Shaping Tomorrow:
AI and Cybersecurity Risks for Today's Professionals

Presented By:
Michael McAllister| Partner,
IS Assurance and Advisory Services

rkl ADVISORS for WHAT'S NEXT

rkl ADVISORS for WHAT'S NEXT

What We Will Introduce

01. Artificial Intelligence risks

Identify key risks associated with the adoption and implementation of AI technologies in professional environments, and evaluate ethical, operational, and regulatory considerations related to AI risk management.

02. Cybersecurity threats and vulnerabilities

Recognize prevalent cybersecurity threats and vulnerabilities impacting organizations today.

03. AI-related and cybersecurity risk management

Best practices for mitigating both AI-related and cybersecurity risks to enhance organizational resilience.

rkl ADVISORS for WHAT'S NEXT

Welcome and Meet Your Presenter

Michael McAllister, CPA.CITP, CISA

Partner / IS Assurance and Advisory Services

As Partner and Leader of RKL's IS Assurance and Advisory Services Practice, his focus lies in supporting the accounting world and helping clients navigate through the issues and concerns that may keep them up at night.

With more than 30 years of experience in accounting and computer science, Michael builds the knowledge bridge between the financial aspects of accounting, and the information technology systems and controls that support each process.

Together with his IS Assurance & Advisory Services team, he serves clients in a variety of industries, ranging from manufacturing to retail, technology and credit unions, creating an extensive background of linking information security and financial audit risks. The financial institution industry has been the primary focus of Michael's internal audit experience for the past 10 years, with extensive experience ranging from the development of risk assessments to the execution of various in-depth audits.

rkl ADVISORS for WHAT'S NEXT

"Science and technology revolutionize our lives, but memory, tradition and myth frame our response."

Arthur Schlesinger (Historian)

rkl ADVISORS for WHAT'S NEXT

Artificial Intelligence Considerations

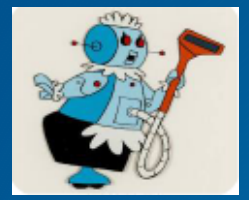
Artificial Intelligence is nothing new…

First AI Character | Early Introductions | Pop Culture | Present / Future

Cybersecurity and AI have been depicted in Pop Culture dating back to the 1920's. The first AI character in a movie was from a silent film called *Metropolis* in 1927.

Artificial Intelligence is nothing new…

First AI Character | Early Introductions | Pop Culture | Present / Future



Rosie on the Jetson's (1962)

Robot in Lost in Space (1965)

Six Million Dollar Man (1973)

R2D2/C3PO – Star Wars (1977)

rkl ADVISORS for WHAT'S NEXT

Artificial Intelligence is nothing new…

First AI Character | Early Introductions | **Pop Culture** | Present / Future

War Games (1983)

Sneakers (1992)

Hackers (1995)

Artificial Intelligence is nothing new…

First AI Character | Early Introductions | Pop Culture | Present / Future

Meet Tilly Norwood – New AI Actress

Meet Xania Monet – First AI-powered artist

rkl ADVISORS for WHAT'S NEXT

Why AI and Cybersecurity Matter

Rapid Adoption of AI

- Where large data sets are available
- Who is adopting AI in the quickest fashion:
  - Information Technology
  - Finance & Insurance
  - Professional Services
- Industries with heavy legacy systems have more of a "lift"

Cybersecurity

- Maintaining a "healthy" IT environment, which would include infrastructure, applications, and cloud services
- Information is one of the most, if not most, valuable assets an organization can control
- Cyber crimes expected to hit $14 Trillion by 2028

Daily Impact

- Digital transformation efforts to find more effective and efficient ways to perform daily operational activity
- Doing more with less, but nothing comes without some level of risk

rkl ADVISORS for WHAT'S NEXT

Types of AI and Functionality Landscape

Narrow AI

- Task specific, no broad understanding
- Siri & Alexa

Generative AI

- Create content, deep learning models
- OpenAI's GPT & DALL-E

Super AI

- Surpass human intelligence on:
  - Problem solving
  - Creativity
  - Decision making
  - Emotional understanding

The Current State of AI

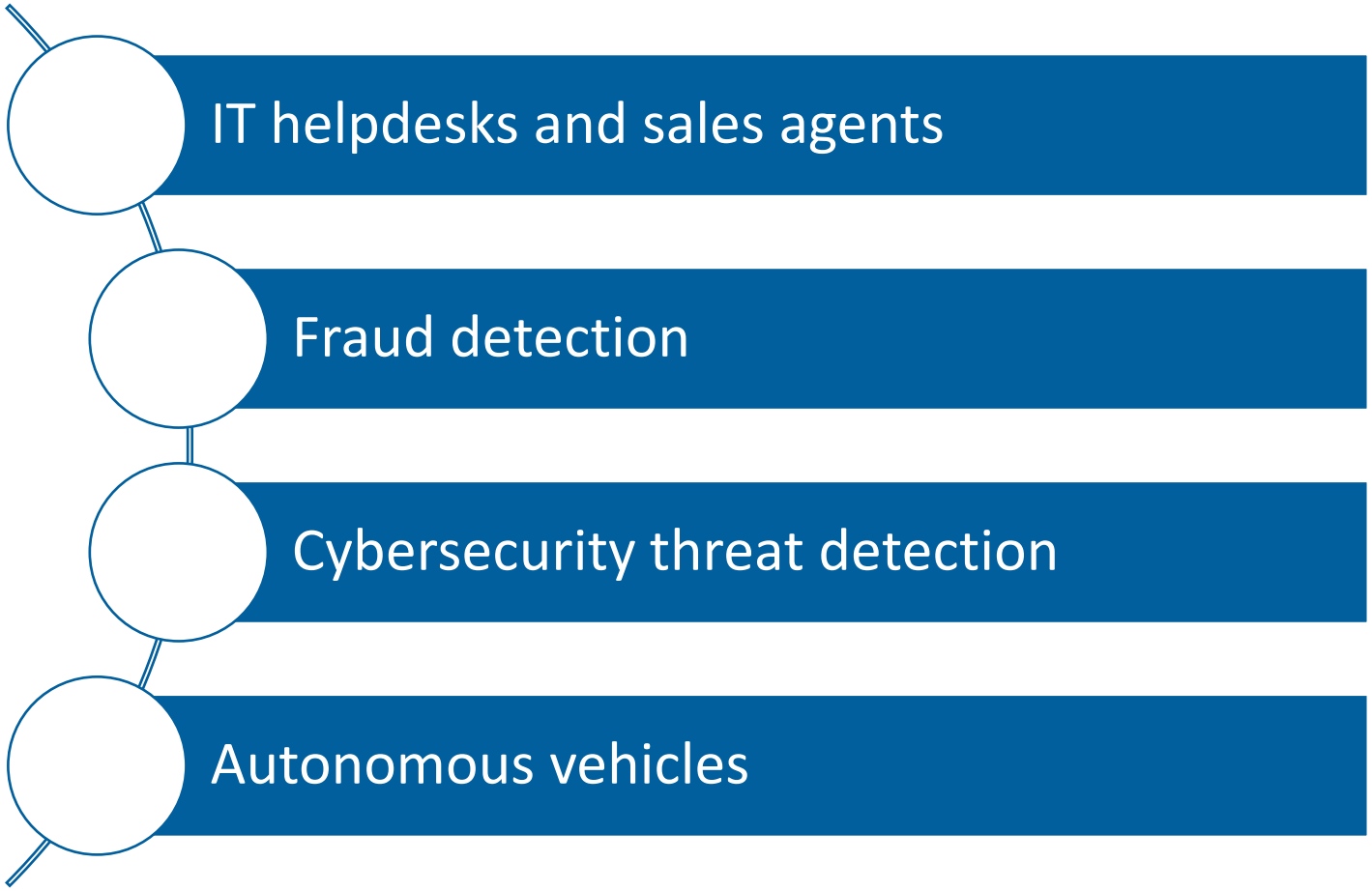
- 77% of companies are using or exploring AI integration, with 83% considering it a high priority
- Expected to contribute $15.7 Trillion to the global economy by 2030
- Technology giants pumping significant money into R&D
- 77% of devices in use today have some form of AI incorporated into their OS
- AI could eliminate 85 million jobs but is expected to create 97 million new ones, net gain of 12 million jobs
- Narrow AI is the most commonly used, i.e., personal assistants, recommendation algorithms

New Kid on the Block – Agentic AI

What is it?

- Considered autonomous AI system
- Proactive and capable of acting independently
- System exhibit features such as:
  - Autonomy
  - Adaptability
  - Collaboration
  - Specialization

Current Examples



rkl ADVISORS for WHAT'S NEXT

Current and Future State of AI

Current state

- Investments into AI technology and the consistent discussion around the "bubble"
- Increased Efficiency & Productivity
  - Automation of routine tasks
  - Reduction in human error
- Enhanced Decision Making
  - Data-driven insights
  - Predictive analytics
- Cost Saving
  - Long-term reduction in operational costs
  - Scaling business operations without proportional increases in staffing

Future (Next 10 years)
Creation of API-driven AI and microservices
No-code or low-code platforms
Hallucination insurance
Quantum leaps
Multimodal AI
Moonshot innovations – neuromorphic and optical computing
Personal and professional AI adoption will be democratized
Reskilling of workforce
Advances in natural language processing and computer vision

rkl ADVISORS for WHAT'S NEXT

Key Risks of AI Adoptions

1. Implementation of AI
2. Unintended consequences and errors
3. Data privacy concerns
4. Self-replication and model forking
5. Autonomy drift
6. Identifying new risk landscape
7. Legal and ethical grey zones

rkl ADVISORS for WHAT'S NEXT

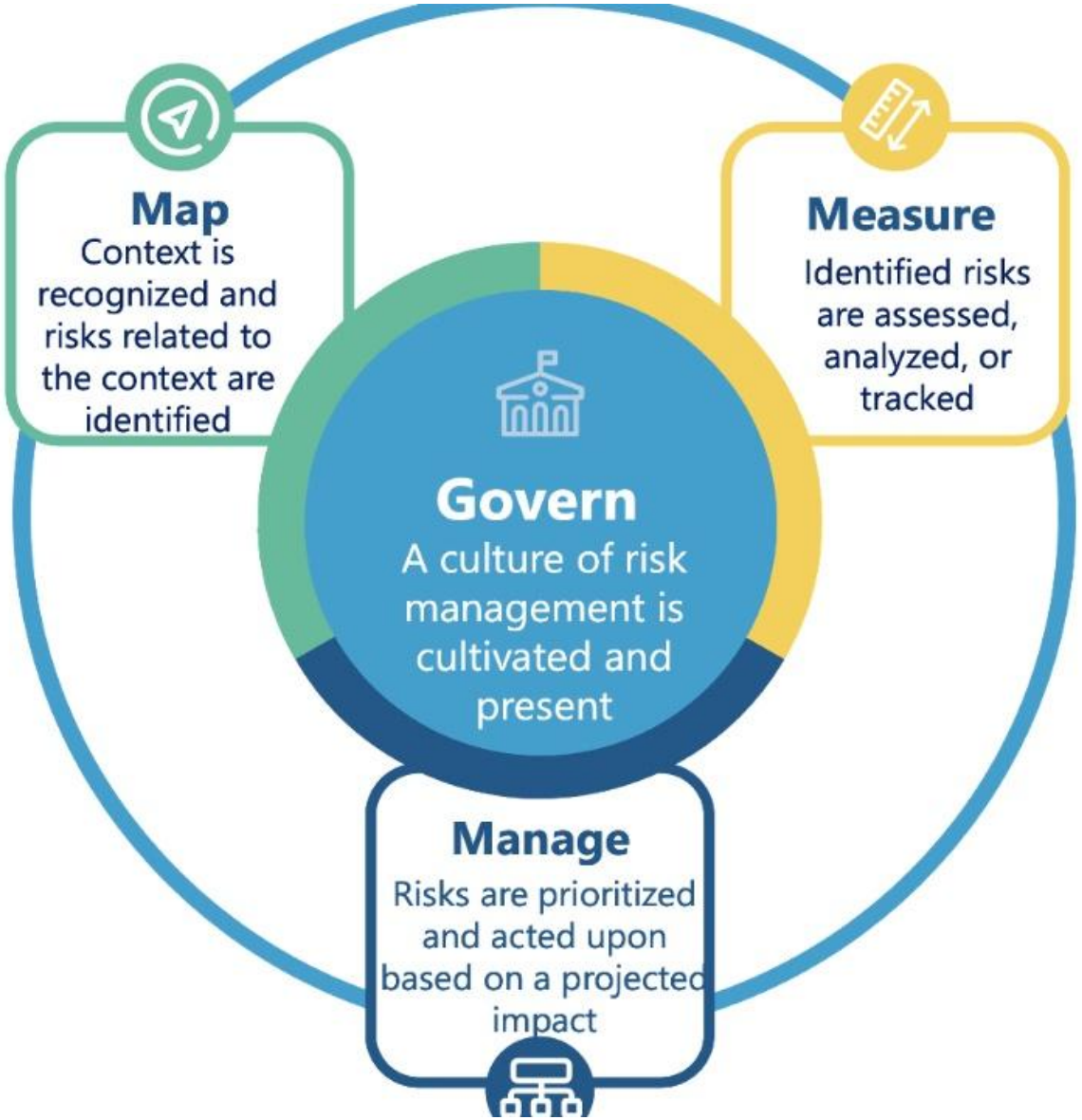
Ethical Considerations in AI

- Fairness in AI system outputs
  - Hallucinations
- Responsibilities of organizations
  - Policies and procedures to provide guidance
  - Avoidance of copyright and plagiarism
  - Verify before trusting the results
- Balancing innovation and ethics

rkl ADVISORS for WHAT'S NEXT

AI Operational Considerations

- AI Governance Framework (good governance is good business)
- How AI changes organization workflow
  - Changing the control environment
- Integrating new technology with legacy systems
- Staff training requirements
  - Prompting, validation of results, and evaluating necessary skill sets



rkl ADVISORS for WHAT'S NEXT

AI Regulatory Landscape

Laws and guidelines

- In the 2025 legislative session, all 50 states have introduced legislation on AI
- 38 States adopted or enacted around 100 measures this year
- Some examples
  - Arkansas – Generated content should not infringe on existing copyrights or IP rights
  - New Jersey – resolution urging generative AI companies to voluntary commitments regarding whistleblower protection
  - Pennsylvania – Image, text or video that used AI in whole or part to create, shall watermark on 30% of the image

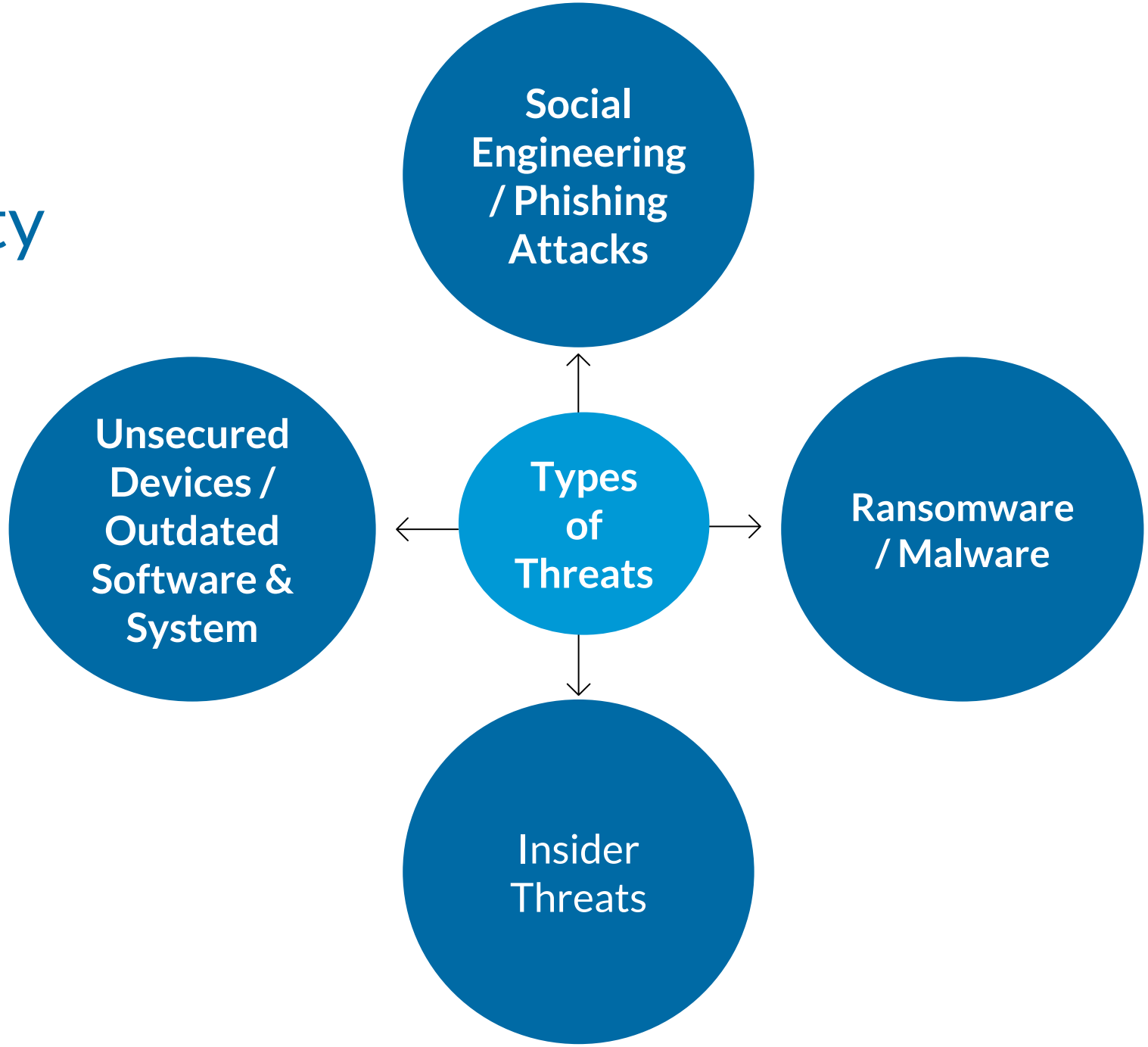
Compliance requirements

- How might it impact privacy?
  - Gramm-Leach Bliley Act
  - HIPAA
  - Consumer privacy laws (GDPR, various states)

rkl ADVISORS for WHAT'S NEXT

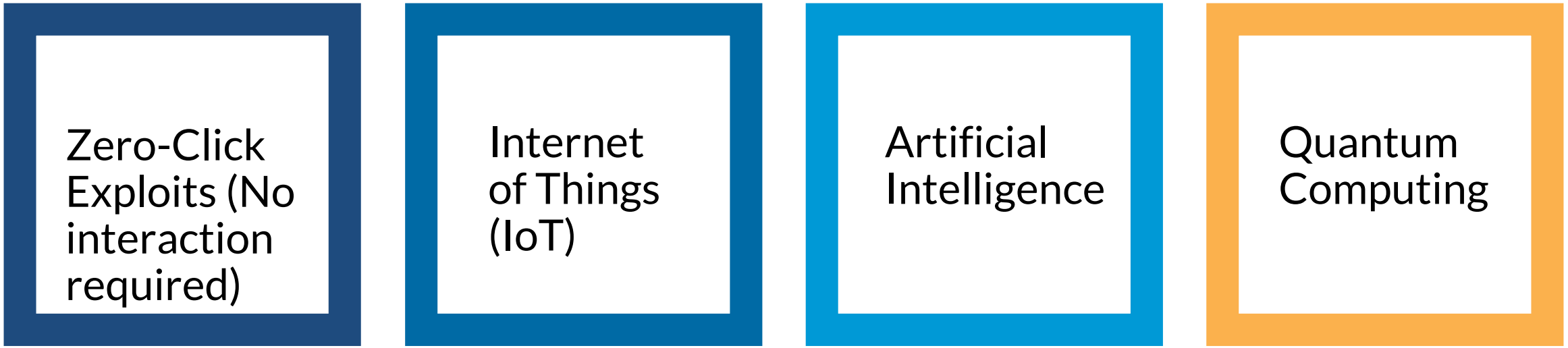
Cybersecurity Considerations

Cybersecurity Threats



rkl ADVISORS for WHAT'S NEXT

Cybersecurity Principles – Threat Trends



Resilience - Technology – Common Vulnerabilities

1. Weak passwords
2. Lack of encryption
3. Inadequate access controls
4. Unpatched software
5. Improper disposal of data
6. Lack of training / personal devices
7. Third-party vendor risks

rkl ADVISORS for WHAT'S NEXT

Risk Mitigation

rkl ADVISORS for WHAT'S NEXT

AI Risk Management

Human-in-the-loop

Manual review for all high-impact decisions tied to key performance indicators

Continuous monitoring

Use "observer agents" to track systems behavior in real time and conduct post-incident reviews

Manage AI like a third-party vendor

Audit training data, contractual SLAs, and review vendor due diligence for bias safeguards

Executive briefing

Leadership remains consistently updated on emerging AI risks, advancement in governance and strategic investments

Organization customized training

Develop team-oriented AI literacy in risk, legal, HR, audit and procurement and designate champions to spot weak signals

Red teaming

Simulate adversarial prompts and test model vulnerabilities

rkl ADVISORS for WHAT'S NEXT

Cybersecurity Risk Management

Cybersecurity Risk Assessments

Essential to understand where cybersecurity risk reside within your organization and create priorities

Regular Staff Training

Review cybersecurity elements to elevate general understanding of terms and attach vectors

Strong Password Policy

Establish a strong password policy across all systems and applications

Update & Patch Management

Systematic approach to ensuring that the network, its components, and applications have the latest update

Multi-factor Authentication

Going beyond the traditional password, MFA should be active on all available systems

IT Governance

Implement a well establish IT framework, along with appropriate policies and procedures – be consistent!

Strategic Leadership

- Make cybersecurity a board-level / C-Suite priority
- Build strategies (AI and cybersecurity) into operations
- Treat technology as a strategic investment, not just a cost center
- Establish executive oversight on resilience initiatives
- Encourage communication between teams

Recap of Key Points

Importance of keeping security in line-of-sight

There are various ways that companies could be exposed

The role that all team members play in keeping the covered entity secure

Strategies for enhancing cybersecurity

Takeaways

- Don't be afraid to "Think outside the box" but make sure you look before you leap. Don't get distracted by "new shiny toys."
- Encourage the concept of "See something, Say something."
- Challenge the current cybersecurity practices.
- Don't be afraid of an assessment.