THE CYBERSECURITY LANDSCAPE IN LATIN AMERICA

Montevideo Uruguay
27 August 2013

Aaron Boyd
Chief Strategy Officer

boyd@abiresearch.com

v.1b

© 2011 ABI Research

Founded in 1990

- First coverage was commercial applications of wireless semiconductors used by the military
- Coverage gradually expanded beyond semis to end-equipment markets and services

Global firm; Boutique support

- Analysts located in all major regions: Americas, Europe and Asia
- Sales and client support in localized markets

Focused on the identifying emerging technology trends first

- Early beachheads provide strong relationships in nascent markets
- Relationships continue as markets mature

Proven research methodology

- Key analyst relationships provide supply-side intelligence
- Enterprise and consumer surveys provide demand-side intelligence

© 2011 ABI Research

Introduction to ABI Research

ABIresearch

> Research Services

Mobile Networks

Mobile Devices

M2M

Telematics & Navigation

Mobile Services

Enterprise

Digital Home

RFID & Smart Cards

NextGen

Security

© 2011 ABI Research

Research Services

Standard Offerings

- Over 30 services tracking rapidly changing industries
- Each service contains a unique package of standard deliverables

Flexible Packaging

- Adjust budget/coverage to meet client needs
- Add services to fill gaps

Consulting Services

- Custom Research Reports
- White Papers
- Competitor Analysis
- Distribution Analysis

Research Deliverables

Products

- Research Reports
- Market Data
- Research Briefs
- ABI Insights
- Executive Briefs
- Vendor Matrices

Analyst Inquiry

- Included with services

© 2011 ABI Research

Cybersecurity Landscape in Latin America

1. State of Cyber Affairs
2. Addressing Critical infrastructure Protection
3. Implementing Policies and Regulation
4. Security Spending
5. Concluding Insights

© 2011 ABI Research • abiresearch.com The material contained herein is for the individual use of the purchasing Licensee and may not be distributed to any other person or entity by such Licensee including, without limitation, to persons within the same corporate or other entity as such Licensee, without the express written permission of Licensor.

© 2011 ABI Research

- Emerging market
- Powerful Telecoms
- Weak national policies in cyber
- Strong need for attention in this area, particularly due to cybercriminal element

Threat Actors	Individuals	Groups
Financial	Lone Actors	Criminal Organizations
Political	Hacktivists	State Actors

© 2011 ABI Research

Cyberhacktivists in Latin America

ABIresearch

Table: Selected Cyberhacktivists Operating in Latin America

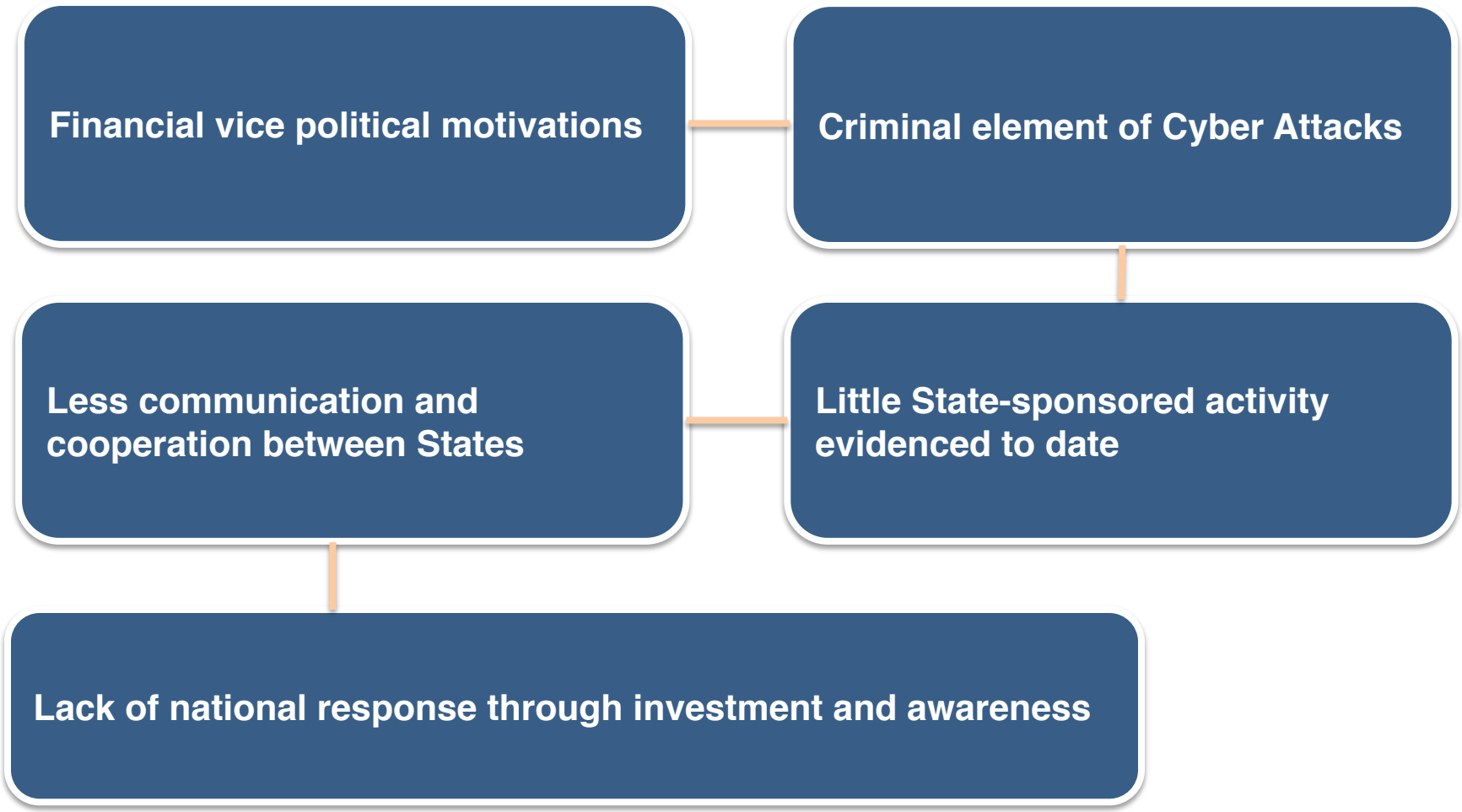
(Source: ABI Research)

Name	Region	Motivation	Targets	Tools and Methods
HighTech Brazil HackTeam	Brazil	Hacktivism	Government, Law Enforcement	SQLi, Data Breach & Dump
Red Eye Crew	Brazil	Hacktivism	Automotive Industry	Web Defacement
Team BCA (Brazilian Cyber Army)	Brazil	Hacktivism	Government, Business	Breached Accounts, Data Leaks/Dumps, SQLi
LulzSec Ecuador	Ecuador	Hacktivism	Government, Industry, Business, NGO	Data Dumps From Server Hacks, SQLi
LatinHackTeam	Regional	Hacktivism	Government, Industry, Business, Petroleum Corp	Web Defacement, Hack And Dump
Yei Zeta	Mexico	Hacktivism	Government, Education, Law Enforcement	Data Dumps From Server Hacks, SQLi
LulzSec Peru	Peru	Hacktivism	Government, Industry, Business, NGO	Data Dumps From Server Hacks, SQLi, Account Hijacking
HighTech Brazil HackTeam	Brazil	Hacktivism	Government, Law Enforcement	SQLi, Data Breach & Dump
Red Eye Crew	Brazil	Hacktivism	Automotive Industry	Web Defacement

© 2011 ABI Research • abiresearch.com The material contained herein is for the individual use of the purchasing Licensee and may not be distributed to any other person or entity by such Licensee including, without limitation, to persons within the same corporate or other entity as such Licensee, without the express written permission of Licensor.

© 2011 ABI Research

Investment in Localized over National Level



© 2011 ABI Research

- Attacks will likely overcome the ability to defend on a localized basis, and could threaten national interests
- Critical sectors are increasingly interconnected and inter-reliant and *currenly vulnerable*
- Argentina, Peru, Columbia, Mexico, Chile, Costa Rica, Panama, Ecuador, and Bolivia: Combined 3,000 industrial control system devices connected to the Internet, which were vulnerable to hacking and publicly viewable on Shodan.

© 2011 ABI Research • abiresearch.com The material contained herein is for the individual use of the purchasing Licensee and may not be distributed to any other person or entity by such Licensee including, without limitation, to persons within the same corporate or other entity as such Licensee, without the express written permission of Licensor.

© 2011 ABI Research

Implementing Policies and Regulation

Our focus for today

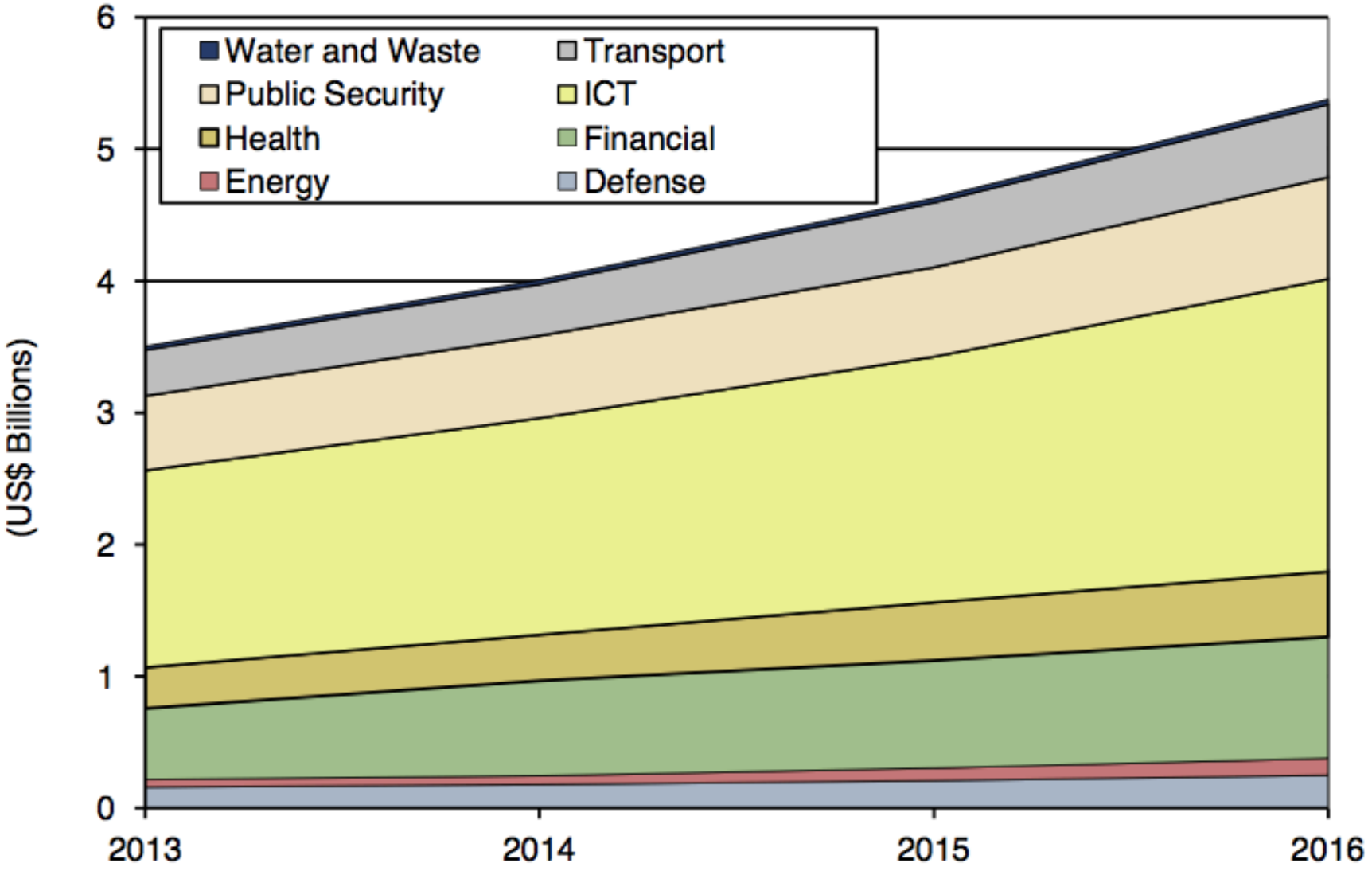
- Importance of national CERT with legal mandate
- Create a favorable environment for promoting careers in technology
- Protect Critical Infrastructure
- Understand strength and weaknesses and reach out to fill gaps
- Build demand for cybersecurity services, sell the economic benefit

© 2011 ABI Research • abiresearch.com The material contained herein is for the individual use of the purchasing Licensee and may not be distributed to any other person or entity by such Licensee including, without limitation, to persons within the same corporate or other entity as such Licensee, without the express written permission of Licensor.

© 2011 ABI Research

Cybersecurity Spending – Critical Infrastructure

ABIresearch



© 2011 ABI Research • abiresearch.com The material contained herein is for the individual use of the purchasing Licensee and may not be distributed to any other person or entity by such Licensee including, without limitation, to persons within the same corporate or other entity as such Licensee, without the express written permission of Licensor.

© 2011 ABI Research

1. Increase in frequency, scale and sophistication of attacks
2. Consumers look to vendors and regulators to manage security
3. Demand for industry regulation and government response
4. Expectation that the bad guys are prosecuted – political ramifications

Bottom line: When there is a large scale attack, consumers will increasingly look to governments/ regulators to provide protection and to hold services providers and vendors accountable for data loss.

© 2011 ABI Research

1. Increase role of government in cybersecurity
2. Harness existing hacker talent pool sources, provide alternatives
3. Leverage large telecommunications market
4. Build global relationships, other CERTs and ITU-IMPACT

© 2011 ABI Research

Contact ABI Reearch

boyd@abiresearch.com

© 2011 ABI Research