THE GREAT DEBATE - THE FUTURE OF SECURITY RISK MANAGEMENT (SRM-PCOM73)

Presented By:
GROUP 3

OCTOBER 2023

THE REVOLUTION

The Rise of Machine Learning (ML) and Artificial Intelligence (AI) - Enhancing Cybersecurity Landscape today and beyond.

Introduction

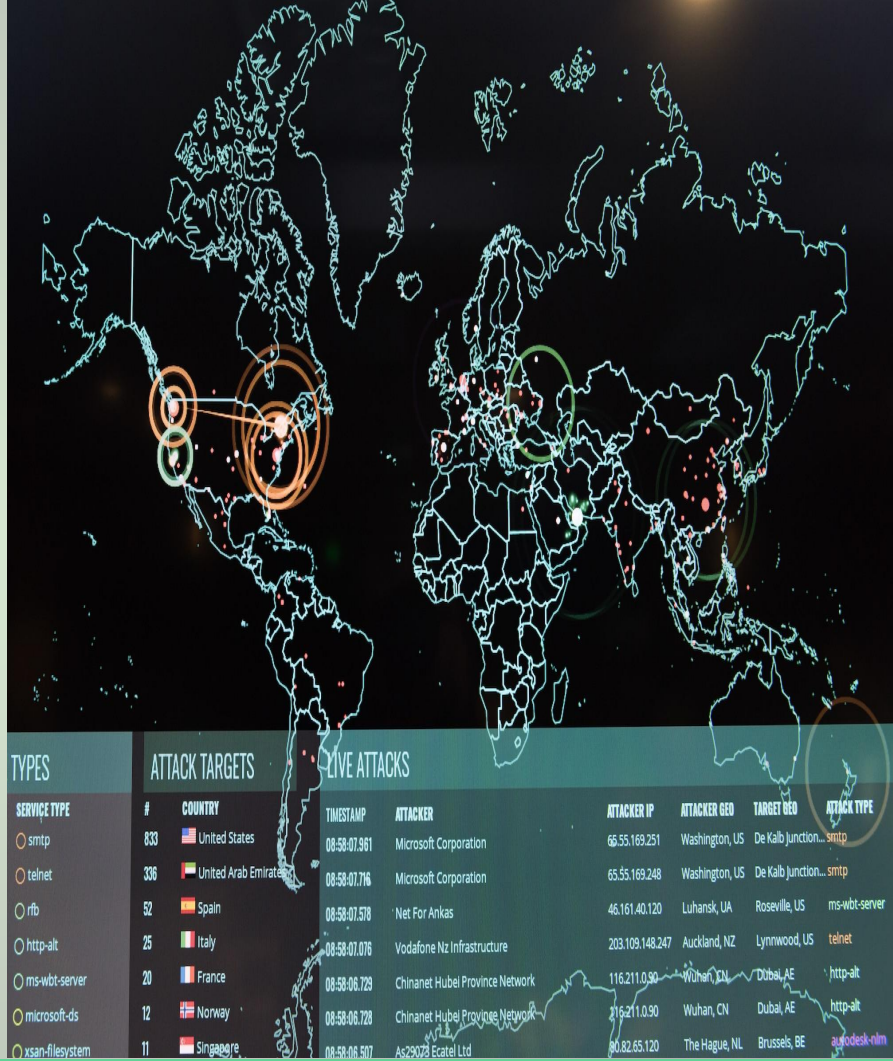
Where we are;

The fourth industrial revolution termed ‘Industry 4.0’ is here and it is characterised by the integration of digital technologies and automation in various industries, including cyber-security. Highlighting concepts like the Internet of Things (IoT), big data, cloud computing, robotics, and artificial intelligence, which transform business processes, operations, and models.

Kovaitė & Stankevičienė (2019)

… CONT’D

ML & AI is advancing human–machine interfaces, cyber–physical systems, cloud computing, authentication tools, fraud detection measures, smart sensors, advanced analytics capabilities, and digital customer profiling.



… CONT’D

This will continue with Reinforced Learning (RL) in the next 5 years. Thereby changing enterprise security risk management (ESRM) in ways the security industry is only starting to understand.

LeTellier, V. (2022)

AI and cyber security risks, threats, and vulnerabilities

The enterprise network defense paradigm is changing due to the integration of autonomous systems (i.e., automated and adaptive systems), cyber defense capabilities of large and complex mission network systems. (Hubbard, D. W., 2019)

...Cont'd

Automated and adaptive integration is made possible by AI/ML algorithms which can recognise patterns and anomalies that may indicate a security breach or vulnerability. This is evident in Advance Anti-virus/Anti-malware solutions, SIEM, SOAR solutions etc.

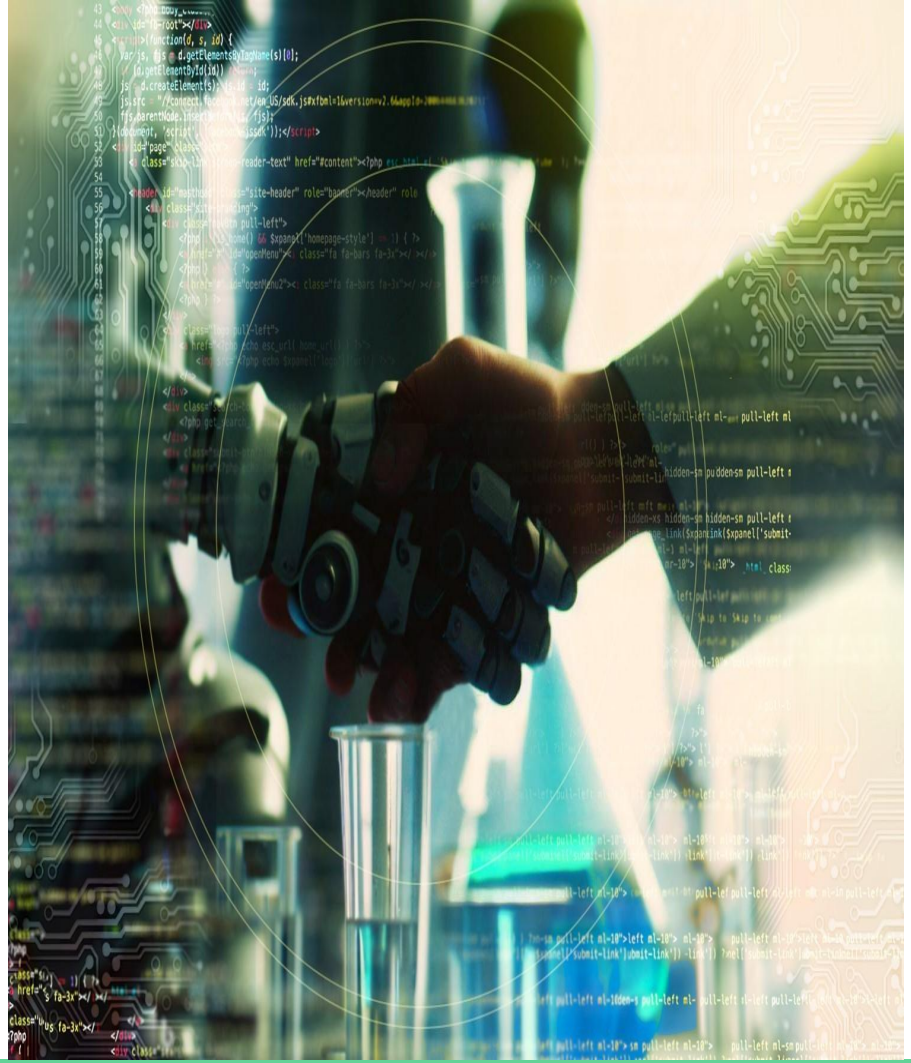
The Future of SRM - ML and AI in view

ML and AI will help in;

- Risk Identification and Assessment

- Threat Detection

- Aiding Vulnerability Assessment



Current Threat Landscape (CTL): Security risks, threats and vulnerabilities in information systems.

The CTL is leaning into sophisticated attacks and it is characterised by the growth in digital technology, the use of ML/AI, adoption of cloud computing, the possibility of work from anywhere (WFA), emerging technologies and status of activity, trends and multi-vector attacks.

REAL-WORLD Examples

- Ransomware Attacks on Healthcare systems (Prospect Medical Holdings, a private equity-backed hospital owner based in Culver City, Califonia has been dealing with ransomware attack since August 2023. This resulted in shutdown of outpatient service) - Bruce, G. (2023)
- DDoS (Largest DDoS attacks ever reported by Google, Cloudflare and AWS happened this October and was reported on 10-10-2023)
- Supply chain: SolarWinds Orion hack demonstrated the potential effectiveness and scale of a supply chain attack.

Methodologies to mitigate and/or solve security risks and their business impact

- Risk Management Framework like Enterprise Risk Management (ERM) encourages a broader perspective when identifying risk. - Lecturecast 6, Unit 10.

- Business impact analysis based on qualitative and quantitative risk assessment methods

...Cont'd

- Establish network access controls (including Firewall, IDS, IPS etc)

- Agile and DevSecOps: is simply security integration with DevOps (development and operations) which is a form of agile integrated security breaking down the traditional silos between programmers and system administrators during the software delivery lifecycle. - Kelly (2022)

Tools and Techniques to mitigate and/or solve security risks and their business impact

1. Machine Learning (ML): This is one of the most popular techniques used to apply artificial intelligence approaches to various fields, including security and risk.
2. Security Information and Event Management (SIEM) and SOAR (Security Orchestration, Automation and Response). Use for threat detection, use for Real-time monitoring, centralized data collection.
3. Inventory management software/up-to-date vulnerability assessment tools

The legal, social, ethical, and professional issues faced by information security and risk professionals

Social/Professional issues

- Ensuring that cybersecurity concerns and findings are written in layman terms which a non-specialist stakeholder can understand.
- Selecting appropriate framework
- Issues with interpreting the assumptions of risk landscape, uncertainties, and likelihood of occurrence to stakeholders.
- Balancing security needs with organisations budget limitations
- Interdisciplinary Collaboration
- Security professionals must work to maintain the public's trust for the organisations they work for.

Legal/Ethical

- Liability in the event of data breach or security incident.
- Ensuring that sensitive data and trade secrets are not exposed to theft or unauthorized access.
- Keeping up with all necessary regulatory bodies like GDPR, NCSC, HIPAA, PCI-DSS etc..
- Insider threat
- Confidentiality: Security professionals will, by the nature of their profession, see and handle personal, private or proprietary information that should be kept strictly confidential (Futureoftech, N.D.).

Conclusion

In conclusion, the advent of Industry 4.0, driven by AI and ML is reshaping the cybersecurity landscape and will continue to do so in the next 5 years. Technological advancements demand continuous vigilance and adaptation. This transformation brings both opportunities and challenges.

As security risks, threats, and vulnerabilities continue to evolve, cyber security professionals must navigate the interdisciplinary web of technology, legal, social, ethical, and professional issues while safeguarding information systems and maintaining public trust in an increasingly digital space.

THANK YOU

References

1. Bruce, G. (2023). The 16 hospitals disrupted in multistate ransomware attack. Available from: https://www.beckershospitalreview.com/cybersecurity/the-16-hospitals-disrupted-in-multistate-ransomware-attack. [Accessed 18 October 2023].
2. Future of tech (N.D.). Ethical Issues in Cybersecurity. Available from: https://www.futureoftech.org/cybersecurity/4-ethical-issues-in-cybersecurity/. [Accessed 18 October 2023].
3. Hubbard, W., D. (2019). The Failure of Risk Management: Why It's Broken and How to Fix It. Available from: https://web.s.ebscohost.com/ehost/detail/detail?vid=0&sid=a65405b8-ab50-4ca9-bcd5-eeea63f3f308%40redis&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#db=nlebk&AN=2381255. [Accessed 15 October 2023].
4. Kovaitė, .K. & Stankevičienė, .J. (2019). Risks of Digitalisation of Business Models. Available from: https://www.researchgate.net/publication/333063956_Risks_of_digitalisation_of_business_models DOI:10.3846/cibmee.2019.039 [Accessed 10 August 2023].
5. Kelly, W. (2022) Lecturecast 6. Future Trends. University of Essex Online.
6. LeTellier, V. (2022). Next Generation Enterprise Security Risk Management. Available from: https://www.asisonline.org/security-management-magazine/articles/2022/03/Next-Generation-Enterprise-Security-Risk-Management/ [Accessed 17 October 2023].
7. Google images