery Custom Research, 2018

Original survey question:
Does your organization currently have the capability to isolate some of its protection storage capacity to prevent malware infections?

Survey respondents:

414 IT, security, and legal professionals in multiple industries globally

This InstaGraphic was created by ESG on behalf of Dell EMC

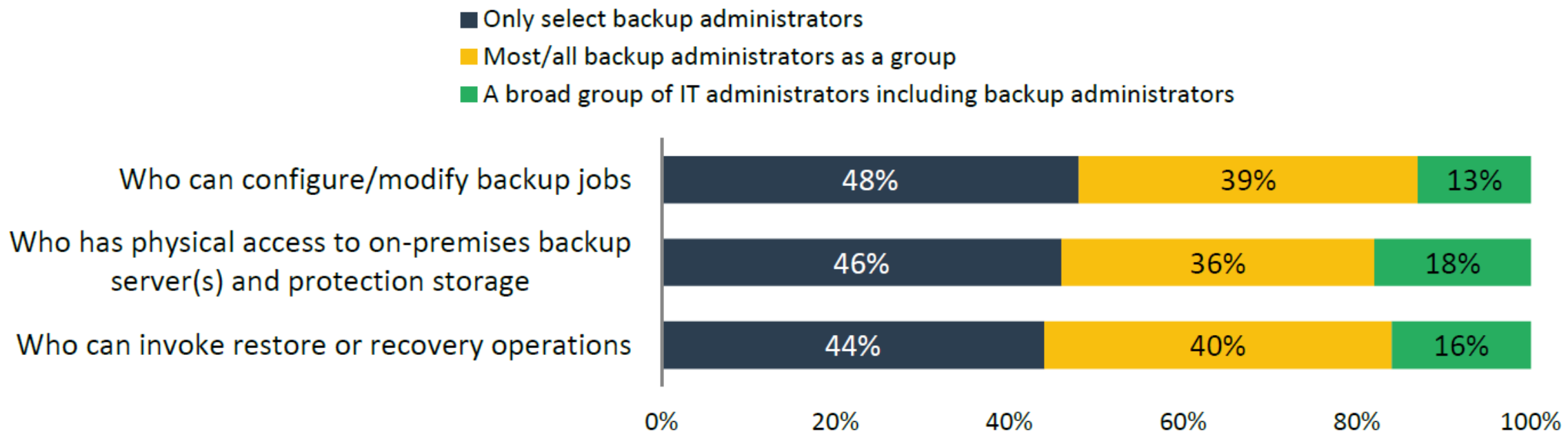
RSA Conference2019

Disaster Recovery ≠ Cyber Recovery

Category	DR	CR
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. failback)	❖ Iterative, selective recovery; part of IR

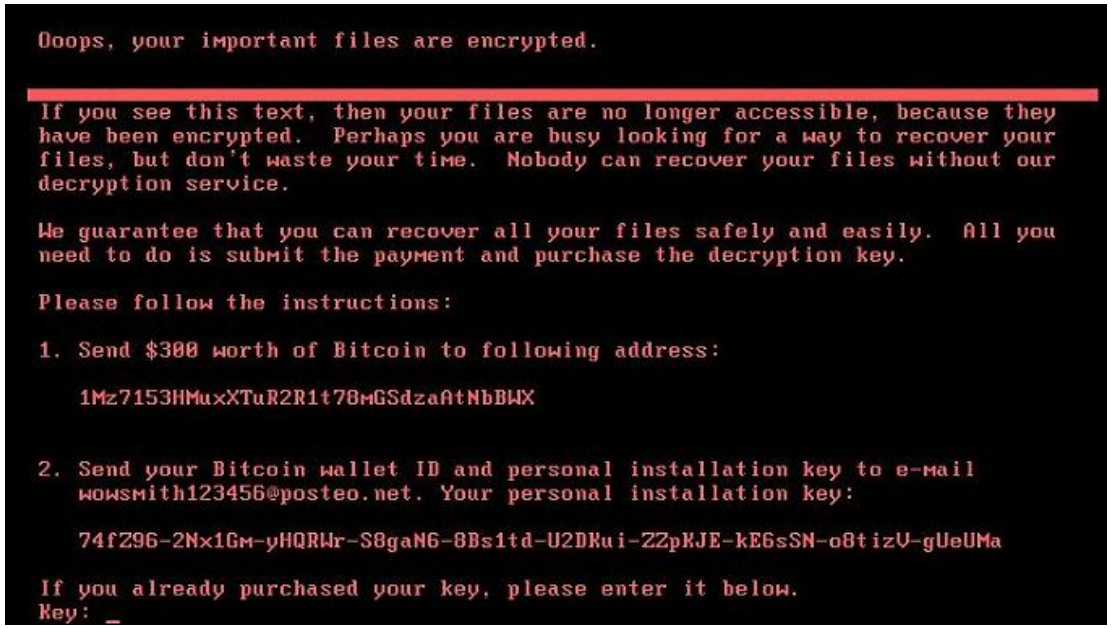
Backup Infrastructure Vulnerable

For each of the following aspects/operations in your organization's backup/recovery environment today, what level of access or control do various IT groups have? (Percent of respondents, N=414)



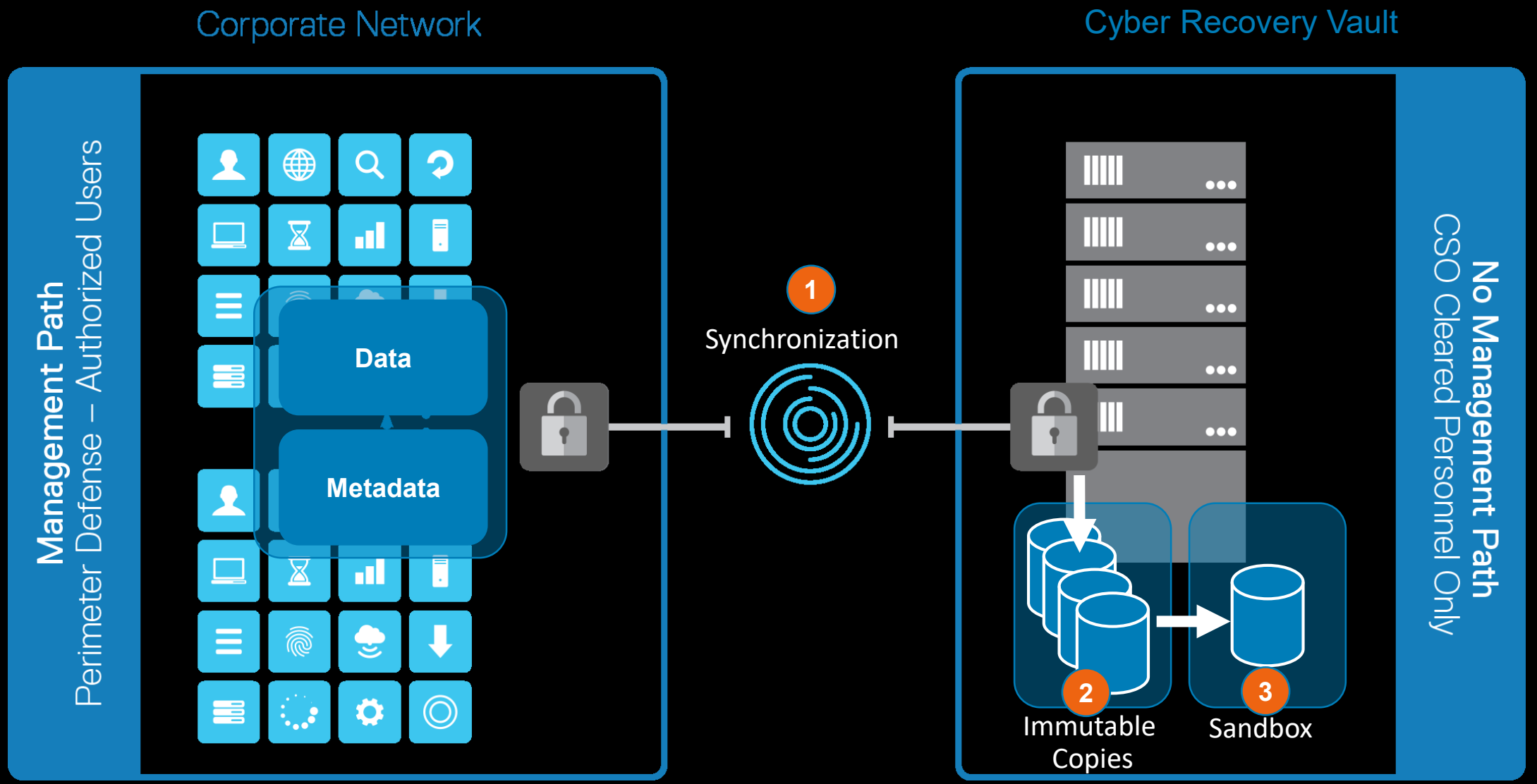
Source: Enterprise Strategy Group

NotPetya CASE STUDY – GLOBAL MANUFACTURER



- Petya/NotPetya Attack Sep 2017
- SW vulnerability of billing software
- 8 Minutes to compromise organization
- 17 factories come to standstill
- 5,000 servers down, 17,000 employees impacted
- 15M Euros lost revenue / day
- Ransom NOT paid
- Lack of Cyber-Recovery Plan
- Tape recovery too slow (weeks estimated)
- Data Domain recovery 4.5 days

A Different Approach to Data Protection



RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: SP01-W10

Ransomware Attack Protection & Recovery: Lessons from the Front Line

MODERATOR: **Peter Beardmore**
Director of Marketing for Digital Risk Management Solutions, RSA
@PBeardmore

PANELISTS: **Amy Blackshaw**
Director, Product Marketing
RSA
@amyblackshaw

Stefan Voss
Sr. Director, Product Management
Dell
@VossmanVoss

Nick Curcuru
VP, Data & Analytics and Cybersecurity Strategist
Mastercard