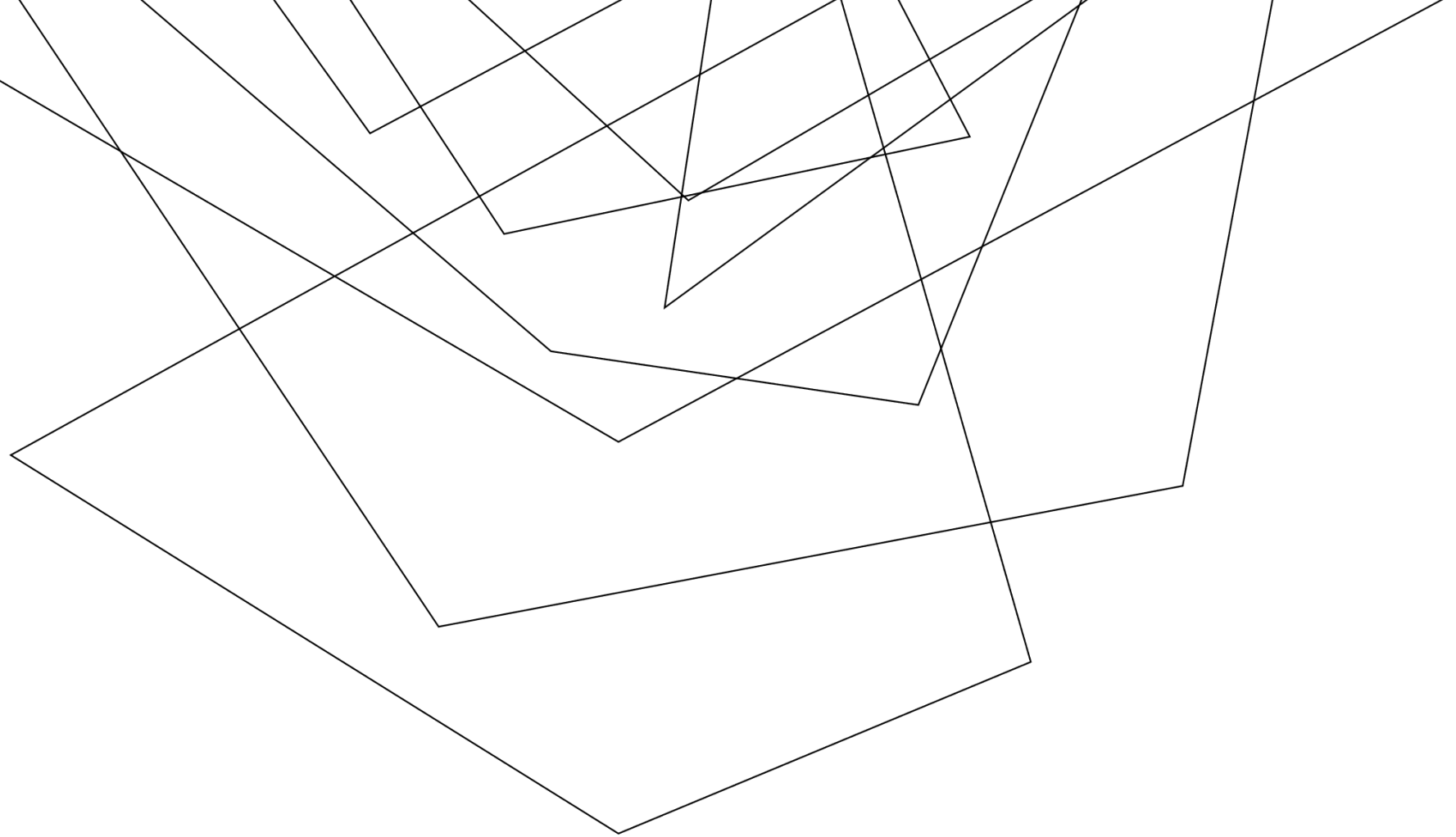


AI INCIDENT RESPONSE:

An Exercise

CROWN

Control

Encryption and access control

Recognize

Monitoring, auditing and detection

Obscure

Fake datasets and network mazes

Withstand

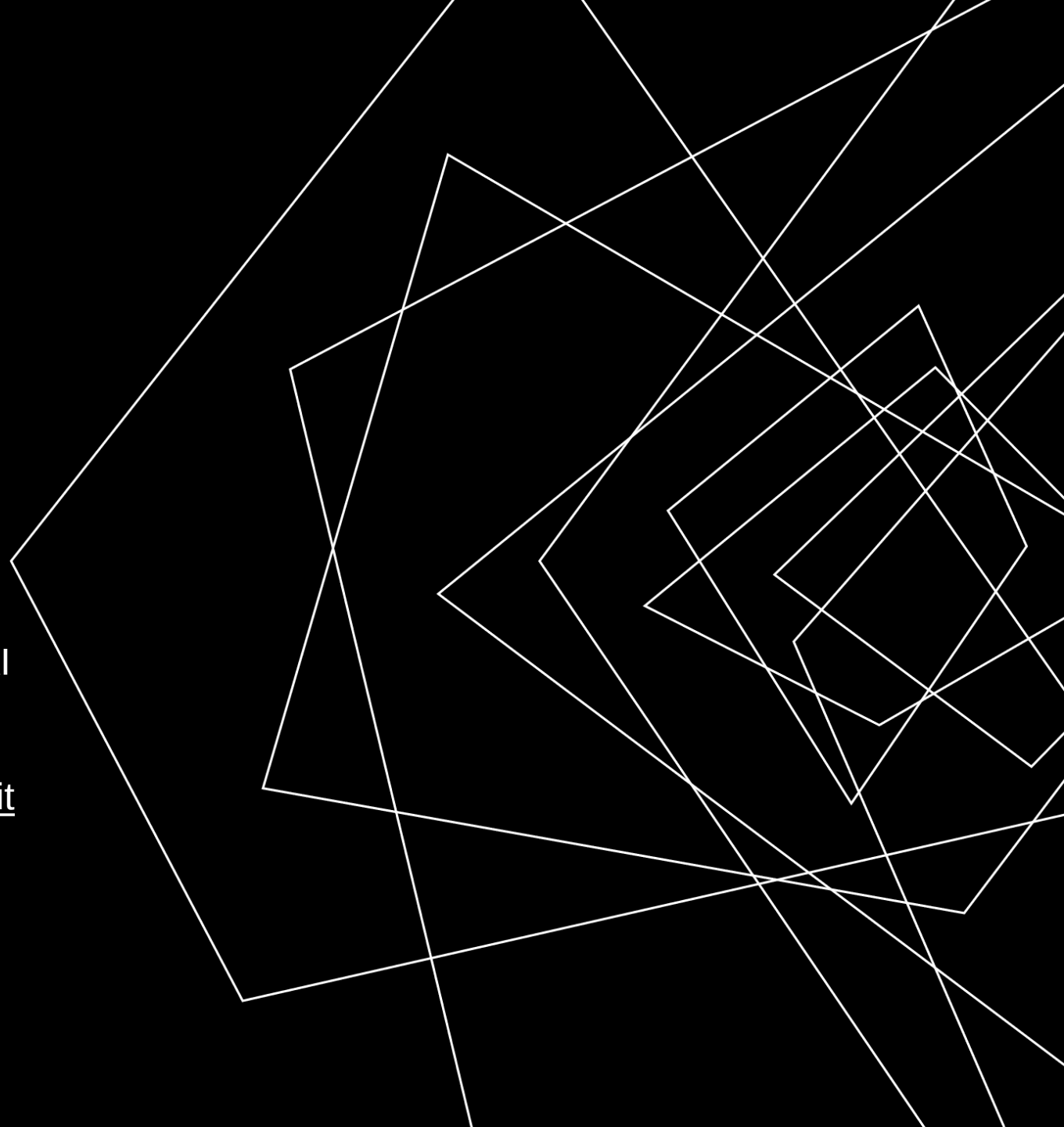
Degradation and redundancy

No BlackBox

Full game visibility

BANK PROFILE

Liongate is a mid-sized regional bank with $5 billion in total assets across 20 branches. Last year, it implemented new AI systems in one city through chatbots and automated fraud detection focusing on illicit transfers.



AI ATTACKS

- Chatbots now giving inaccurate account info to customers

- Fraud models failed to identify suspicious transactions

TENSION IN C-SUITE

C-Suite Roles	Priority	Competing Priority	Strategic Dilemma
Chief Marketing Officer Vs Chief Legal Officer	Customer Trust	Transparency	Proactive communication OR Liability Risk?
Chief Business Officer Vs Chief Information Officer	Restoring Systems Rapidly (Business Continuity)	Modeling New Threats	Immediate fixes OR in-depth reviews?
Chief Compliance Officer Vs Investor Relations Officer	Regulatory Disclosure	Protecting Reputation	Urgent Reporting OR Avoiding Market Overreaction

CONVERSATIONS FROM THE C-SUITE MEETING

CLO: *“It’s necessary to maintain public accountability after this AI incident. We can’t hide problems and must make a public statement ASAP”*

CMO: *“Going public will hurt people’s confidence and our reputation!”*

CBO: “*Restoring our AI systems to full functionality right away is my priority to limit business disruptions. We can refine on the go”*

CIO: *“Reactivating compromised systems before full security reviews invites potential threats we simply haven’t modeled”*

CCO: *“I know we are still investigating, but we have external compliance timelines to disclose an incident initial overview by end of the week”*
IRO: “*We can't share scraps and spook investors before having real damages numbers!*”

TENSION IN C-SUITE

C-Suite Roles	Priority	Competing Priority	Strategic Dilemma
Chief Marketing Officer Vs Chief Legal Officer	Customer Trust	Transparency	Proactive communication OR Liability Risk?
Chief Business Officer Vs Chief Information Officer	Restoring Systems Rapidly (Business Continuity)	Modeling New Threats	Immediate fixes OR in-depth reviews?
Chief Compliance Officer Vs Investor Relations Officer	Regulatory Disclosure	Protecting Reputation	Urgent Reporting OR Avoiding Market Overreaction

CONVERSATIONS FROM THE C-SUITE MEETING

CLO: *"It's necessary to maintain public accountability after this AI incident. We can't hide problems and must make a public statement ASAP"*

CMO: *"Going public will hurt people's confidence and our reputation!"*

CBO: *"Restoring our AI systems to full functionality right away is my priority to limit business disruptions. We can refine on the go"*

CIO: *"Reactivating compromised systems before full security reviews invites potential threats we simply haven't modeled"*

CCO: *"I know we are still investigating, but we have external compliance timelines to disclose an incident initial overview by end of the week"*
IRO: *"We can't share scraps and spook investors before having real damages numbers!"*

POTENTIAL SOLUTION

Transparency vs Reputation

(Phased Announcement)

- Initial public statement satisfies minimal disclosure requirements on incident occurrence/scope

- Follow-up communiqué outlines details and attribution insights

Business Continuity vs Caution

(Tiered Isolation)

- Graceful degradation to secondary (lower risk)models of chatbots

- Immediate rollback of compromised systems and introduction of contingency models

Compliance vs Investors

(Why Not Both?)

- Draft reports to compliance agencies

- Hire experts for guidance with investor relations

THANK YOU

Jamila El-Gizuli

jelgizuli@cyguardconsult.com

www.cyguardconsult.com