Guy Carpenter

AI-DRIVEN SYSTEMIC INSURANCE RISK

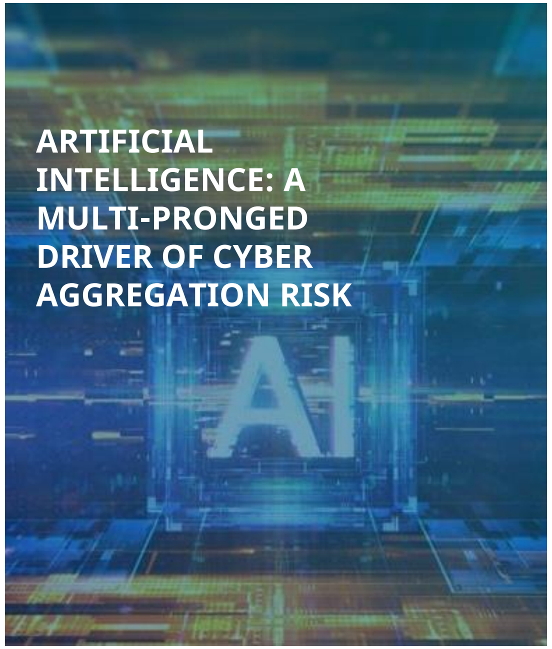
December 12, 2024

A business of Marsh McLennan

Advancing Understanding of AI-Driven Systemic Risk

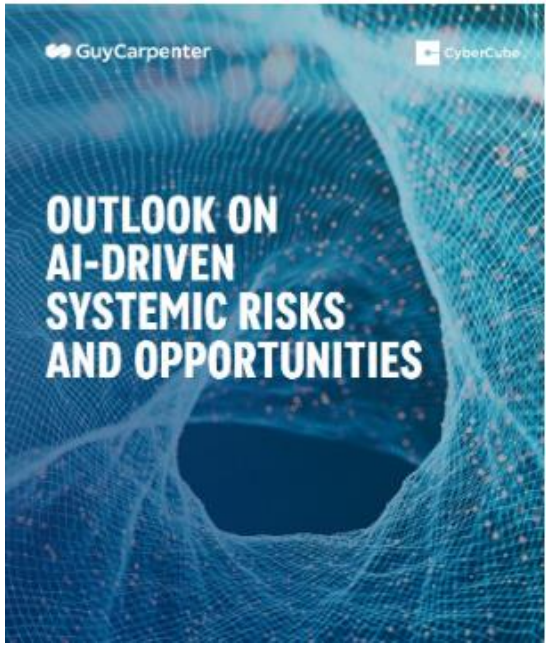
Guy Carpenter's 3-Paper Series on Artificial Intelligence and the Insurance Industry

Conceptual Discussion


ARTIFICIAL INTELLIGENCE: A MULTI-PRONGED DRIVER OF CYBER AGGREGATION RISK
AI

- AI presents an additional software supply chain threat
- AI presents a new attack surface
- AI presents a data privacy threat
- AI in security roles

Analytical Examination



- Exploring an analytical framework for AI risk quantification
- Examining AI Implications of Historical Events

Quantitative Evaluation

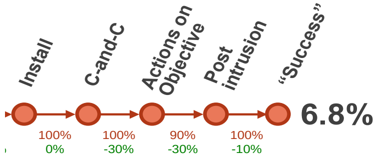
- Develop a concrete pathway to assess and quantify the impact of artificial intelligence on cyber risk

CyberCube Model Framework for AI Impact Exploration

Scenario Catalog | 33 cat scenarios modeled with nearly 500 points of failure

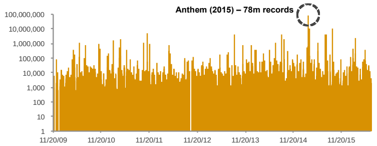
1 Scenario Frequency

Probabilistic Kill Chain Framework

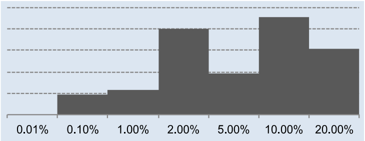


Threat Modeling

Historical Model



Expert Model



Historical Data

>700 aggregation events, theoretical attacks and near misses

Expert Surveys

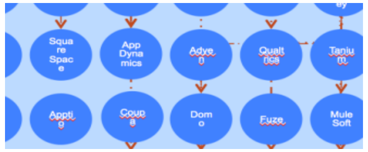
130-person expert panel

How often will cyber catastrophe events happen?

2 Footprint

Interconnections

Firmographics



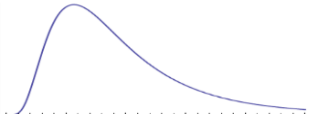
Organizational Statistics

> 23m company data set

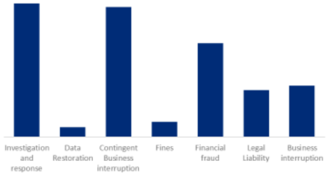
Which organizations are affected?

3 Severity

Cost Modelling



Cost Components



Detailed Coverage Level Results

CyberCube modelling based on >50k publicly disclosed cyber events

What is the financial impact?

AI Impacts on the CyberCube Framework

Frequency

- Increased automation of attack process across the kill chain allowing threat actors to more efficiently carry out a greater number of attacks with improved success rate
- Improved Large Language Models (LLMs)
  - Drives easier identification of vulnerabilities
  - Promotes more effective phishing campaigns leveraging deep fakes
- Access to superior AI technology gives defenders an advantage in detecting threats

Greater volatility in defender/threat actor cycle

Footprint

- Pre-intrusion phases (Reconnaissance & Weaponization) made more effective
  - Increases ability to attack many simultaneous targets in a cost-effective manner
- More compromised assets and greater volume of exposed records drive greater leverage in extortion negotiations
- Polymorphic malware
  - Automate learning and command and control phases
  - Avoid detection through continual mutation

Extent of AI defense implementation will influence impacts

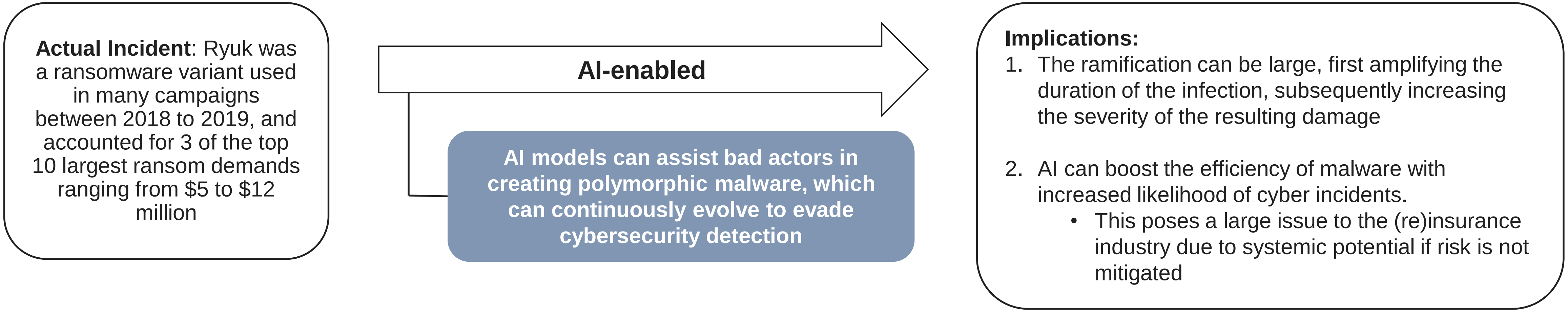
Severity

- Enhancement of post-intrusion phases (Delivery & Exploitation, Installation, & Command & Control)
  - Improved lateral movement, privilege escalation, evasion of detection, and efficient data exfiltration.
  - Polymorphic malware increases dwell time
- Faster and more stealthy data exfiltration
  - Reduction of extraction file sizes
  - Automation of mass data analysis to identify valuable data.
- Improved differentiation ability for cybersecurity efforts

Increased dwell time, exfiltration, but an improvement in monitoring for defenders

Exploring The Implications of AI Through Counterfactuals

Counterfactual 1: Ryuk Ransomware



Actual Incident: Ryuk was a ransomware variant used in many campaigns between 2018 to 2019, and accounted for 3 of the top 10 largest ransom demands ranging from $5 to $12 million

AI-enabled

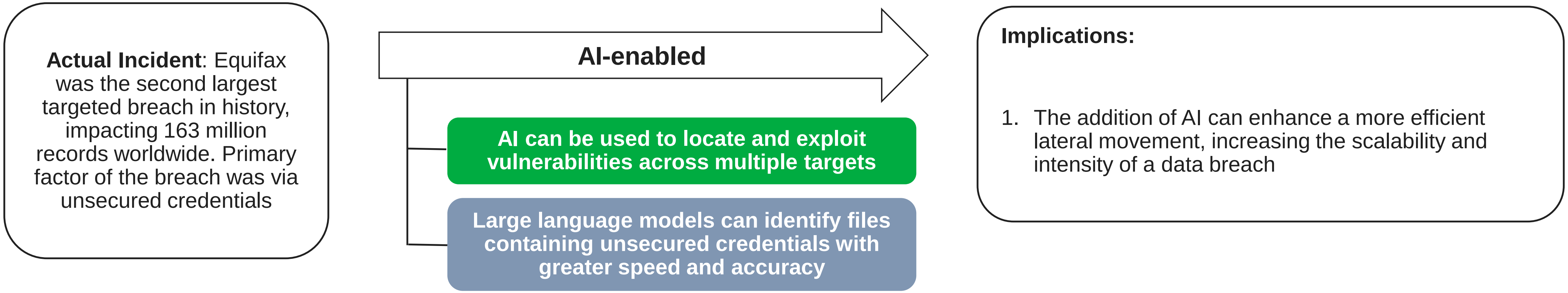
AI models can assist bad actors in creating polymorphic malware, which can continuously evolve to evade cybersecurity detection

Implications:

1. The ramification can be large, first amplifying the duration of the infection, subsequently increasing the severity of the resulting damage

2. AI can boost the efficiency of malware with increased likelihood of cyber incidents.
   - This poses a large issue to the (re)insurance industry due to systemic potential if risk is not mitigated

Counterfactual 2: Equifax Data Breach



Actual Incident: Equifax was the second largest targeted breach in history, impacting 163 million records worldwide. Primary factor of the breach was via unsecured credentials

AI-enabled

AI can be used to locate and exploit vulnerabilities across multiple targets

Large language models can identify files containing unsecured credentials with greater speed and accuracy

Implications:

1. The addition of AI can enhance a more efficient lateral movement, increasing the scalability and intensity of a data breach

Legend

🟦 **Frequency** 🟩 **Footprint** ▨ **Severity**

Continuing Our Investigation

Topics for Future Research Report and Thought Leadership Publications

○ Will the prevailing impacts of artificial intelligence drive insurance claims frequency or severity?

○ Will AI advancements provide more benefit to cyber defenders or threat actors? How can models avoid overestimation of AI loss impact?

○ AI can enhance the exploitation of vulnerabilities but to what extent is AI itself an accumulation path for systemic cyber attacks?

Guy Carpenter will continue to encourage deeper understanding of the implications of AI through future research and projection of AI impact to the insurance industry.

GuyCarpenter

This document and any recommendations, analysis, or advice provided by Guy Carpenter are intended solely for the entity identified as the recipient herein ("you"). This document contains proprietary, confidential information of Guy Carpenter and may not be shared with any third party without Guy Carpenter's prior written consent. Any modeling, analytics, or projections is subject to inherent uncertainty, and could be materially affected if any underlying assumptions, conditions, information, or factors are inaccurate or incomplete or should change. The information contained herein is based on sources we believe reliable, but we do not guarantee its accuracy or completeness. Guy Carpenter makes no representations or warranties, express or implied [(including the application of (re)insurance contract wordings or the financial condition or solvency of (re)insurers)]. [Guy Carpenter makes no assurances regarding the availability, cost, or terms of (re)insurance coverage.] [Although Guy Carpenter may provide advice and recommendations, all decisions regarding the amount, type or terms of coverage are the sole responsibility of the (re)insurance purchaser, who must decide on the specific coverage that is appropriate to its particular circumstances and financial position.]

Statements concerning tax, accounting, legal or regulatory matters should be understood to be general observations based solely on our experience as (re)insurance brokers and risk consultants, and may not be relied upon as tax, accounting, legal or regulatory advice, which we are not authorized to provide.

Guy Carpenter undertakes no obligation to update or revise publicly any historical, current or forward-looking statements, whether as a result of new information, research, future events or otherwise.

This document or any portion of the information it contains may not be copied or reproduced in any form without the permission of Guy Carpenter.

The trademarks and service marks contained in this document are the property of their respective owners.

A business of Marsh McLennan