Cyber Threat Intelligence Sharing: Lessons Learned, Observations, Recommendations

Bob Gourley, Partner, Cognitio
September 9, 2015

How we think.

Disclaimer

There is a great deal of text on these slides. Don't try to read them now, I'll verbally summarize and will email you a copy to read slowly later.

About This Presentation

- Cyber Threat Intelligence is information on the adversary (capabilities, intentions, ongoing action) of use to enterprise defense.
- Goal is to mitigate risks by knowing your adversary, their intent and even their next move.
- This session provides lessons in cyber threat intelligence from across government and industry in ways designed to help inform your approach to cyber threat intelligence

Foreshadowing

- There is cyber threat intelligence in both industry and government. If parties on both sides could increase their sharing it would be good for collective defense. Understanding the issues each face and some key perceptions may help enhance this sharing.
  - There is info in government of value to enterprises, but when information is provided it is usually provided too late or is not of value.
  - There are some cases where information is shared to those with clearances and that has been called very valuable by some CISOs.
- There is information in industry that can help government better defend itself and help government help industry.
- A frequently overlooked challenge to info sharing is culture.

Table of Contents

Methodologies

Know Cyber Intel

- Know the threat
- Know technology
- Know defensive concepts
- Know standards
- Know cultures of who is involved

Know The Law and Gov Policy and Regulations

- Includes SOX, GLBA, SEC and FINRA guidance, HIPAA and many others (see business.usa.gov)
- Global privacy regulations

Know What Info Is Available In Gov and Industry

- What might gov have that industry would want?
- What might industry have that gov might want?

Draft Assessments and Lessons Learned

- Generate assessments, conclusions and recommendations
- Check assumptions by asking trusted CISOs with government and industry experience to review conclusions and comment

Conclusions

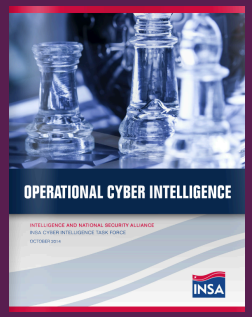
- Seek to produce conclusions that can help people get things done
- Look for new insights vice just revamping old conclusions and assessments
- Keep iterating to ensure conclusions of value to real decision-makers

I discussed conclusions with many, but blame me for any faults here… and let me know what you think.

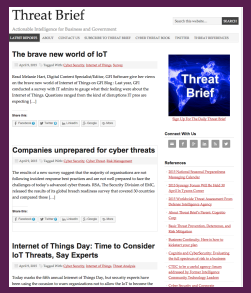
This presentation was reviewed by over 150 security executives in industry, government and academia.

More On Our Bias and Background

- TheCyberThreat.com
  - Lessons from history and current ops
  - Insights from companies under attack
  - Ways to Enhance Cyber Intelligence Support



- Insaonline.org
  - Products resulting from government-industry partnership study of cyber intelligence issues
  - Best practices and lessons learned from the IC



- ThreatBrief.com
  - Free daily report on cyber threat actors and their strategic actions and impact

Security Officers/CISOs We Spoke With

- We spoke with security executives In several industries
  - Finance
  - Retail
  - Food and Beverage
  - Automotive
  - State/Local/Federal Government

  Note: we did not speak with and large DIB members on this, they may well have different views if they get classified info.

- We asked the readership of ThreatBrief.com to provide inputs on lessons learned and observations on the current state of cyber intelligence information sharing

Results Follow

The Rise Of Cyber Intelligence

- Legacy firms are enhancing their cyber intel practices and offerings
- New startups are attracting significant investments
- Data feeds of threat intelligence are growing and hard to track (see ThreatIntelligenceReview.com)
- Most firms now leveraging managed security service providers in some capacity, providing new ways to make intel actionable.
- Secure collaboration spaces and managed service providers are very hot topics

Now For The Meat

- The slides that follow capture relevant lessons and recommendations for
  - Industry
  - Government
  - Academia

Observations For Government

- Many in industry see value in cyber threat intel from gov. But many others view it as not relevant. Many view sharing with government as a one way street.
  - Many big company security professionals have doubts that the situation will ever improve.
- Some government info is helpful to industry, but there is nothing government had that could have prevented attacks on Sony, Home Depot, JP Morgan, Anthem etc…
- Many companies (especially mid-sized ones) find information from law enforcement (FBI and Secret Service) useful.
- The commercial trend towards managed security services is one to watch and leverage.
- There are many legal and contractual reasons why industry cannot share some key cyber threat intel information.

Recommendations For Government

- It may be sub-optimal to spend too much energy to try to enhance info sharing, so focus on what is important (see comment below on speed). Share what you are best at, like standards, methods, models, experiences. And hold more events like this one.
- Understand that info has a time value. If sent too late it will have zero impact on defense. If you find ways to speed info release, that might help you help industry.
- Understand that industry is prevented from sharing some cyber threat info due to law, regulations and contractual issues. Be empathetic.
- Consider how you can leverage commercial managed service providers and commercial threat intel feeds. This will enhance your cyber intelligence capabilities.
- When industry shares information with government that must be well protected. Loss of data in a breach will hurt trust and hurt future information sharing efforts.
- Continue your support and encouragement for ISACs. Support ISACs for the good they do the nation.

Observations For Industry

- The government is larger than you realize. No single agency, department or branch speaks for entire government.
- For many in industry best source of gov cyber threat intel is NCICC and their US CERT (us-cert.gov)
- Greatest sources of actionable information for business are groups like the ISACs, commercial cyber intelligence firms and managed security service providers. Informal Info sharing between industry is also important. Spend more time on this than you spend seeking info from gov.
- Cyber information shared by the FBI and Secret Service can be helpful to small to mid-sized businesses.
- There are risks to sharing info with government. If done wrong you can violate law, industry regulations and your contracts with others. There are also risks to your business that you need to mitigate.

Recommendations For Industry

- Since you cannot expect any one office to speak for the entire government on issues of information sharing you need to know the facts about who you are working with and how they work with others.

- If you had to pick just one organization in government to share with, pick the US CERT. But it is also advisable to establish relationships with either the FBI or Secret Service. When you get breached you will wish you knew your local agents by first name.

- Since there are risks to sharing information with government, engage your CRO and GC in your information sharing strategy. If they are not involved you may be putting yourself in danger of violating law, government regulations, or contracts, even if you are sharing with good intentions. You may also be putting your firm at risk.

- If you are not involved in your sector ISAC engage with them now. Also critical to build trust-based relationships with your peers for informal sharing. Find the right managed services provider for your firm.

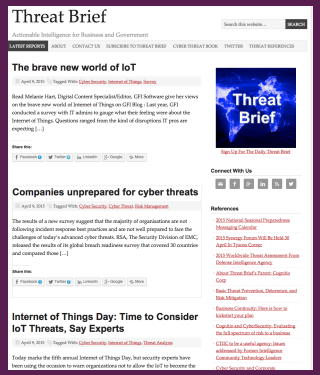
For Academia

- Observations:
  - The nation would benefit from more education and training around cyber intelligence. Large companies need a workforce educated in cyber intelligence methodologies and trained in technologies that make up the modern enterprise. Government needs this too.
  - Work by INSA is a huge start in outlining what is needed for a cyber intelligence curriculum.

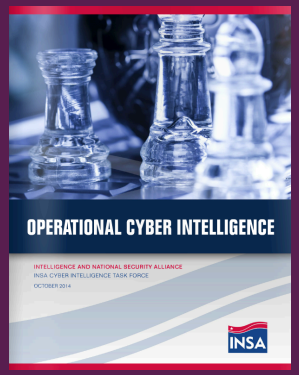
- Recommendations:
  - Cyber intelligence is a multi-disciplinary activity, and education/training in that should be as well.
  - Engage with INSA to accelerate development of cyber intelligence curriculum development
  - This field gets technical quick. Ensure you are teaching details of policy, technology and information sharing standards

Concluding Recommendation

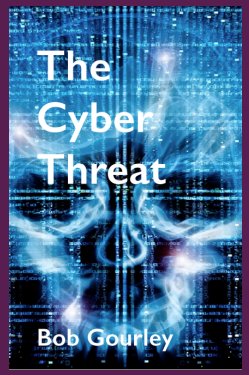
Knowing The Threat Will Help You Share Intelligence On The Threat and Will Help You Craft The Best Intelligence Sharing Programs, So, Never Stop Studying The Threat



ThreatBrief.com



Insaonline.org



TheCyberThreat.com

Contact Us

Bob Gourley **bob.gourley@cognitiocorp.com**

Twitter: @bobgourley
Twitter: @CognitioCorp
On-line: ThreatBrief.com
On-line: CTOVision.com

Cognitio Corp
1750 Tysons Blvd, Ste 1500
McLean, VA 22102
(703)738-0068

How we think.