

DELIVERING OPERATIONAL RESILIENCE IN AN AGE OF RANSOMWARE & DIGITAL TRANSFORMATION

Chris Beckett
Security Sales Engineer, Rubrik X

chris.beckett@rubrik.com

www.rubrik.com

Come and see us! Booth F25



**ADVERSARIES
HAVE FIRST MOVER
ADVANTAGE**





ADVERSARIES ADAPT

RISK EQUATION

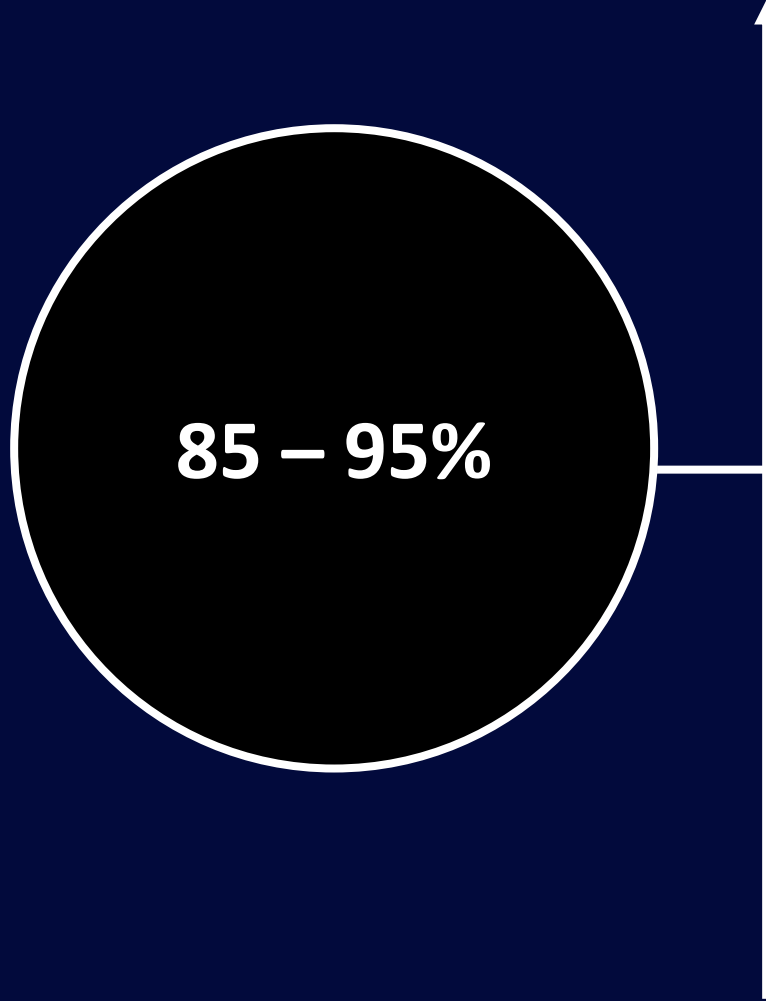
LIKELIHOOD

| | | | | |
|---------------|---------------|---------------|---------------|----------------|
| Moderate | High Moderate | High | Very High | Extremely High |
| Low Moderate | Moderate | High Moderate | High | Very High |
| Low | Low Moderate | Moderate | High Moderate | High |
| Very Low | Low | Low Moderate | Moderate | High Moderate |
| Extremely Low | Very Low | Low | Low Moderate | Moderate |

IMPACT

AVERAGE CYBER SECURITY BUDGET ALLOCATION

LIKELIHOOD



IMPACT

CISO IN THE AGE OF TOOL SPRAWL

- + Budget
- + Headcount
- + Complexity
- + Licensing Costs
- + Attack Surface
- + Alerts
- + User Friction
- + Reduced Agility



Average enterprise has over 130 different cyber security tools deployed

Deloitte.

75% of organisations that pay ransoms have up-to-date network & endpoint security tools deployed

SOPHOS

PRE-RANSOMWARE LOSS EVENTS

REPUTATION
LITIGATION
REGULATOR
Y

SECONDARY



LIKELIHOOD

| | | | | |
|---------------|---------------|---------------|---------------|----------------|
| Moderate | High Moderate | High | Very High | Extremely High |
| Low Moderate | Moderate | High Moderate | High | Very High |
| Low | Low Moderate | Moderate | High Moderate | High |
| Very Low | Low | Low Moderate | Moderate | High Moderate |
| Extremely Low | Very Low | Low | Low Moderate | Moderate |

IMPACT



POST-RANSOMWARE LOSS EVENTS

INABILITY TO
EXECUTE
ORGANISATION'S
MISSION

PRIMARY

LIKELIHOOD

| | | | | | | | |
|---------------|---------------|---------------|---------------|----------------|----------------|----------------|----------------|
| Moderate | High Moderate | High | Very High | Very Very High | Extremely High | Ultra High | Unsustainable |
| Low Moderate | Moderate | High Moderate | High | Very High | Very Very High | Extremely High | Ultra High |
| Low | Low Moderate | Moderate | High Moderate | High | Very High | Very Very High | Extremely High |
| Very Low | Low | Low Moderate | Moderate | High Moderate | High | Very High | Very Very High |
| Extremely Low | Very Low | Low | Low Moderate | Moderate | High Moderate | High | Very High |

IMPACT



**WITH ALL THIS INVESTMENT IN PREVENTION &
DETECTION THE BOARD OFTEN HAVE AN EXPECTATION
THAT INCIDENTS WON'T HAPPEN**

**35% OF ORGANISATIONS THAT HAVE HAD A RANSOMWARE
ATTACK SUFFERED C-LEVEL RESIGNATIONS OR FIRINGS AFTER
THE INCIDENT**



SHARED INCIDENT RESPONSIBILITY



INCIDENT

SECURITY

IT

RECOVERY

A yellow excavator with a hydraulic arm is shown in the process of demolishing a multi-story building. The building's structure is partially collapsed, with debris visible. The excavator is positioned on the left side of the frame, and its arm is extended towards the building.

REBUILD

A yellow excavator is shown demolishing a building, with a large pile of debris in the foreground. The excavator is positioned on the left side of the frame, and its arm is extended towards the building. The debris pile is composed of various materials, including wood, metal, and concrete.A photograph of a desert landscape featuring sand dunes and sparse, low-lying green vegetation. The sand is a light brown color, and the vegetation consists of small, scrubby bushes.

ANTICIPATE

A photograph of a desert landscape featuring sand dunes and sparse, low-lying green vegetation. The sand is a light brown color, and the vegetation consists of small, scrubby bushes.

PREVENT

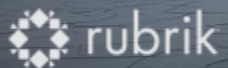
A photograph of a desert landscape featuring sand dunes and sparse, low-lying green vegetation. The sand is a light brown color, and the vegetation consists of small, scrubby bushes.

ADAPT

A photograph of a desert landscape featuring sand dunes and sparse, low-lying green vegetation. The sand is a light brown color, and the vegetation consists of small, scrubby bushes.

RESILIENCE

IT EVENT RESILIENCE



CYBER EVENT RESILIENCE



IT

USE CASES

DATA RESILIENCE



**Enterprise
Data Protection**



**Cloud
Data Protection**

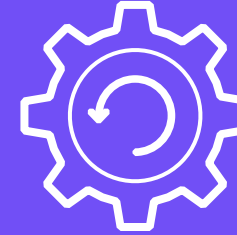


M365 Protection



**Invulnerable to
Ransomware &
Wiper Attacks**

DATA RECOVERY



Mass Recovery

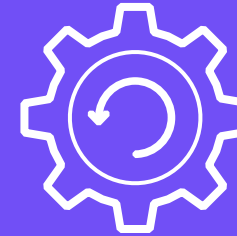


Orchestrated App Recovery

**DATA
OBSERVABILITY**



**DATA
RECOVERY**



CYBER

USE CASES



**Ransomware Monitoring
& Investigation**



**Wiper & Malicious Insider
Monitoring & Investigation**



**Sensitive Data
Discovery**



Permission Auditing



Threat Hunting



Filesystem Forensics



Threat Containment



Vulnerability Containment



Artefact Extraction



**Digital Twins for Cloud Migration, Pen Testing,
Vulnerability Management & Deception**

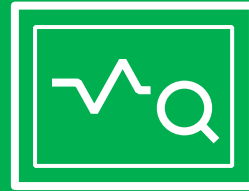
IT

USE CASES

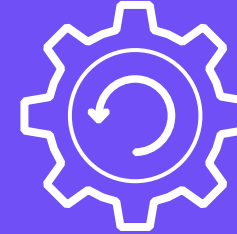
DATA
RESILIENCE



DATA
OBSERVABILITY



DATA
RECOVERY



CYBER

USE CASES



Enterprise
Data Protection



Cloud
Data Protection



M365 Protection



Invulnerable to
Ransomware &
Wiper Attacks



Ransomware Monitoring
& Investigation



Wiper & Malicious Insider
Monitoring & Investigation



Sensitive Data
Discovery



Permission Auditing



Threat Hunting



Filesystem Forensics



Mass Recovery



Orchestrated App Recovery



Threat Containment



Vulnerability Containment



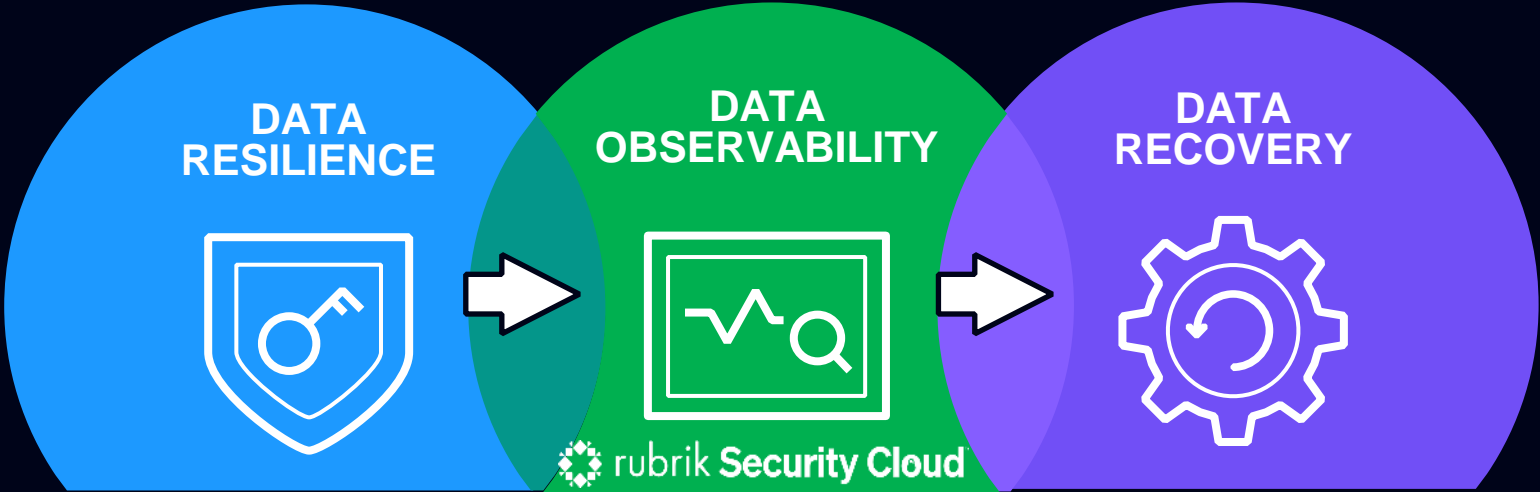
Artefact Extraction



Digital Twins for Cloud Migration, Pen Testing,
Vulnerability Management & Deception

RUBRIK SECURITY CLOUD: THE PLATFORM FOR OPERATIONAL RESILIENCE

IT
USE CASES



CYBER
USE CASES

- | | | | | | |
|---|--|--|--|---|--|
|  | Enterprise Data Protection |  | Ransomware Monitoring & Investigation |  | Mass Recovery |
|  | Cloud Data Protection |  | Wiper & Malicious Insider Monitoring & Investigation |  | Orchestrated App Recovery |
|  | M365 Protection |  | Sensitive Data Discovery |  | Threat Containment |
|  | Invulnerable to Ransomware & Wiper Attacks |  | Permission Auditing |  | Vulnerability Containment |
| | |  | Threat Hunting |  | Artefact Extraction |
| | |  | Filesystem Forensics |  | Digital Twins for Cloud Migration, Pen Testing, Vulnerability Management & Deception |

DELIVERING VALUE ACROSS DAY-TO-DAY CYBER OPERATIONS



**Sensitive Data
Discovery**



Permission Auditing



**Ransomware
Detection**



Artefact Extraction



Mass Recovery



Penetration Testing



**Wiper & Malicious
Insider Detection**



Filesystem Forensics



Orchestrated App Recovery



**Breach & Attack
Simulation**



Threat Hunting



Threat Containment



**Invulnerable to
Ransomware &
Wiper Attacks**



Deception



Vulnerability Containment

WHAT THIS MEANS FOR THE CISO



Don't Backup. Go Forward.

