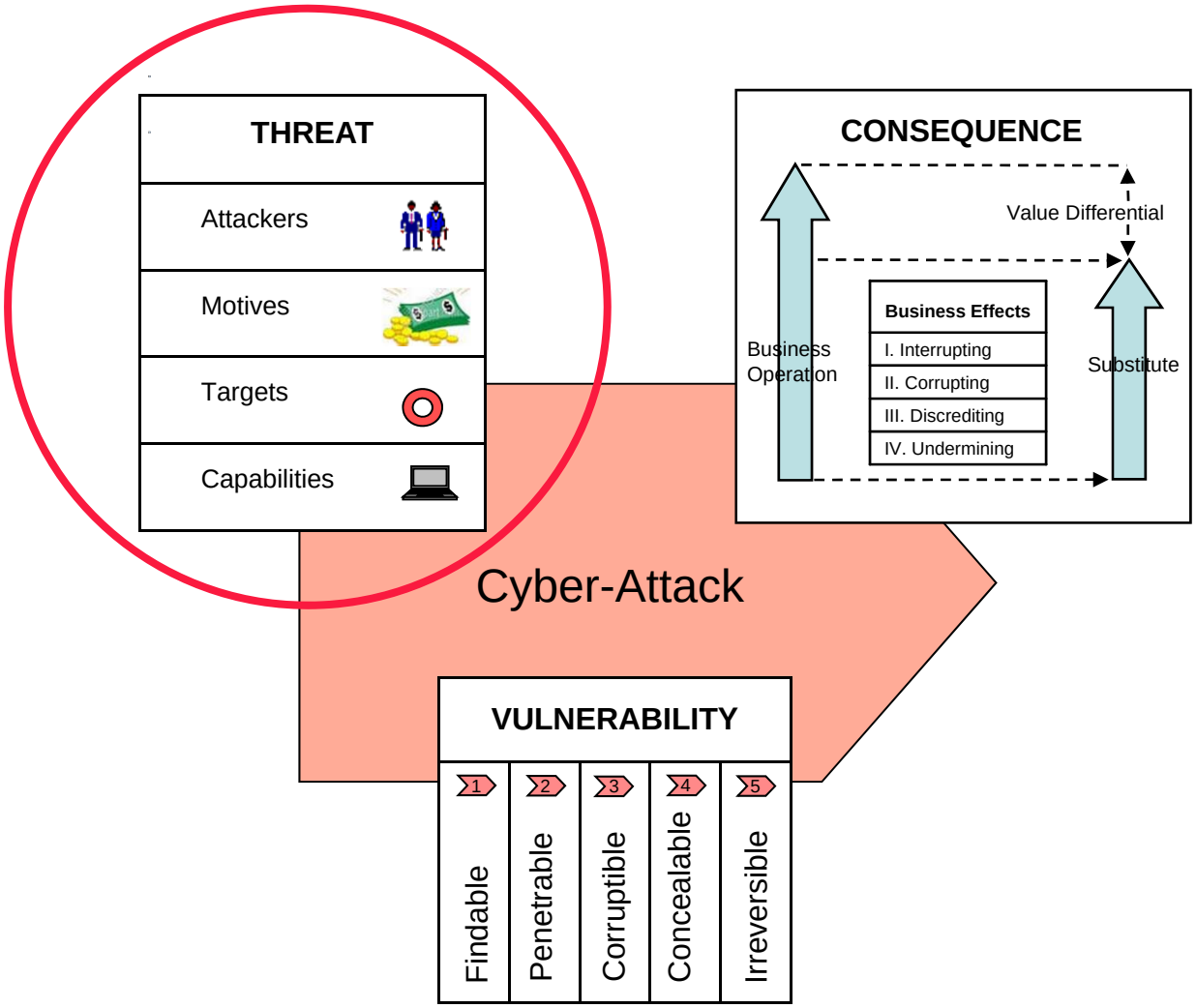
Estimating the Likelihood of Cyber Attacks When There's "Insufficient Data"

Scott Borg
Director and Chief Economist
U.S. Cyber Consequences Unit

Session ID: HT1-403
Session Classification: Intermediate



RISK = THREATS x CONSEQUENCES x VULNERABILITIES

The Five Main Types of Potentially Dangerous Cyber Attackers

1) Vindictive Insiders
2) Financial Criminals
3) Ethno-nationalists
4) Ideological Militants
5) Nation States

The Seven Ways for a Cyber Attacker to Gain

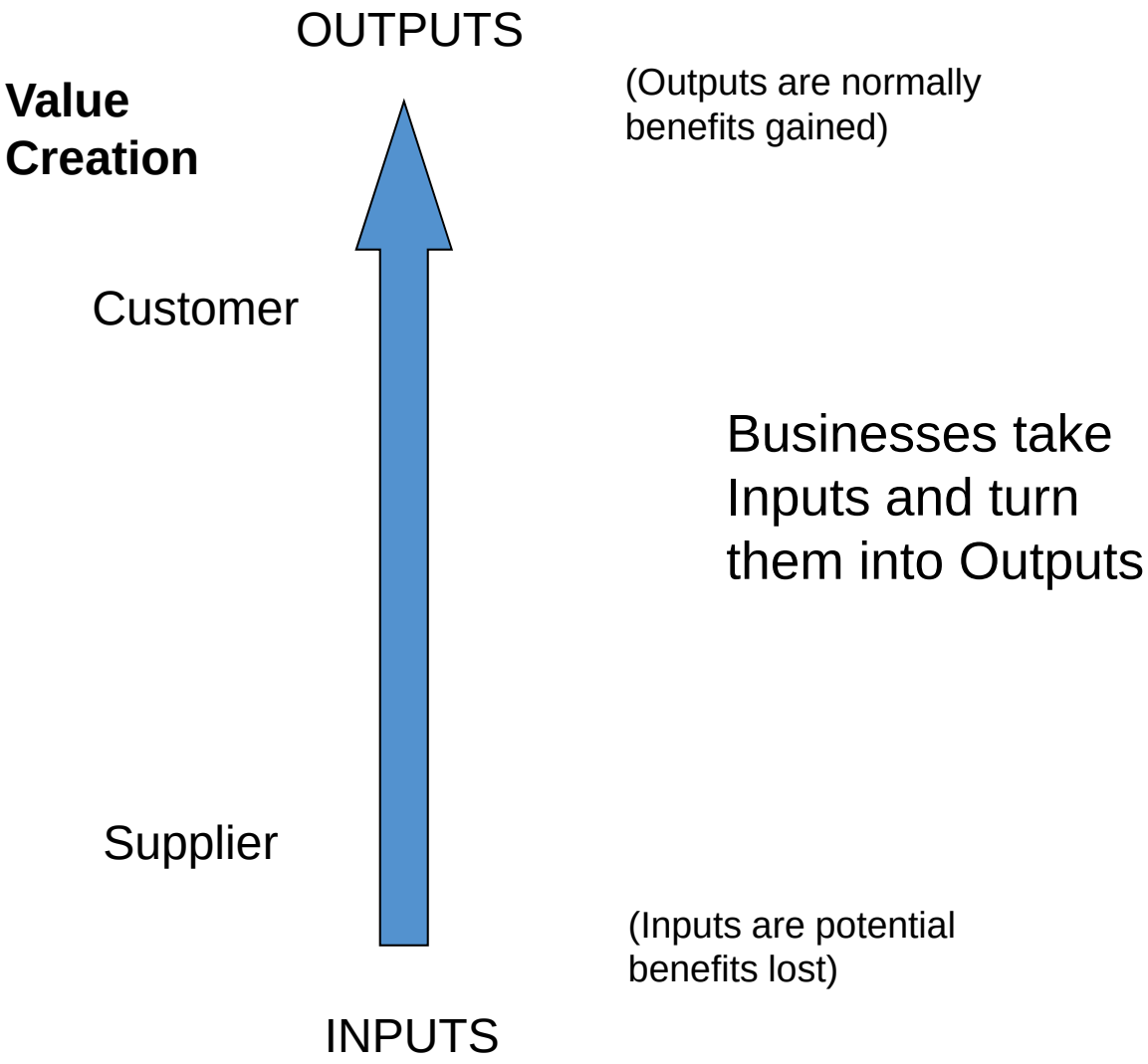
FOUR DIRECTLY FINANCIAL MOTIVES

1) Increase the value of an enterprise by damaging a competing enterprise
2) Divert the delivery of value to someone for whom it was not intended
3) Manipulate the value of a financial instrument
4) Make credible a coercive threat

THREE MOTIVES LESS DIRECTLY FINANCIAL

5) Advertise a business, cause, or movement
6) Stop by direct intervention an activity perceived as destroying value
7) Reduce an opponent's defensive or destructive capabilities

BASIC BUSINESS ACTIVITY



The Three Kinds of Information Systems That Need Special Attention

I. Information systems indispensable to the functioning of the other business systems

II. Information systems essential to those business activities that create the most value for that business or for its customers

III. Information systems with the potential to cause the greatest liabilities if they go wrong

THE INFORMATION SYSTEMS THAT ARE CRITICAL FROM A BUSINESS STANDPOINT (BORG ANALYSIS)			
	Systems That Are Indispensable to the Most Processes	**Systems That Create the Most Value**	**Systems That Could Cause the Greatest Liabilities**
Management of Outputs	Order receiving and processing; Customer account and relationship management	Systems handling customer lists and profiles; Marketing and promotional campaign plans; Information on negotiating positions with customers, and alternative customer bids	Authentication codes for customer accounts
Management of Production	Project tracking; Automation control systems for routine processes	Systems handling technological R&D; Systems handling new product features, recipes, designs, and prototype lessons; Optimum settings and configurations; Support systems for the organization's specialties	Automation controls that could affect quality of output; Automation controls for dangerous processes
Management of Inputs	Purchasing systems; Delivery receiving; Inventory management	Systems handling supplier lists and profiles; Information on negotiating positions with suppliers, most valued features, and alternative supplier offerings	Authentication codes for accounts with suppliers; Automated ordering
Coordination Across Functions	Corporate communications	Systems handling strategic positioning plans; Expansion, acquisition, and divestment plans	Shared information covered by non-disclosure agreements

The Four Fundamental Ways in Which Cyber-Attacks Could Interfere with What Businesses Do

1) They could interrupt business operations

2) They could corrupt business operations
(causing businesses to operate in a defective way)

3) They could discredit business operations
(preventing people from engaging in the right business)

4) They could undermine the basis for business operations
(removing the information differentials that make a business possible)

THE FOUR CATEGORIES OF CYBER ATTACKS APPLIED TO THE FOUR GROUPS OF INFORMATION SYSTEMS
(BORG SYSTEM)

	Interrupting	Corrupting	Discrediting	Undermining
Managing Outputs				
Managing Processes		All of the Cyber Attacks a Business Faces		
Managing Inputs				
Coordinating Functions				

Four Areas of Expertise Necessary for a Successful Cyber Attack

I. Business Expertise

(to chose the specific targets and types of attacks that would allow the attacker to benefit)

II. Access Expertise

(to devise ways of getting into the relevant information systems and to obtain actual entry)

III. Process Expertise

(to know what exact information inputs or disruptions would produce the desired results)

IV. Programming Expertise

(to write the code and data entries that would produce the desired disruptions)

EXPERTISE RATINGS FOR CYBER ATTACKS (BORG SCALE)	**Comparative Score**
Level Seven Expertise Nearly unique intellectual gifts or knowledge of highly secret systems	1,000,000
Level Six Expertise Deep insider experience or very elite, specialized training	100,000
Level Five Expertise Substantial industry experience after a mid-level degree	10,000
Level Four Expertise Solid mid-level university degree in the relevant subject	1000
Level Three Expertise Relevant undergraduate coursework	100
Level Two Expertise Sustained interest in a relevant discipline	10
Level One Expertise A few days of web surfing by an intelligent student	1
Level Zero Expertise No special skill or knowledge whatsoever	0

SOME MINIMUM EXPERTISE RATINGS & SCORES

	Business Expertise	Access Expertise	Process Expertise	Program Expertise	Total Score
Common Worms and Viruses	Zero 0	Three 100	Zero 0	Two 10	**110**
Typical Credit Card Cyber Fraud	Three 100	Three 100	Two 10	Three 100	**310**
Larger Criminal Enterprise Attack	Three 100	Four 1000	Four 1000	Three 100	**2,200**
Significant Infra-structure Attack	Three 100	Four 1000	Six 100,000	Five 10,000	**111,100**
National Cyber Assault Component	Five 10,000	Six 100,000	Six 100,000	Six 100,000	**310,000**

STAGES OF TACTICAL EXPLOIT DEVELOPMENT
Stage One Attention to a general category of attack vector and a general exploit strategy
Stage Two Conceptual articulation of a specific attack vector and a specific exploit strategy
Stage Three Proof-of-concept exploit, possibly functioning only in one or more specific situations or with custom adjustment
Stage Four Generalized exploit, functioning in most of the relevant situations, but requiring considerable expertise to apply
Stage Five Downloadable exploit, capable of being used by someone with little or no expertise, but still requiring human application
Stage Six Autonomous, deliverable exploit, capable of being carried in a worm or easily incorporated into another program

Example of an American Electrical Company Assessing Likelihood of Sophisticated Cyber-Attack on Its Large Generators

	Criminal Conspiracies	Ethno-Nationalists	Ideological Militants	Nation States
Possible attacker?	Yes	Yes	Yes	Yes
Current motivation?	Some	Some	Yes	NO
Reason to choose this target?	NO	NO	Some	Yes
Relevant attack capabilities?	Some	Some	NO	Yes
Signs of preparation?	NO	NO	Some	Yes

Thank you!

For more information or permission to use this material, please contact:

Scott Borg
U.S. Cyber Consequences Unit
P.O. Box 1390
Norwich, VT 05055

scott.borg@usccu.us
802 – 649 - 3849