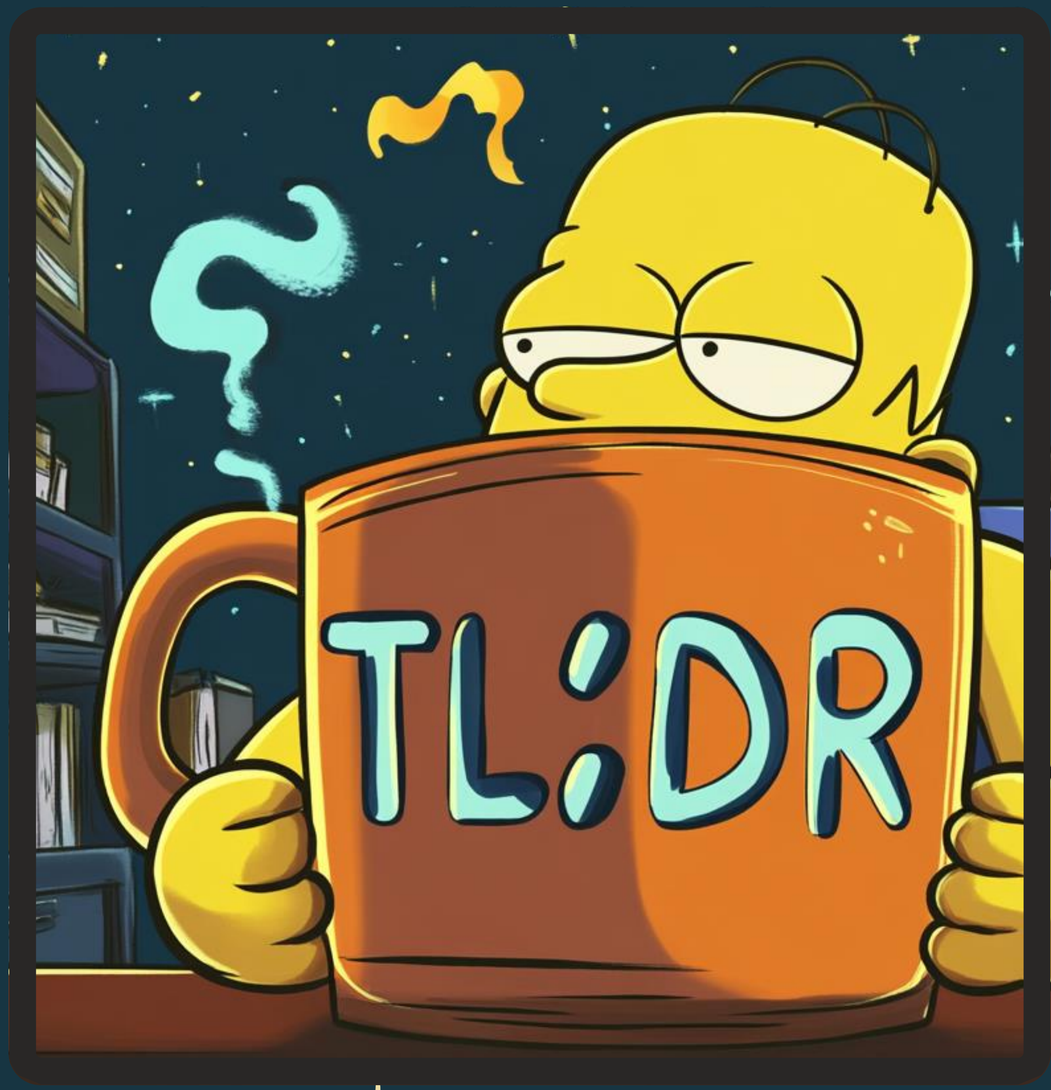
N2WS

TL;DR WEBINAR SERIES

Episode 14:

INSIDER THREATS



HOSTED BY

Sebastian Straub

Principal Solutions Architect

Jon Myer

CCO Myer Media

The 3 flavors of insider threats ⬇

1. Malicious

Unusual, unauthorized behavior for personal gain or vengeance

2. Negligent

Human error, careless, stressed or distracted employee

3. Compromised

Stolen credentials, manipulated by phishing, social engineering

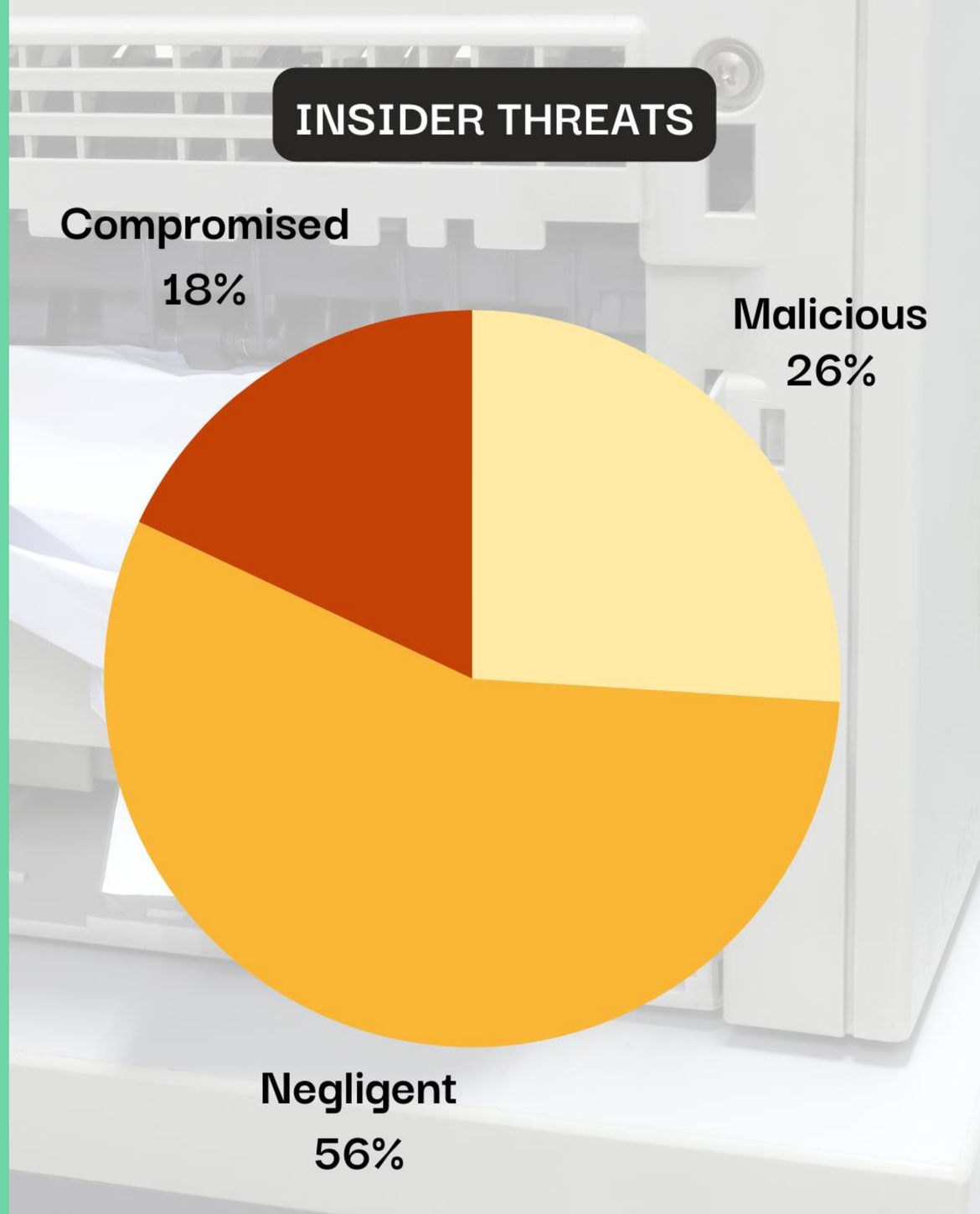
The insider threat breakdown

Average cost per incident type:

- Malicious incident is $650K
- Negligent incident is $485K
- Compromised incident is $800K

TL·DR on N2WS

get.n2ws.com/tldr



Insider incidents by the numbers ↓

83%

OF ORGANIZATIONS REPORTED INSIDER ATTACKS IN 2024

500%

REPORTED INCREASE OF ATTACKS SINCE 2023

$18M

AVERAGE YEARLY COST OF INSIDER THREATS

86

AVERAGE NUMBER OF DAYS TO REPORT AN INSIDER INCIDENT

TL·DR on N2WS

get.n2ws.com/tldr

How are organizations securing themselves?

1

MONITORIN G

- Behavioral analytics, understand usage patterns
- Real-time endpoint monitoring

2

INCIDENT RESPONSE

- Guarantee full environmental failover and granular restore
- Automatic regular DR drills
- Implement layered security: cross account, immutability and cross-cloud DR (ideal)

3

EDUCATION

- Deliver security awareness training to employees
- Conduct regular anonymous surveys
- Check-in and encourage open communication

TL·DR on N2WS

get.n2ws.com/tldr