CYBER RESILIENCE AWARENESS DAY

Quantifying Cyber Resilience Readiness

ISSA
Information Systems Security Association



Quantifying Resilience:
Start With the Humans, Not the Tools

Dr. Jessica Parker | Wise Bites LLC

Hours to Exploit. Months to Contain.

TIME TO EXPLOIT IN 2025

24-48 hours

Source: Torres, A., Santos, D., & Manky, D. (2026). *2026 Global Threat Landscape Report: Insights from FortiGuard Labs*. Fortinet, Inc.

TIME TO IDENTIFY AND CONTAIN

247 days

Source: IBM. (2026). *Cost of a data breach report 2026: The AI tipping point*. https://www.ibm.com/reports/data-breach.

Start With the Humans, Not the Tools

Organizations are asking the same question:

"We've invested in AI tools. Has this made our organization more resilient?"

The answer lives in the humans — not the technology.

"When execution is cheap, verification becomes more valuable."
— Christian Catalini, MIT research scientist

Source: Catalini, C. (2026, October 2). *AI is making verification the bottleneck for companies*. Harvard Business Review. https://hbr.org/2026/10/ai-is-making-verification-the-bottleneck-for-companies

Today’s Agenda

01 The Problem

02 The Study

03 So What?

SECTION 01

The Problem

Organizations are investing in AI. Are they safer as a result?

THE STAKES ARE HIGH

~3,850

global exploitation attempts per SECOND

Source: Torres, A., Santos, D., & Manky, D. (2026). *2026 Global Threat Landscape Report: Insights from FortiGuard Labs*. Fortinet, Inc.

The Knowledge Gap

WHAT WE KNOW

GAI adoption in cybersecurity is accelerating

Technical capabilities are advancing rapidly

AI can automate repetitive security tasks

Threat volumes are growing

WHAT WE DIDN'T KNOW

How technology leaders make GAI decisions in practice

What governance practices enhance resilience

How human expertise integrates with AI tools

Whether AI deployments build or erode resilience

SECTION 02

The Study

12 technology executives. Real conversations. Doctoral rigor.

Research Design

HOW

Qualitative Phenomenological

- Semi-structured interviews
- April – July 2025
- Thematic coding

Participants anonymized

WHO

12 Technology Executives

Actively integrating GAI into cybersecurity programs

- Cross-industry
- Decision-making authority over security strategy

Five Themes Emerged from the Data



THEME 1
Risk Management & Quality Control

AI Output Validation

Leadership Role: *Ensure Human Oversight*

Levers: PROCESS (technology)



THEME 2
Strategic AI Governance & Implementation

Cross-Functional Leadership

Leadership Role: *Establish Governance Structure*

Levers: PROCESS (people)

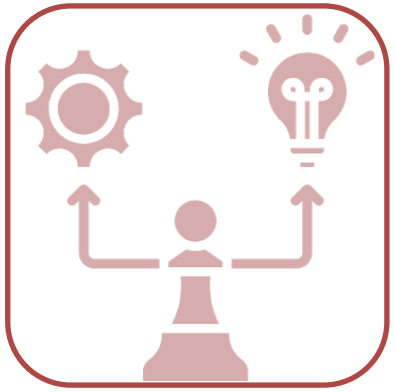


THEME 3
Human-AI Collaboration

Collaborative Intelligence

Leadership Role: *Define Collaboration Models*

Levers: PEOPLE (process)



THEME 4
Strategic Resource Amplification

Workforce Capability Enhancement

Leadership Role: *Measure Strategic Impact*

Levers: PEOPLE (technology)



THEME 5
Third-Party Vendor Impl. & Oversight

Vendor Risk Assessment

Leadership Role: *Govern AI Tools Purchased*

Levers: TECHNOLOGY (process)

PARTICIPANT: “JADE”

“As good as AI is, AI can still hallucinate. And with security tools, we already have false positives. So do we make false positives potentially worse by putting hallucinations on top of that?”

Resilience Implication

Human validation of AI outputs is required by design. Mature organizations build this in from day one.

T1: Risk Management & Quality Control

Source: Parker, J. (2025). *Integrating GAI into cybersecurity: A study of organizational practices* (Publication No. 3255587859) [Doctoral dissertation, Marymount University]. ProQuest Dissertations and Theses Global.

SECTION 03

So What?

Translating research into resilience readiness

Every Day Down, You Pay Two Bills

Your daily cost during recovery, in plain English

Today's cost

Any single day of recovery

Daily cost on day t

=

Response cost

Staff, overtime, outside help. This bill stays flat.

d

+

Revenue not yet back

Shrinks as systems are restored

r × (1 − R(t))

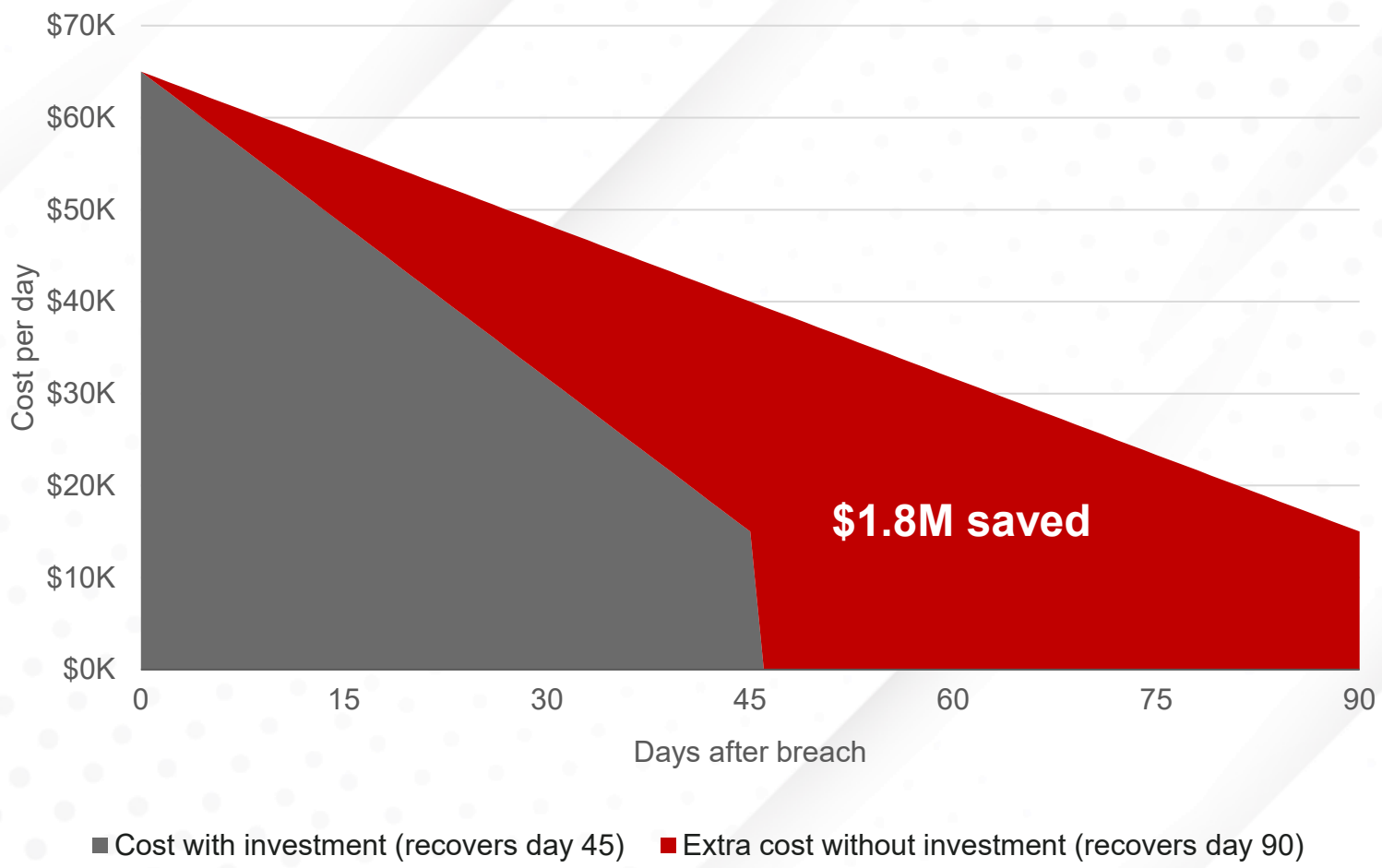
Recover sooner, and the second bill disappears sooner. That is what resilience investment buys.

d = daily response cost · **r** = daily revenue · **R(t)** = share of operations restored on day t (0 = fully down, 1 = fully back)

Formula: Parker (2026).

Halving Recovery Time Saves $1.8M

ILLUSTRATIVE EXAMPLE



$3.6M

Total cost without investment

$1.8M

Total cost with investment

800% return

on $200K a year, if a major incident hits

Assumes $50K/day revenue, $15K/day response cost, and steady restoration. Formula: Parker (2026).

How Long Can You Last?

$$\frac{\text{Cash you can reach}}{\text{Average daily cost during recovery}} = \text{Survival runway (days)}$$

Shortcut from the last slide: average daily cost ≈ d + r ÷ 2

Count only cash you can reach within days: reserves and committed credit lines. Insurance rarely pays out while you're still down.

Formula: Parker (2026).

The test

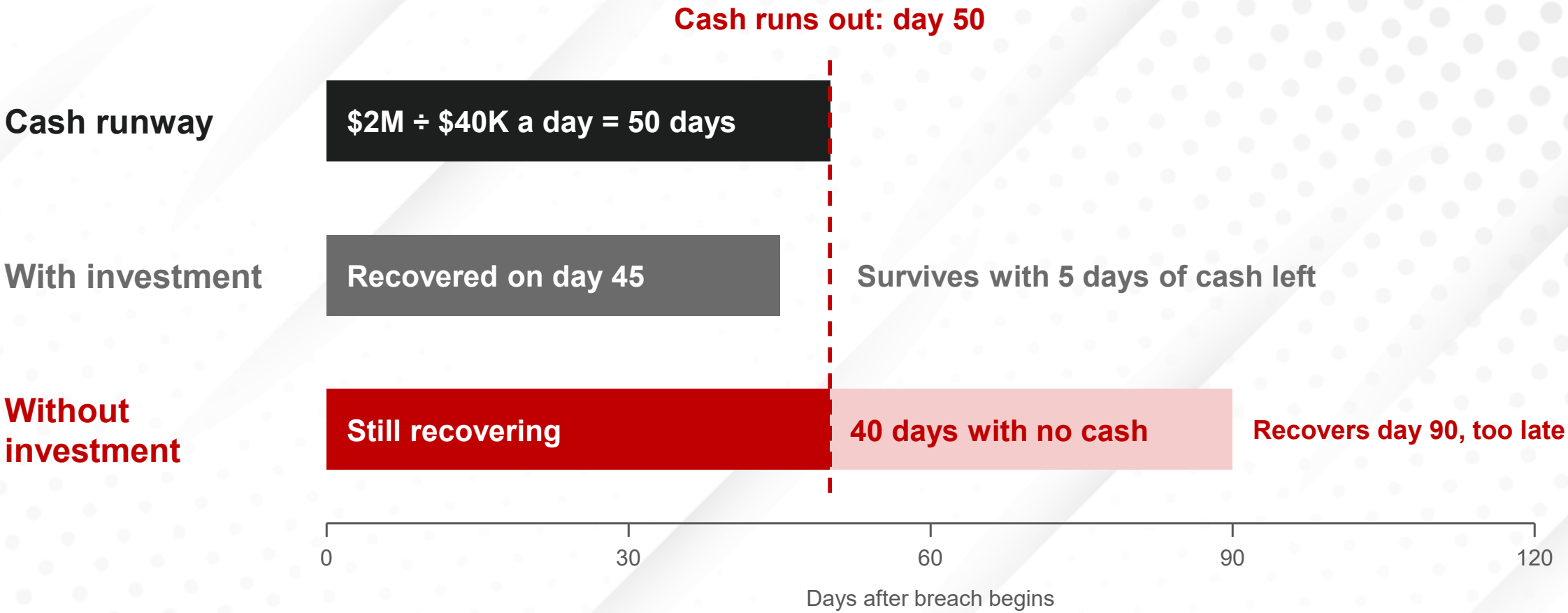
- **Runway > recovery time**
  You survive.
- **Runway < recovery time**
  Cash runs out before systems come back.

In the chat:

Do you know your runway number? Type Y or N.

Same Cash. Different Finish Line.

ILLUSTRATIVE EXAMPLE



The runway didn’t change. The finish line moved.

Assumes $2M reachable cash and $40K average daily cost (from the previous example). Formula: Parker (2026).

Five Questions to Assess Your GAI Maturity

Download Toolkit

Score each: Yes = 2, Partial = 1, No = 0. Any ‘No’ is a resilience gap.
Any ‘Partial’ is a maturity opportunity.

Usage isn’t readiness.

Q1 (T1: Process) Do you have documented governance for what data AI cybersecurity tools can access and who reviews AI outputs before action is taken?

Q2 (T2: Process) Does your organization have a formal AI use policy defining acceptable and prohibited uses across your security team?

Q3 (T3: People) Can you map every AI automation touchpoint in security operations to a named human decision authority?

Q4 (T4: People) For each AI tool in your stack, can you articulate its specific business value and the conditions under which you would remove it?

Q5 (T5: Technology) Do your vendor contracts include AI-specific provisions for data sovereignty, model training rights, and liability?

Mapping to the CR-CMM Framework

ANTICIPATE + WITHSTAND

Anticipate → T2 + T5
Strategic governance (T2) and vendor risk (T5) are core Anticipate capabilities — predicting and preparing before threats materialize.

Withstand → T1 + T3
Risk management (T1) and human-AI operations (T3) determine whether you can absorb active threats without catastrophic disruption.

RECOVER + ADAPT

Recover → T3 + T4
Human-AI workflows (T3) enable faster recovery; resource amplification (T4) ensures capacity even under constraint.

Adapt → T2 + T4
Governance built for change (T2) and intentional adoption (T4) are hallmarks of organizations that continuously improve.

THE CENTRAL FINDING

“Successful GAI cybersecurity implementation fundamentally depends on human expertise orchestration rather than technological sophistication alone.”

Start with the humans. The tools follow.

Source: Parker, J. (2025). *Integrating GAI into cybersecurity: A study of organizational practices* (Publication No. 3255587859) [Doctoral dissertation, Marymount University]. ProQuest Dissertations and Theses Global.

Thank You

QUESTIONS?

Dr. Jessica Parker
jessica@wisebitesllc.com
linkedin.com/in/jessica-parker-pmp
Dissertation: proquest.com/docview/3255587859

ISSA
Information Systems Security Association

Download Presentation

Download Toolkit

Sponsors

rubrik

ECSO
EUROPEAN CYBER SECURITY ORGANISATION

CSA cloud security alliance®

WOMEN IN SECURITY AND PRIVACY

GLOBAL RESILIENCE FEDERATION