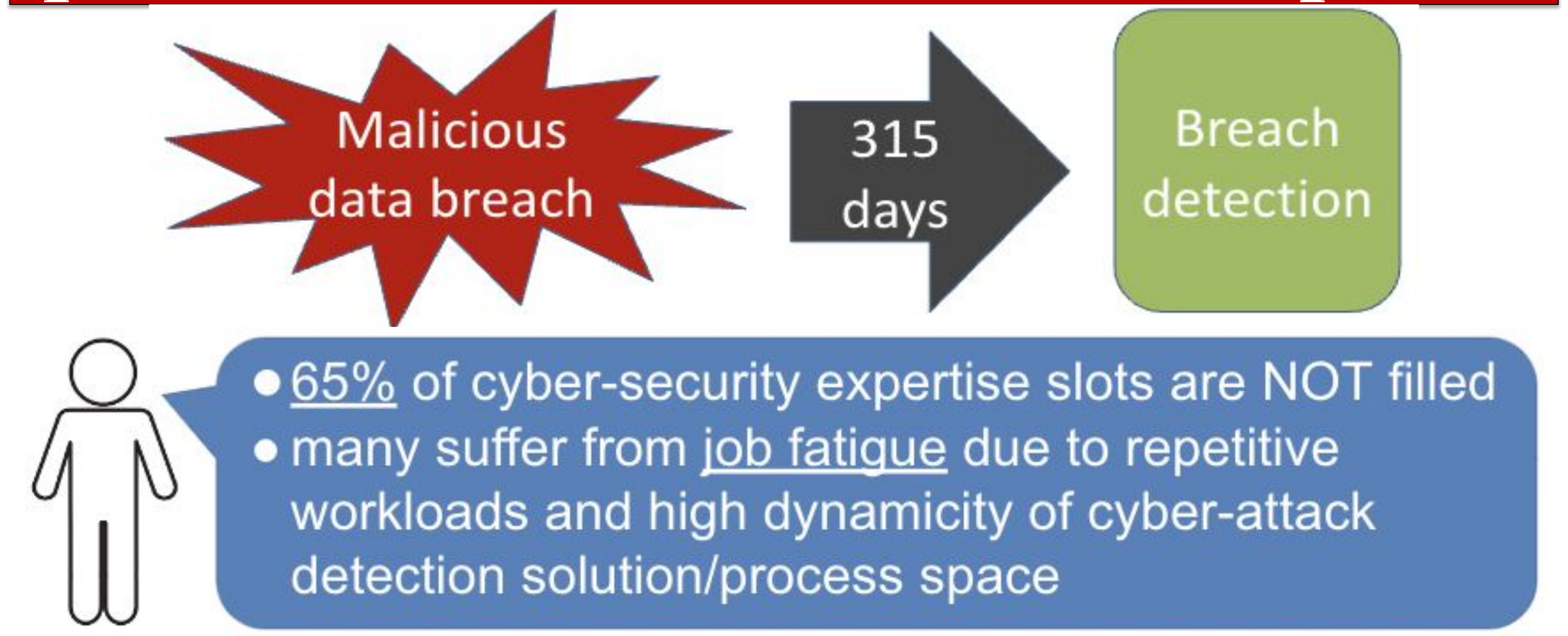
(Gen)AI for Cybersecurity via a Lens of Business Strategy

GOAL (Research in Progress) : strategically leverage, using (Gen)AI, the power of cybersecurity tools and processes within (IT/OT) driven businesses to <u>boost cyber-resilience</u> and <u>sustain market competitiveness</u>

Cynthia Zhang*, Ranjan Pal*, Corwin Nicholson, Michael Siegel

1. IT/OT challenges (and $ impact) to quick data breach detection+response



- <u>65%</u> of cyber-security expertise slots are NOT filled
- many suffer from <u>job fatigue</u> due to repetitive workloads and high dynamicity of cyber-attack detection solution/process space

The average data breach in 2022 cost **$4.35 million**.

Source: 2022 IBM “Cost of a Data Breach” Report

(Gen)AI is a solution to the challenge. Can it strategically aid boosting an enterprise’s <u>cyber-resilience</u> and <u>competitive strategy?</u>

2. (Gen)AI can boost IT/OT resilience

(Gen)AI boosts cyber-resilience in the following ways in comparison to human intelligence/manual effort:

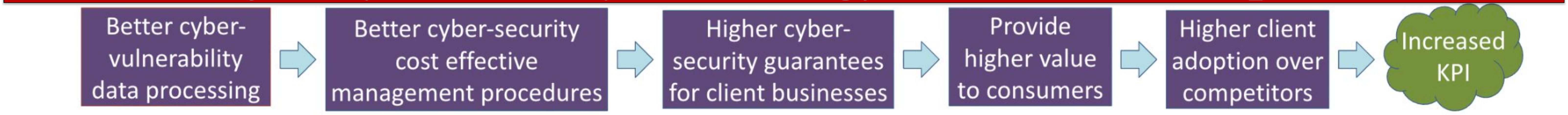
[*cyber-resilience* - incident response ability (NIST)]

1. <u>Automates</u> intelligent intrusion detection.
2. Can precisely <u>identify root cyber-attack causes</u>.
3. Can find <u>complex correlational patterns</u> between threat indicators and between incidents.
4. Can <u>parse through large/noisy traffic datasets</u> to equip SOC personnel with structured information.
5. <u>Is fast</u>. (Gen)AI can process real-time threat data quickly to generate accurate threat intelligence.
6. GenAI can <u>identify vulnerabilities</u> or bugs in code.
7. GenAI can <u>understand malware’s functionality</u> and impact and generate remediation responses.
8. GenAI can <u>streamline implementation</u> of security policy via generating code from text commands.

3. Market survey of enterprises benefitting from the use of (Gen)AI based cybersecurity tools boosting cyber-resilience of IT/OT services

enterprise types strategic elements	Transactional Vendors	Hardware, Software, Firmware Suppliers	Security as a Service
What kind of enterprise is this?	point-of-sale products (e.g. retail stores)	Enterprises supplying a product (e.g. AWS)	Enterprises selling security solutions (e.g. CrowdStrike, Trellix)
What type of AI cybersecurity tools should be adopted?	AI for secure operation POS devices	AI for gathering client environment data	AI that analyzes client environment data and client cyber-posture information
What is an example of tools to be used?	*Feedzai* - banking	*Cortex XSIAM* (by Palo Alto Networks) - attack surface monitoring	Trellix's *XDR platform* - data analysis and response

4. *(Gen)AI for Cybersecurity* as strategy for market competitiveness


Better cyber-vulnerability data processing
Better cyber-security cost effective management procedures
Higher cyber-security guarantees for client businesses
Provide higher value to consumers
Higher client adoption over competitors
Increased KPI

5. The *AI for Cybersecurity* strategy fits well with the *Cusumano* and *Porter* strategy recommendations to sustain market competitiveness

Elements fitting Cusumano’s Eight-Fold Strategy

Enterprises that supply cybersecurity as a service:

1. are part of a potentially attractive, untapped, <u>growing market</u>
2. provide compelling cybersecurity ingrained products/services that <u>customize to customer needs</u> (e.g. CharlotteAI, a genAI assistant)
3. are in a market with strong evidence of <u>client/customer interest</u> (e.g. CAMS members)

Any enterprise with a cybersecurity strategy/vision has:

4. price/service quality economic model showing growth and significant future profit (ongoing research)

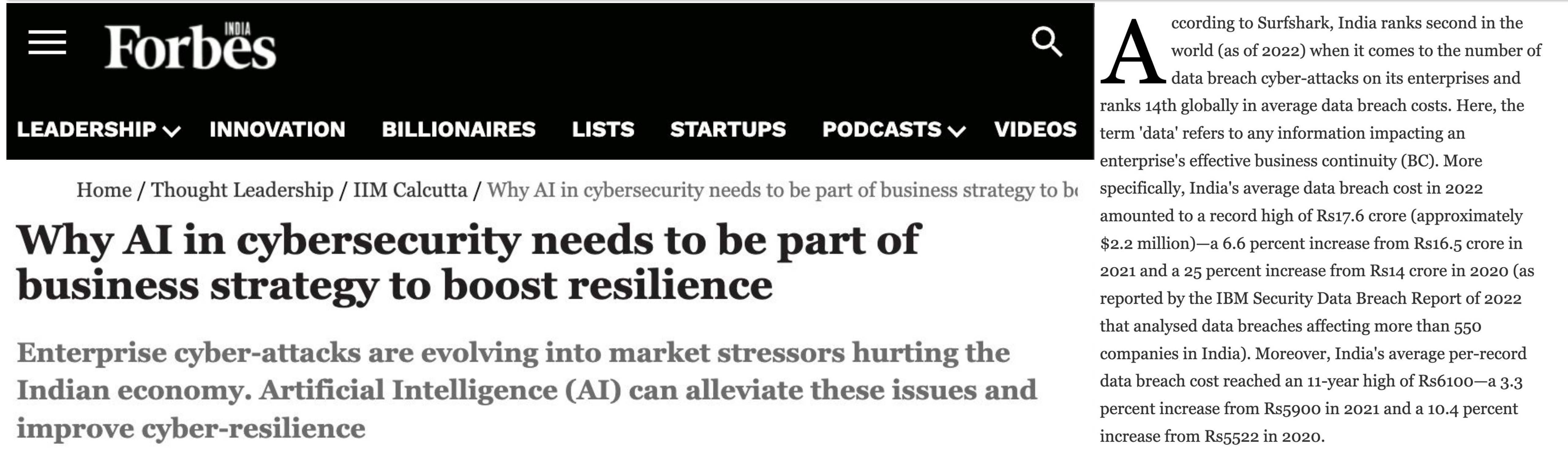
Elements fitting Porter’s Five-Forces Strategy

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.

6. Read more about our work published in Forbes



Home / Thought Leadership / IIM Calcutta / Why AI in cybersecurity needs to be part of business strategy to b

Why AI in cybersecurity needs to be part of business strategy to boost resilience

Enterprise cyber-attacks are evolving into market stressors hurting the Indian economy. Artificial Intelligence (AI) can alleviate these issues and improve cyber-resilience

According to Surfshark, India ranks second in the world (as of 2022) when it comes to the number of data breach cyber-attacks on its enterprises and ranks 14th globally in average data breach costs. Here, the term 'data' refers to any information impacting an enterprise's effective business continuity (BC). More specifically, India's average data breach cost in 2022 amounted to a record high of Rs17.6 crore (approximately $2.2 million)—a 6.6 percent increase from Rs16.5 crore in 2021 and a 25 percent increase from Rs14 crore in 2020 (as reported by the IBM Security Data Breach Report of 2022 that analysed data breaches affecting more than 550 companies in India). Moreover, India's average per-record data breach cost reached an 11-year high of Rs6100—a 3.3 percent increase from Rs5900 in 2021 and a 10.4 percent increase from Rs5522 in 2020.

SCAN ME

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