CYBER INCIDENT RESPONSE

ONLY THE STRONG SURVIVE

Sean McKee, Sr. Manager, Cyber Resilience, TD Bank Group

CYBER THREAT LANDSCAPE

- Cyber Fraud
- Supply Chain Attacks
- Phishing
- Insider Threats
- Advanced Persistent Threat
- Geopolitical

ATTACKER/DEFENDER ASYMETRY

Attackers	**Defenders**
Cybercrime is a *business*	Battlefield of our own making
True agile methodology	Agile is a marketing term
Patience & skill	Demonstrate ROI
No price for failure	High price for failure
No rules of engagement	Regulated & law abiding
Unlimited funds	Resource challenges

CHALLENGES TO EFFECTIVE CYBER INCIDENT RESPONSE

- Talent Gap
- Attacker/Defender Asymmetry
- Reputational Impacts
- Legal Privilege
- Coordinated Response with Critical 3rd Parties
- Reliance on Common Supplier

PREPARE FOR WHEN, NOT "IF"

- Focus on "cyber resilience"
- Apply Business Lens to response
- Have a Plan: Playbooks & Protocols
- Strategic and Tactical Response

READINESS ASSURANCE

- Exercise & Testing Strategy/Plan
- Technical Security Controls Testing
- Resourcing for Success
- Continuous Improvement

CYBER RANGE EXERCISES

- "Live fire" environment to test & train your geeks
- Exercise with critical third-party vendors
- Real data schema, real processes, real attackers
- Exercise enterprise crisis response
- Off-site & in-person
- Visual & human stressors simulate reality
- Always be learning – nobody must be idle!

FRONT-LINE LESSONS LEARNED

- Cybersecurity is a *business problem*
- Drive "Top Down" Culture of cyber awareness
- *Everyone* is a cyber risk manager
- Commander's Intent enables freedom of action
- Comms procedures with 3rd parties are essential
- Exercising is $$$ well spent – ignore it at your peril