The Future of Security Risk Management (SRM)

7 TOP SECURITY AND RISK MANAGEMENT TRENDS FOR 2022

- Trend #1: Attack Surface Expansion
- Trend #2: Digital supply chain risk
- **Trend #3: Identity threat detection and response**
- Trend #4: Distributing decisions
- Trend #5: Beyond Awareness
- Trend #6: Vendor Consolidation
- Trend #7: Cybersecurity Mesh

- Information source: Gartner
- STAMFORD, Conn., (2022). *Gartner Identifies Top Security and Risk Management Trends for 2022*. Available from: https://www.gartner.com/en/newsroom/press-releases/2022-03-07-gartner-identifies-top-security-and-risk-management-trends-for-2022 [Accessed 25 Oct 2022]

TECHNOLOGY TRENDS IMPACTING SRM

- The ability to continue adapting SRM methods to the future of work and ensure the safety of the entire workforce is made possible by new technologies combined with strong management strategies.

- **Predictive analysis**
  - Having the appropriate information at the right time.
  - Visualize risks and anticipate events using better data obtained through modern technology.

Artificial Intelligence (AI) or Machine Learning(ML)

AI has significant advantages for Cyber Security and SRM by simulating human intelligence and processes
It does not get tired or bored, and is able to process at rates far exceeding those using human interaction

Benefits of Artificial Intelligence (AI) or Machine Learning(ML)

- Can detect anomalies with traffic or process flows
- Can be used as part of an automatic response to an incident
- AI can process a lot of data
- "Boring" processes can be automated to reduce unintended risk
- AI can "learn and predict" future breach areas, and help to mitigate against them – essentially performs an ongoing security audit
- Deep learning through AI helps to predict and detect zero-day attacks by learning suspicious patterns – can protect CORE apps + endpoints (Handys or PCs etc)
- AI decreases response time
- Results learnt from AI can be used as part of Cyber Risk Quantification/Risk Assessments, to determine focus of Security Teams.

Negatives of Artificial Intelligence (AI) or Machine Learning(ML)

- Automation of phishing or other attacks. Can scale beyond existing norms
- Internet of Things is potential minefield. Not specific to AI but with more devices online all the time, security becomes harder and vulnerabilities easier to expolit. Ignorance of users to danger only exaccerbates the risk
- In same way AI learns to defend, AI can also learn to attack by exploiting discovered weaknesses through patterns in discovery – as it works, it is learning and adapting the whole time.

Sources

https://geekyants.com/blog/how-ai-and-ml-can-help-in-cybersecurity-risk-management/

https://www.linkedin.com/pulse/how-ai-changing-future-cyber-security-threat-protection-cetarkcorp