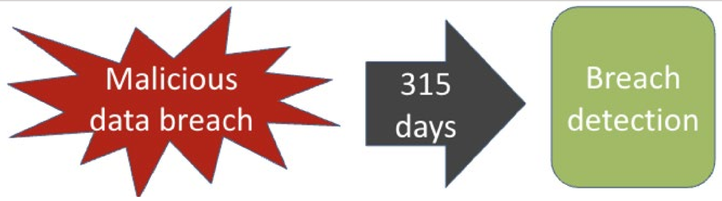
AI in Cybersecurity as a Business Strategy

GOAL: leverage the power of AI in cybersecurity tools to implement a cybersecurity-centric business strategy and boost an organization's cyber-resilience

Cynthia Zhang, Ranjan Pal, Corwin Nicholson, Michael Siegel

1. Challenges to quick detection and containment of data breaches



- 65% of cyber-security expertise slots are NOT filled
- many suffer from job fatigue due to repetitive workloads and high dynamicity of cyber-attack detection solution/process space
- Human error accounts for 95% of cyber-breaches

2. AI aids human cyber personnel

AI boosts cyber-resilience in the following ways when compared to human intelligence solely:

1. AI automates repeatable tasks, contributing to less personnel fatigue, therefore boosting focus.
2. AI can precisely identify root causes of an attack, which is computationally infeasible for humans.
3. AI can find complex patterns between threat indicators and between incidents.
4. AI can parse through large, noisy datasets to provide personnel with structured and concise information needed to respond to incidents.
5. AI is fast. It can work with real-time threat data and quickly generate accurate threat intelligence.

3. CAMS introduces AI cybersecurity tools as a business strategy

AI	Cybersecurity	Examples of use as a business strategy
✓	✗	e.g. spam filters, smart searches, content curation, etc.
✗	✓	e.g. cybersecurity training, firewalls, secure passwords, etc.
✓	✓	Not yet seen. To be discussed in this poster (CAMS)

4. AI cybersecurity tools as a business strategy boosts revenue

5. Which AI security elements should an enterprise adopt?

strategic elements \ enterprise types	Transactional Vendors	Hardware, Software, Firmware Suppliers	Security as a Service
What kind of enterprise is this?	Enterprises offering services such as the use of point-of-sale products (e.g. retail stores)	Enterprises who have a locked-in set of enterprises as customers (in a supply chain) who are being supplied a product (e.g. AWS)	Enterprises that sell security solutions and provide solution consultation to its clients (e.g. CrowdStrike, Trellix)
How much should this enterprise spend on AI cybersecurity tools?	Must spend on security-boosting AI and related automation costs pertaining to secure operation POS devices.	Must spend enough on AI cybersecurity tools to gather client environment data. This minimizes the likelihood of a business-disrupting malicious intruder entering IT/OT systems.	Must spend on AI that collects and analyzes both client environment data (to protect the enterprise's systems) and client cyber-posture information to generate effective alerts (to secure the client)
What is an example of tools to be used?	*Feedzai* is used across the banking industry and leverages AI to detect and prevent fraud in real-time by tracking behavioral and transactional patterns.	A *real-time system orchestrated AI* that performs continuous monitoring across the entire attack surface. *ScadaShield* (by Cyberbit) performs as described and can be combined with ESOC automation to trigger workflows that accelerate cyber-attack root cause identification and mitigation.	Trellix's *XDR platform* uses AI and data from threat intelligence from billions of sensors across corporate and government enterprises to reduce malicious intruder probabilities and boost enterprise cyber-resilience.

6. AI cybersecurity tools as a business strategy fit well the *Eight-Fold* and *Five Forces* strategy models for businesses.

Elements fitting Cusumano's Eight-Fold Strategy	Elements fitting Porter's Five-Forces Strategy
Enterprises that supply cybersecurity as a service: 1. are part of a potentially attractive, untapped, growing market 2. provide compelling cybersecurity ingrained products/services that customize to customer needs 3. are in a market with strong evidence of client/customer interest Any enterprise with a cybersecurity strategy/vision has: 4. a business model showing growth and significant future profit	For enterprises that supply cybersecurity as a service (e.g. Trellix): 1. the threat of new entrants (e.g. Trellix competitors) 2. product substitutes (e.g. other AI driven platforms like HVS) 3. high bargaining power of customers (e.g. Trellix's clients) 4. low bargaining power of suppliers (e.g. Trellix) pushes enterprises to adopt AI cyber-security tools as a business strategy to boost KPI.

7. How can the research outcome help CAMS member interests?

With a good management to drive the vision charted by AI as a cyber-security strategy, AI will boost an enterprise's cyber-resilience and drive profits by filling in gaps where humans fall short and providing cyber-security guarantees for client businesses.

Contacts: {zcynthia*, ranjanp*, corwin77, msiegel}@mit.edu