ECHELON RISK + CYBER

EXPAND YOUR CRITICAL SKILLS WHILE INCORPORATING ARTIFICIAL INTELLIGENCE

TPRM professionals are looking to embrace the inclusion of ChatGPT and other AI tools into their toolbox but like any useful tool, it can have consequences if they're not used properly. By not wisely thinking through the methodology and usage of these powerful tools you can leave your program vulnerable to incomplete or bad data and allow you to reach conclusions that may not be within your organizations risk tolerance. In this session, we'll discuss possible pitfalls along with strategies to ensure the successful adoption of AI tools into your program.

September 27, 2023

Introducing… Echelon Risk + Cyber's Tom Garrubba

Tom.garrubba@echeloncyber.com

Tom Garrubba is an internationally recognized thought leader in business, cyber and privacy risk. He has over 20 years of experience in cyber, privacy, audit and compliance, and consulting. He is an instructor for the Shared Assessments' Certified Third Party Risk Professional (CTPRP) and Assessor (CTPRA) programs. He has been featured in numerous industry publications and podcasts, and is the host of "TPRM Tidbits" a weekly LinkedIn podcast on current TPRM topics. He is also a member of the Forbes Technology Council and the InfraGard - Pittsburgh chapter.

Education

- MS - Information Technology Management, Robert Morris University
- BSBA - Finance, Robert Morris University

Certifications

- CISA – Certified Information Systems Auditor
- CRISC – Certified in Risk & Information Systems Controls
- CIPT – Certified Information Privacy Technologist
- CTPRP – Certified Third-Party Risk Professional
- CTPRA – Certified Third-Party Risk Assessor

AGENDA

1. Top Four AI risk TPR Professionals Need to Know
2. Strategies to Deliver the Risk Message
3. Third Parties Using AI to Process Your Data
4. Using TPRM in Your Assessment Process
5. Summary & Next Steps

1. Bias and Fairness

- Risk: AI systems can inherit biases present in their training data, leading to discriminatory outcomes or unfair treatment of certain groups.
- Delivery: Explain the concept of bias in AI, provide real-world examples, and emphasize the potential legal and reputational consequences. Illustrate how third-party AI systems can introduce bias into decision-making processes.

2. Security Vulnerabilities:

- Risk: AI systems are susceptible to cyberattacks, data breaches, and adversarial manipulation, which can compromise sensitive information and decision integrity.
- Delivery: Highlight the security implications of AI, such as the risk of model poisoning or adversarial attacks. Emphasize the need for rigorous security assessments of third-party AI vendors and their solutions.

3. Transparency and Explainability:

- Risk: Many AI models are opaque and difficult to interpret, making it challenging to understand how they arrive at specific decisions or predictions.
- Delivery: Stress the importance of transparency in AI models and their decision-making processes. Discuss the potential for regulatory and compliance issues when using opaque AI systems from third parties.

4. Ethical and Regulatory Compliance

- Risk: Failure to comply with evolving AI ethics and regulations can result in legal penalties, fines, and damage to an organization's reputation.
- Delivery: Outline the evolving landscape of AI regulations and ethical guidelines. Stress the need for third-party AI vendors to adhere to these regulations and describe the potential legal consequences for non-compliance.

STRATEGIES TO DELIVER THE RISK MESSAGE

Third-party risk professionals can employ the following strategies in order to effectively convey these risks to stakeholders:

1. **Use Real-world Examples:** Provide concrete examples of AI failures or incidents in similar organizations or industries. This helps illustrate the potential impact of these risks.

2. **Quantify Risks:** Whenever possible, quantify the risks in terms of financial impact, compliance costs, or reputational damage. This makes the risks more tangible.

3. **Scenario Analysis:** Develop scenarios or case studies that demonstrate how AI risks could materialize within your specific organization. This helps stakeholders understand the practical implications.

STRATEGIES TO DELIVER THE RISK MESSAGE

4. **Visual Aids**: Simplify complex concepts with charts and infographics to make it easier for non-technical stakeholders to grasp the risks.

5. **Engage in Continuous Education**: Regularly update stakeholders on the evolving landscape of AI risks, regulations, and best practices.

6. **Collaborate with Legal and Compliance Teams**: Work closely to ensure that AI-related risks are well-integrated into risk management strategies and are communicated effectively.

Value Add: TPRM professionals can help their organizations make informed decisions when it comes to adopting AI technologies from external vendors by addressing these AI risks and employing effective communication strategies.

THIRD PARTIES USING AI TO PROCESS YOUR DATA

What's your organization's attitude towards third parties using AI?

- Are you ok with third parties using it on your data?
- Do you need contractual protections or obligations?
- Can you obtain testing results?
- What about assessments?

Shareholder awareness is critical!

- First Line – make them aware of the vendors use of AI and explain the risks
- Second Line – ensure buy-in from…
  - IT Security – Addition to their risk register
  - Privacy – PII data awareness and data transfers
  - Legal – contractual issues or new legal language
- Audit – Keep them in the loop for internal and regulatory purposes

USING TPRM IN YOUR ASSESSMENT PROCESS

Decide where it makes sense in your DDQ to ask your AI questions (aka., SCOPE it properly!)

- Application Security
- Infrastructure and Security Tools
- Operations Management (e.g., change control, patching, etc.)
- Business Continuity/Disaster Recovery

USING TPRM IN YOUR ASSESSMENT PROCESS

Don’t use AI tools for assessments unless…

- They’ve been adopted and supported internally within the IT enterprise and the second line.
- Have been fully tested by the TPRM team to ensure quality of data (i.e., no GIGO)
  - Vendor repository
  - Internal corporate risk guidelines and standards
  - Industry standards or guidelines
  - Contractual requirements
- They are approved by TPRM management and other stakeholders for use

FINAL THOUGHTS

- All of the new threats have already been anticipated – there really isn't anything different
- Solutions to addressing any threats are very similar to existing threats we've addressed
- People are using AI in a less centralized way –people just go and use it when it's not centralized.
- https://owasp.org/www-project-ai-security-and-privacy-guide/

Tom Garrubba

Director of TPRM Services

CISA, CRISC, CIPT, CTPRP, CTPRA

e. tom.garrubba@echeloncyber.com

p. +1 (412) 720-4248

w. https://echeloncyber.com/

ECHELON
RISK +
CYBER

ECHELONCYBER.COM