



Securing the Enterprise in the Age of AI

An Interesting Conundrum

Presented By: Tina Lampe

Discussion Points:

1. The Conundrum (Puzzle)!
2. Managing Enterprise AI risks – Trustworthy AI
3. Enhancing Cyber Defenses using AI
4. Enhancing the Security Team Impact with AI
5. Future Focus – Challenging Issues in which AI may provide some relief
6. Actionable Take Aways

Overall Goals of our Discussion:

1. Each of us to learn something new.
2. Each of us to uncover at least one helpful 'tidbit' in which to take action.

1. The Conundrum (Puzzle)

The background of the slide is a grayscale, high-contrast image of a complex geometric pattern. It features a grid-like structure with various lines and shapes, possibly representing a puzzle or a diagram. The pattern is composed of many small, interconnected elements, creating a dense and intricate visual. The overall appearance is that of a technical drawing or a complex geometric construction.

How does your enterprise approach AI usage?



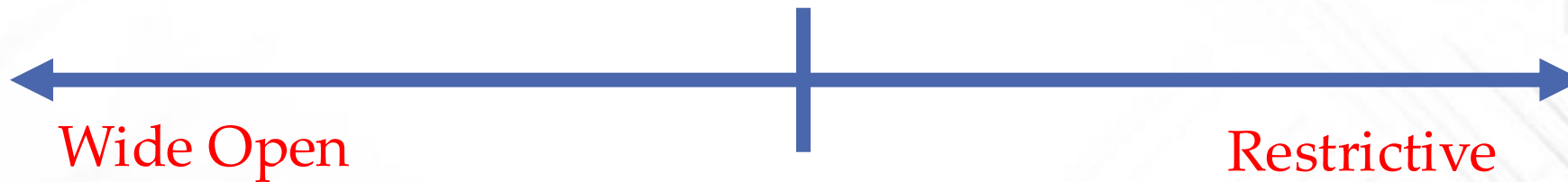
'Bury your head and hope for the best'



Active Governance



Block the Usage



Wide Open

Restrictive

Artificial Intelligence (AI)

What is meant when we use the term AI?

- * GenAI has become more mainstream within the last 12 months and has introduced some confusion as to the meaning of AI.
- * Traditional AI has been around for many years.

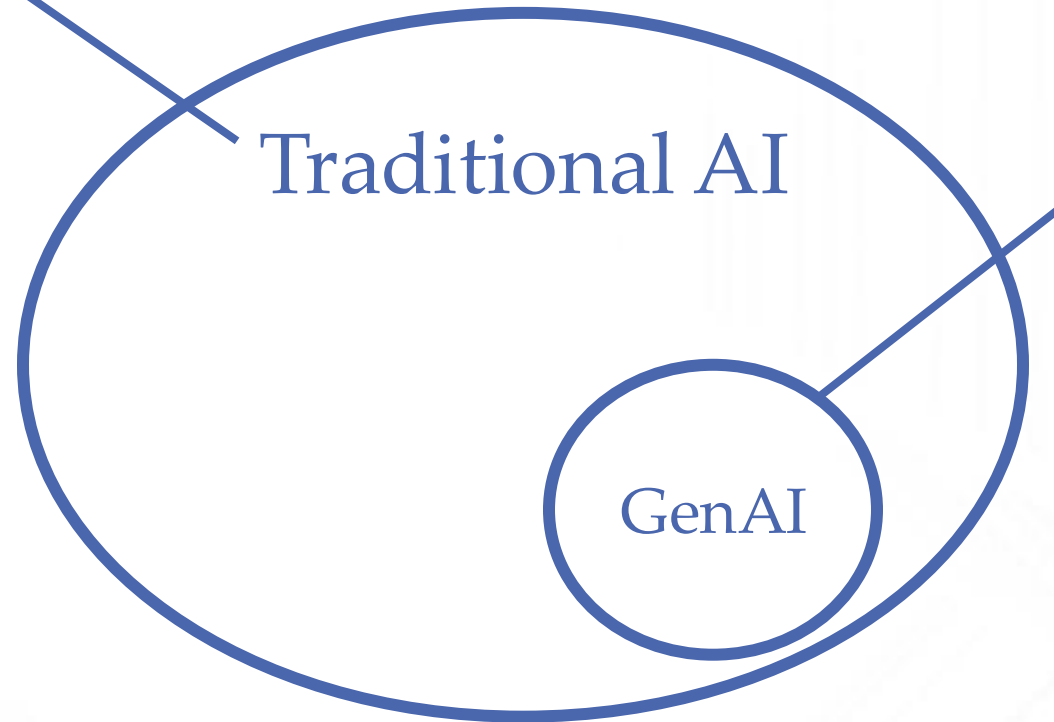
Traditional Artificial Intelligence (AI)

-vs-

Generative Artificial Intelligence (GenAI)

Traditional AI:

- Trained to make effective decisions based on a **specific set of rules**
- Recognizes **existing patterns**
- Powers predictive analytics through data analysis
- In general, **does not create new rules, content, etc.**



GenAI:

- Subset of Traditional AI
- **Creates new** images, music, text, code, patterns
- Trained with a set of data for **learning new patterns** and **generating new data**
- Ability to interact with GenAI using **everyday language**

Interesting AI Statistics

A Large Global Life Sciences Company:

- Performed an internal study on the use of GenAI and realized a **Minimum of 30 minutes per day** savings for the most casual user up to a significant **85% time savings** for deep knowledge workers.

From authorityhacker.com:

- **35% of businesses** have already adopted AI.
- **77% of devices in use** feature some form of AI.
- **9 out of 10 organizations** support AI for a competitive advantage.
- AI will contribute **\$15.7 trillion** to the global economy by 2030.
- **80% of retail executives** plan to adopt AI automation by 2025.
- **72% of executives** think AI will become the most significant business advantage in the future.

The Business Conundrum – AI Introduces both Threats and Opportunities for the Business

Opportunities

- Efficiency Gains
- Personalization of Customer Experience
- Innovation

Threats

- Intellectual Property Data Loss
- Reputation Damage
- AI enabled attacks

* One of the most significant risks companies face in times of major industry advances is the risk of being 'left behind'

Don't get Left Behind.....



What lessons can we learn from the past?

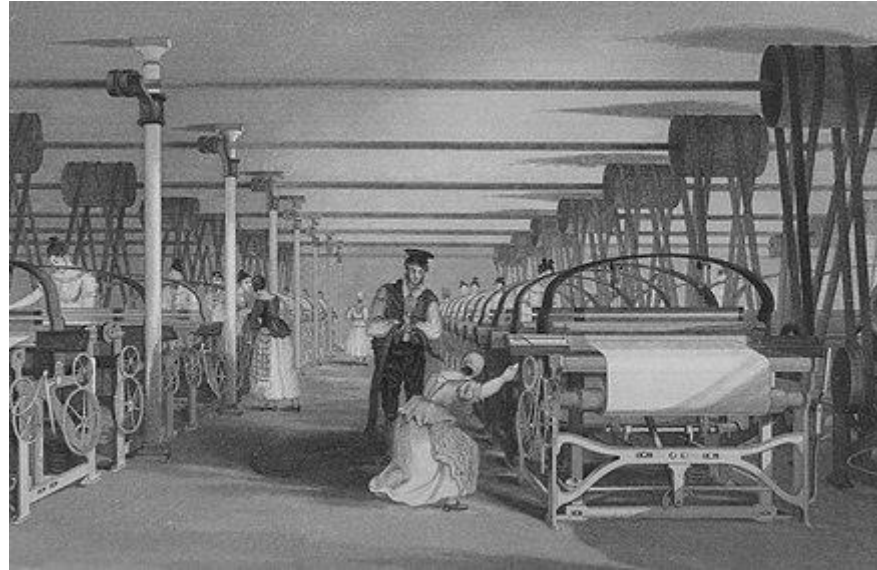
First Industrial Revolution

Characteristics of Disruption:

- Timing: Late 1700s
- Main Result: Movement from Hand Production Methods to Machines
- Disruptors:
 - Mechanization
 - Weaving Looms
 - Cotton Gin

Business Response examples:

- New Industry Born:
 - Textile Industry



Second Industrial Revolution

Characteristics of Disruption:

- Timing: Late 1800s
- Main Result: Mass Production
- Disruptors:
 - Assembly Lines
 - Electrical Energy
 - Telegraph
 - Railroad

Business Response examples:

- New Industries Born:
 - Large scale iron and steel production
 - Automotive



Third Industrial Revolution (The Digital Age)

Characteristics of Disruption:

- Timing: Late 1900s
- Main Result: economy centered on information technology
- Disruptors:
 - Computers
 - Internet
 - Electronics
 - Automation



Business Response examples:

- Companies Left Behind:
 - Blockbuster
 - Kodak
- Companies that successfully managed (or were invented) through the Industry Shift:
 - Amazon
 - NetFlix

Fourth Industrial Revolution

Characteristics of Disruption:

- Timing: Now
- Main Result: Joining of Technologies that blur the lines between the physical, digital, and biological worlds
- Disruptors:
 - **Artificial Intelligence**
 - Gene Editing
 - Advanced Robotics
 - Internet of Things (IoT)

Business Response examples:

- Companies Left Behind:
 - TBD
- Companies that Strategically managed (or were invented) through the Industry Shift:
 - TBD



The AI Conundrum within the Cybersecurity Landscape

Attacker:

- **Lowers the bar*** for cybercriminals to stage a sophisticated cyberattack
- **Fabricated** versus human-generated media is becoming **harder to distinguish**
- Attackers will continue to take advantage of AI **regardless of any internal policies**



Defender:

- **Enhanced defenses** against AI assisted attacks
- Increased ability to **focus on true alerts** instead of false positives
- Most experts are optimistic that **AI will be a game changer for the defenders.**

* Rob Joyce, director of cybersecurity at the National Security Agency, said at the International Conference on Cyber Security at Fordham University in Manhattan that less capable people are using AI to guide hacking operations they would not have otherwise been able to carry out themselves.

Source: reuters.com

An aerial, high-angle photograph of a modern building with a glass facade. The building's structure is visible, showing a grid pattern of windows and structural elements. The image is in black and white, with a slight blur, giving it a dynamic, architectural feel. The text is overlaid on the left side of the image.

2. Managing Enterprise AI Risks – Trustworthy AI

Trustworthy AI

How many of you have heard of or have experience with Responsible or Trustworthy AI?

Why Focus on Trustworthy AI?

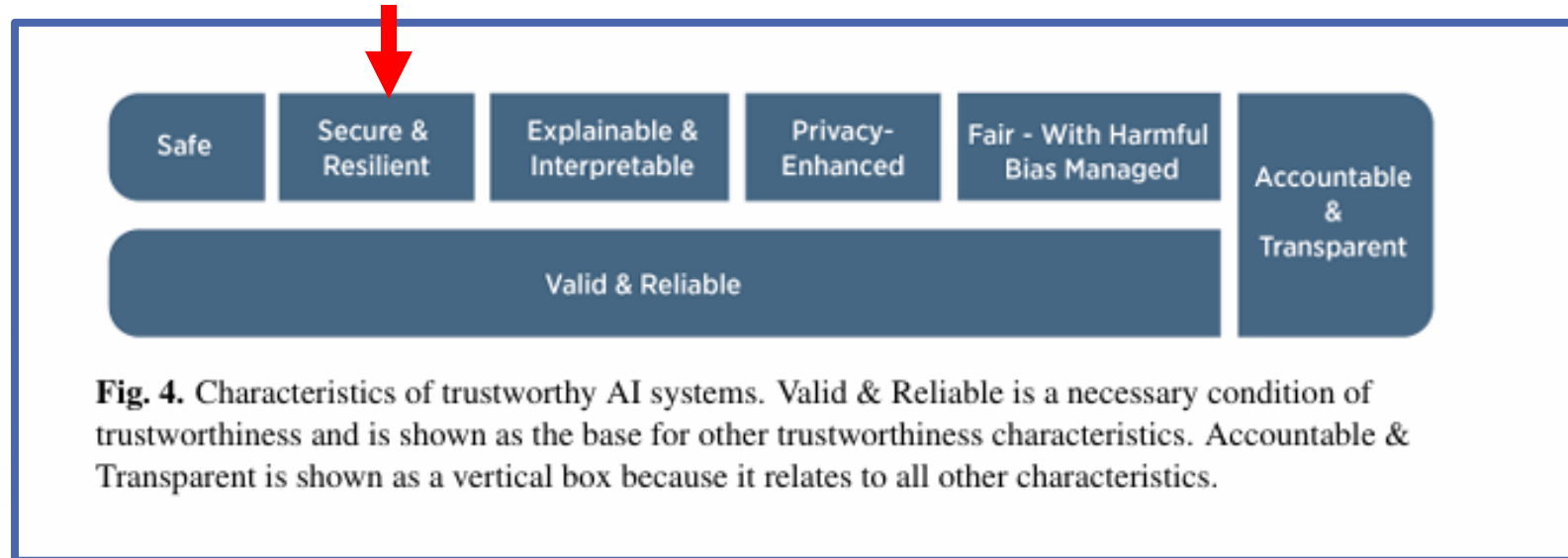


Fig. 1. Examples of potential harms related to AI systems. Trustworthy AI systems and their responsible use can mitigate negative risks and contribute to benefits for people, organizations, and ecosystems.

Source: NIST AI 100-1

Trustworthy AI

- Source: NIST AI 100-1:



- Secure & Resilient
 - Integral to Trustworthy AI
 - Ties directly into NIST Cybersecurity Framework and Risk Management Framework
- Cybersecurity is a critical component of trustworthy AI as well as industrial enhancement.


AI Governance

How many of you have some form of AI Governance in place?


AI Governance – Where to Start?

- ✓ Due to **variations in regulatory environments**, it is important to gather information regarding which countries will be impacted by the AI usage in your company
- ✓ Both NIST and ISO have **AI Governance Frameworks** which provide a good starting point
- ✓ **Organizations** can also choose to **build their own** frameworks
- ✓ Most consulting vendors can be **hired** to implement AI governance in your organization if needed
- ✓ ISO introduced **ISO/IEC 42001** in December 2023 to manage risks and opportunities with AI (**balancing innovation with governance**)
- ✓ Since the AI regulatory environment around the world is changing rapidly, it is important to **review AI governance guidelines** frequently for any needed updates. (every 3-6 months?)

ISO Stated Benefits of Implementing ISO/IEC 42001

What are the main benefits of implementing ISO/IEC 42001? 

- **Responsible AI:** ensures ethical and responsible use of artificial intelligence.
- **Reputation management:** enhances trust in AI applications.
- **AI governance:** supports compliance with legal and regulatory standards.
- **Practical guidance:** manages AI-specific risks effectively.
- **Identifying opportunities:** Encourages innovation within a structured framework.



3. Enhancing Cyber Defenses using AI

AI and Cyber Defense

Have any of you already added AI tools
(or Products with AI) to aid in your cyber
defense?

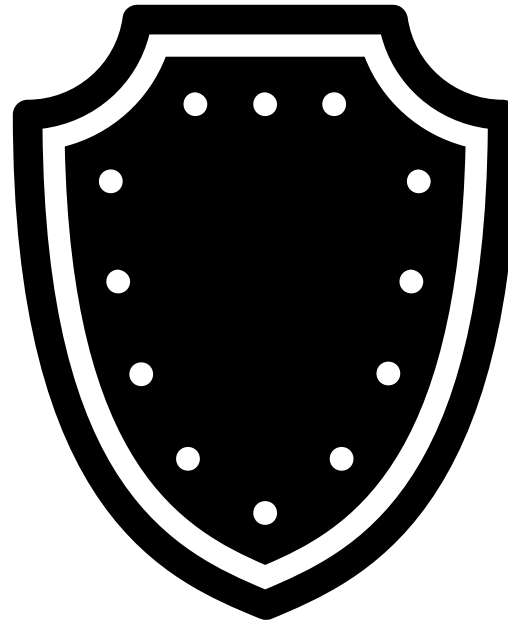
AI Enhanced Defense

* 'Finding the needle in the haystack' by processing and interpreting large amounts of data.

The Goal: An Efficient, AI Enhanced SOC

Uncover hidden priority threats

Predict future attacks



Automatic response to mitigate risks

Auto-Adapt defense tactics to evolving threats

Behavior Analysis

Zero Trust Architecture Support

AI Powered Threat Intelligence Platforms
(aggregate and analyze data from various sources)

Case Study: IBM Using Watson for Cybersecurity (eastgate-software.com)

AI -vs- 

- AI analyzes and interprets data **50 times faster** than human
- AI reduced the number of false positive alerts **by 30%**
- AI is much more scalable than humans

Case Study: Microsoft Intelligent Security Graph (eastgate-software.com)

AI -vs- 

- AI improved average threat detection and response from 24 hours to **less than 1 hour**
- AI increased malware and phishing threat detection of attacks **by 40%**
- AI proactive defense mechanism **decreased successful cyber attacks 60%**

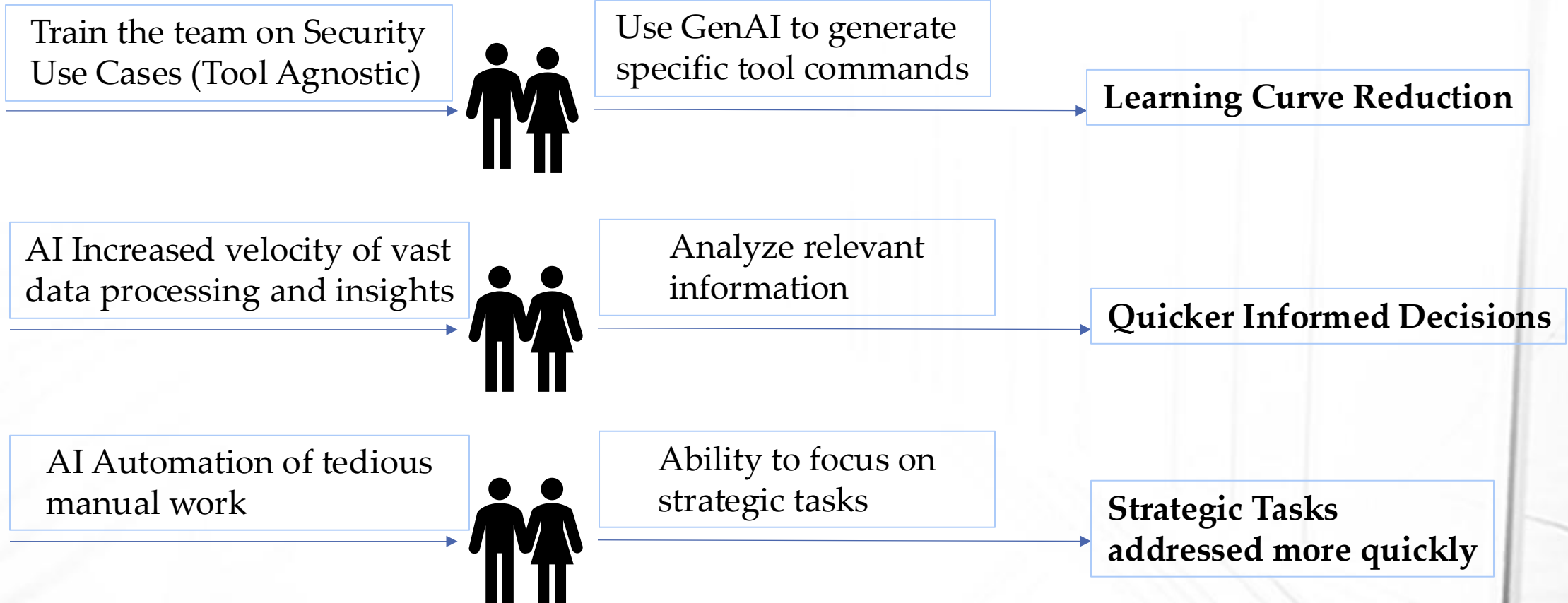
An aerial, black and white photograph of a city street grid. A semi-transparent grid is overlaid on the image, consisting of thin lines that align with the street patterns. The perspective is from a high angle, looking down on the city. The text is centered in the upper-left quadrant of the image.

4. Enhancing the Security Team Impact with AI

Security Team Use of GenAI

Have any of your security teams started using GenAI?

Using AI to Enhance the Existing Security Team Impact

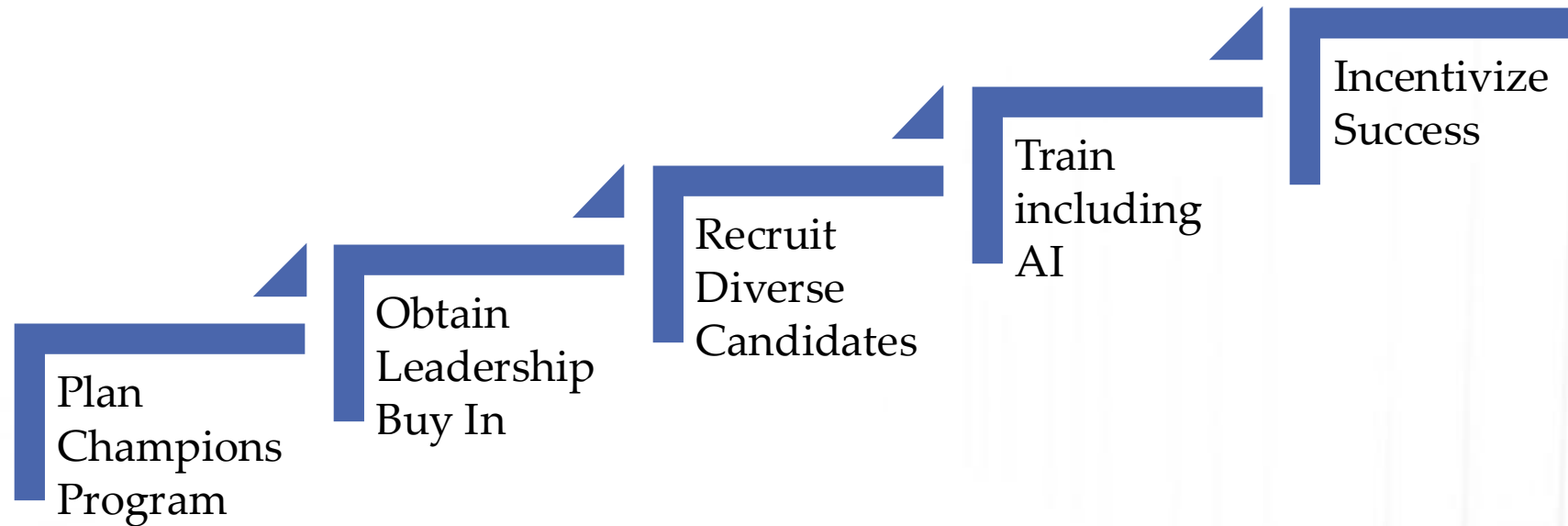


- Microsoft research has shown that when using Copilot for Security, analysts were **26% faster across all tasks** (forbes.com)

Cybersecurity and/or AI Champions Program

Do any of you have a cybersecurity and/or AI Champions Program within your company?

Building and/or Enhancing an Enterprise Cybersecurity/AI Champions Program



- Provides the ability to enforce and enhance enterprise governance
 - recruit diverse candidates from each department
 - champion cybersecurity and responsible AI usage
 - **be a spokesperson for challenges faced by their area of the enterprise.**

An aerial, black and white photograph of a city grid. A large, circular structure, possibly a stadium or arena, is visible in the lower-left foreground. The city streets form a dense grid pattern that recedes into the distance. The text is overlaid on the left side of the image.

**5. Future Focus – Challenging Issues
in which AI may provide some relief.**

Future Focus

What are some of your biggest current cybersecurity challenges in which you believe that AI may provide some relief?

Future Focus – Challenging Issues in which AI may Provide Some Relief

Cyber Resilience and Agility

Targeted Organization
Rankings and Remediations
Based on Business Impact

Refinement of Cyber
Defenses near real time



Scaling Cyber Defense
Activities when Needed

Continuous Compliance
Assessments

Freeing the Security Team
to work on Strategic Tasks

An aerial, black and white photograph of a city grid. A large, light-colored circular area, possibly a park or a large open space, is visible in the center-left. The grid lines are clearly visible, and a large building with a grid-like facade is prominent in the upper right corner.

6. Actionable Take Aways

Actionable Take Aways

1. Support Active Governance of AI in your organization through the NIST and ISO standards in which we spoke – and/or creating your own policies. This will allow AI innovation while managing AI risks in a responsible manner – and hopefully will keep your company from being “left behind.”
2. If your organization’s governance permits, Empower your security team to become more tool agnostic through the use of GenAI.
3. Build Responsible AI and Security Advocates within the enterprise to expand the governance impact.
4. And, Finally, Feel a sense of pride around being a cybersecurity practitioner because your importance in support of “riding the wave” of the AI, business and industry transformation cannot be overstated.



Questions?

Additional Q/A depending on time:

1. Do you believe it is valid for some organizations to Block AI Usage all together?
2. Do you believe it is valid for some organizations to allow wide-open AI usage without governance?
3. How do you think AI will change your specific industry?
4. Do you have any predictions as to which companies/industries may get left behind in this 4th industrial revolution?
5. Do you have any predictions as to which companies/industries may be created with the 4th industrial revolution?

7. Wrap up

Did We Meet Our Goal?

1. Did you learn something new?
2. Did you uncover at least one helpful 'tidbit' in which to take action?

That's a Wrap

Feel Free to Connect with me on LinkedIn:
<https://www.linkedin.com/in/tina-lampe>

Thanks for your time and insights today!