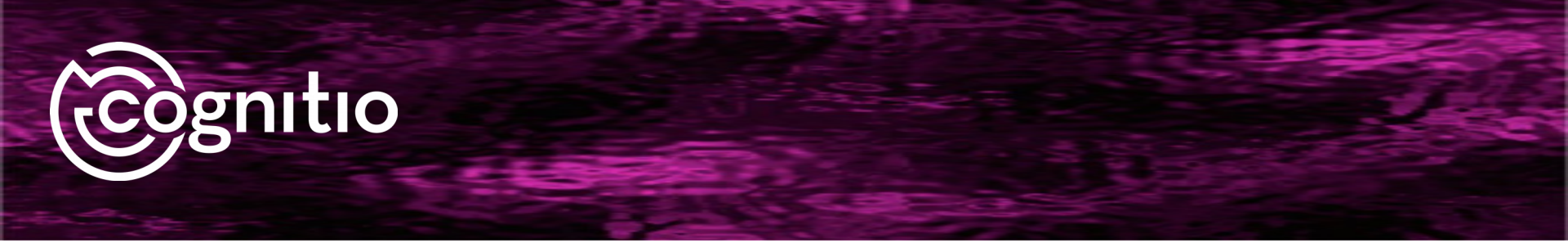
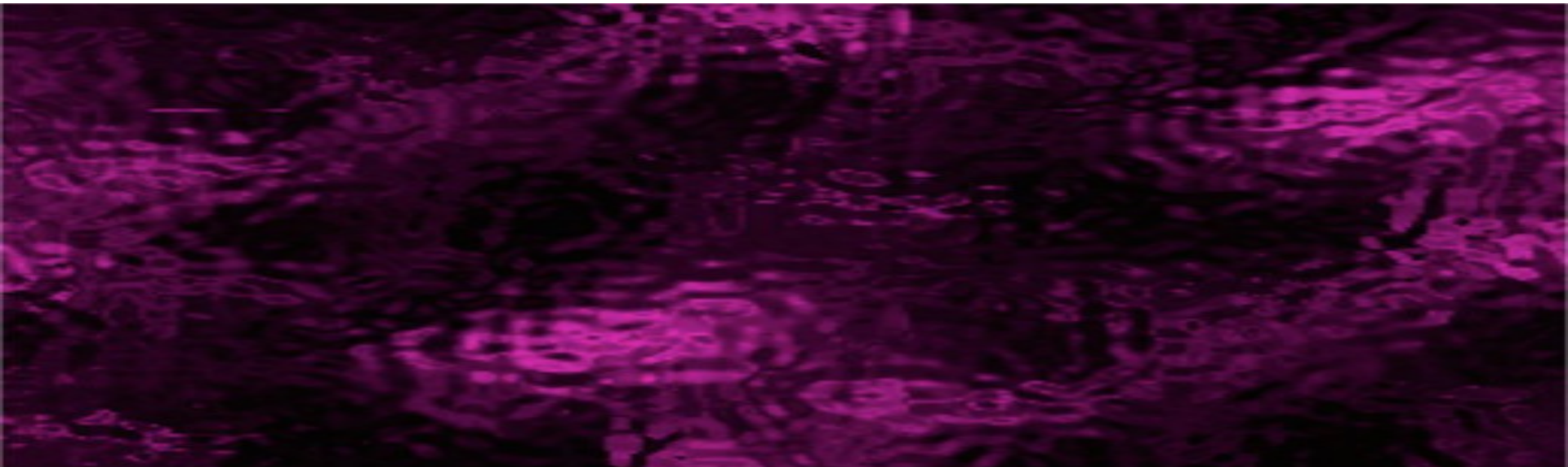


Cyber Threats

Insights from history and current operations

May 5, 2015



About Cognitio

Cognitio 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.

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

We Do Three Things

Cyber Security

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

Innovation

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

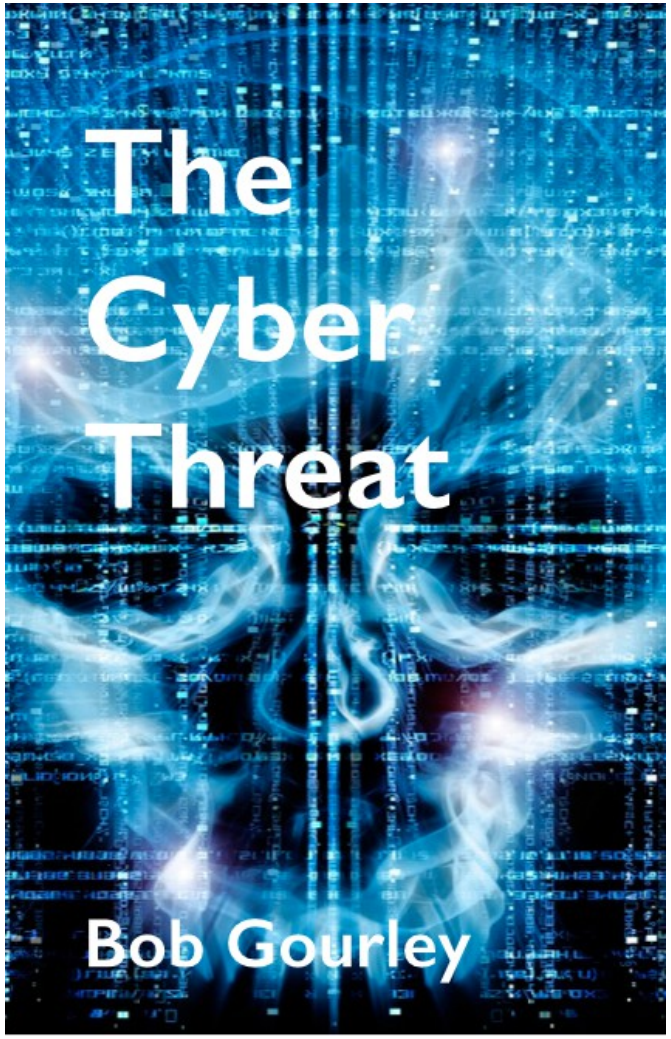
Data/Analytics

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.

Purpose of this Brief

- Provide facts and observations on the cyber threat in ways that can inform your decision-making
- Discuss best practices in the domain of cyber intelligence
- Provide recommendations that help enhance our collective defense
- Share and discuss ways of expressing the threat you may find useful in your own threat briefings

About The Cyber Threat Book



Lessons from history and current ops

Insights from companies under attack

Ways to Enhance Cyber Intelligence Support

- Strategic levels
- Operational levels
- Tactical levels

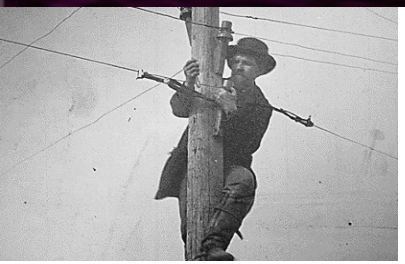
TheCyberThreat.com

Lets Start With The Conclusion

Action	Description
Assess	Conduct assessment of cyber intelligence activities & prioritize improvement plans
Get Informed	The more you know about the threat the more you can educate others the better. Sign up for the daily Threat Brief at ThreatBrief.com
Threat Briefs	Ensure executives on the team understand cyber threat to their business objectives
Understand Yourself	Know what data, systems, capabilities are most important to protect. Use access control.
Automate	Few organizations have automated their ability to analyze operational and tactical threat indicators. Fewer have automated their ability to respond. Automate your IT management and access control as well.
Collaborate	No single organization can defend against all attackers. Sophisticated attacks require collaboration.
Network	Find your peers and build a community before you need it and seek inputs on how they leverage cyber intelligence in their organization (CSA, SINET, FBI, ISACs, SANS, AFCEA, INSA, FedCyber.com, ThreatBrief.com)
Prepare for breach	Plan for how you would respond to the worst case scenario and exercise your responses.
Love your people	Consider assigning an insider threat manager to lead your insider mitigation program and remember it is not about tech here, it is about people and processes. And if you love and lead your good people they will help find the bad people.

We will return to this slide after a review of the cyber threat

The Condensed History of the Cyber Threat



- **Civil War:** Both sides attacked, exploited, passed false orders.
- **1986 Hanover Hacker:** Shows collaboration is critical
- **1988 Morris Worm:** Plan for collaboration before you need it
- **1997 Solar Sunrise:** Plan cyber intelligence data flow in advance
- **1998 Moonlight Maze:** It takes a nation to fight a nation
- **2006-11 Shady Rat:** Big organizations can attack large target sets, Collaborative intelligence work by good guys can save the day
- **2007 Estonia:** Be ready to weather a storm
- **2008 Georgia:** Expect cyber attacks timed to military ops
- **2008 Turkey Pipeline Explosion:** Largest known cyber to physical attack
- **2009 GhostNet:** When a powerful adversary wants in nothing will stop them. Collaborative cyber intelligence can inform response
- **2011 Wikileaks:** Know the human element. Know balance between info sharing and protection
- **2013 Mandiant Report Released:** Cyber intelligence can make a strategic difference
- **2013 Snowden Leaks:** Know the threat before it strikes
- **2013 NYT:** Just because someone should know doesn't mean they do
- **2013/14 Banks and Retail:** Nothing stops a persistent adversary

The State of the Hack

- 2014 Forensics study of 1,000 organizations reveal 84% infected with malware. Most had at least one bot in network. Few were aware. Rates up from last year.
- Even leading anti-virus vendors now admitting that “anti-virus is dead”
- Verizon Data Breach Investigations Report (DBIR) proves attackers get in fast (minutes or hours) and remain undetected for months or years. Converged or blended attacks are the norm.
- Manual removal of detected threats takes significant financial and management resources and months of effort.

Malware Is Associated With Almost All Breaches

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 a good person 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

Actor	Motive	Targets
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

Method	Summary	Lessons
Espionage Methods	Human-guided use of tools to find and extract information	Prioritize, classify, and protect data
Web Application Attacks	Breaking into web sites or applications	Don't host web sites on your network; use robust DMZs
Malicious Code	Viruses, worms, etc	Automatic detection and remediation
Exploit poor configuration	Take advantage of bad design	Understand your applications – alter default configurations
PoS Attacks	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

Think of Cyber Intelligence like the National Security Community Does

- Three levels of cyber intelligence
  - Strategic: serving longer term decisions and strategies
  - Operational: serving day to day leadership decisions
  - Tactical: direct support to defenders in the fight

- Benefits of this approach:
  - Ensure right allocation of required resources to accomplish cyber intelligence objectives and to serve decision-makers
  - Ensure the right architecture is put in place to support the different kinds of decisions made

The National Security Community has Intelligence Agencies. Who can industry turn to?

The Rise of the Cyber Intelligence Discipline

- The hottest sector of the cyber security business right now is the cyber intelligence sector
- The old/established firms are enhancing their cyber intelligence practices and offerings
- New startups are attracting significant investments
- Data feeds of threat intelligence are hot commodities
- A new construct called “Web Intelligence” is emerging
- Secure collaboration spaces are hot

Concluding Thoughts

- 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
- But a well-instrumented enterprise with a mature cyber intelligence program can detect and mitigate adversary actions
- Focus on protecting the data, and prioritize which data to protect the best
- Secure collaboration is required to defeat the threat, including secure collaboration with external organizations
- Cyber Intelligence is required to ensure you can have a secure collaboration capability

Which Leads Back To Our Recommendations

Steps To Enhance Our Use of Cyber Intelligence and Our Collective Cyber Defense

Action	Description
Assess	Conduct assessment of cyber intelligence activities & prioritize improvement plans
Get Informed	The more you know about the threat the more you can educate others the better. Sign up for the daily Threat Brief at ThreatBrief.com
Threat Briefs	Ensure executives on the team understand cyber threat to their business objectives
Understand Yourself	Know what data, systems, capabilities are most important to protect. Use access control.
Automate	Few organizations have automated their ability to analyze operational and tactical threat indicators. Fewer have automated their ability to respond. Automate your IT management and access control as well.
Collaborate	No single organization can defend against all attackers. Sophisticated attacks require collaboration.
Network	Find your peers and build a community before you need it and seek inputs on how they leverage cyber intelligence in their organization (CSA, SINET, FBI, ISACs, SANS, AFCEA, INSA, FedCyber.com, ThreatBrief.com)
Prepare for breach	Plan for how you would respond to the worst case scenario and exercise your responses.
Love your people	Consider assigning an insider threat manager to lead your insider mitigation program and remember it is not about tech here, it is about people and processes. And if you love and lead your good people they will help find the bad people.

Do you concur?

Steps You Can Take Now

Sign Up For The Daily Threat Brief

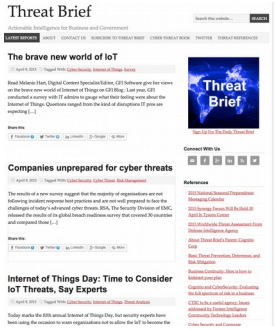
http://ThreatBrief.com

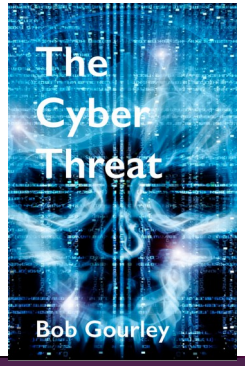
Read our paper on the Five Questions CEOs Should Ask Regarding Cyber. Then ask yourself those questions!

http://threatbrief.com/ceo-questions

Read the book The Cyber Threat

http://TheCyberThreat.com





Contact Information

Bob Gourley
bob.gourley@cognitiocorp.com

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

Sources and Methods

- We continuously research and review threat and response trends at ThreatBrief.com

- Other insights provided from
  - 2015 Verizon Data Breach Investigations Report
  - 2014 Annual Check Point Security Report
  - RSA Sponsored Security for Business Innovation Council on Transforming Security
  - SANS reference library
  - Interviews of leading community CISOs
  - Our book The Cyber Threat