HERREN

2016 Professional Development and Training Workshop

The Cost of Cyber

Software and Information Technology Track (SI05)

Ann E. Hawpe | **Jeffrey M. Voth**

International Cost Estimating & Analysis Association (ICEAA)
Grand Hyatt I Atlanta, GA

June 8, 2016

Presented at the 2016 ICEAA Professional Development & Training Workshop - www.iceaaonline.com/atlanta2016

Presentation Agenda

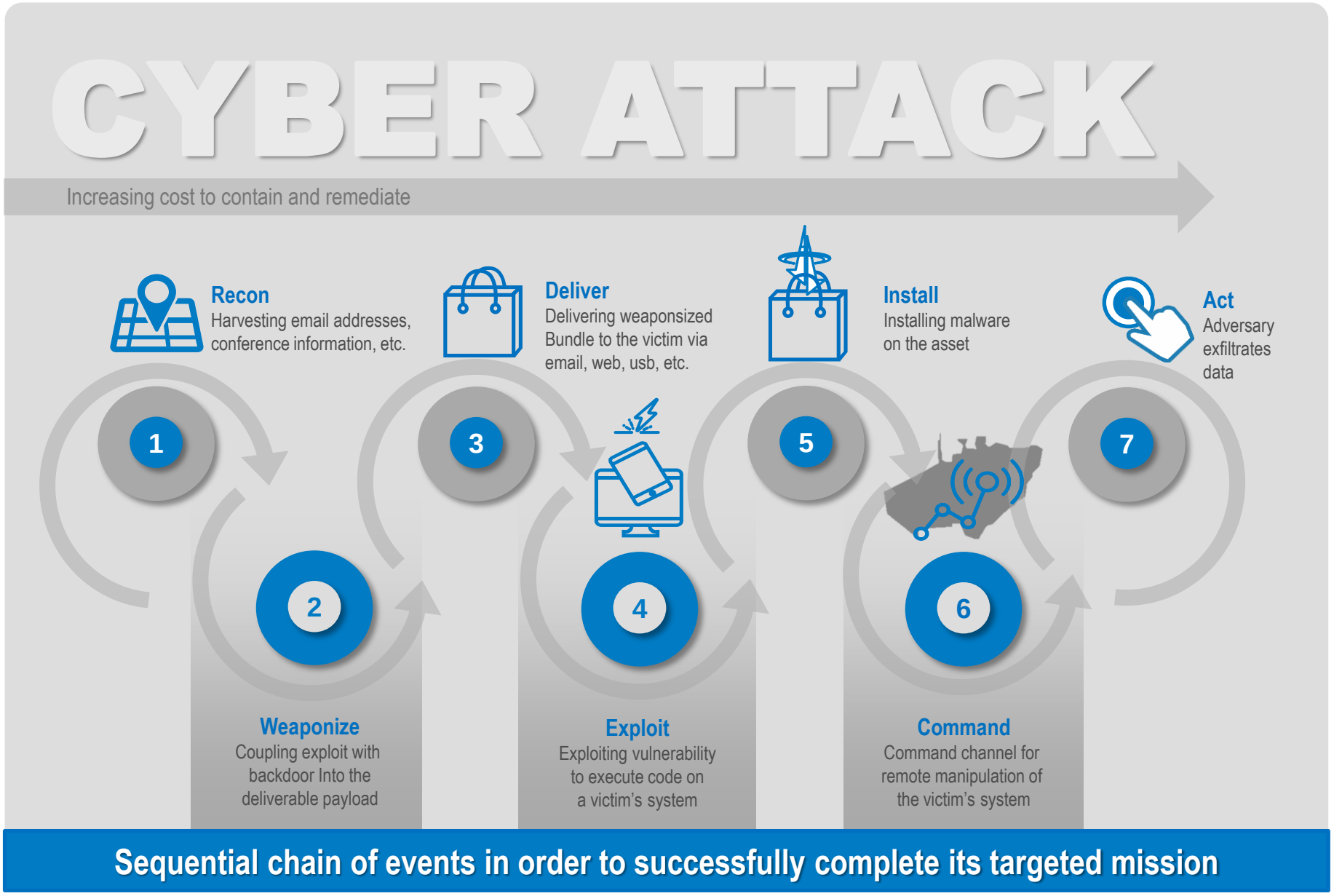
- **Introduction** 2

- **Discussion on cyber investment** 7
  - **Analyze potential loss** 10
  - **Assess probability of occurrence** 11
  - **Allocate resources appropriately** 12

- **Summary** 13

Presented at the 2016 ICEAA Professional Development & Training Workshop - www.iceaaonline.com/atlanta2016

Addressing the Cyber Kill Chain



Growing need to address challenges facing federal systems

GAO

United States Government Accountability Office

Testimony

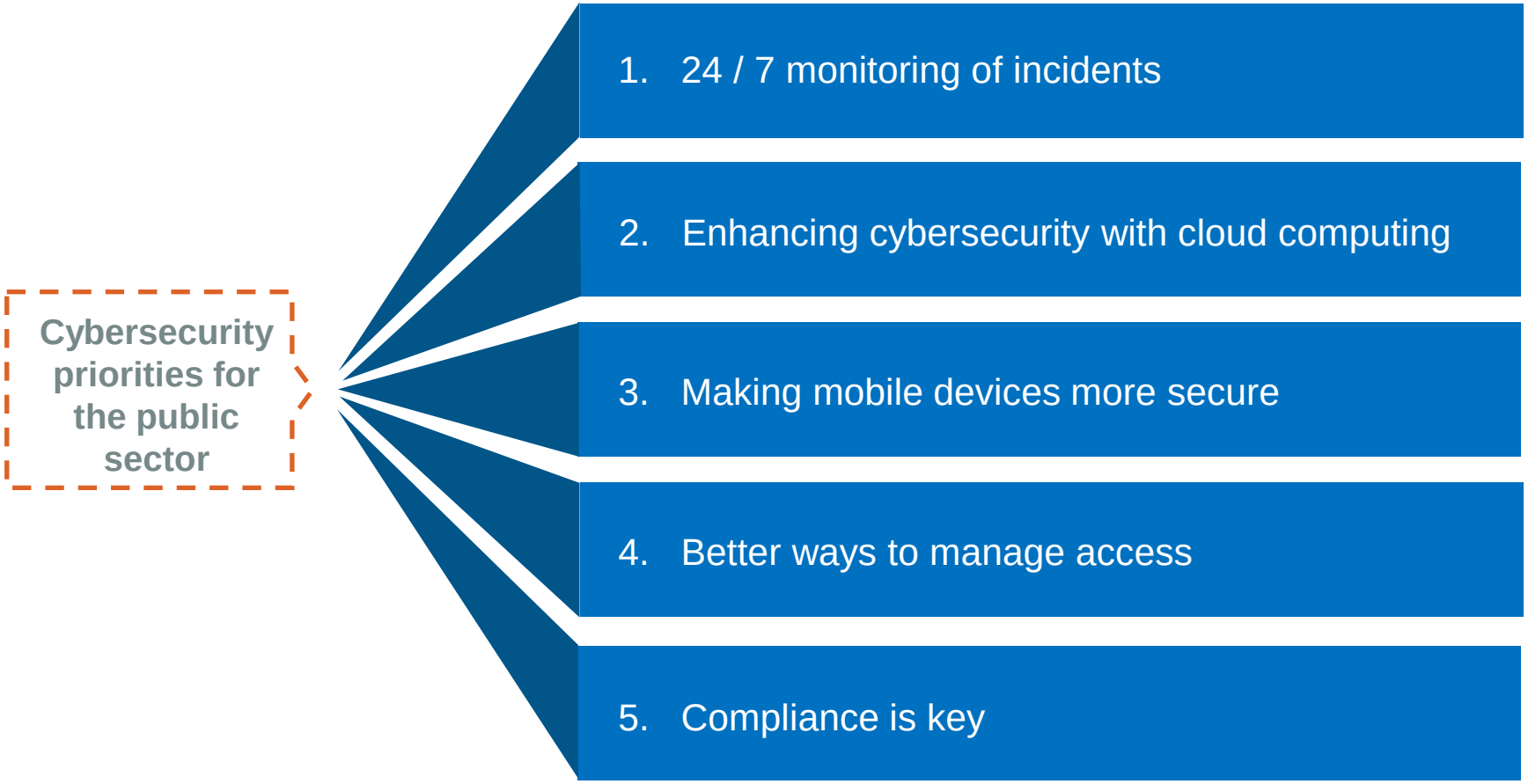
Before the Committee on Oversight and Government Reform, House of Representatives

19 of 24 major federal agencies reported deficiencies in information security controls

Inspectors general at **23 of 24** agencies cited information security as a major management challenge

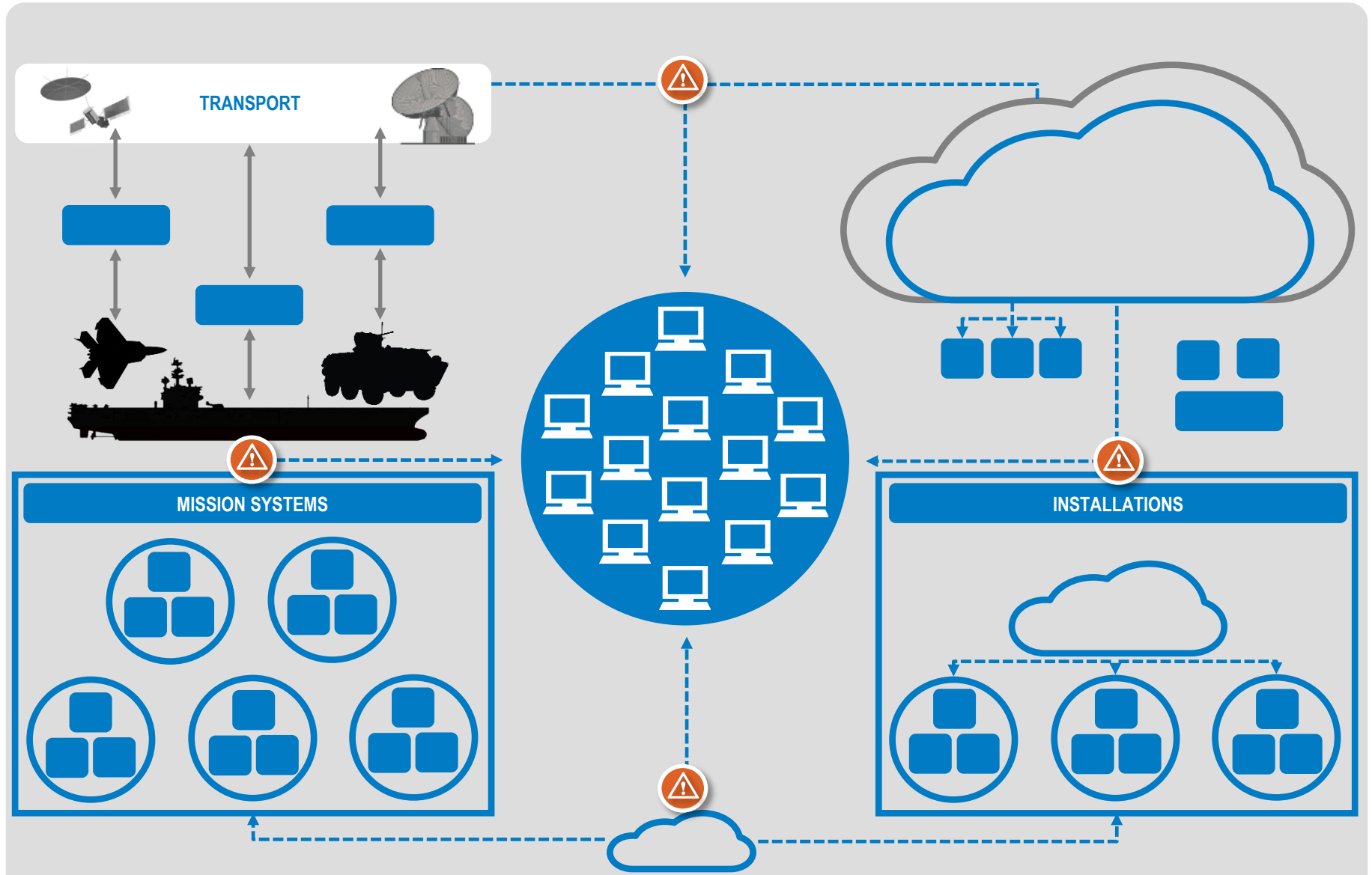
Agencies are implementing new methods to counter threats

Vast majority of public sector agencies have adopted one or more risk-based cybersecurity frameworks, and organizations are collaborating to share intelligence



Presented at the 2016 ICEAA Professional Development & Training Workshop - www.iceaaonline.com/atlanta2016

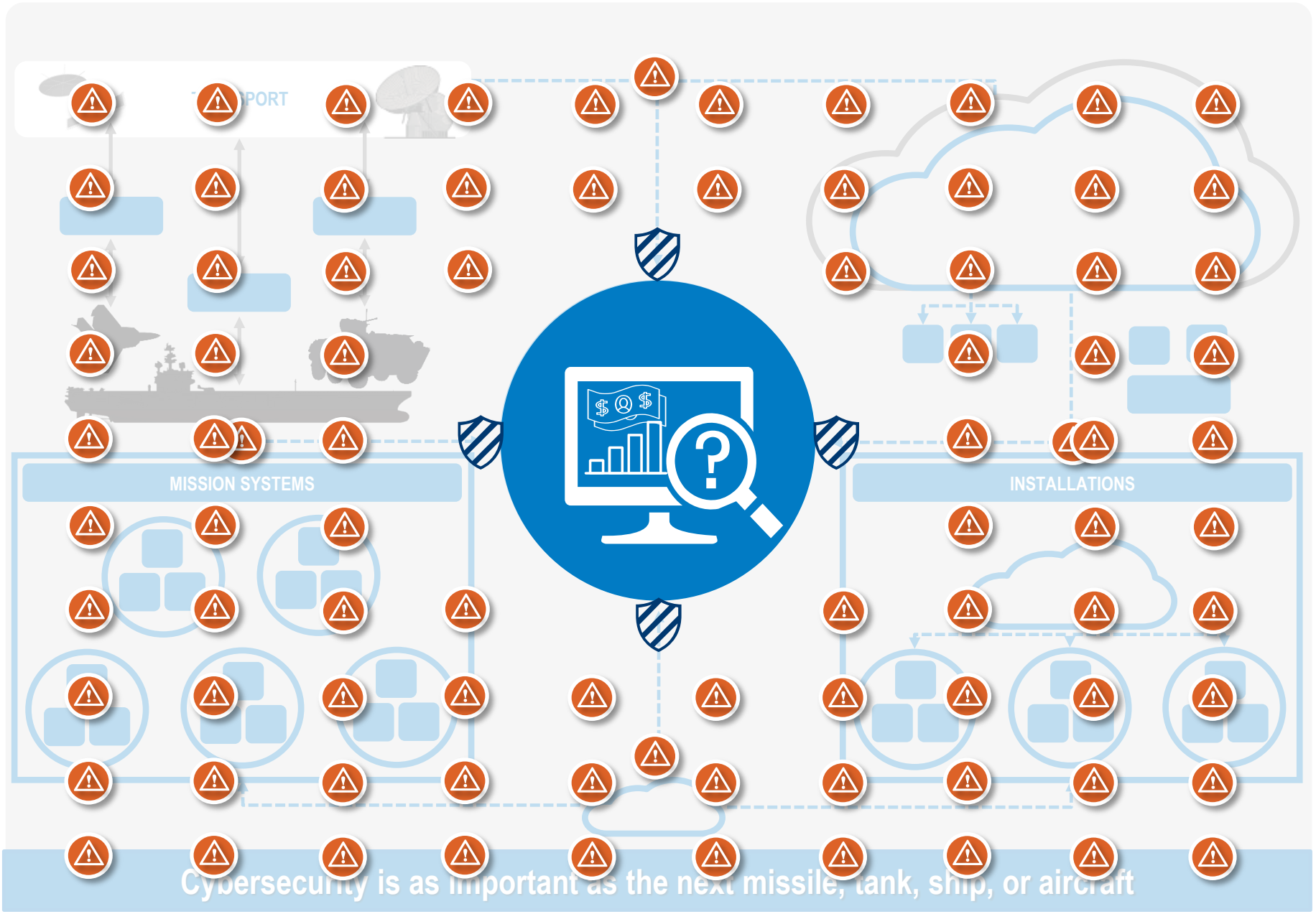
Mitigating the Vulnerabilities and Risks



Cybersecurity is as important as the next missile, tank, ship, or aircraft

Presented at the 2016 ICEAA Professional Development & Training Workshop - www.iceaaonline.com/atlanta2016

Cybersecurity Threats Continue to Evolve



Measuring the ROI for cybersecurity is challenging

Most organizations have difficulty measuring the effectiveness of cybersecurity investments while capturing the total program cost

$$\text{Return on Investment} = \frac{\text{Benefits - Cost}}{\text{Cost}}$$

	C_0	t_1	t_2	t_3
Initial investment	$10,000,000			
Annual benefit		$20,000,000	$20,000,000	$20,000,000
Annual cost		- 15,000,000	- 15,000,000	- 15,000,000
Net cash flow	-10,000,000	5,000,000	5,000,000	5,000,000
ROI	**$5,000,000**			

Three-year ROI for $10M investment

Need to compare anticipated benefits and costs over time

Discount investments and costs over time to today's value

Standard criteria for justifying investments on economic principles:
- Invest if the NPV > 0

Net Present Value = PV (Benefits) – PV (Costs)

	C_0	t_1	t_2	t_3
Initial investment	$10,000,000			
Annual benefit		$20,000,000	$20,000,000	$20,000,000
Annual cost		- 15,000,000	- 15,000,000	- 15,000,000
Net cash flow	-10,000,000	5,000,000	5,000,000	5,000,000
NPV	- 10,000,000	$(5,000,000) / (1.10)^1$	$(5,000,000) / (1.10)^2$	$(5,000,000) / (1.10)^3$
NPV	- 10,000,000	4,545,455	4,132,231	3,765,574
NPV	**- $2,443,260**			

Three-year NPV for $10M investment, assuming a 10% discount rate

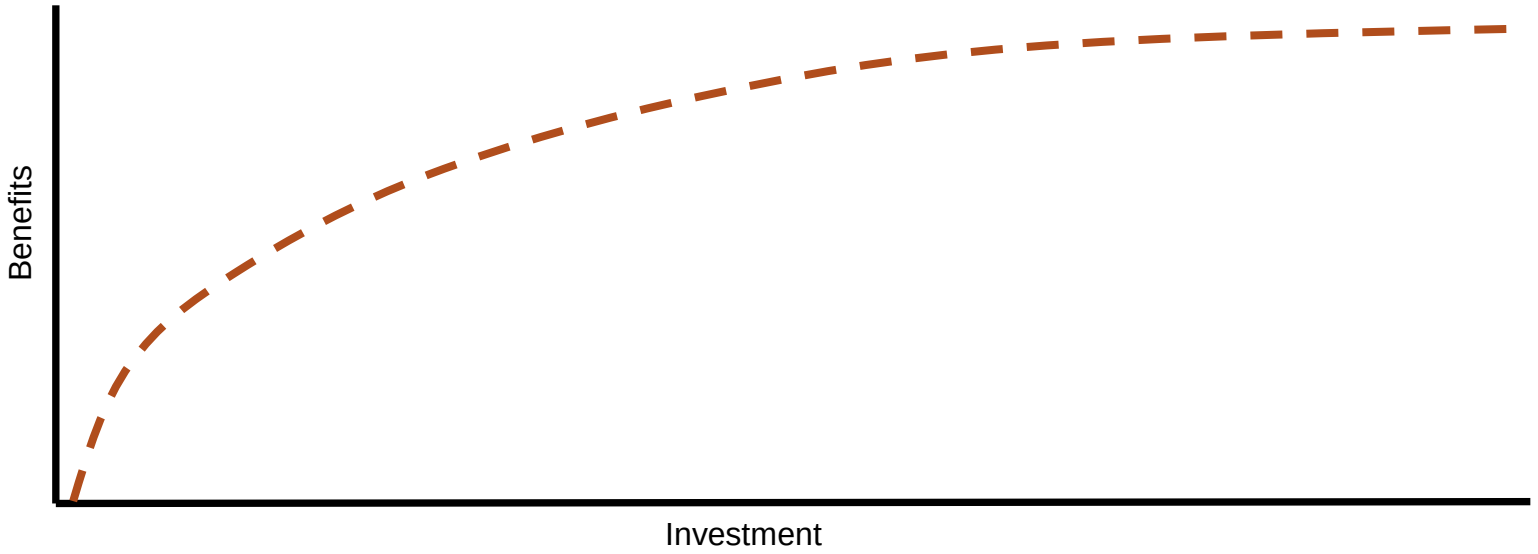
Assuming a 10% discount rate, the project has a negative NPV

So how much should be invested in cybersecurity activities?

Since agencies have a finite amount of resources, answering this question involves a resource allocation decision. Finding the optimal level of investment will be key

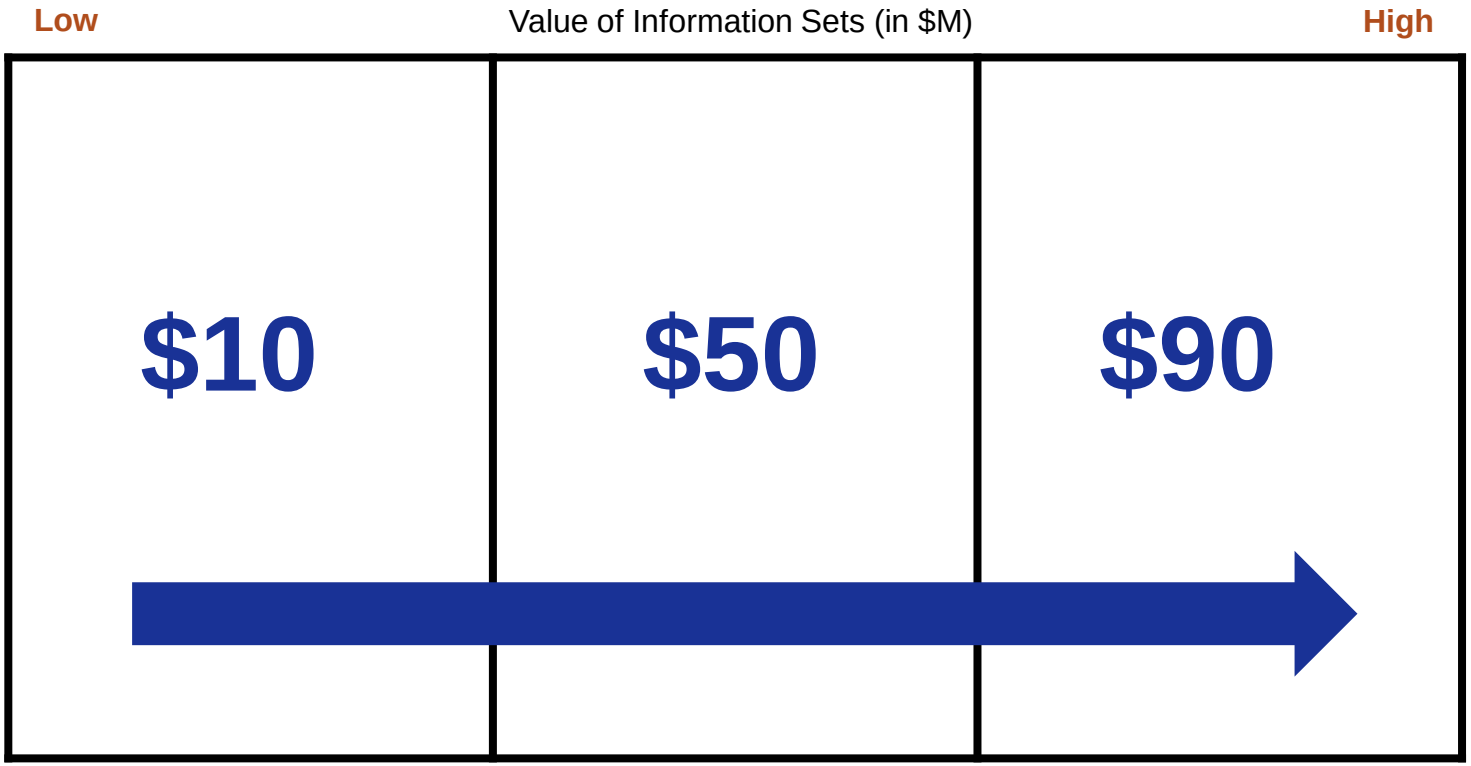
Brief review of the Gordon-Loeb Model in a practical setting

1. Analyze potential loss
2. Assess probability of occurrence
3. Allocate resources appropriately



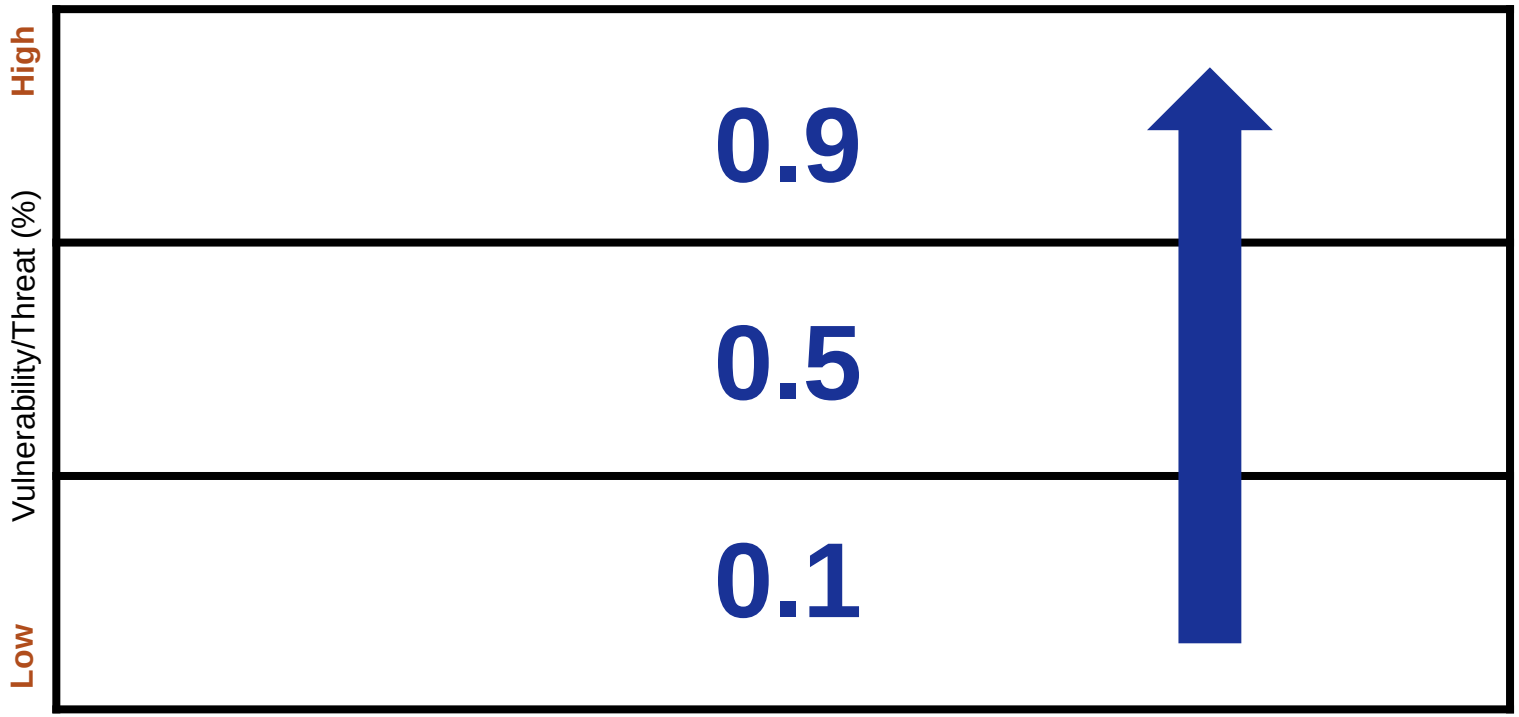
Analyze Potential Loss

Estimate loss from security breach for each set of information. The inverse becomes the value of information (categorized as high, medium, low)



Assess Probability of Occurrence

Estimate the likelihood that an information set will be breached by examining its vulnerability/threat to attack (categorized as high, medium, low)



Allocate Resources Appropriately

Create a grid with all possible combinations of the first two steps representing the expected loss of a cybersecurity breach

Vulnerability/Threat (%)	Value of Information Sets (in $M)		
	$10 (Low)	$50	$90 (High)
0.9 (High)	9	45	81
0.5	5	25	45
0.1 (Low)	1	5	9

Allocate Resources Appropriately

Consider cost-benefit aspects of investing additional funds on each information set

"How much will we save through the reduction of expected loss, by investing another $1M in cybersecurity activities?"

Low Productivity: $s(z,v) = \frac{v}{(1+z)}$ for Low Vulnerability/Threat

Medium Productivity: $s(z,v) = \frac{v}{(1+z)^2}$ for Medium Vulnerability/Threat

High Productivity: $s(z,v) = \frac{v}{(1+z)^3}$ for High Vulnerability/Threat

s(z,v) = Security breach probability function
v = Vulnerability
z = Investment in Cybersecurity

Vulnerability/Threat (%)	$10 (Low)	$50	$90 (High)
0.9 (High)	9	45	81
0.5	5	25	45
0.1 (Low)	1	5	9

Value of Information Sets (in $M)

Allocate Resources Appropriately

Values greater than 1 indicate the information sets where it is still beneficial to make the next $1M investment

z = 1

Vulnerability/Threat (%) \ Value of Information Sets ($M)	Low		High
High	7.9	39.4	70.9
	3.8	18.8	33.8
Low	0.5	2.5	4.5

z = 2

Vulnerability/Threat (%) \ Value of Information Sets ($M)	Low		High
High	0.8	4.0	7.1
	0.7	3.8	6.3
Low	0.2	0.8	1.5

z = 3

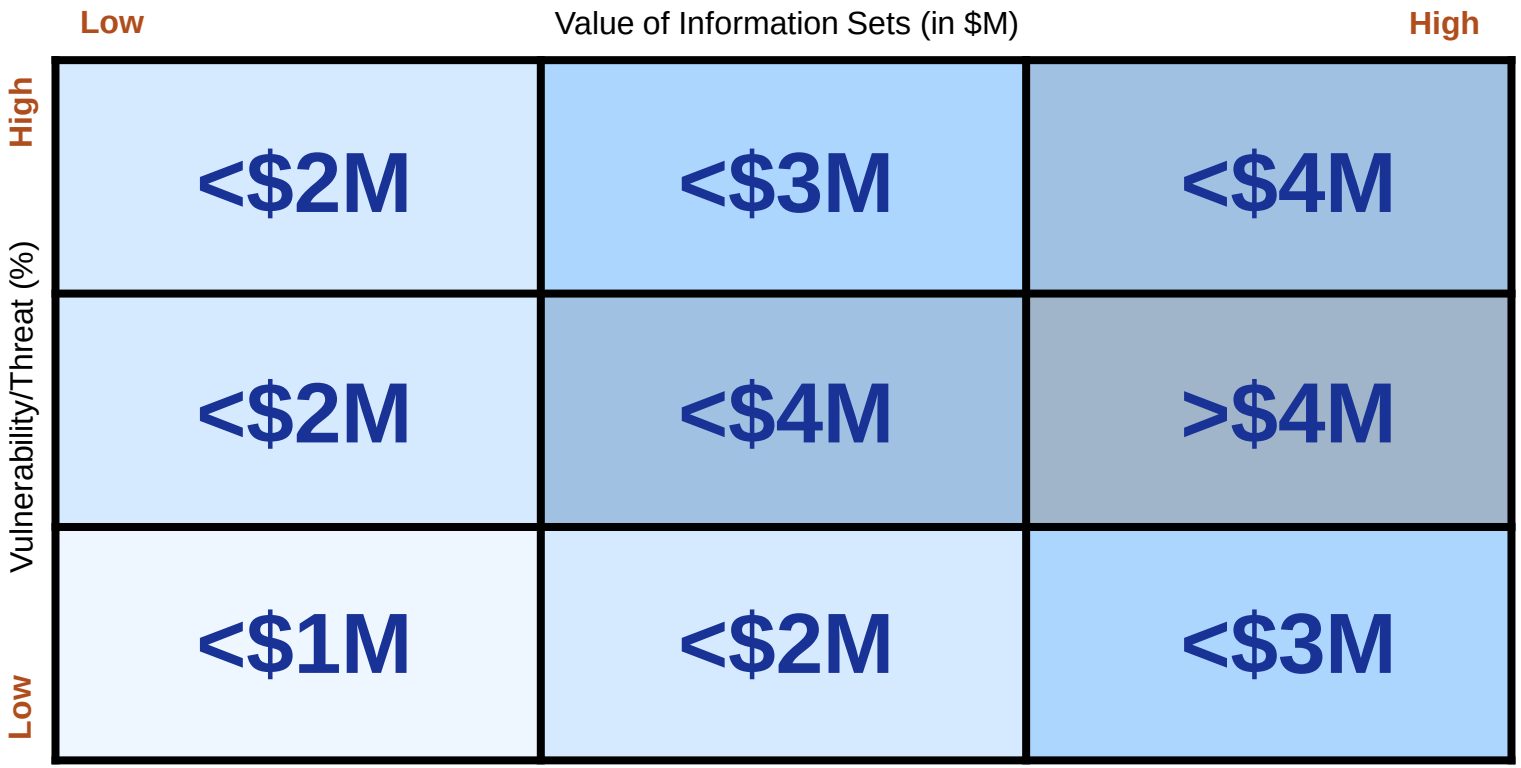
Vulnerability/Threat (%) \ Value of Information Sets ($M)	Low		High
High	0.2	0.9	1.7
	0.2	1.2	2.2
Low	0.1	0.4	0.7

z = 4

Vulnerability/Threat (%) \ Value of Information Sets ($M)	Low		High
High	0.1	0.4	0.6
	0.1	0.6	1.0
Low	0.1	0.3	0.4

Investment Amounts

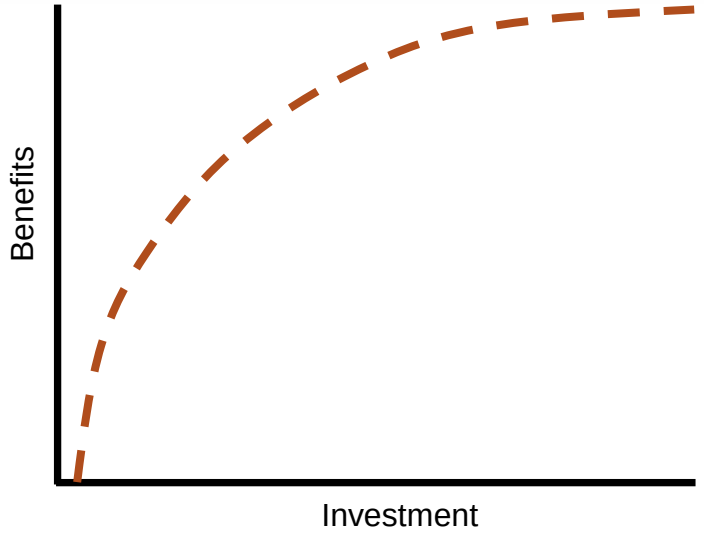
Focus investment in cybersecurity activities where it will deliver the largest net benefits



Not all investments in cybersecurity are equal

Spend should not exceed roughly **1/3** of total expected losses from cybersecurity breaches

Optimal amount of spending to protect information does not always increase with increases in information set vulnerability



Presented at the 2016 ICEAA Professional Development & Training Workshop - www.iceaaonline.com/atlanta2016

Comments/Questions