CYBERSECURITY & EMERGING TECHNOLOGY

A SECURITY INTEREST GROUP EVENT

Key learning from the trenches of cybersecurity & emerging technology

February 7, 2019

New York City

DISCUSSION LEADER & PANELISTS

Alex Beigelman

Discussion Leader

Alex is the former Head of Technology/Cybersecurity Risk at JPMorgan Chase as well as the InfoSec Leader at UBS Wealth management Americas. He is the founder of Beigelman Risk Advisors, serves on the Rutgers University Cybersecurity Advisory Board and is the Chairman of the Board for the National Cybersecurity Society.

Karl Scott

Panelists

Karl is an accomplished IT leader with a proven track record in data center, cloud computing, technology architecture, and security. He is a trusted technology advisor, has authored white papers/practical guides and leads Satori's Cybersecurity capability.

Josh Tomkiel

Josh is a leader within Schellman's Penetration Testing Practice. Josh has deep background in application penetration testing, mobile penetration testing activities and phishing programs.

INTRODUCTION

The objective of the Security Interest Group (SIG) event was to provide practical insight into breakthrough technologies, their cybersecurity issues, and considerations to manage risk. The breakthrough technologies include ***5G, Artificial Intelligence (AI), and FinTech***.

This document provides a summary of informative discussion and action items to consider. The SIG event scratched the surface and there are several layers to consider when adopting these breakthrough technologies.

5G

What is it?

5G is the next generation mobile network beyond 4G long term evolution (LTE)/WiMax.

Why is it relevant?

This technology significantly increases our connectedness and is a gateway to a new class of services. These enhancements fall into one of three categories:

- Enhanced mobile broadband - high definition video
- Massive machine type communication - smart cities
- Ultra-reliable and low latency communication - autonomous vehicles

Key features of 5G:

- 1-20 Gbps throughput
- <1ms latency
- Dense coverage
- Highly reliable connectivity

5G DISCUSSION SUMMARY

The following 5G key themes were discussed. The predominant view is *5G will open the door to additional threats in the future*.

- 5G is a gateway technology that enables delivery of new services and expands existing services such as IoT
- Risk is increased due to
  - Expanded attack surface due to additional devices connecting to the network
  - Services such as IoT possess proven, significant vulnerabilities
  - The increased bandwidth changes the game for data exfiltration
- Huawei poses a risk due to the potential for espionage and network disruption (Nation-State bad actors – either real or perceived)
- Pilot 5G rollouts are ongoing and commercial deployments will pickup in 2019
- 5G rollout will take time due to the significant carrier investment

5G KEY TAKEAWAYS

The following key takeaways resulted from the 5G discussion. The most pressing action to *take is preparing to respond to the volume of data and threats, and understanding risk associated with new solutions*.

- Focus on automation to address the increased volume of threats
- Thoughtful risk management must be performed when adopting 5G enabled services
- Identify solutions to mitigate increased threats introduced by 5G (e.g., massive DDoS)
- Prepare for the increased deployment of edge computing
- Understand telco deployment to ensure true 5G capability

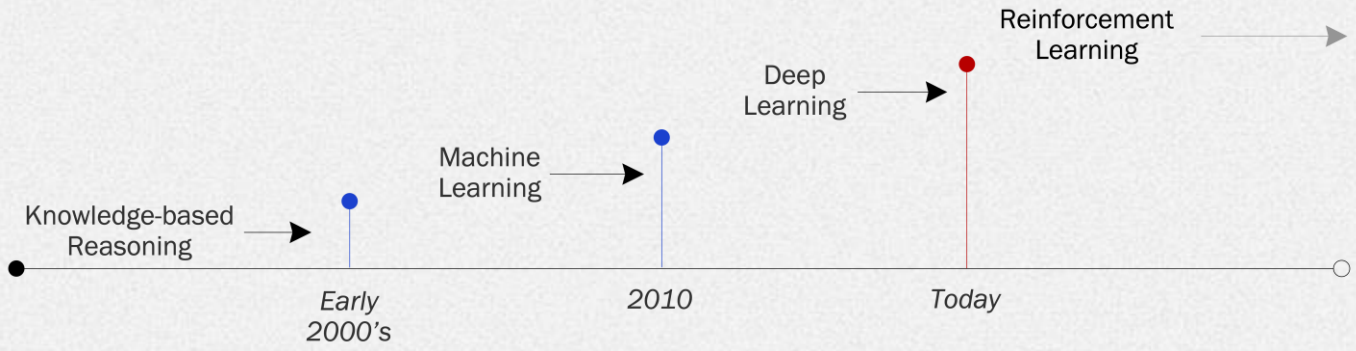
ARTIFICIAL INTELLIGENCE

What is it?

Use of computer-based logic to process information and simulate the ability to reason and problem solve.

Why is it relevant?

The availability to large data sets (big data), improved processing capability (GPUs), and tools to develop algorithms has propelled AI into the mainstream. AI impacts many aspects of business and society – autonomous vehicles, advertising (ad tech), prison sentencing and defense systems.



Shifts in Artificial Intelligence

AI DISCUSSION SUMMARY

The following AI key themes were discussed. The predominant view is *several threats exist to AI-based solutions and regulation should be considered where significant harm to individuals and society exists*.

- There are several threats to consider when using AI-based solutions – poisoning of input data, incomplete data or algorithms, and unethical algorithms
- Identifying noise in data is a challenge for AI based solutions
- AI used to create more sophisticated malware that can be hard to detect
- GDPR does not prohibit the use of AI, the focus is to ensure algorithms are explainable, fair, and transparent
- Regulation of AI is an ongoing discussion.
  - Pro - AI that can cause significant harm (e.g., algorithmic trading, autonomous vehicles) and algorithms must be audited to ensure risk is managed. Risk is too high and government oversight is needed.
  - Con – Government must not stifle innovation and let markets decide. Businesses can provide adequate oversight.

AI KEY TAKEAWAYS

The following key takeaways resulted from the AI discussion. The most pressing action is to *ensure the integrity of the data (includes data poisoning) and assess algorithms for fairness and transparency.*

- Organizations must understand and explain algorithms used in AI solutions – ensure they are complete, fair, and transparent
- Protect the integrity of big data sets
- Consider independent AI auditing to validate algorithms

FINTECH

What is it?

Startups/ventures that leverage technology to offer innovative financial services – mobile payments, microloans, robo-advisers etc.

Why is it relevant?

FinTech companies have brought Silicon Valley innovation and speed to the financial industry that is not historically used to moving at these speeds. The technology innovation also has the potential to drastically change business models (e.g. blockchain removing the need for trusted intermediaries).

FINTECH DISCUSSION SUMMARY

The FinTech themes discussed are described below. The predominant view is *FinTech organizations must be subject to the same risk management and cybersecurity rigor as other companies*. The data collected, processed, and stored can be sensitive.

- FinTech companies must manage the risk to sensitive data the same as financial institutions
- In some instances, FinTechs can be more secure due to the lack of legacy systems and technical debt
- Cybersecurity isn't a product that can be purchased. It takes a blend of people, process and technology to build security into the culture and continually manage risk.
- Cybersecurity can be perceived as a losing battle due to the lack of executive support; however, the issue of risk management continues to come to the forefront. Organizations experience greater success when continual risk awareness, privacy by design, and build security in practices are adopted.
- Regulators hold companies accountable when their contracted third-parties engage in non-compliant activity
- Cybersecurity insurance continues to be challenge due to the lack of standards to assess and measure risk.

FINTECH KEY TAKEAWAYS

The following key takeaways resulted from the FinTech discussion. The most pressing action is performing due diligence *to validate cybersecurity effectiveness within FinTech*. Data must be managed in accordance with leading practices.

- Focus on governance of third parties – manage risk
- Agile methodology does not prohibit effective security – ensure security is built into the product development process. Data protection impact assessment (DPIA) is a tool FinTechs must consider
- Organizations must identify principles to guide risk management and build security in (e.g., data minimization and least privilege)
- The cyber insurance industry is continually evolving. Understand the value of insurance policies before making the purchase.

Thank you

More info or briefing:
cyber@satoriconsulting.com