Phenomenati

Global Cyber Security Landscape

for Mass Tech Networking audience
20 May 2021

Scott Foote, Phenomenati Consulting

Cyber Threat Landscape

Actors

Violation of…

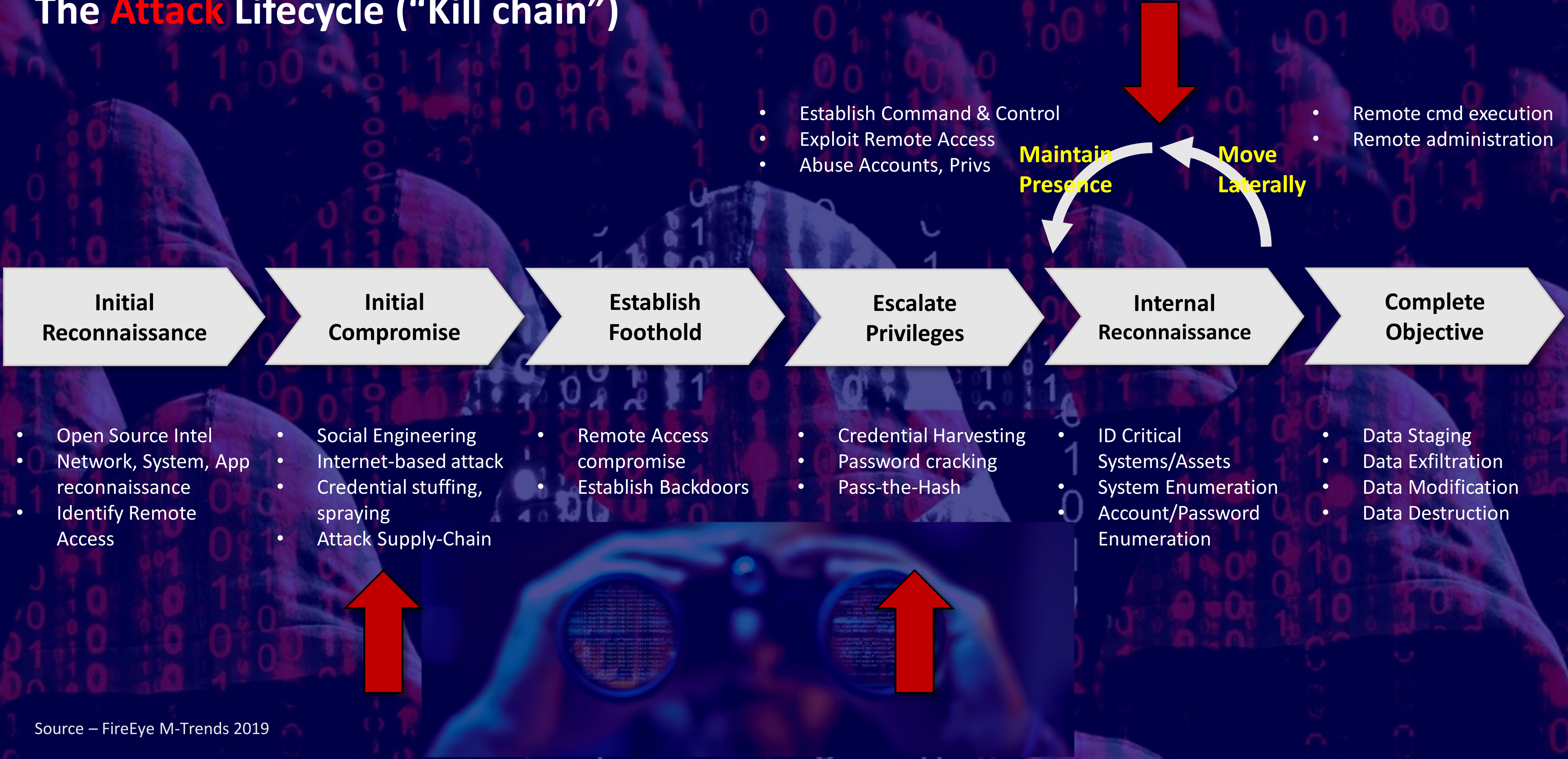
	Hacktivists, Politically Motivated	Criminals	Nation State Actors
Integrity	e.g., Defacement e.g., Social Sentiment e.g., Deep Fakes	e.g., Domain Squatting e.g., Malware distribution e.g., Exec Impersonation e.g., Disinformation	e.g., Information Operations e.g., Supply Chain Compromise
Availability	e.g., DDoS	e.g., DDoS e.g., Ransomware	e.g., Destabilize Critical Infrastructure
Confidentiality	e.g., Doxing	e.g., Fraud e.g., IP Theft e.g., Extortion	e.g., Espionage e.g., Surveillance e.g., *Regulation*

Cyber Vulnerability Landscape

		Seriousness		
		Low	Medium	High
Targets	People	e.g., Ignorance e.g., Weak SFA (password) e.g., Bias toward being Helpful	e.g., Negligence, Misdelivery e.g., Blind Trust e.g., Naïve Arrogance	e.g., Ignore Obligations (Legal) e.g., Malicious Insider
	Processes	e.g., Poorly Defined (Bus & IT) e.g., Asset & Config Mngmnt	e.g., Defined, but no Controls e.g., Help Desk	e.g., Short Cuts, circumvent Controls
	Technology	e.g., Rush-to-Market e.g., Cost Pressures e.g., Weak Security Testing	e.g., Rush-to-Adopt e.g., Poorly Deployed e.g., No Risk Assessment (e.g., web app, email svr, desktop, phones/tablets, IOT)	e.g., Complexity Obfuscates Dependencies e.g., Lack of "Impact Analysis“ (e.g., RDP/VNC)

Phenomenati

The Attack Lifecycle (“Kill chain”)



- Establish Command & Control
- Exploit Remote Access
- Abuse Accounts, Privs

Maintain Presence

Move Laterally

- Remote cmd execution
- Remote administration

Initial Reconnaissance

- Open Source Intel
- Network, System, App reconnaissance
- Identify Remote Access

Initial Compromise

- Social Engineering
- Internet-based attack
- Credential stuffing, spraying
- Attack Supply-Chain

Establish Foothold

- Remote Access compromise
- Establish Backdoors

Escalate Privileges

- Credential Harvesting
- Password cracking
- Pass-the-Hash

Internal Reconnaissance

- ID Critical Systems/Assets
- System Enumeration
- Account/Password Enumeration

Complete Objective

- Data Staging
- Data Exfiltration
- Data Modification
- Data Destruction

Source – FireEye M-Trends 2019

Cyber Consequence Landscape

- Increased **Scrutiny**
  - By **Clients**, increasing Cost of Sales
  - By **Insurance** Companies, increasing Cost of Policies, reducing Coverage

- **Confidentiality**
  - **Privacy** Regulations are creating new incentives for Criminal Actors, thru new Consequen
    - Extortion or (*and*) Regulatory **Fines** continue to grow (www.enforcementtracker.com)
    - *Too many Data Breach notifications to list…*
  - Intellectual Property **Theft**, Espionage
    - 2020 – U.S. deported many foreign nationals and charged U.S. researchers suspected of "Academic Espionage"
    - 2020 – Heavily targeted market sector of "**Professional Services**" (e.g., Law Firms); threat actors seek to exploit their trusted advisor role
  - Average **Cost** of a Data Breach in 2020
    - **$3.86M** (globally), **$8.64M** (US only)… ref. IBM/Ponemon Institute's annual Data Breach Report
- **Availability**
  - **Ransomware** is accelerating; targeting the most vulnerable markets (e.g., Healthcare, Energy, Utilities, Law Firms)
    - 5/14/21 – Attack on **Irish Health Service Executive** (HSE), major disruption in services
    - 5/7/21 – DarkSide attacks **Colonial Pipeline** *back office systems*, $5M ransom payment, claims economic consequences were "unintended"
  - **DDoS** is (surprisingly) still on the rise; leveraging IOT (Mirai), new volumetric records regularly (~2.3 Tbps, and climbing)
    - 5/4/21 – Attack on Belgian ISP **Belnet**, impacted 100s of government, parliament, universities and research institutes.
  - **Cost** of a Ransomware attack in 2020
    - **$847,344/$312,493** (average demand/paid), **$30M/$10M** (maximum reported demand/paid)… ref. Palo Alto Networks latest Threat Report
- **Integrity**
  - Exploiting **Trust** in information sources (propaganda), partners, providers, supply chain, etc.
    - 3/2/21 – Hafnium (Chinese actor) attacks **MS Exchange** using several zero day vulnerabilities; aiming to establish massive surveillance capability
    - 2/8/21 – Attack on **Water Dept** of the City of Oldsmar, Florida… Attempt to raise the level of lye additive (sodium hydroxide) 100x.
    - 12/13/20 – FireEye discovers malware (Russian actor) within **Solarwinds** Orion update, led to 10,000s of compromised gov't & commercial organizations
    - 2015 – Present – Russian SVR backed **disinformation campaigns** targeting both major US political parties, aiming to discredit democracy
  - **Cost** of an Integrity attack in 2020
    - Order of $x Millions to primary comprised organizations (e.g., Solarwinds estimating $18M and climbing)
    - Order of $x00,000 to secondary compromised organizations (to identify and remediate breached systems)
    - Too many variables and Nth Order impacts to estimate accurately

Phenomenati

Cyber Security Controls Landscape

Stage of Compromise

Control Type

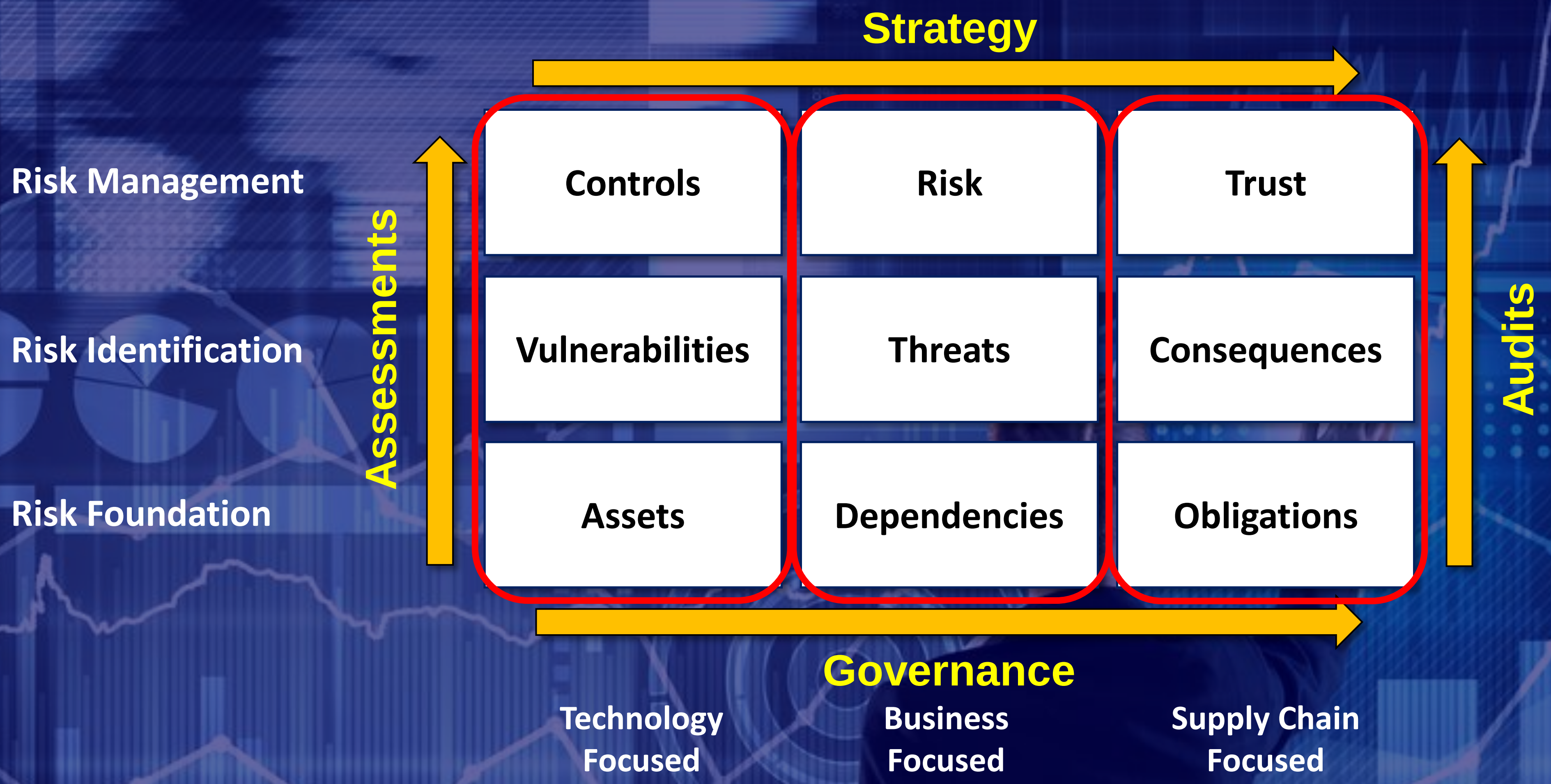
	Preventative	Detective	Corrective
Technical	e.g., Authentication e.g., Authorization e.g., FWs, Gateways, Proxies e.g., Data Loss Prevention	e.g., Audit Trails (logs) e.g., Detection Analytics e.g., Honeypots/nets e.g., Canaries (“DRM”)	e.g., Traffic Redirect e.g., Account Lock e.g., Software/System Quarantine e.g., System Restore
Administrative	e.g., Policies & Procedures e.g., NDAs, Security Training e.g., Patch Management e.g., Principle of Least Privs	e.g., Auditing / Threat Hunting e.g., Separation of Duties e.g., Job Rotation e.g., Risk ID & Assessment	e.g., Disaster Recovery Plan e.g., Business Continuity Plan e.g., Cyber Insurance
Physical	e.g., Guards, Gates, Badges e.g., Locks, Secure Areas e.g., Encryption	e.g., Audio/Video Surveillance e.g., RFID, GPS e.g., Heat Sensors	e.g., Fire Suppression e.g., Redundant Systems/Site e.g., Restore from Backup

Phenomenati

Basic Information Security Investments

	Stage of Compromise		
Control Type	Preventative	Detective	Corrective
Technical	e.g., Multi-Factor Authentication e.g., Use VMs, sandboxes e.g., + Russian lang support	e.g., EDR software e.g., Use Canary tokens	e.g., MDR service
Administrative	e.g., Policies & Procedures e.g., Security Training e.g., Patch Management	e.g., Separate Admin account e.g., Darkweb scans	e.g., Cyber Insurance
Physical	e.g., Badges e.g., Secure Areas e.g., Encryption	e.g., Video Surveillance	e.g., Restore from Offline Backup

A *Comprehensive* Information Security & Privacy Program



Strategy

Assessments

Audits

Governance

	Technology Focused	Business Focused	Supply Chain Focused
Risk Management	Controls	Risk	Trust
Risk Identification	Vulnerabilities	Threats	Consequences
Risk Foundation	Assets	Dependencies	Obligations

Questions?

Contact Info:

scott@phenomenati.com