Cyber Resilience

What we learned in 2021

FUSION
RISK MANAGEMENT

Today's Presenters

Paula Fontana

Senior Director, Product Marketing

David Halford

VP, Integrated Continuity

Agenda

- Cyber Resiliency Trends
- 2021 BCI Survey Highlights
- Using Fusion to Managed Cyber Resilience

Cyber and Operational Resiliency Trends

FUSION RISK MANAGEMENT

Resiliency was Purpose-Built for this Moment

Trends

"Disruption as BAU"
Disruptive events happening with more frequency

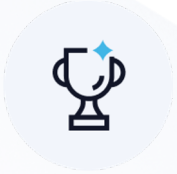
"Sitting on sprawl"
Increase in organizational complexity (digital business, remote work)

"Race to deliver great experiences"
Increasing competition and customer expectations

Risk & Resilience Outcomes

Deploy signal and stop threat before it escalates; find opportunity

Drive simplicity out of complexity; unlocks agility



Prioritize the actions that matter most to your customer

The Journey from Reactive to Proactive Resiliency

Manual

Stuck in spreadsheets or documents.

Little to no mechanism to coordinate dynamically.

Risk and incident management done manually by the team.

No integration in place.

Reactive

Always firefighting.

No defined process for managing risks or incidents.

Risks and incidents managed in silos.

Select source system information integrated into Fusion.

Responsive

Resolving issues as they happen.

Federated teams begin to take coordinated responsibility for service ownership.

Key source system information integrated on a real-time basis.

Proactive

Seamless, coordinated risk and incident management.

Issues are detected and teams/systems are deployed quickly and in an integrated fashion.

Relevant information about risks and incidents delivered in real-time to the right people.

All source system information integrated in real-time.

Preventative

Get ahead of issues before they happen.

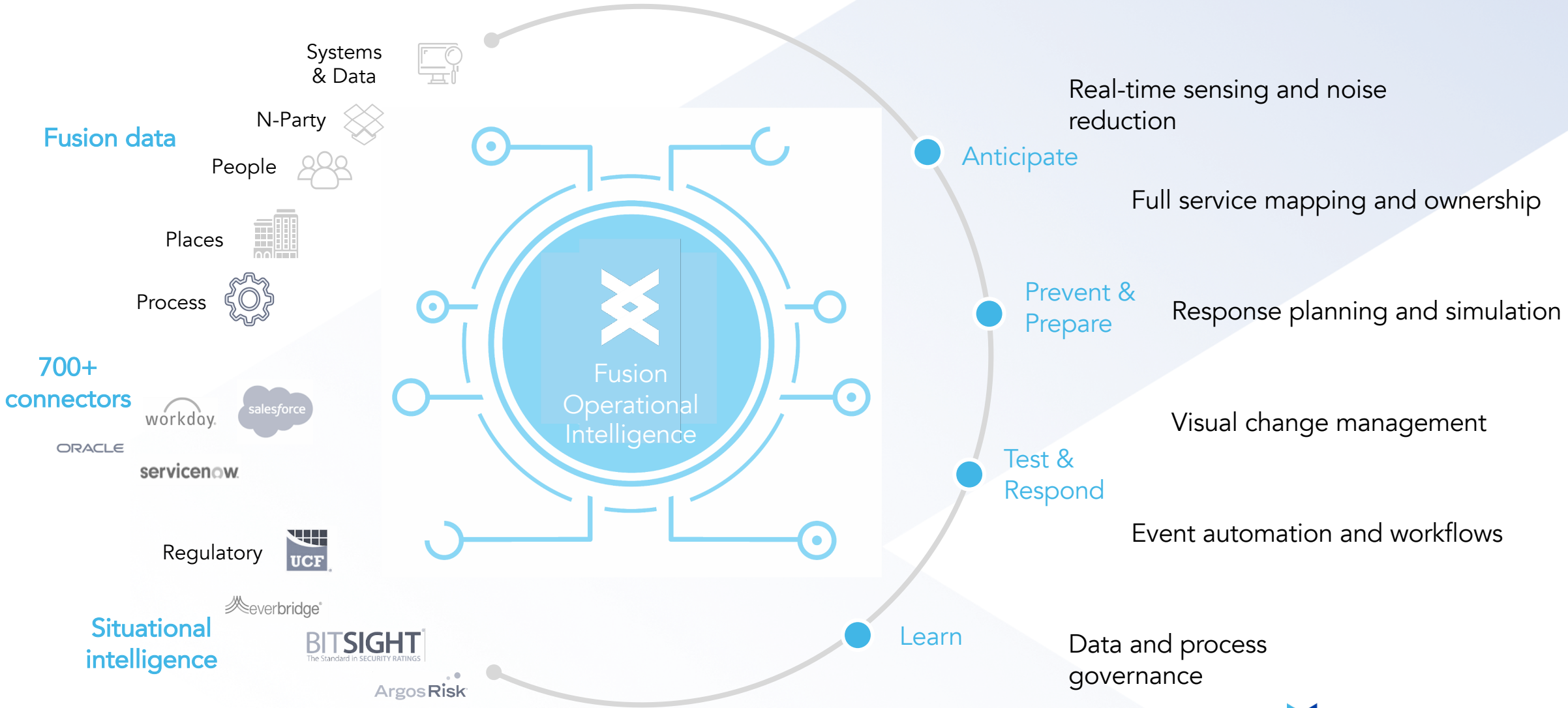
Leverage predictive insight to address risks before they escalate.

Teams understand the impact of change before it happens.

Continuous learning, improvement, and prevention woven into the daily cadence of operations.

True operational single pane of glass, insights delivered where teams live and work.

Risk & Resilience is the nerve center for the modern enterprise



Highlights from the BCI Cyber Resilience Report 2021

FUSION RISK MANAGEMENT

About the Report

Nature of the Cyber Threat

FUSION RISK MANAGEMENT

Number of attacks is increasing, but so is our ability to respond

25.6%
0

41.7%
1-5

5.8%
6-10

4.6%
11-20

2.1%
21-50

1.2%
51-100

1.2%
101-250

1.2%
251-500

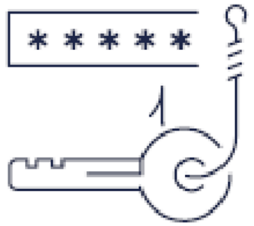
1.7%
501-1000

2.5%
1000+

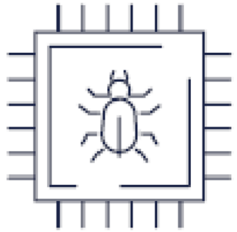
12.4%
I don't know

Phishing is the most prevalent type of attack

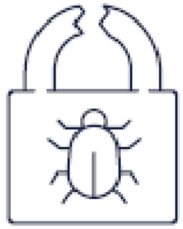
What types of cyber security incidents have caused disruption to your organization in the last 12 months? (Top 5 responses)



65.7%
Phishing, spear phishing



51.4%
Malware



33.6%
Denial of Service or Distributed Denial of Service

28.6%
Social engineering

25.7%
Ransomware

Ransomware is the greatest threat

Which of the following do you feel are of greatest threat to your organization over the next five years in terms of cyber security?

79.6%
Ransomware attack

40.9%
Government-sponsored cyber attacks

39.4%
Reputational damage

39.4%
Network perimeter and endpoint security

35.8%
Lack of available talent/skilled professionals to employ

31.4%
Internet of things devices

29.2%
Cyber attacks with physical security consequences

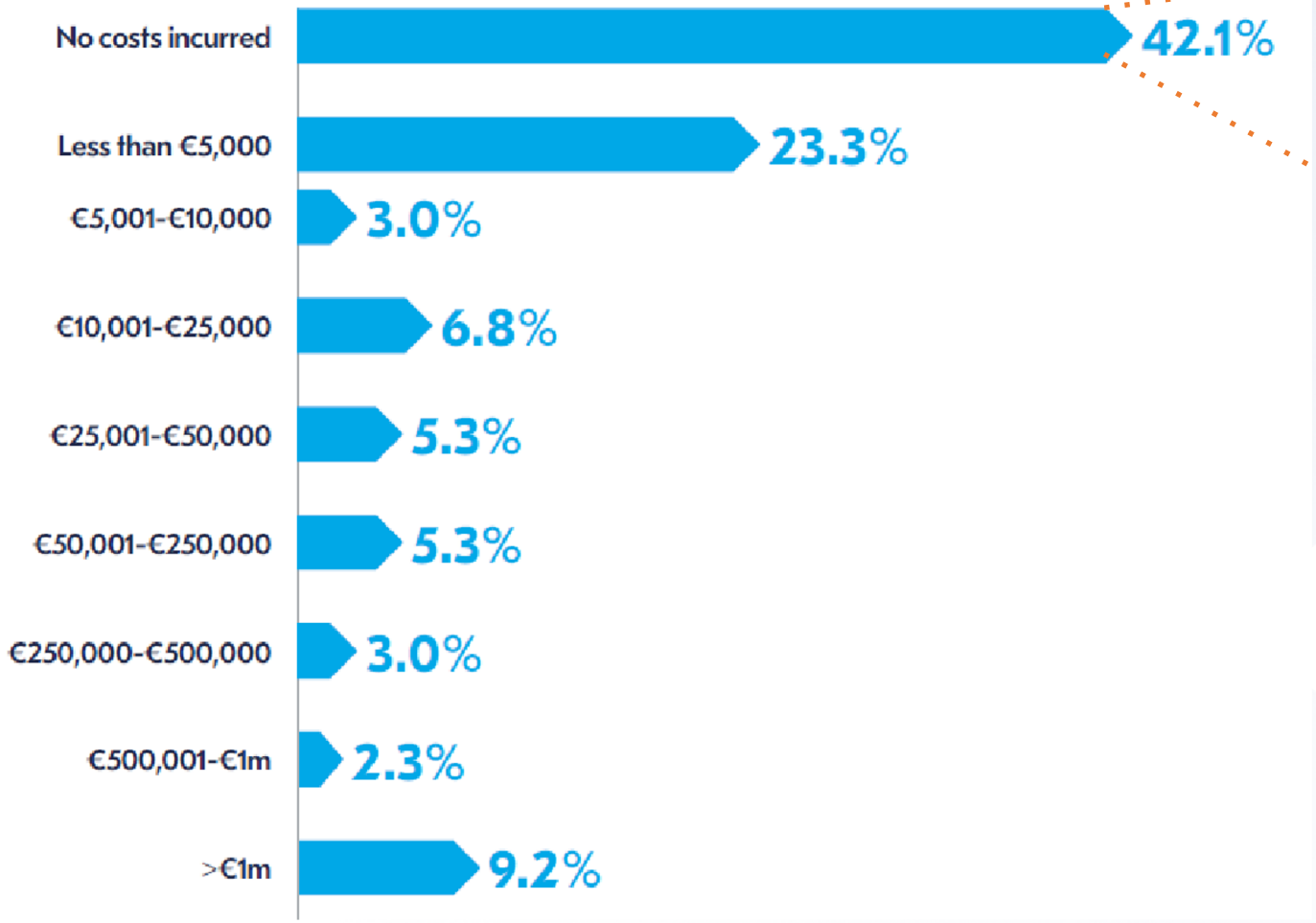
24.1%
Hacktivists

Leadership and Cyber Resiliency

FUSION RISK MANAGEMENT

Leadership buy-in is crucial to keeping cyber crime costs low

What was the approximate financial cost of your cumulative cyber incidents in the last 12 months?

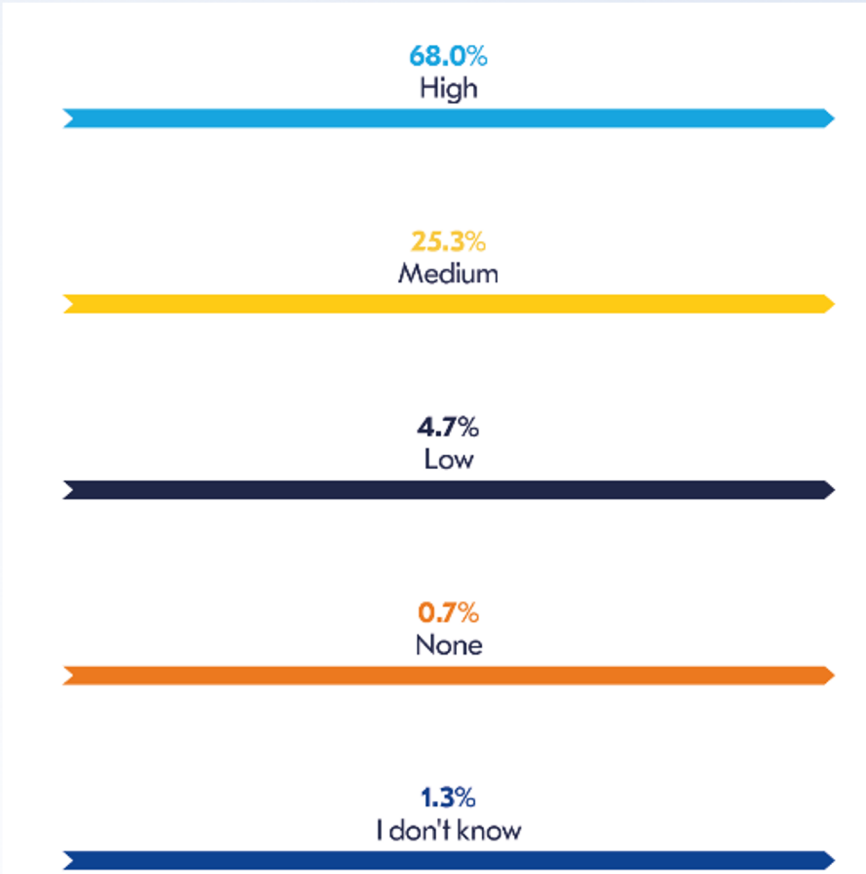


Level of management commitment to cyber crime

Zero, low or medium:
32.6% incurred no costs

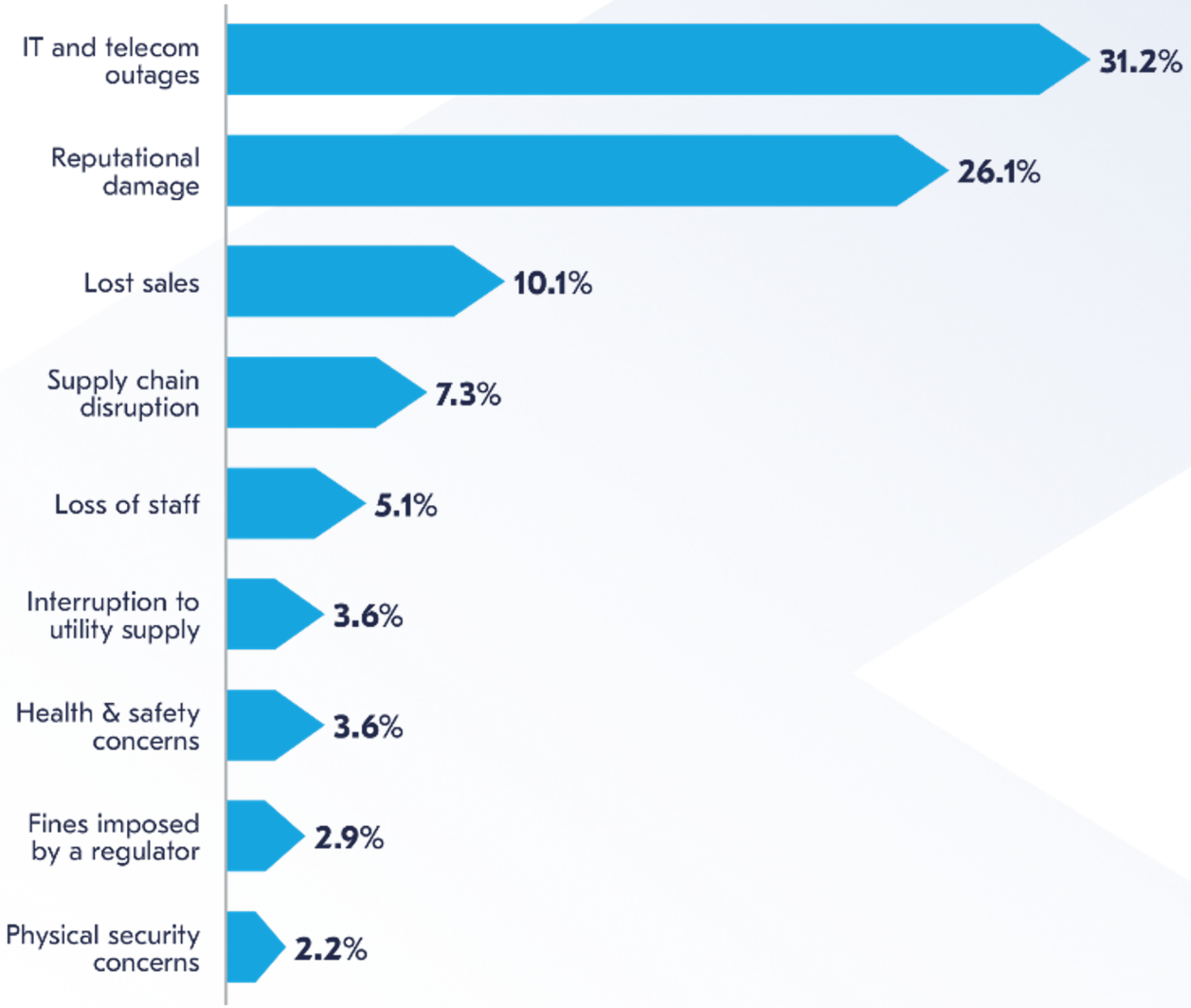
High: **50.0%**
incurred no costs

68% of companies report a high degree of leadership commitment



Cyber attacks are increasingly causing strategic disruption

What secondary effects has your organization experienced as a result of a cyber security incident in the past year?



Cyber Resiliency in Practice

FUSION RISK MANAGEMENT

90% of organizations have cyber controls/indicators in place

Do you have controls and indicators in place to manage your cyber security risk posture?

37.5%
Yes, and they are well tested and mature

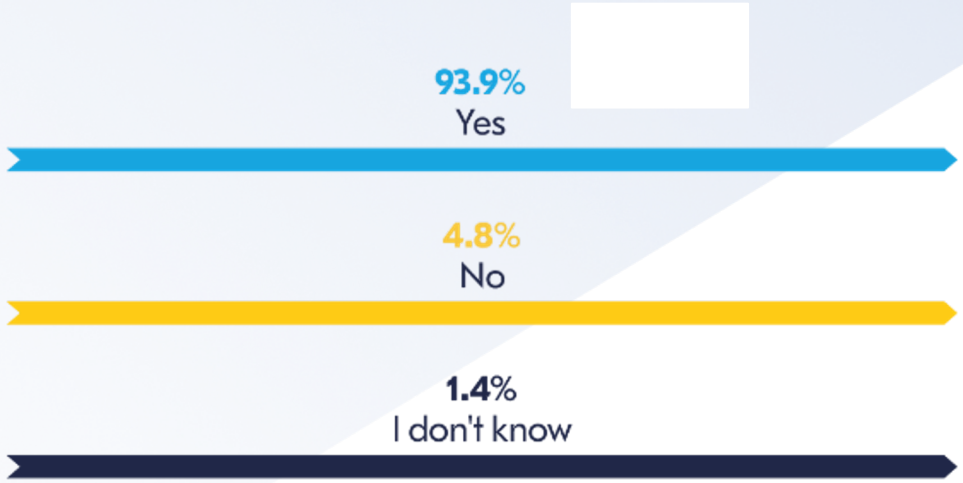
52.2%
Yes, but they are still evolving

6.5%
Not yet, but this is something we are actively working on

1.6%
Not yet, but will be a priority for 2022

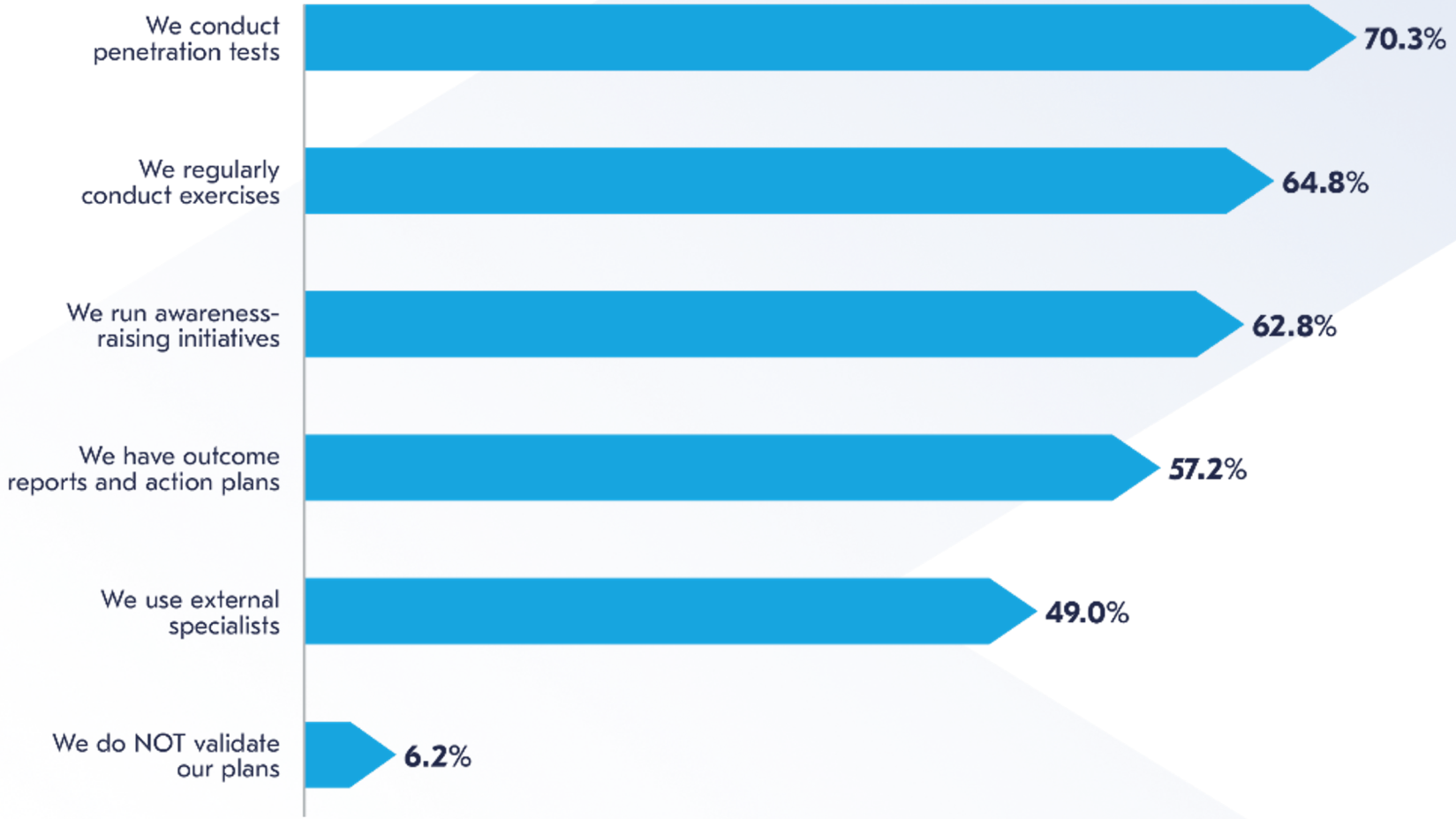
2.2%
No, this is not a priority

Nearly all organizations had cyber BC arrangements



Most organizations validate plans regularly

How does your organization validate its own plans against cyber security incidents?



BC is increasingly covering strategic aspects of the business

How do business continuity arrangements help you deal with cyber security incidents?

88.7%
They ensure a faster recovery

59.2%
They mitigate financial losses

55.6%
They help detect attacks at an early stage

54.2%
They ensure there is a consistent PR strategy to mitigate reputational losses

43.7%
They reduce the likelihood of human error

43.0%
They thwart attacks before they impact the organization

Cybersecurity and Technology

FUSION RISK MANAGEMENT

Less than a third of companies have a cyber single source of truth

31.1%
We have one primary system of cyber risk and resilience information

52.0%
No single hub: We pull from a variety of internal systems

5.4%
This is a gap; we are not able to get the information at this time

11.5%
This is a gap; we currently have no reporting in place

Many teams are involved in cyber resilience

38.1% Cyber security

29.3% IT

12.9% Senior management

6.8% Business continuity

2.0% Risk management

1.4% Disaster recovery

0.7% Crisis management

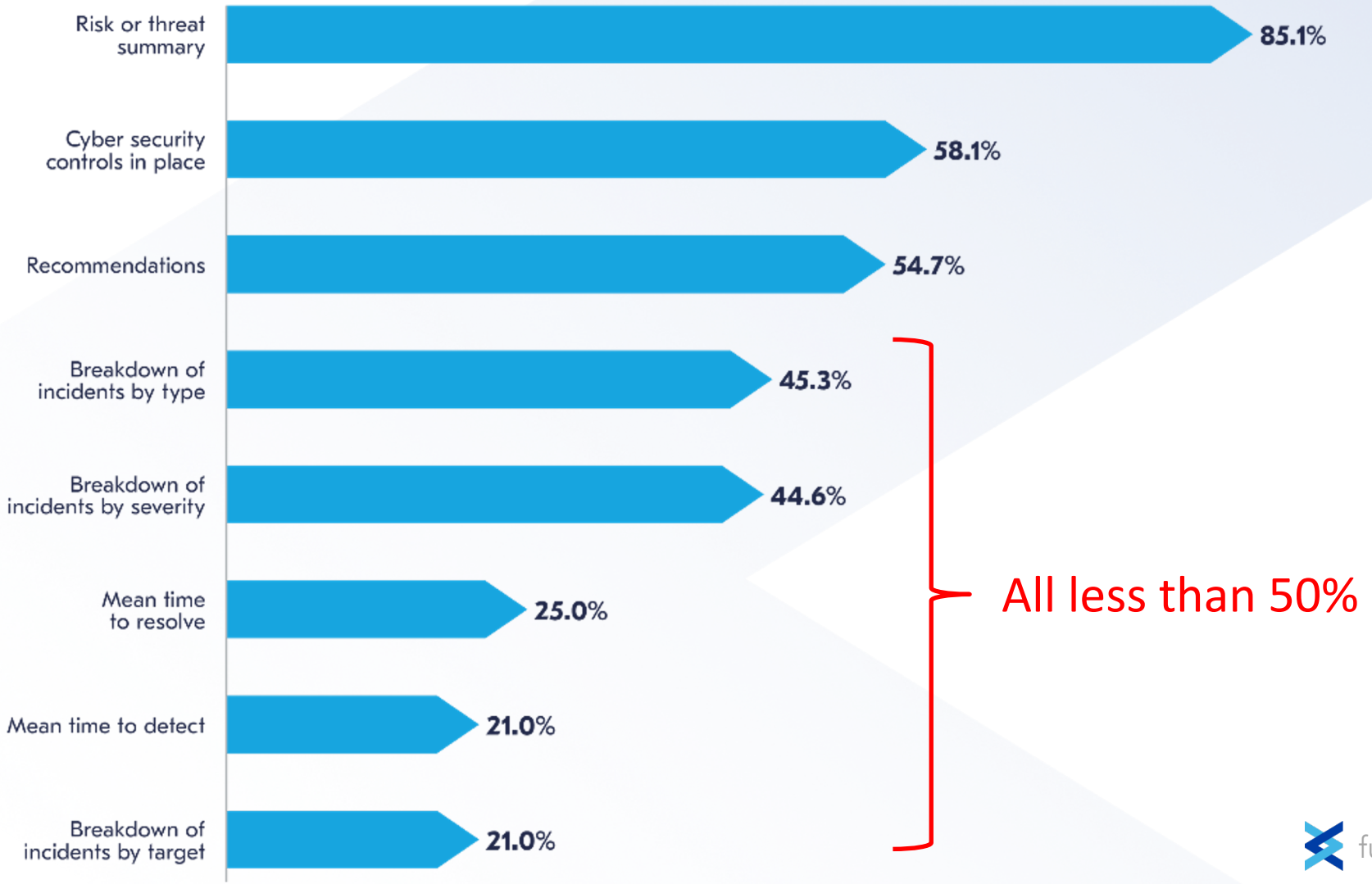
0.7% Operations management

0.7% I don't know

7.5% Other

Gaps remain in cyber insights required by senior leadership

What cyber resiliency information are you expected to report to the board and/or senior management?



Using Fusion for Cyber Resiliency

FUSION RISK MANAGEMENT

Your Technology and Cyber Resilience, Unified

Fusion is your single pane of glass into holistic threat and response

Improve risk metrics and key risk indicators

Simplify cyber and operational risk reporting

Enhance toolkits and increasing automation

Bolster data quality and capture

Cyber risk quantification

Align frameworks to evolving regulation

Nearer real-time reporting

Improved prioritization

Personalize information and experiences

Cyber Risk & Information Security – Telemetry Integration

Beyond a Critical Partnership

Vulnerabilities & Malware Analysis

IT Cyber Security solutions focused on identifying technology vulnerabilities, cyber penetration, and malware risks

Data Security & Classification

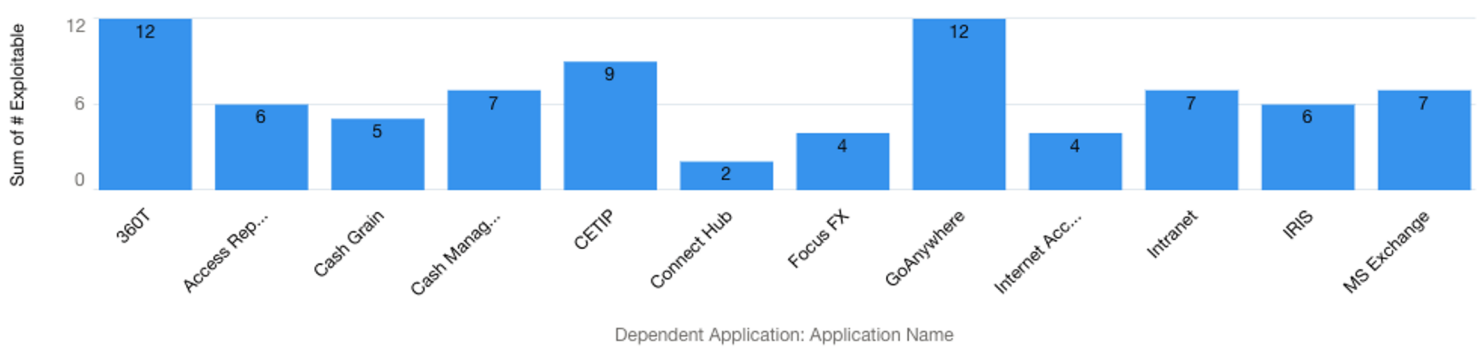
Identification of assets that represent risk relative to Data & Information Security

Business Risks & Information Alignment

Align and communicate Telemetry Risks based on business & client impacts

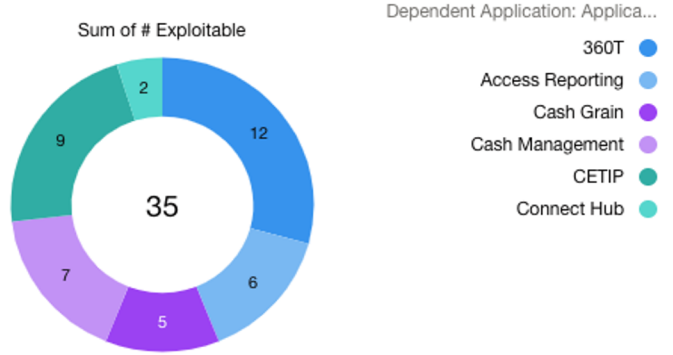
Cyber Risk & Information Security Vulnerabilities

Apps with Exploitable Vulnerabilities



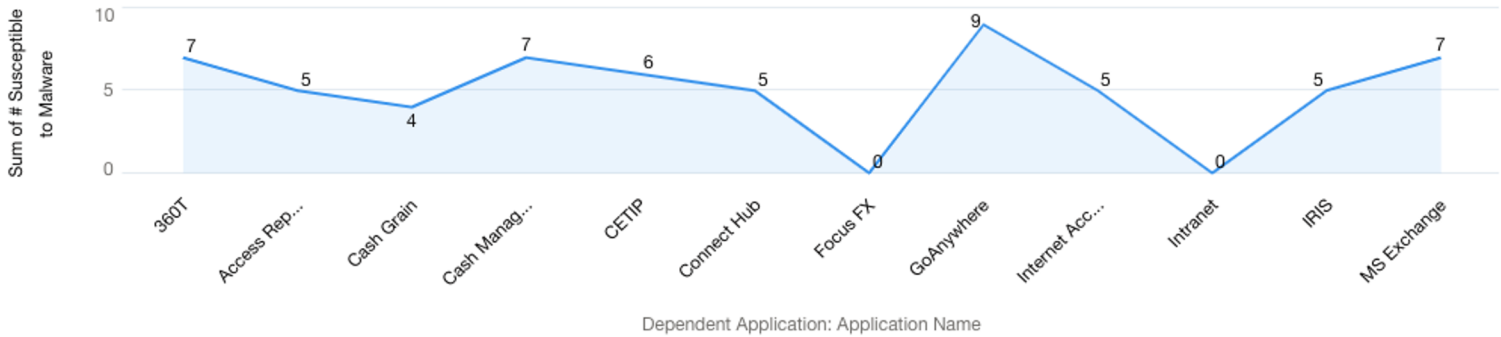
View Report (Components with CyberRisk w Apps)

Application with Exploitable Risks



View Report (Components with CyberRisk w Apps)

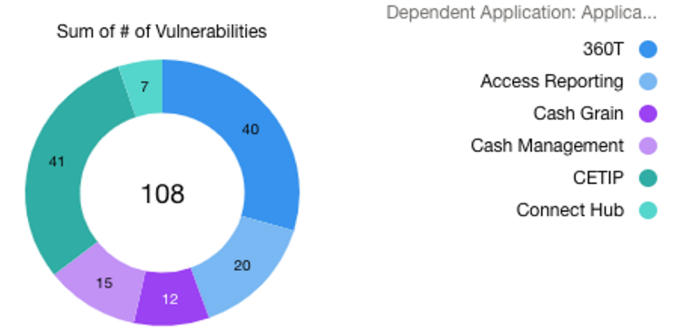
Application with suspected Malware



View Report (Components with CyberRisk w Apps)

Application Vulnerabilities (Total)

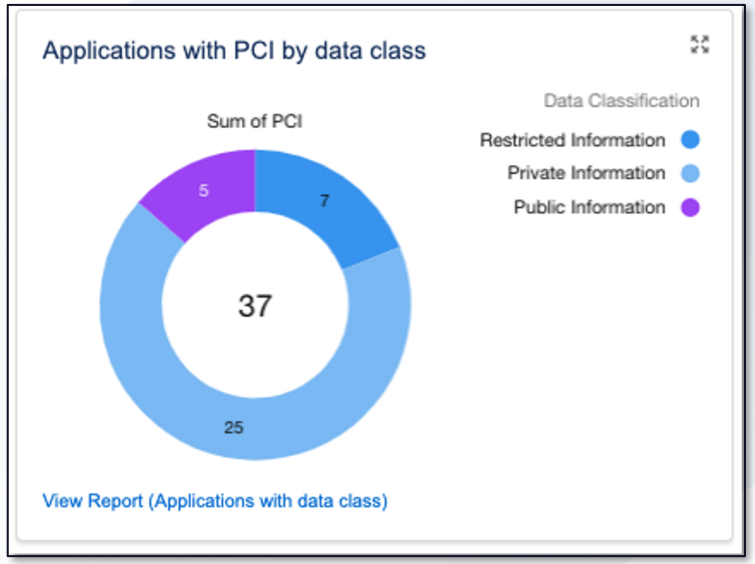
Sum of Vulnerabilities

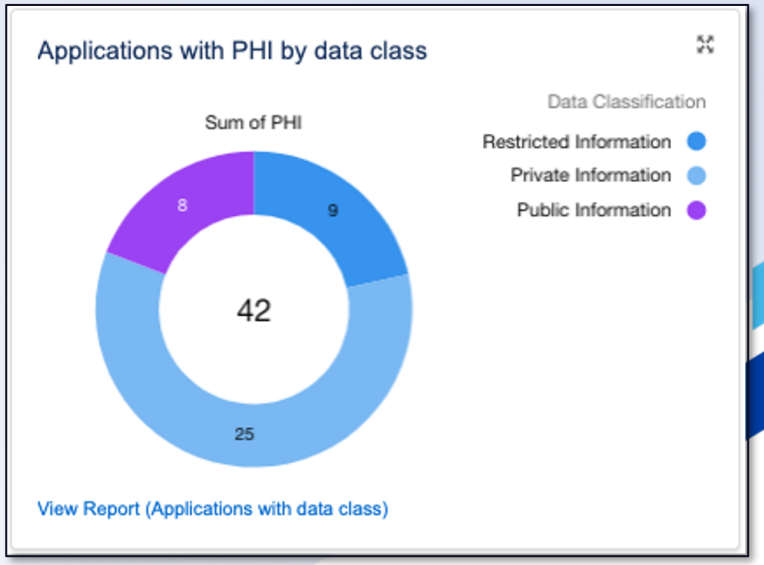


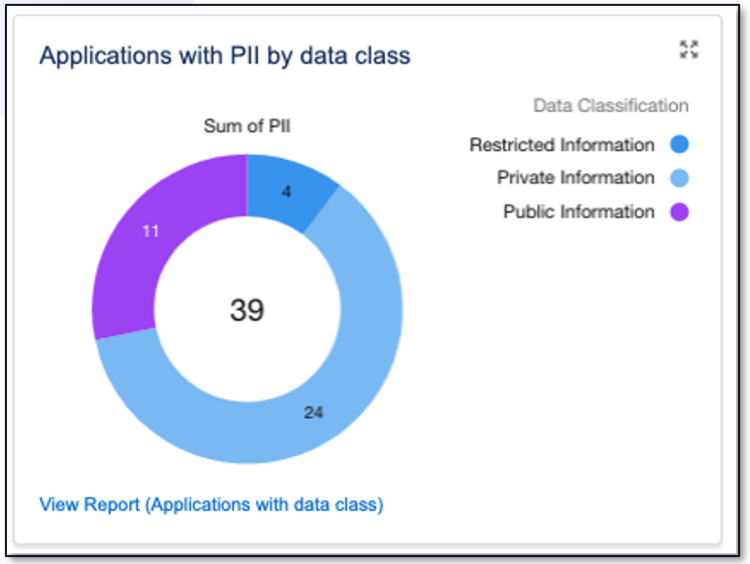
View Report (Components with CyberRisk w Apps)

Data Security & Classification

- Applications with Regulated Data
  - PHI, PCI, PII
- Application Data Classification
  - Restricted Information
  - Private Information
  - Public Information







Cyber Risk – Telemetry Integration

- Gather information at Component / Server
- Map risks to processes & Business Services
- Communicate Risks based on business & client impacts

Report: Components with Application Component Dependencies and Applications
Components with CyberRisk w Apps

Total Records	Total # Exploitable	Total # of Vulnerabilities	Total # Susceptible to Malware
26	35	108	28

Dependent Application: Application Name	Component: Component Name	# Exploitable	# of Vulnerabilities	# Susceptible to Malware
360T (3)	MXP345PRD	5	9	7
	MXP421PRD	4	8	0
	MXP311PRD	3	23	0
Subtotal		12	40	7
Access Reporting (3)	Exchange Server	2	7	5
	Citrix cluster 1	2	6	0
	Linux Server	2	7	0
Subtotal		6	20	5
Cash Grain (1)	Windows Blade Server - 1	5	12	4
Subtotal		5	12	4
Cash Management (2)	MXP345PRD	5	9	7
	Citrix cluster 1	2	6	0
Subtotal		7	15	7

Telemetry example using Rapid7

Availability & Resilience Metrics

Data Integration considerations

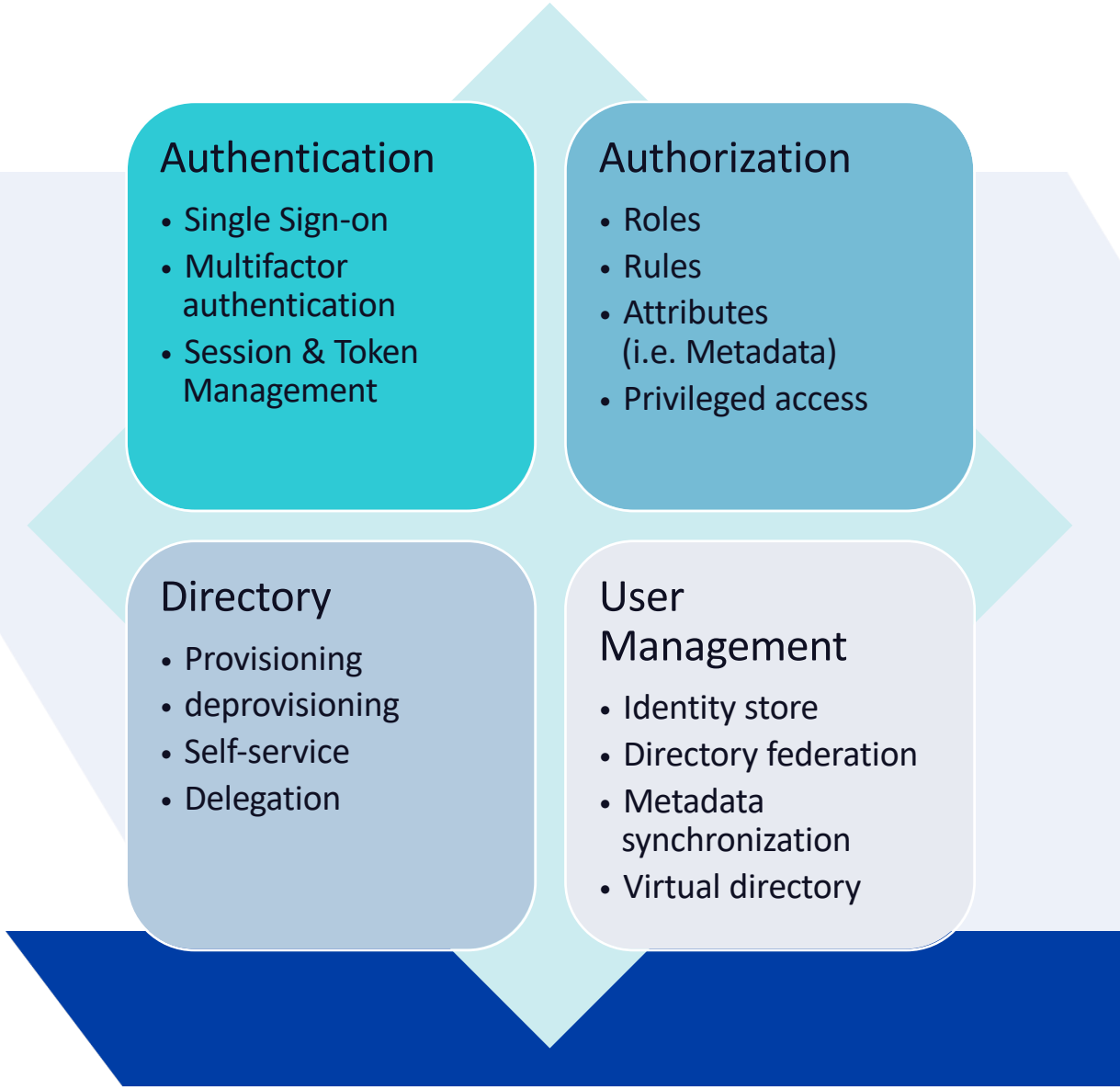
- Availability Metrics
- Systems with Resilient Architecture
- Maintenance & System refresh status

	Description
Availability	Uptime percentage, as defined by the SLA
Outage Occurrence Rate	Outage frequency relative to system unavailable
Average Downtime	Mean time of System unavailability – should be tracked at system & component level
Mean time between Failures	MTBF – duration of operations between failures

Identity & Access Management

Risk Metrics & Data Integration Considerations

- Alignment & levels of service with business risk
- Attack & phishing metrics
- Policies aligned & influenced by data classification



Q&A

FUSION RISK MANAGEMENT

Thank You

fusionrm.com

@fusion-risk-management

@FusionRiskManagement

@FusionRiskMgmt