RSAConference2022
San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **PART2-W09**

Protect Valuable Data as Employee Turnover Rages

Joe Payne

President & CEO
Code42

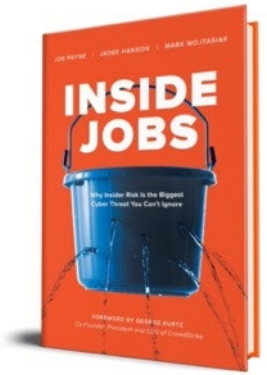
Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

Introduction

Joe Payne is the President and CEO of Code42 Software, the leader in Insider Risk Management that focuses on reducing the risk of data leakage from insiders while enabling the collaboration culture. Payne is a seasoned executive with more than 20 years of leadership experience and a proven track record leading high growth security and technology companies. He previously served as CEO of Eloqua and eSecurity, and was President of iDefense. Payne recently co-authored the book, Inside Jobs, which highlights the data risks related to insiders.



Insider Risk: Departing Employee takes source code

Insider Risk: Unintentional data infiltration

The resurgence of Insider Risk

- Insider Risk or Insider Theft has been a problem for a long time
- What has changed to make this threat an urgent problem?
- Why do cyber-security teams need to pay attention in 2022?

There are 3 key drivers that have changed the prevalence and urgency around Insider Risk

RISK DRIVER

DIGITAL TRANSFORMATION

IS CHANGING HOW WE WORK TOGETHER

Organizations are pursuing digital strategies

90%

of organizations are digitizing their data and business processes

Source: Virtru, 2021

Another part of digital transformation is collaboration technology

88%

of CIOs want to make employee productivity & efficiency a top priority

Sources: Gartner CEO Survey 2019, Code42 2019 Data Exposure Report

CIOs have deployed cloud-based tech to collaborate and share information

RISK DRIVER 2

KNOWLEDGE WORKERS

WORK FROM ANYWHERE

The workforce is working from anywhere

PRE-COVID:

Knowledge workers spent 23% of their working week outside the office and 19% of the week working from home

Source: Code42 2019 Data Exposure Report

TODAY:

Fewer than 1 in 4 workers willing to return to “almost entirely in the office” work models

Source: PwC study

IT no longer controls
the tools, networks,
and applications
where work gets done

37% of workers use unauthorized apps daily, while 26% of them use them weekly to share files with colleagues

Source: Code42 Data Exposure Report, 2020

RISK DRIVER

3

PEOPLE ARE CHANGING JOBS FASTER THAN EVER

…and that's not changing anytime soon

The average employee tenure is decreasing

Generations Y & Z make up 59% of the workforce and their average tenure is less than 3 years

Source: US Bureau of Labor Statistics, 2021

The Great Resignation:
4.5 million Americans voluntarily left their jobs in November

Source: US Bureau of Labor Statistics, 2021

75% of GenZ and 67% of Millennials will change jobs in the next 12 months

Departing employees are taking company data with them

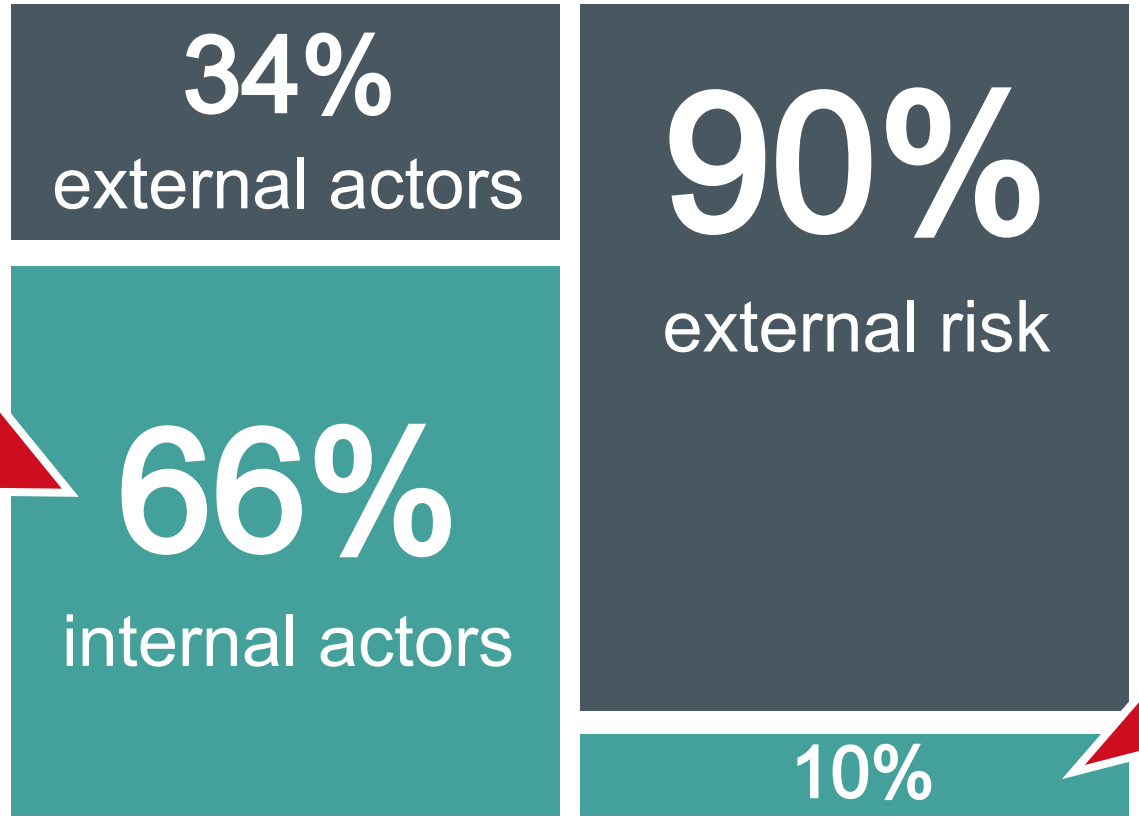
63%

of departing employees admit to taking data to help them in their new job.

Source: Code42 2020 Data Exposure Report

The perfect storm for insider threats

66% of data breaches in the last 12 months were inside jobs.



Only 10% of security budgets are dedicated to insider risk.

Source: Code42 2019 Data Exposure Report; Code42 2022 Data Exposure Report

Malware Risk

- Bad Actor
- Fast Moving / Propagating
- Isolate / Disconnect / Quarantine
- Interrogate
- Security can handle response
- Never accidental
- Education useless
- You can get fired for not reacting
- No hesitation about legal issues
- I have years of expertise

Insider Risk

- Colleague
- Contained / Doesn't Spread
- Investigate / Understand
- Question
- Need HR and maybe even Legal
- Often accidental
- Education critical
- You can get fired for over-reacting
- No idea what the legal issues are
- I THINK have years of expertise

Insider Risk Management Programs require a different approach in a modern, collaborative world

How to Apply this in your organization: The Three Ts of an Insider Risk Management Program

Transparency

Training

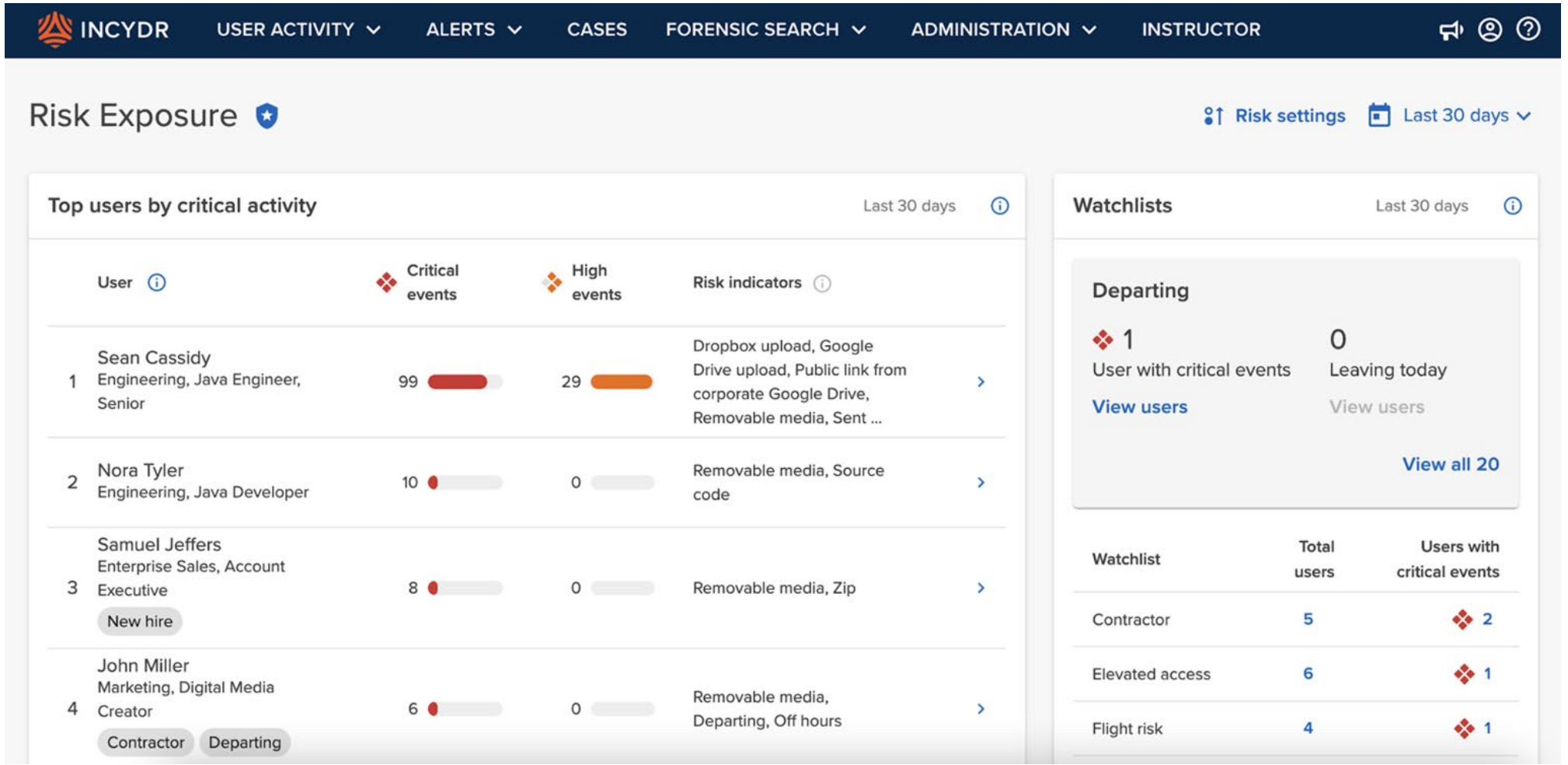
Technology

Transparency

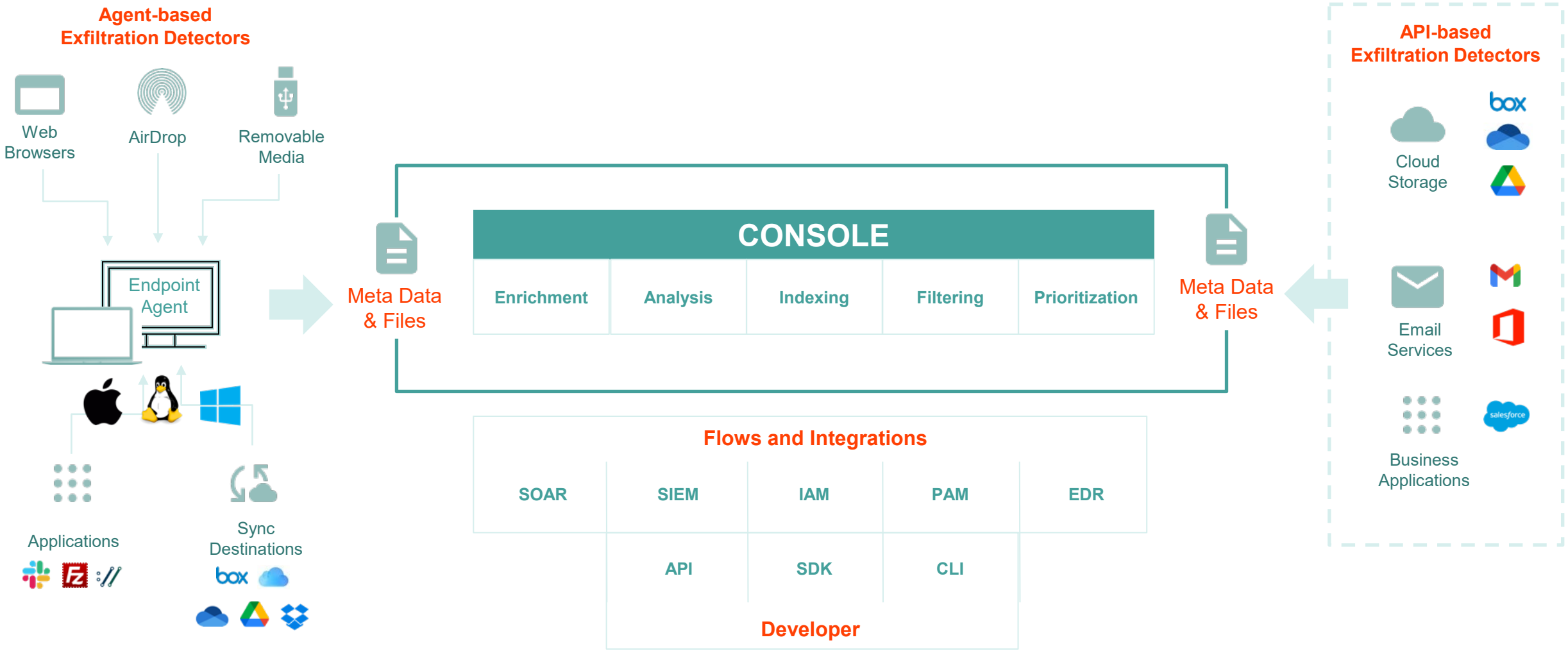
Training (Education)

- Many employees don’t know the rules
- What can I take? What can I use? Am I entitled to it? Do you even care?
- Start with Proactive Training to clearly answer all these questions
- Offer Different Lessons for different types of employees
  - Developers need source code rules
  - Salespeople need Salesforce rules

The last T is technology: Trust but Verify



Insider Risk Management
Endpoints, and Clouds without getting in the users' way.



Apply: Getting Started
Investigative and Response Process




	Inquire	Educate	Resolve	Contain
Objective	• Improve/Reinforce Understanding of Policies and • Reduce future data exposure	• Assign micro-training • Send policy for acknowledgement	Determine if investigation is required if so escalate to appropriate parties	• Assign micro-training • Send policy for acknowledgement
Action	• Assume positive intent via corporate communication platform	• Assign micro-training • Send policy for acknowledgement	• Require action from user - attest to data removal • Escalate to manager • Escalate to HR • Escalate to Legal	• Conditional access controls • Disable USB • Stop local sync apps • Network contain • Lock device