



Managing Human Security Cybersecurity and AI Risks: Create Resilience

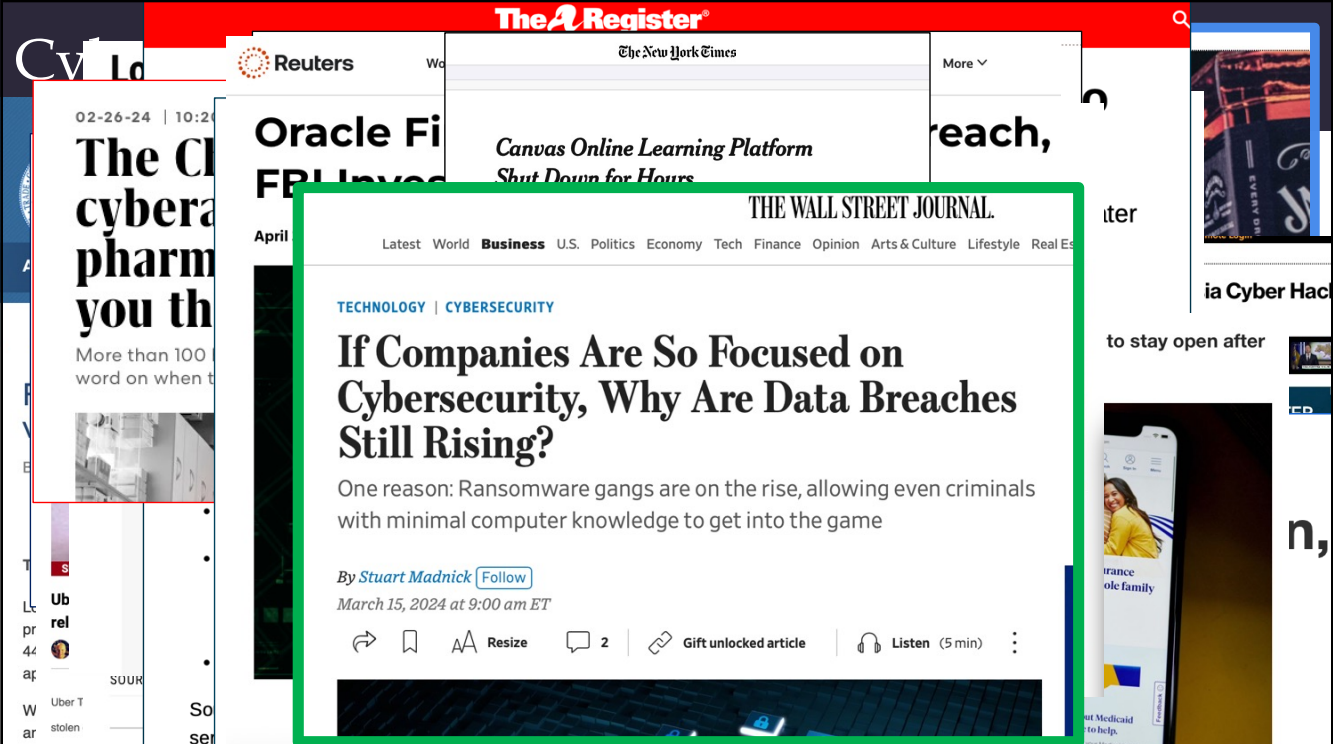
July 9, 2026

Dr. Keri Pearlson • Principal Research Scientist • Sloan School of Management



July 9, 2026
Fab Futures Cybersecurity
Virtual Session

0



The A Register

Reuters

The New York Times

Oracle Financial Services

Canvas Online Learning Platform Shut Down for Hours

reach,

THE WALL STREET JOURNAL

Latest World **Business** U.S. Politics Economy Tech Finance Opinion Arts & Culture Lifestyle Real Estate

TECHNOLOGY | CYBERSECURITY

If Companies Are So Focused on Cybersecurity, Why Are Data Breaches Still Rising?

One reason: Ransomware gangs are on the rise, allowing even criminals with minimal computer knowledge to get into the game

By [Stuart Madnick](#) [Follow](#)

March 15, 2024 at 9:00 am ET

[Share](#) [Bookmark](#) [AA](#) [Resize](#) [2](#) [Gift unlocked article](#) [Listen \(5 min\)](#)

Oracle Financial Services

Canvas Online Learning Platform

reach,

ter

ia Cyber Hack

to stay open after

n,

ance

ole family

ut Medicaid

To help.

1

Cybersecurity is a Big Problem

- The Goal is to get to your customer's systems (supply chain attacks), or stealing your IP/other assets (nation-states)
- It's not just about making money (malware), disrupting your business (ransomware), using you or your business to get to your customer's systems (supply chain attacks), or stealing your IP/other assets (nation-states)
- Recovering is not always possible.

2

We need new mechanisms to be cyber resilient

My BHAG (Big, Hairy Audacious Goal):
Raise the Cyber- Resilience Of Every Organization

© 2026 Keri Pearson. All Rights Reserved. For copies or to use any of these materials, please contact kerip@mit.edu

3

How well-protected are you and your organization from a cyber-attack?

How fast would your organization recover if there was a major cyber incident?

© 2026 Keri Pearson. All Rights Reserved. For copies or to use any of these materials, please contact kerip@mit.edu

4

4

Why Can't We Be Protected Enough?



The US National Institute of Standards and Technology (NIST) Cybersecurity Framework provides a great outline of the most important areas for your cybersecurity strategy.

Most organizations spend 80% of time and resources on protection plans and 20% on response and recovery plans.

But we still see many successful cyber attacks.... Why?

© 2026 Keri Pearson. All Rights Reserved. For copies or to use any of these materials, please contact kerip@mit.edu

5

MIT Research: Cyber Resilience or Cyber Protection



If we cannot completely protect our organization from cyber attacks, we need a different way to think about the problem.

© 2026 Keri Pearson. All Rights Reserved. For copies or to use any of these materials, please contact kerip@mit.edu

6

Resilience is a Different Way Of Thinking Than Protection



Protection: keeping the bad guys out

Resilience: assume the bad guys will get in and have a plan to minimize damage and restore operations



* source: National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity. <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>.

© 2026 Keri Pearson. All Rights Reserved. For copies or to use any of these materials, please contact kerip@mit.edu

7

7

MIT Research: Cyber Resilience or Cyber Protection



Our vision: When your organization experiences an attack, there is zero damage...

No impact on operations

No impact on financial health

No data loss or compromise

No impact on your reputation

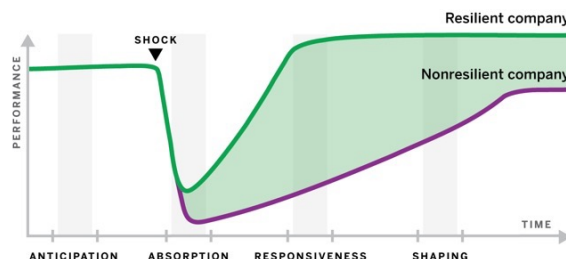
© 2026 Keri Pearson. All Rights Reserved. For copies or to use any of these materials, please contact kerip@mit.edu

8

Design for Resilience



Resilience: *The ability to anticipate then experience a shock, absorb it without significant loss, then respond in a manner that brings the organization back to equivalent or higher performance level.*



Anticipation: activities that prepare an organization for known and unknown cyberthreats

Absorption: activities that reduce the immediate impact of a breach

Responsiveness: activities that reduce the duration of a breach

Shaping/ Reimage: activities that embed lessons learned and prepare for future events

© 2026 Keri Pearson. All Rights Reserved. For copies or to use any of these materials, please contact kerip@mit.edu

9

9

Mechanisms Used to Build Cyber Resilience

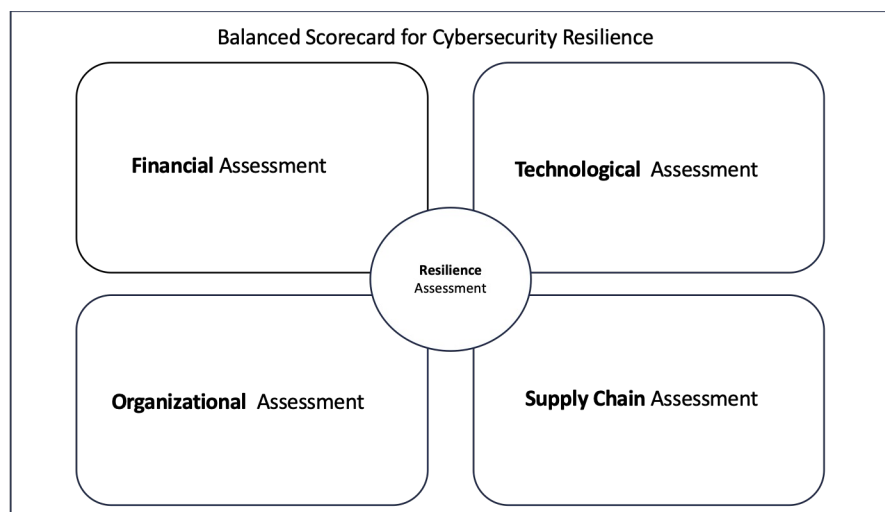


© 2026 Keri Pearson. All Rights Reserved. For copies or to use any of these materials, please contact kerip@mit.edu

10

10

We Built a Balanced Scorecard For Boards to Use to Govern and Manage Cyber Risk and Resiliency



* source: National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity. <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>.

© 2026 Keri Pearson. All Rights Reserved. For copies or to use any of these materials, please contact kerip@mit.edu

11

11

MIT Research: Cyber Resilience or Cyber Protection



MIT Sloan
Management Review

MENU

RESEARCH HIGHLIGHT

An Action Plan for Cyber Resilience

It's impossible to avoid all cyber risk. Here's how to make your company more resilient in the face of new threats.

Michael Coden, Martin Reeves, Keri Pearson, Stuart Madnick, and Michael Berriman
January 04, 2023

SUBSCRIBE PERMISSIONS AND PDF



©2026 Keri Pearson and Cybersecurity at MIT Sloan (CAMS). All Rights Reserved. For copies or to use any of these materials, please contact kerip@mit.edu

Protect ourselves

Cyberattacks Are Inevitable. Is Your Company Prepared?

by Dr. Keri Pearson, Brett Thorson, Stuart Madnick, and Michael Coden
March 09, 2021

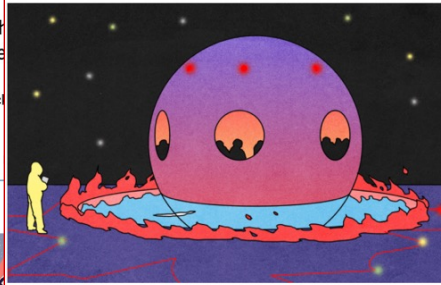


Illustration by Maria Medem

Cybersecurity And Digital Privacy | A Tool to Help Boards Measure Cyber Resilience

Cybersecurity And Digital Privacy

A Tool to Help Boards Measure Cyber Resilience

by Keri Pearson
October 04, 2023



Busk Photography/Getty Images

Summary. During our research, we asked cybersecurity leaders, board directors and other subject matter experts about board cybersecurity discussions and the reporting given to boards in preparation for these discussions. All respondents had strong opinions about... [more](#)

By now most boards know that cybersecurity is a business risk that they must oversee and ensure proper mitigations are in place. In an earlier article, we

13



One Component of Cyber Resilience is your Cybersecurity Culture

©2026 Keri Pearson. All Rights Reserved. For copies or to use any of these materials, please contact kerip@mit.edu

14

**This is a human-centric issue as much as
it is a technology issue.**

**We need human-centric solutions as well
as technology solutions to be effective.**

© 2026 Keri Pearson. All Rights Reserved. For copies or to use any of these materials, please contact kerip@mit.edu

15

Let's dive deeper...

**People in our organizations are
still a common entry point for
cyber issues.**

- 
- people use poor passwords**
 - people click on links**
 - people fall for phishing**
 - people share company assets**
 - people use business processes without
considering security**

© 2026 Keri Pearson. All Rights Reserved. For copies or to use any of these materials, please contact kerip@mit.edu

16

MIT Research: Building a Culture of Cybersecurity



Our research studies...

**How can we reduce the human risks from
our team members?**

**How can we create a culture of
cybersecurity?**

© 2026 Keri Pearson. All Rights Reserved. For copies or to use any of these materials, please contact kerip@mit.edu

17

Defining Cybersecurity Culture



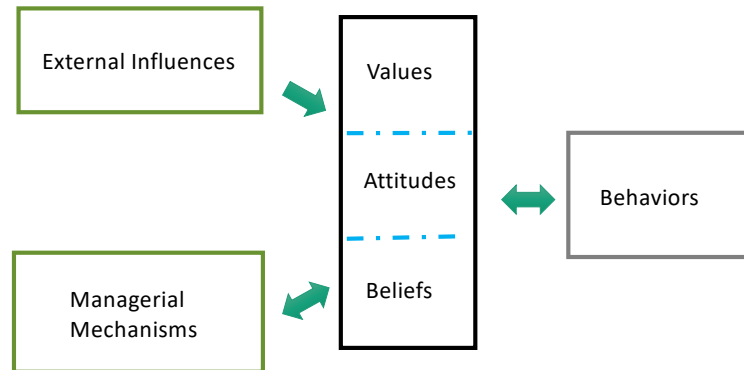
**A Cybersecurity Culture:
The **Beliefs, Values and Attitudes** that drive
cybersecure **Behaviors** in an organization**

© 2026 Keri Pearson. All Rights Reserved. For copies or to use any of these materials, please contact kerip@mit.edu

18

18

Cybersecurity Culture Model

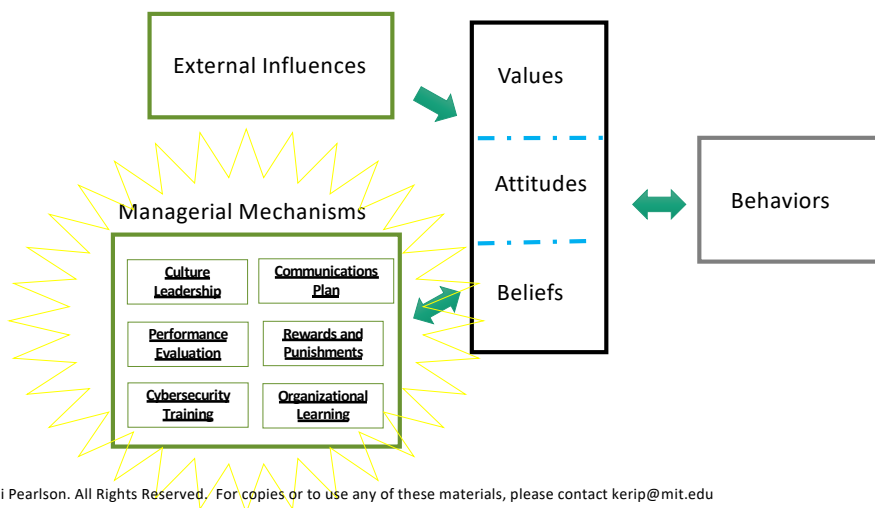


© 2026 Keri Pearson. All Rights Reserved. For copies or to use any of these materials, please contact kerip@mit.edu

19

19

Cybersecurity Culture Model

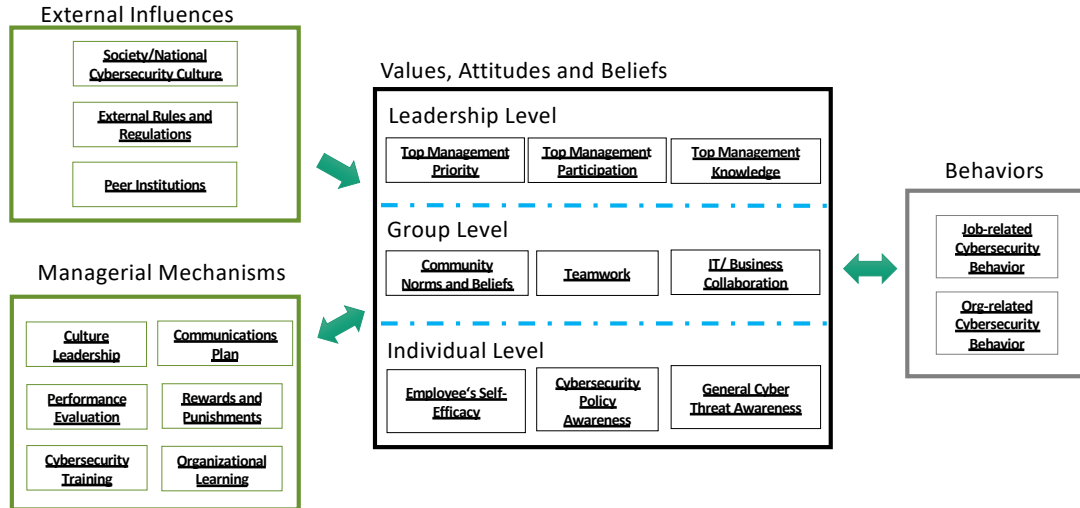


© 2026 Keri Pearson. All Rights Reserved. For copies or to use any of these materials, please contact kerip@mit.edu

20

20

Cybersecurity Culture Model

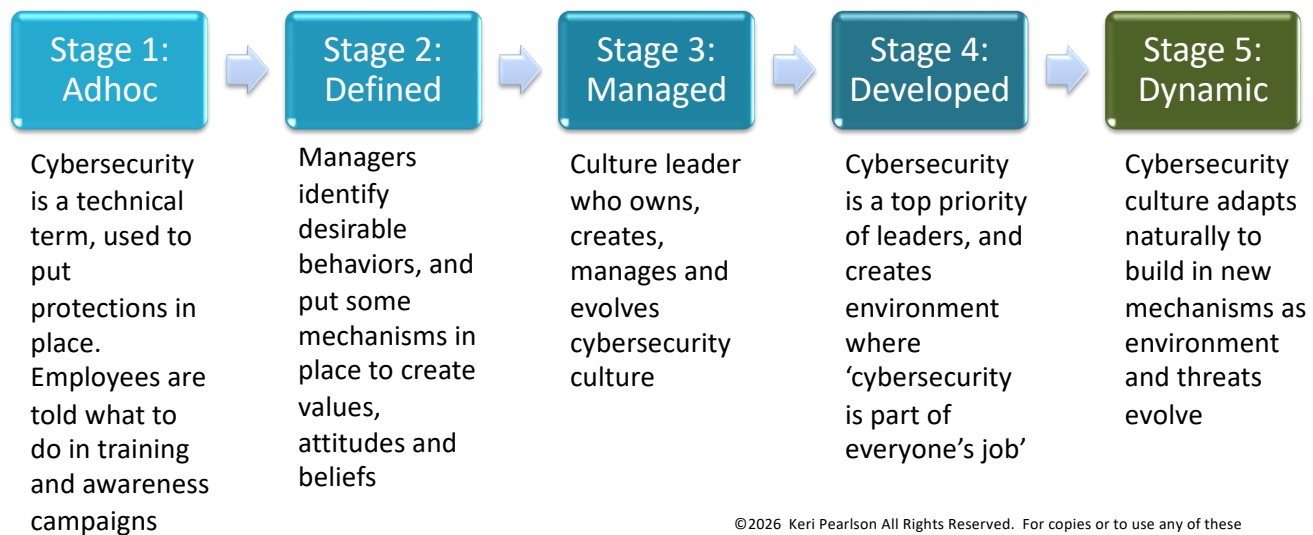


© 2026 Keri Pearson. All Rights Reserved. For copies or to use any of these materials, please contact kerip@mit.edu

21

21

Increasing Effectiveness: Cultivate Culture



© 2026 Keri Pearson All Rights Reserved. For copies or to use any of these materials, please contact kerip@mit.edu

22

MAPS: Our Cyber Culture Effectiveness Measurement Model



Strategy:

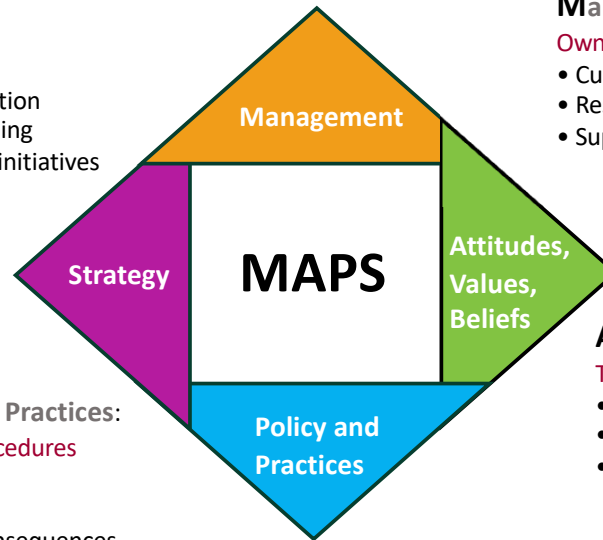
Goals and Plans

- Group Collaboration
- Just in time learning
- Funding culture initiatives

Management/Leadership:

Ownership and motivator for culture

- Culture leader
- Resilience plans
- Supervisor involvement



Policies and Practices:

Rules and procedures

- Training
- Compliance
- Rewards/consequences

Attitudes/Values/Beliefs:

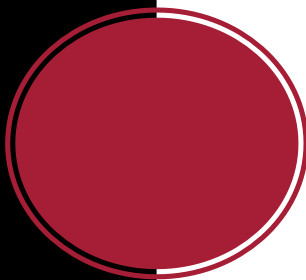
The unwritten rules

- Individual empowerment
- Individual responsibility
- Team support

©2026 Dr. Keri Pearson. All Rights Reserved.

23

MIT Research: Measuring Effectiveness of Cybersecurity Culture



Our current research on cybersecurity culture assesses the values, attitudes, beliefs and perceptions to identify ways to increase effectiveness.

We are testing our approach right now.

©2026 Keri Pearson. All Rights Reserved. For copies or to use any of these materials, please contact kerip@mit.edu

24

MIT Research: Building a Culture of Cybersecurity



How can
cybers
and fa



ons

ing values
o creating

© 2026 Keri Pearson. All Rights Reserved

26



Using AI Securely

© 2026 Keri Pearson. All Rights Reserved. For copies or to use any of these materials, please contact kerip@mit.edu

27

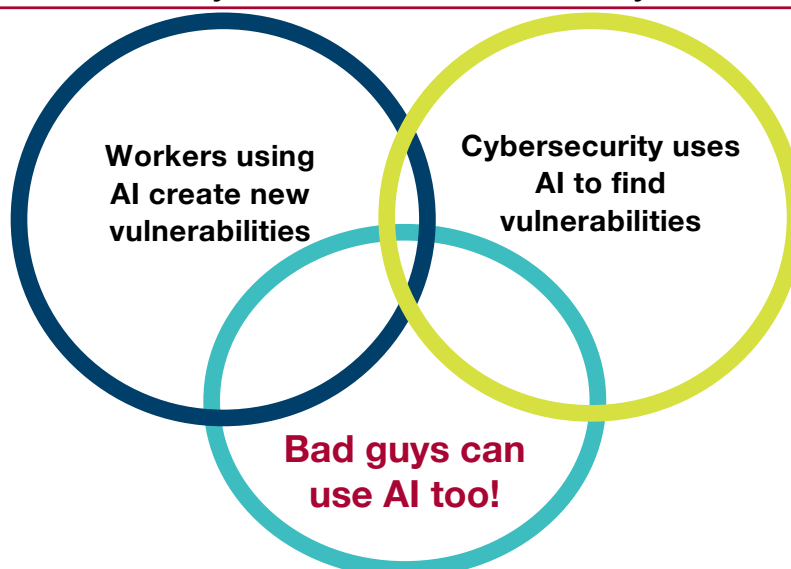
Seen on the NYC Subway:



28

AI and Cybersecurity

There are 3 ways AI intersects with cybersecurity today:



29

Changing Threat Landscape

New Threat	Example
Social Engineering at Scale	- AI generated phishing are highly personalized - Deepfake voice and video impersonate people we know - Chatbots can conduct believable conversations
Content Manipulation creates Misinformation	- Deepfakes sway public opinion - AI can create fake articles and posts at scale - Reputational damage from making it appear that someone said or did something they never did
Offensive and Technical Attacks	- Craft malicious inputs (images, prompts, data, etc) to cause AI to make wrong decisions - Insert adaptable malware that avoids detection by changing it's signature or behavior.
Advanced Automation of Attacks	- Bots controlled by AI optimize DDoS attacks - Break passwords using AI to prioritize likely passwords - Use AI to create fake identities that pass verification protocols
Attacks on AI Systems	- Use AI to Modify malicious content so detection tools miss it - Use unsecured, unsanctioned AI tools (shadow AI) to get inside organization - Use prompts with proprietary information for training data



30



AI Security Requires Different Mechanisms to Reduce Risks from AI Use

© 2026 Keri Pearson. All Rights Reserved. For copies or to use any of these materials, please contact kerip@mit.edu

32

AI is delivering unprecedented gains across the enterprise.

The temptation to use AI is overwhelming. Managers and workers see seductive gains in productivity, and vendors are embedding AI into their new service offerings.

© 2026 Keri Pearson. All Rights Reserved. For copies or to use any of these materials, please contact kerip@mit.edu

NotebookLM

33

But conventional risk management only sees the tip of the iceberg.

Productivity Gains New Capabilities Efficiency

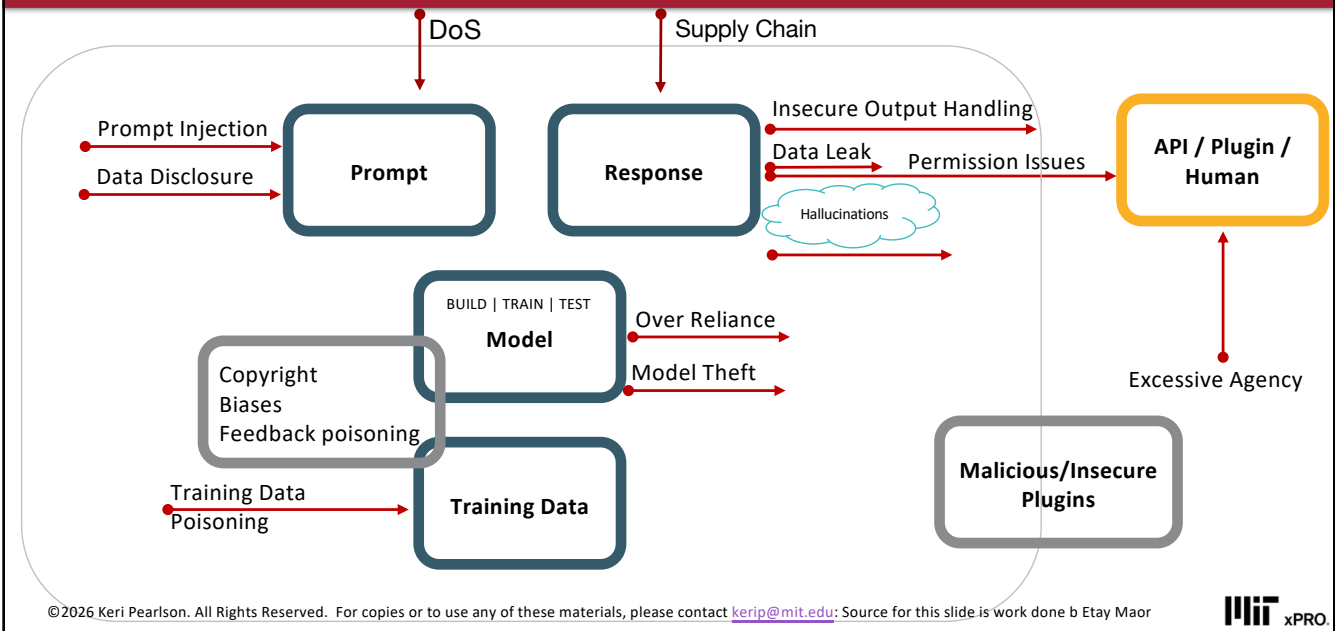
Hidden Human & Cultural Risks

While managers attempt to mitigate these risks through training and awareness activities... these are just not enough.

© 2026 Keri Pearson. All Rights Reserved. For copies or to use any of these materials, please contact kerip@mit.edu

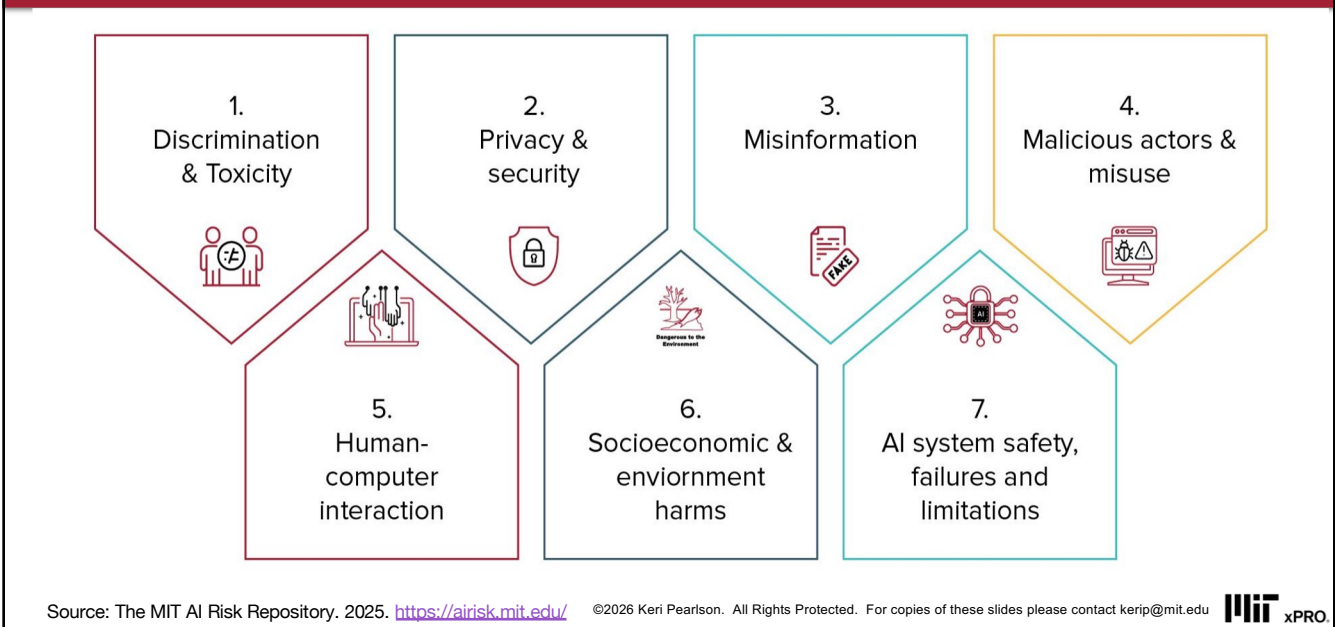
34

AI (LLMs) Have Many Attack surfaces



35

MIT AI Risk Taxonomy: 7 Categories of Risks



36

AI amplifies human risk factors that must be managed



Hallucinations & Wrong Decisions



Data Leakage & Privacy Violations



Inherent Bias



Employee Deskilling



Deep Fakes & Misinformation



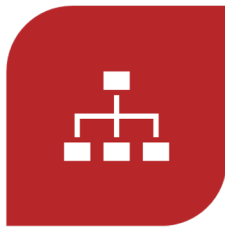
Data Poisoning

© 2026 Keri Pearson. All Rights Reserved. For copies or to use any of these materials, please contact kerip@mit.edu

37

AI governance mitigates these risks

Good AI governance includes:



STRUCTURES



PROCESSES



PRINCIPALS

To ensure that AI is used responsibly, safely, and in alignment with organizational values.



© 2026 Keri Pearson. All Rights Reserved. For copies of these slides please contact kerip@mit.edu

39

Why organizations need AI governance



Assigns Responsibility

Establishes clear ownership and accountability for AI systems across teams and leadership



Ensures Ethical Use

Promotes fairness, transparency, and responsible AI deployment in line with organizational values



Mitigates Risks

Without governance, organizations are vulnerable to:

- Bias in decision-making
- Privacy violations
- Ethical lapses
- Misuse of AI

Key challenges include lack of expertise, collaboration issues, and fragmented data.

©2026 Keri Pearson. All Rights Reserved. For copies of these slides please contact kerip@mit.edu



40

Components of Good Governance of AI for Organizations

01

Executive Oversight

02

Governance Policies

03

Controls for Risk, Use, and Impact

04

Design, Develop, and Deployment Guidelines

05

Monitoring and Management Processes

©2026 Keri Pearson. All Rights Reserved. For copies of these slides please contact kerip@mit.edu



41

Components of Good Governance of AI for Organizations

01

Executive Oversight

Includes:

- Board's Role
- Committees and their Role
 - Ethics Committee
 - Responsible AI Use Committee
- C-level Executives Role
 - Chief AI Officer
 - Chief Risk (AI Risk) Officer
 - Chief Technology Officer
 - Chief Information Officer
 - Chief Data Officer

02

Governance Policies

03

Controls for Risk, Use, and Impact

04

Design, Develop, and Deployment Guidelines

05

Monitoring and Management Processes

©2026 Keri Pearson. All Rights Reserved. For copies of these slides please contact kerip@mit.edu



42

Components of Good Governance of AI for Organizations

01

Executive Oversight

02

Governance Policies

Includes:

- Compliance and Regulation Policies
- Responsible, Ethical, and Acceptable Use Policies
- Risk Management Policies

03

Controls for Risk, Use, and Impact

04

Design, Develop, and Deployment Guidelines

05

Monitoring and Management Processes

©2026 Keri Pearson. All Rights Reserved. For copies of these slides please contact kerip@mit.edu



43

Components of Good Governance of AI for Organizations



44

Components of Good Governance of AI for Organizations



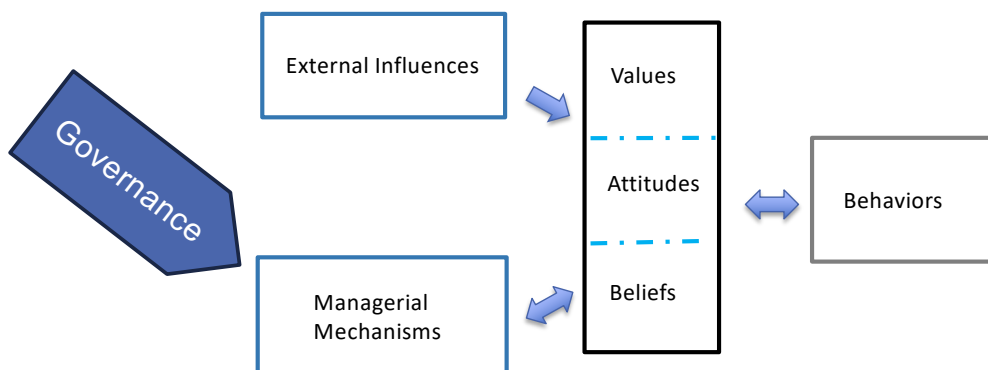
45

Components of Good Governance of AI for Organizations



46

Governance Contributes to the Culture

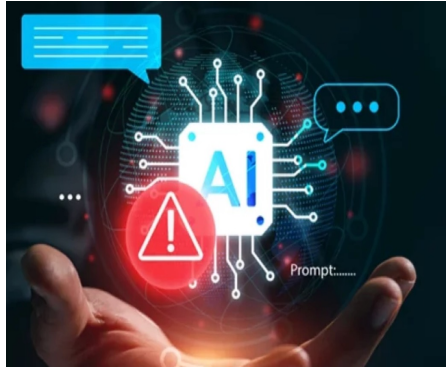


© 2026 Keri Pearson. All Rights Reserved. For copies or to use any of these materials, please contact kerip@mit.edu

47

47

We Are Currently Researching AI Security Beliefs... We Are Asking...



1. What do employees know about the risks and vulnerabilities from using GenAI?

2. How can we create a culture of AI security to manage these risks?

© 2026 Keri Pearson. All Rights Reserved. For copies or to use any of these materials, please contact kerip@mit.edu

Copyright © 2025 by Dr. Keri Pearson and MIT Sloan. Reproduction and use with permission only. All Rights Reserved.

48

48

Why Managing Human Risk Matters

AI impacts people, not just systems.

Bias is built in

Poorly designed AI can replicate and amplify discrimination.

Overtrust leads to oversight failure

Humans defer judgment, especially when AI appears confident.

Autonomy & skills can erode

When humans become passive executors, skills atrophy over time.

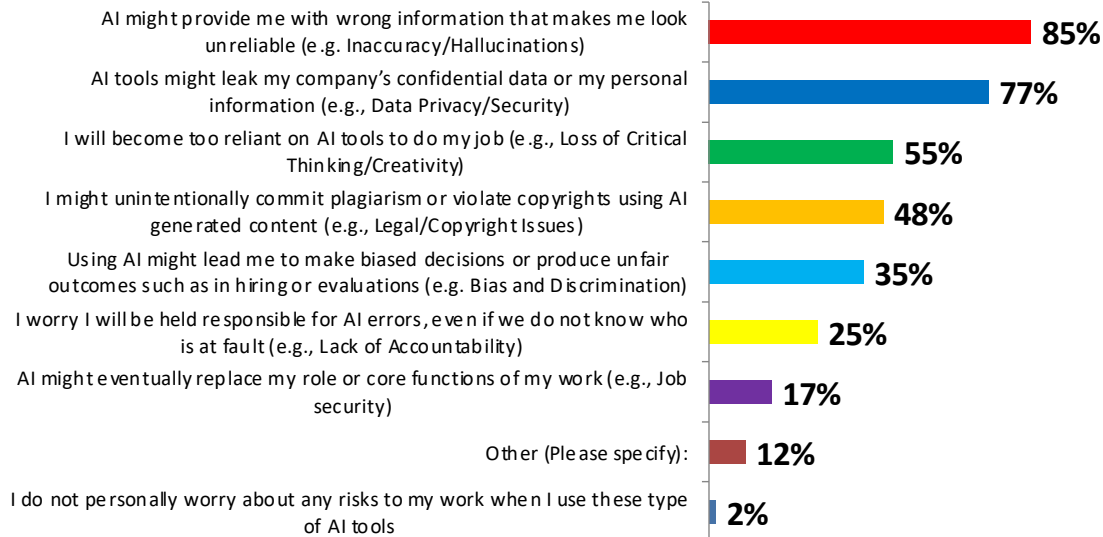
The cost is expensive

From lawsuits to reputational loss — AI-related failures impact more than IT.



49

Preliminary Results*: What Risks do you Consider when you use GenAI?

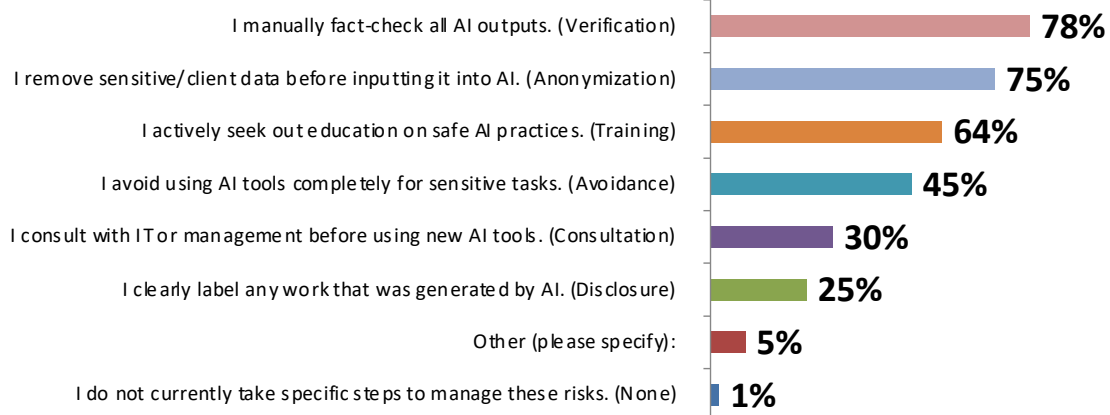


* This data is from responses from 40 individuals in the xPro AI Class March 2026

©2026 Keri Pearson. All Rights Reserved. For copies or to use any of these materials, please contact kerip@mit.edu

50

Preliminary Results*: What do you do to Mitigate or Manage these Risks?

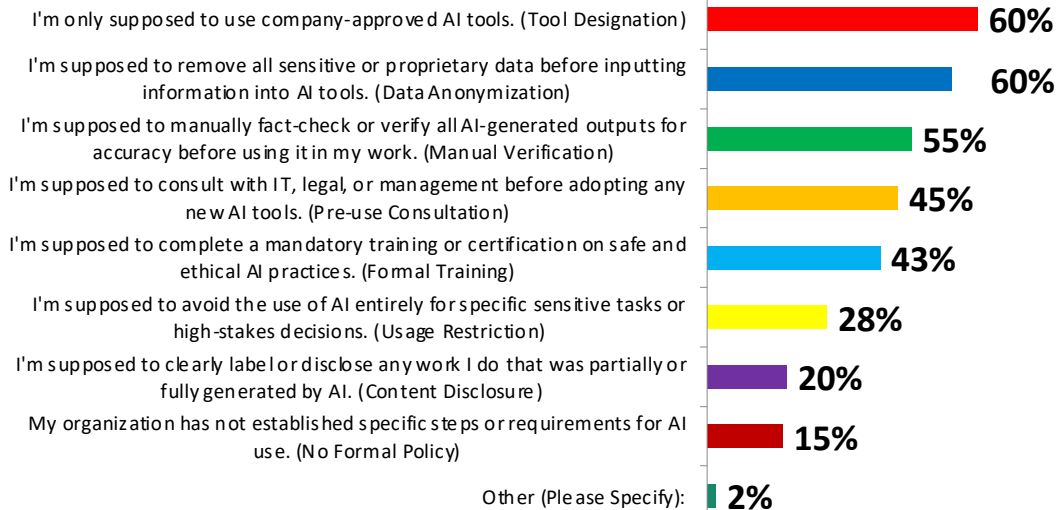


* This data is from responses from 40 individuals in the xPro AI Class March 2026

©2026 Keri Pearson. All Rights Reserved. For copies or to use any of these materials, please contact kerip@mit.edu

51

Preliminary Results*: What Does Your Organization Want you to do?

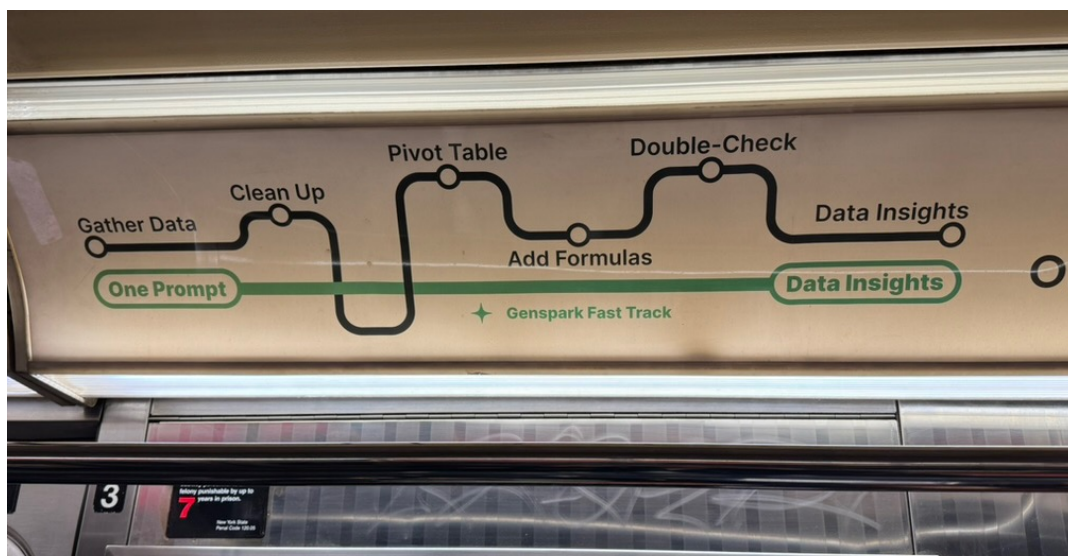


* This data is from responses from 40 individuals in the xPro AI Class March 2026

©2026 Keri Pearson. All Rights Reserved. For copies or to use any of these materials, please contact kerip@mit.edu

52

Seen on the NYC Subway:



53

Let's Discuss... (in the chat)



AI risks can compromise the work done by your employees. We want to build a culture of AI security.

Thinking about the human-centric risks, and using our culture framework, what behaviors do you want to see when your employee use AI?

What can you do to build those values, attitudes and beliefs?

©2026 Keri Pearson. All Rights Reserved. For copies or to use any of these materials, please contact kerip@mit.edu

54

Action Plan: Build Cyber and AI Resilience



- **Find ways to personally step up:** Model the behaviors necessary to keep your organization, your family and yourself secure. Shine light on being part of the solution.
- **Make heroes of the people who do cybersecure behaviors:** Others will follow. This will create the values, attitudes and beliefs that drive a cybersecure culture.
- **Implement AI with risk management in mind:** Find ways to insure skills are not lost and AI actions/results are not blindly followed.
- **Create resilience in addition to protection:** Build processes to respond/recover quickly and practice, practice, practice.

©2026 Keri Pearson. All Rights Reserved. For copies or to use any of these materials, please contact kerip@mit.edu

55

