City of Houston Cyber Threat Landscape

STATE, LOCAL, TRIBAL AND TERRITORIAL (SLTT) GOVERNMENT OUTLOOK

- Risks will continue to expand beyond traditional network boundaries, with apps, the Internet of Things (IOT), social media, smart cities, cloud computing, mobile devices, point of sale (PoS) systems, supply chains, and third parties playing an increasingly large role in cyber events
- Sophistication of malware, cyber threat actors, and tactics, techniques, and procedures (TTPs) will continue to increase
- Financial gain will remain the most prevalent cybercrime motivation
- Attacks will continue to be opportunistic in nature
- Greater recognition of SLTT governments' role in the nation's cybersecurity efforts

Source: MS-ISAC

BACKGROUND AND MAGNITUDE OF THE COH CYBER CHALLENGE

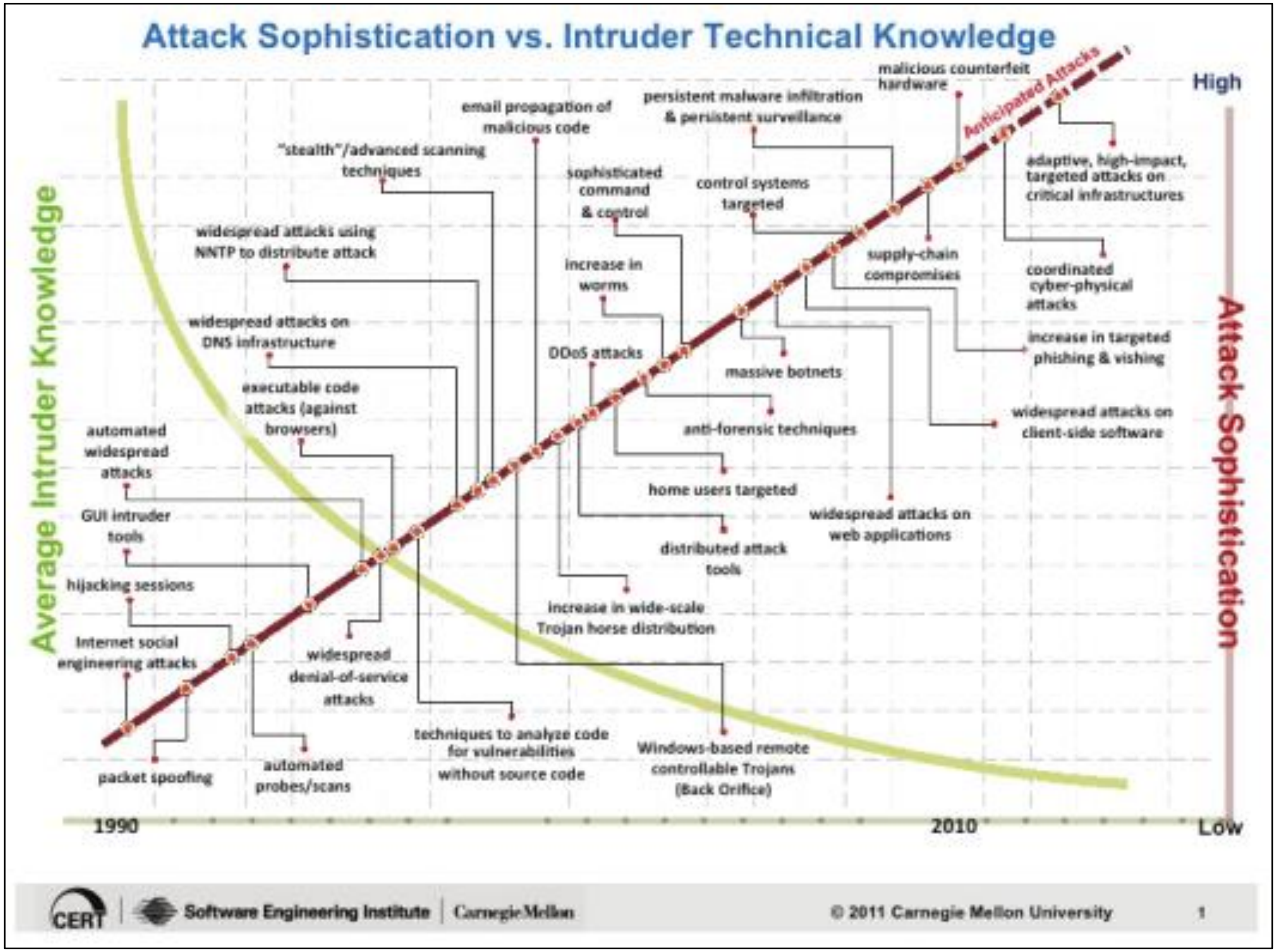
Nation States/Cyber Terrorists

Cyber/Organized Criminals

Hacktivist Groups

Insiders

ATTACK SOPHISTICATION vs. INTRUDER TECHNICAL KNOWLEDGE



Source: Carnegie Mellon

ESTABLISHING REALITY: TARGETING @ CITY OF HOUSTON

Entity	Motivators	Threat Description/Vectors	Impact	Potential COH Impact
Nation States/Cyber Terrorists	▪ National Security ▪ Global Competition ▪ Fraud ▪ Ideology ▪ Political ▪ Disenfranchised ▪ Malicious havoc	▪ Targeted, long-term cyber campaigns with a strategic focus ▪ Third-party service providers ▪ Insiders ▪ Opportunistic vulnerabilities	▪ Loss of intellectual property ▪ Disruption to critical infrastructure ▪ Monetary loss ▪ Destabilize, disrupt and destroy assets	***ALL***
Cyber/Organized Criminals	▪ Illicit Profit ▪ Identity Theft ▪ Fraud	▪ Individual identity theft ▪ Data breaches and intellectual property theft ▪ Ransomware ▪ Insiders ▪ Third-party service providers	▪ Loss of identity ▪ Monetary loss ▪ Intellectual property loss/access ▪ Privacy	***FIN, HHD, CTR, ARA, HR, HPL, LGL, MCD, HPD, HFD***
Hacktivist Groups	▪ Political cause rather than personal gain ▪ Ideology	▪ Target organizations that stand in the way of their cause ▪ Insiders ▪ Third-party service providers	▪ Disruption to operations ▪ Destabilization ▪ Embarrassment ▪ Public relations ▪ Regulatory	***HPD, MYR, IT, LGL, MCD, HHD, HAS***
Insiders	▪ Seeks validation ▪ Strong sense of entitlement ▪ Financial gain	▪ Trusted employees ▪ Vendors ▪ Contractors ▪ Interns ▪ Third-party service providers	▪ Loss or compromise of controlled or sensitive information ▪ Monetary loss ▪ Loss of identity ▪ System/equipment sabotage	***ALL***

COH CYBERSECURITY MASTER PLAN RECAP

- Intelligence driven plan executed over four years
- Provides a roadmap to improve the COH cybersecurity posture and reduce the organizational risk footprint; each year of the plan has a focused theme
- Highlights the implementation of viable administrative, technical and operational controls designed around people, processes and technology
- Control selections are targeted at preventing, detecting and responding to attacks from nation states/cyber terrorists, cyber organized criminals, hacktivist groups and insiders
- Projects and activities map back to the National Institute of Standards and Technology (NIST) Cybersecurity Framework

THE HARD TRUTH: RECALIBRATING THE DEFINITION OF WINNING

- Compromise is inevitable
- Adversaries compromise us on their terms, not ours
- Adversaries want our data and some want significant system control
- Adversaries routinely attempt to recompromise organizations they have previously compromised
- Offensive cyber will remain dominant as adversaries find the one flaw overlooked, unknown or unpatched – defenders have to consider/protect everything