



# The Cyber Threat

Bob Gourley, Partner, Cognition  
June 22, 2016

# About This Presentation

- Based on decades of experience in cyber conflict
- Including cyber defense, cyber intelligence, cyber attack and analysis
- Informed by understanding of the complexities of technology and the critical nuances of policy and process in our system
- Validated by what works in defense across multiple sectors of the economy.
- Salient lessons fit on one slide

That One Slide Follows

# Know The Threat To Beat The Threat

## The Threat

A great deal is known about who is attacking and what their motivations are. By studying them we can build better defenses before attack and respond smarter during attack. Get the right info for strategic, operational and tactical decisions.

### Adversaries Are:

**Nations Crime Groups Extremists Hackers Insiders**

Successful Attacks Are By Organizations

## Unique Tech Factors

Aircraft, cars, roads, trains, ships and organizations increasingly interconnected. But cyberspace is hard to observe and security hard to access. Well instrumented systems overseen by trained/experienced people are key to defense.

### Tools To Consider:

**Encryption ID Management 2FA Automated Patching**

Ensure Tech is Independently Assessed

## The Situation

Every sector of the economy and every government and every citizen is under almost constant attack. Most suffer ongoing infections with malware. Attackers get in fast and remain undetected for months. But risk can be reduced/mitigated.

### Top Lessons Are:

**Attackers are persistent, we must prepare for breach**

Defenders Should Collaborate on Lessons

## Your Action

Lead with understanding that cybersecurity is not just an IT function. Must have your personal leadership and engagement by your entire team. Ensure external verification and validation of your strategy, policy, process and tech.

### Top Actions:

**Engage with ISACs, Collaborate with Peers, Study Threats**

Victory Must Be Earned

# The Details

# About Cognito

## We Do Three Things

Cognito is a strategic consulting and engineering firm led by a team of former senior technology executives from the U.S. Intelligence Community.

We have a track record of safeguarding some of the nation's greatest secrets, equipping U.S. leadership with actionable intelligence that helps protect lives and driving technology innovation that kept key government agencies generations ahead.

Cognito leverages that vast knowledge to enable companies across disparate industries to effectively manage technology, maximize technology investments, and reduce overall institutional risk.



We provide cyber assessment, awareness, remediation and containment strategies. Our process, the Cyber360, includes best practices from government and industry.



Continued innovation is required for market success. Innovation requires well thought out action plans informed by knowledge of both legacy and new technologies.



We know the "so-what" of data, it is there to enhance your ability to achieve your business objectives. And we know the infrastructure and applications required to let you take advantage of your data.

Reach Us On Pre-Competed GWAC Vehicle

# Defense Lessons From All Industries

- Everyone is under continuous attack
- Most organizations have ongoing infections with malware
- Converged/blended attacks the norm
- Attackers get in fast, but remain undetected for months
- Awareness of threat is seen as helpful, it helps people understand what to do and who to notify of anomalous activity

Transportation Sector Can Learn From Other Sectors

# Hot Topics From The Daily Threat Brief

- Cyber attacks against transportation sector are growing and dangerous (but attacks against healthcare sector growing faster)
- Ransomware evolving/becoming harder to prevent/beat
- Most visible/attention getting demonstration is the 2015 Charlie Miller/Chris Valasek demonstrations. But vulnerabilities in many vehicles and infrastructure systems
- For organizations, Phishing remains dominant path in... exploits human traits of compassion and curiosity.
- IoT is coming to transportation sector. Awareness of IoT vulnerabilities becoming more widespread, but little indication of security solutions
- Mobile device vulnerabilities: exploited to gain account info

All Indications Are Attacks Will Continue

# The Condensed History of the Cyber Threat



- Civil War: Both sides attacked, exploited, hacked
- 1998 Moonlight Maze: It takes a nation to fight a nation
- 2007 Estonia: Be ready to weather a storm
- 2008 Georgia: Expect cyber attacks timed to military ops
- 2008 Turkey Pipeline: Large cyber to physical attack
- 2009 GhostNet: When a powerful adversary wants in nothing will stop them. Collaborative cyber intel can inform response
- 2011 Wikileaks: Know the human element. Know balance between info sharing and protection
- 2013 Mandiant Report: Cyber intel is strategic
- 2013 Snowden Leaks: Know the threat before it strikes
- 2013/14 Banks and Retail: Nothing stops this adversary
- 2015 Warsaw's Chopin Airport DDoS: Transportation is a target
- 2015 Healthcare and Governments: No sector immune
- 2015 Cars and Embedded IT: Threat actors will find a way
- 2016: Ukraine power grid: Infrastructure a target



# Who is Attacking?

- Successful attacks are conducted by organizations
- Organizations are groups of people acting together for a common purpose
- By studying those organizations and how they behave and what they want we can help deter their actions and mitigate some of their capabilities
- When under attack we can better defend
- When penetrated we can more quickly respond

The four categories of organizations: Nations, Criminals, Extremists, Hactivists




# The Special Case of the Insider

- The term “Insider Threat” has a special use in the security community. Can be a person you trust who you have given credentials to your most sensitive networks and accounts.
- Can be good one day then change intent the next
- Could be operating as an extension of one of the organizational categories described above
- Cannot be stopped by technology alone (but technology can help).
- Requires policies, process and a highly functioning team of good people to catch the bad ones

# The Threat Actors

 <b>ACTOR</b>	<b>MOTIVE</b>	<b>TARGETS</b>
Nation States	Economic or Military	IP or Infrastructure
Organized Crime	Financial Gain	IP, Banks, PoS
Terrorists / Extremists	Cause Support	Highly Visible Targets
Hackers / Hacktivists	Publicity, Watch it burn	Anything and Everything
Trusted Insiders	Revenge, Financial Gain	Your Data and/or Networks

# Attack Patterns

 <b>METHOD</b>	 <b>SUMMARY</b>	 <b>LESSONS</b>
<b>Espionage Methods</b>	Human-guided use of tools to find and extract information	Prioritize, classify, and protect data
<b>Web Application Attacks</b>	Breaking into web sites or applications	Don't host web sites on your network; use robust DMZs
<b>Malicious Code</b>	Viruses, worms, etc	Automatic detection and remediation
<b>Exploit poor configuration</b>	Take advantage of bad design	Understand your applications - alter default configurations
<b>PoS Attacks</b>	Financial transactions are always vulnerable	Ensure access to tactical threat intelligence; Red Teams

# Bad Actors and Their Code

- Modern malware is designed to stay under the radar
  - Old anti-virus solutions do not work against new threats
  - Malware hops between media
  - Slow, hard to observe communications
  - Sandboxing, honeypots/nets not the entire solution
- Even sophisticated adversaries and modern malware can be detected
  - No adversary can be invisible
  - Well trained incident response teams find them
  - However, non-automated methods are overwhelmed and cannot scale
- Automation is key, including automating cyber intelligence

Foundational Work Has Been Done Enabling Automation

# What Can We Do About It?

- **Assess and Understand:** Know what data, systems and capabilities are most important to the function of your organization, and maintain continuous automated awareness of their status.
- **Enhance Defenses (but prepare for breach):** The adversary in cyberspace is continuing to innovate, which means we must continue to review our defenses and modernize. Even with this continual defense, history proves that the adversaries eventually get in.
- **Design for Containment:** Early detection and rapid incident response will be aided if systems are designed to contain adversaries. Containment of attacks is especially important in malicious code.
- **Ensure Backup:** Every critical system must have a backup, and recovery methods must be defined and tested.

# What Can We Do About It?

- **Coordinate Early:** Work with those that are critical to responding to attack. For example, the FBI, the US CERT, and the appropriate ISAC (Surface Transportation ISAC, Aviation ISAC, Public Transportation ISAC, Multi-State ISAC). Build bonds of trust before an incident.
- **Leverage Experience of Others:** No transportation organization can match the technical talent of the modern cyber criminal or nation. This requires seasoned professionals who constantly focus on learning threat tactics and mitigation strategies.
- **Automate Defenses and Enhance Monitoring:** Here too external help is almost always the right path forward. Find the a team that provides analysis of anomalies in your network in ways that give the best of both automation and experience professionals (Gartner calls this Managed Detection and Response or MDR).

# Review

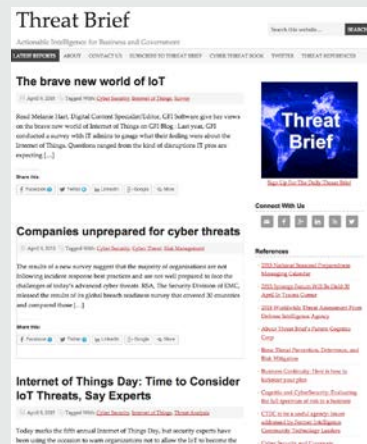
- Every citizen you serve, every company you work with or support, every supplier you have, and every other member of the transportation sector, are all facing the same threat
- Adversaries have objectives they are going to fight to achieve
- History has shown they will never stop
- History also shows the bad guys will always get in, eventually
- A well-instrumented enterprise with well engineered automation and experienced external help can detect and mitigate adversary actions

Which Leads To Our Concluding Recommendations



# Concluding Recommendations

Continually Learn!  
Know and Improve Your Policies!  
Communicate!



[ThreatBrief.com](http://ThreatBrief.com)

[TheCyberThreat.com](http://TheCyberThreat.com)

[Bob.gourley@cognitiocorp.com](mailto:Bob.gourley@cognitiocorp.com)



Bob Gourley

[bob.gourley@cognitiocorp.com](mailto:bob.gourley@cognitiocorp.com)