Advancing Cybersecurity: Management, Strategy and Organizational Issues

Module 5

PROFESSIONAL EDUCATION

CSAIL
MIT COMPUTER SCIENCE AND ARTIFICIAL INTELLIGENCE LABORATORY

Advancing Cybersecurity: Management, Strategy and Organizational Issues

Michael Siegel

Principal Research Scientist - Sloan School of Management

Computer Science and Artificial Intelligence Laboratory (CSAIL)

Massachusetts Institute of Technology

TOPICS FOR TODAY

- **Cybersecurity is Important**

Not a surprise

- **Thinking about Vulnerabilities: Friends and Enemies?**

Understanding white hats and black hats
The vulnerability ecosystem
Bug bounty programs
The white hat workforce

- **Making Things Better: A Systems View of Cybersecurity**

Reducing vulnerabilities: Playing better defense
Examining metrics and ROI

- **Management and Goverance of Cybersecurity**

Education
Cybersecurity frameworks
Instructions on a simulation(separate module)

FILLING IMPORTANT NEED FOR IMPROVED SECURITY OF CRITICAL INFRASTRUCTURE

- **Security of conventional information systems is recognized as important …**
  - But still not fully effective (e.g., Target, Sony, HSBC, US OPM, etc.)
- **Security of our Cyber-Physical Infrastructure and IoT …**
  - E.g., computer controlled utilities, home sensors, oil & gas sites, chemical, water, financial services, autonomous vehicles, telecom, infrastructure, etc.

… is even more important, but much less research has been done.

- **Most research focused on improving hardware and software**
  - Helpful, but …
  - Majority of events (estimates 70-80%) are aided or abetted by insiders
- **Need to address managerial, organizational, and strategic aspects of cybersecurity**

CYBERSECURITY IS IMPORTANT TO EVERYONE

- White House Executive Order: "… cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront ..."
  - $19B proposed in FY2017 budget for Cybersecurity

- U.S. Secretary of Energy Ernest Moniz: "… nation's oil and gas industry … cyber threats continue to increase in frequency and sophistication …"
  - December 2015 attack on Ukrainian electric distribution

- SEC Commissioner Luis A. Aguilar warned that "… boards that choose to ignore, or minimize the importance of cybersecurity oversight responsibility, do so at their own peril …"

THINKING ABOUT VULNERABILITIES: FRIENDS AND ENEMIES?

-UNDERSTANDING WHITE HATS AND BLACK HATS
-THE VULNERABILITY ECOSYSTEM

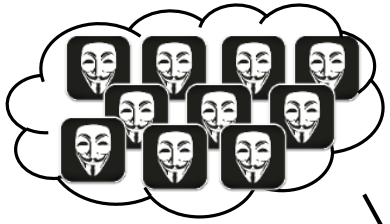
VULNERABILITIES AND SECURITY

ALL VULNERABILITIES ARE NOT THE SAME: A TOPOLOGY

Vulnerability Characteristics	Quantity of Vulnerabilities	➢ Scarce - Numerous
	Priority of Vulnerability	➢ Critical – Low Acceptable Risk
	Likelihood of Vulnerability Rediscovery	➢ Low - High
Patching Dynamics	Technical Difficulty of Remediation	➢ Easy - Hard to Fix
	Logistical Difficulty of Remediation	➢ Easy - Hard to Access
	Discovered /Patch Available	➢ Yes/Yes Yes/No **No/No**
Market Dynamics	Third Party Market for Vulnerability	➢ Offensive, Defensive, Mixed, Etc.
	Market Size	➢ Small - Large
	Bug Bounty Program	➢ Yes, No
Human Dynamics	Attackers	➢ Criminals, States, Patriots, Etc.
	Researcher Pool	➢ Small - Large
	Attacker Motivation	➢ Political, Financial, Reputational

Overview of Offensive and Defensive Markets

Black Hat Hackers



- ✓ Vulnerability/Exploit Sharing;
- ✓ Cyber-crime as a service;
  - ➢ Provide / Consume

- ✓ Vulnerability/Exploit Sharing;
- ✓ Cyber-crime as a service;
  - ➢ Provide / Consume
- ✓ Hire black hat hackers;

- ✓ Organized Cyber-Crime;
  - ➢ No lone wolves; 80% attack;
  - ➢ Become business

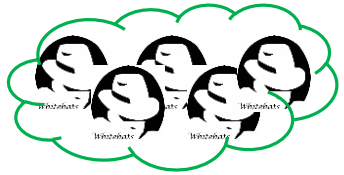
Offensive Market

Flow

Attack

Attack

White Hat Hackers



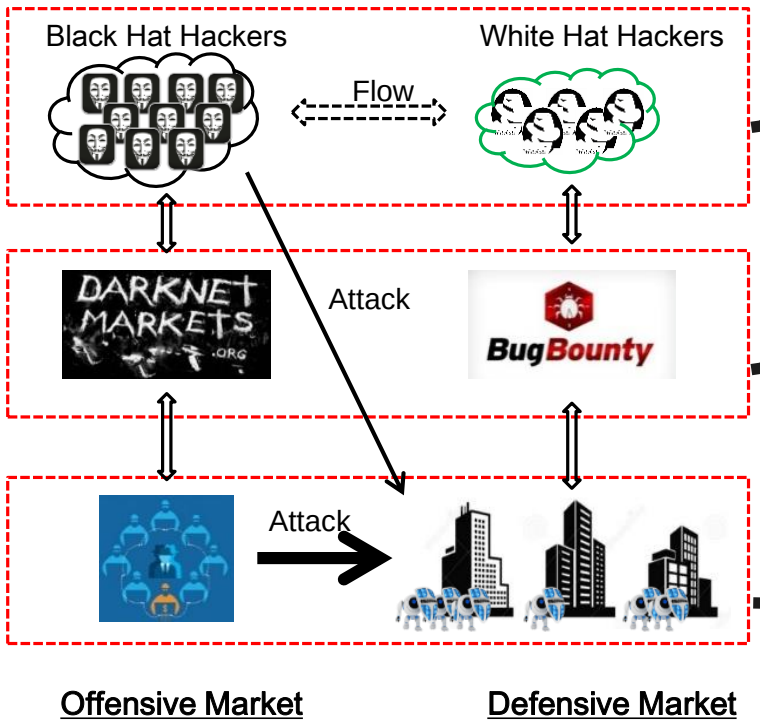
- ✓ Work for Bug Bounty Program (BBP);
- ✓ Gain Reward;
- ✓ Build Reputation;

- ✓ Employ outside experts;
- ✓ Solve potential vulnerability before being attacked;
- ✓ Hire high quality experts;

- ✓ Investment to improve security;
  - ➢ Limited budget;
  - ➢ Many assets to protect;

Defensive Market

What Issues Can we Address by Examining these Markets?



Growth into Black Hats or White Hats

- ✓ How hackers become black hats, white hats or join a company working as a security expert?
- ✓ Motivation, workforce behavior
- ✓ Tools and Practices – both common and different

BBP to improve security:

- ✓ Discover vulnerabilities & reduce risk
- ✓ Can BBP reduce the dark market?
- ✓ What is the effect of BBP on software reliability?

Protection Optimization:

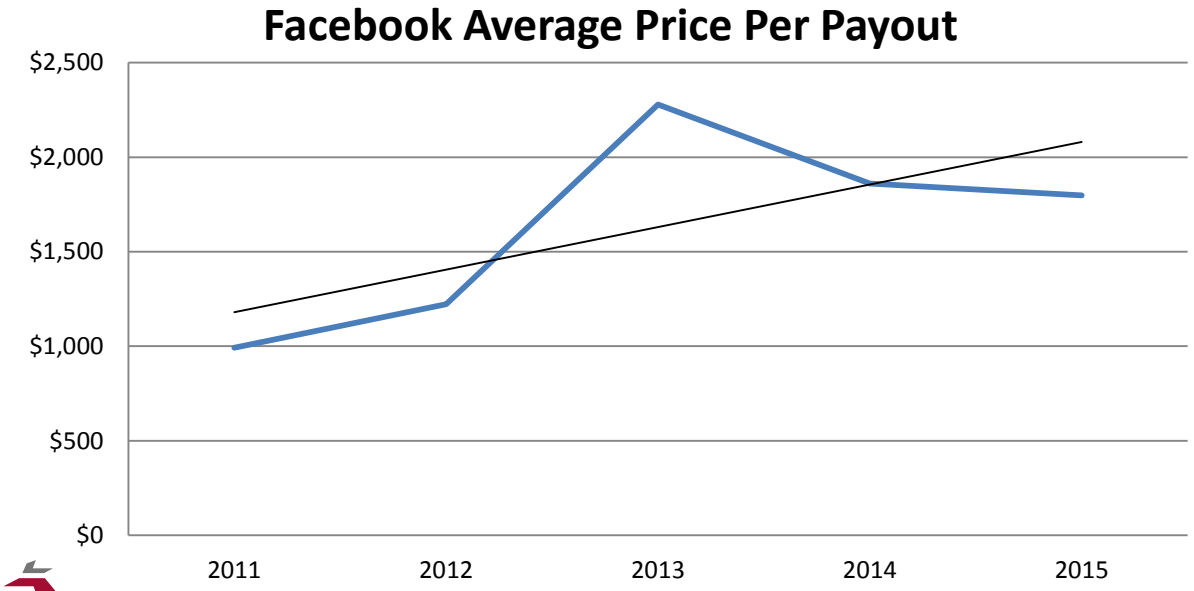
- ✓ Given the limitation budget, the assets to protect, how does one optimize their investments:
  - ✓ Balance between launching BBP, buying from dark market, internal programs
  - ✓ Impact on software/hardware choices
  - ✓ Rank the priority of assets for protection

THINKING ABOUT VULNERABILITIES: FRIENDS AND ENEMIES?

-BUG BOUNTY PROGRAMS

THE NEW SECURITY WORKFORCE: BUG BOUNTY PROGRAMS

- Over 250 firms offer bug bounty programs (e.g., Google, Facebook, Yahoo)
- Facebook has had over $3.5 million in payouts (2015)
- HackerOne has had over $4 million in payouts since inception (2015)
- Private bug bounty programs (e.g., Linkedin, Apple)
- Many bugs are bountied for charity or recognition
- Represents “defensive capability” of over 25,000 security researchers
- Provides some insight into “offensive capability”



Hack the Pentagon

The first U.S. Government commercial bug bounty program.

www.defense.gov · @DeptofDefense

Thank you for your interest in HackerOne's Department of Defense (DoD) "Hack the Pentagon" pilot--the first ever U.S. Government commercial Bug Bounty program. This was an effort for the Government to explore new approaches to its cybersecurity challenges, and evolve to adopt the best practices used by the most successful and secure software companies in the world, the DoD can ensure U.S. systems and warfighters are as secure as possible.

The Hack the Pentagon Bug Bounty Pilot ran from Monday, April 18, 2016 to Thursday, May 12, 2016.

We appreciate the efforts of all of the participants, especially those who submitted valid issues. A list of successful participants can be found on the Thanks page above.

Program Overview Statistics

- Total registered participants: 1,410
- Total reports submitted: 1,189
- Unique valid reports: 138
- Average bounty amount: $588
- Total bounties paid: $71,200

The most common vulnerability type reported was Cross-Site Scripting (XSS), followed by Information Disclosure and Cross-Site Request Forgery (CSRF).

The most severe vulnerability submitted and the highest awarded was a SQL Injection.

Hackers thanked (157)

mlitchfield
Reputation: 461

m0arcatz
Reputation: 303

popeax
Reputation: 180

hogarth45
Reputation: 125

craigarendt
Reputation: 107

All Hackers

Hack the Pentagon Bug Bounty Program: Does it Make a Difference?

"Already a staple for companies such as Google and Facebook, the bug bounty program – which pays friendly hackers to do the sorts of things that recreational hackers might do for fun, and that criminals like to do for far more nefarious purposes – **was so successful that Pentagon officials say that they are considering another bug bounty program for later this year. Other federal agencies, they add, would do well to follow their lead. "`**

And that saves the Pentagon money – **the bug bounty pilot program cost $150,000**.

"It's not a small sum but if we had gone through the normal process of hiring an outside firm to do a security audit and vulnerability assessment, which is what we usually do, it would have cost us over $1 million," said **Defense Secretary Ash Carter**.

The **DOD paid $5 million over three years to one vendor, which found less than 10 vulnerabilities.**
In total, 1,400 eligible ethical hackers – otherwise known as "white hats" – were invited to take part in the program, and more than 250 of them found and submitted at least one vulnerability. Of these, 138 were found to be "legitimate, unique, and eligible for a bounty," said Secretary Carter.
Equally important, by allowing outside hackers to find holes and vulnerabilities**, it frees up the US military's own cyberspecialists "to spend more time fixing them than finding them**," Carter added. **"The pilot showed us one way to streamline what we do to defend out networks and correct vulnerabilities more quickly**."

http://www.csmonitor.com/World/Passcode/Security-culture/2016/0705/Meet-David-Dworken-the-teenager-who-hacked-the-Pentagon

GM embraces white-hat hackers with public vulnerability disclosure program

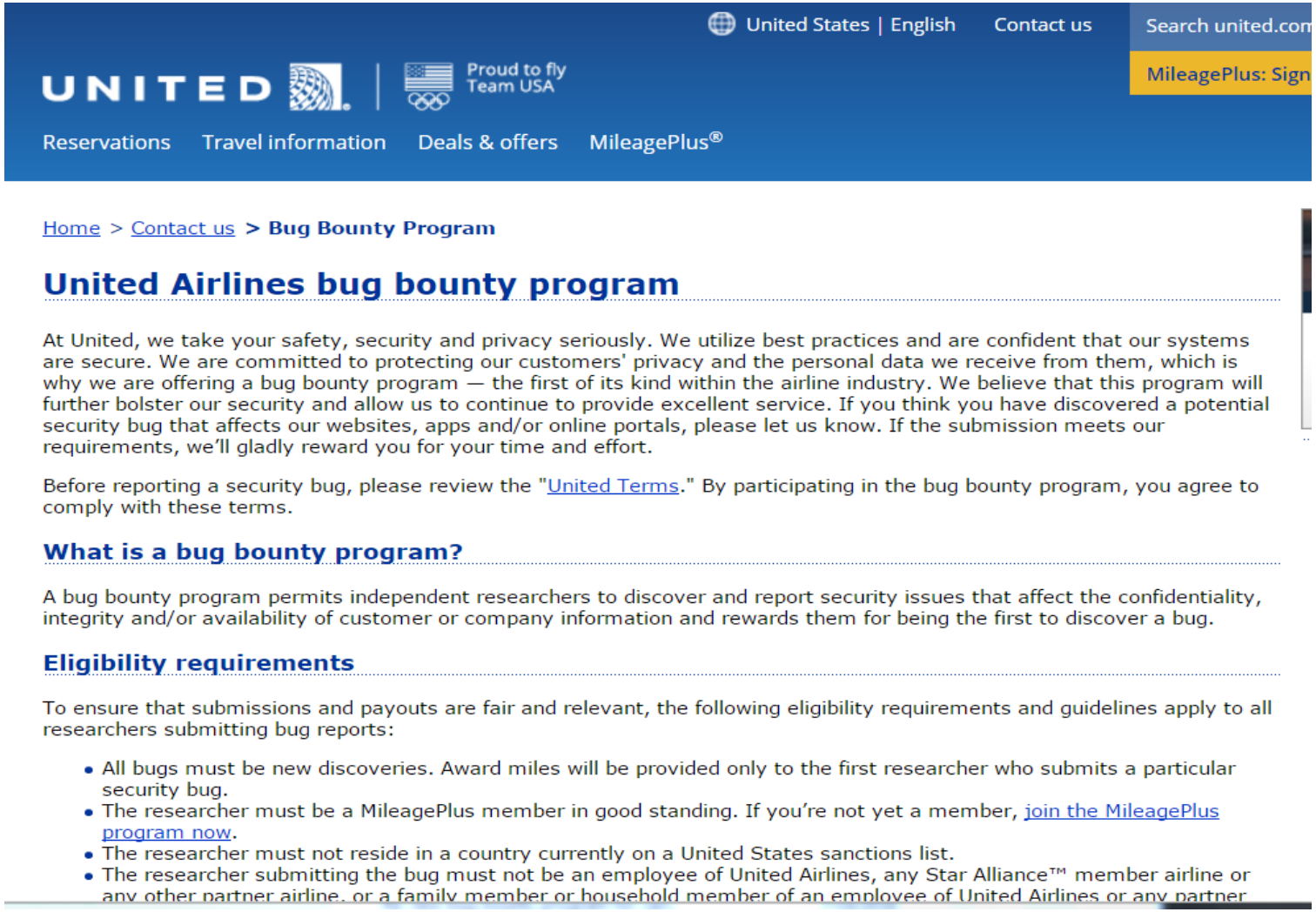
First major automaker (aside from Tesla) to issue guidelines promising not to sue researchers.

On January 5, General Motors quietly flipped the switch on Detroit's first public security vulnerability disclosure program, launched in partnership with the bug bounty and disclosure portal provider HackerOne. General Motors Chief Cybersecurity Officer Jeff Massimilla told Ars the new portal was a first step in creating relationships with outside security researchers and increasing the speed with which GM discovers and addresses security issues.

"We very highly value third-party security research," Massimilla said. He explained that under the program, those third parties can reveal vulnerabilities they find with the guarantee that GM will work with them and not take legal action—as long as they follow the fairly straightforward guidelines posted on the program's portal.

Arstechnica SEAN GALLAGHER - **1/8/2016, 10:44 AM**

United Airlines



https://www.united.com/web/en-US/content/Contact/bugbounty.aspx

United Airlines waits 6 months to patch critical flaw submitted to bug bounty program

It took six months after submitting a critical flaw to United Airlines bug bounty program, and a threat of public disclosure, before the serious vulnerability was patched.

A security researcher found and reported a critical vulnerability to United Airlines that could allow an attacker to “completely manage any aspect of a flight reservation using United’s website.” He claims United Airlines, which announced a bug bounty program about six months ago, didn’t deploy a fix for five months and only plugged the holes after he threatened to publicly disclose the unpatched vulnerability.

…

Bug bounty programs are important for creating better security, but Westergren added, “Running one effectively is critical.” Although his “intention to publicly disclose the vulnerability appears to have pressured United to fix it,” he suspects “that the request for comment by media personnel ultimately forced them to take the necessary action.”

United launches bug bounty, but in-flight systems off limits

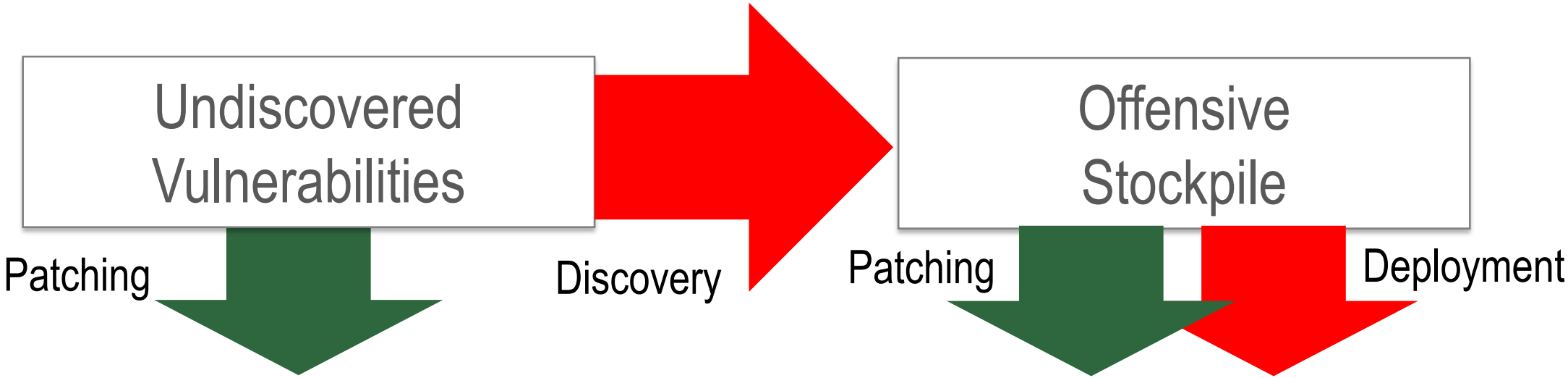
- How (and why) to launch a bug bounty program
- Extortion or fair trade? The value of bug bounties

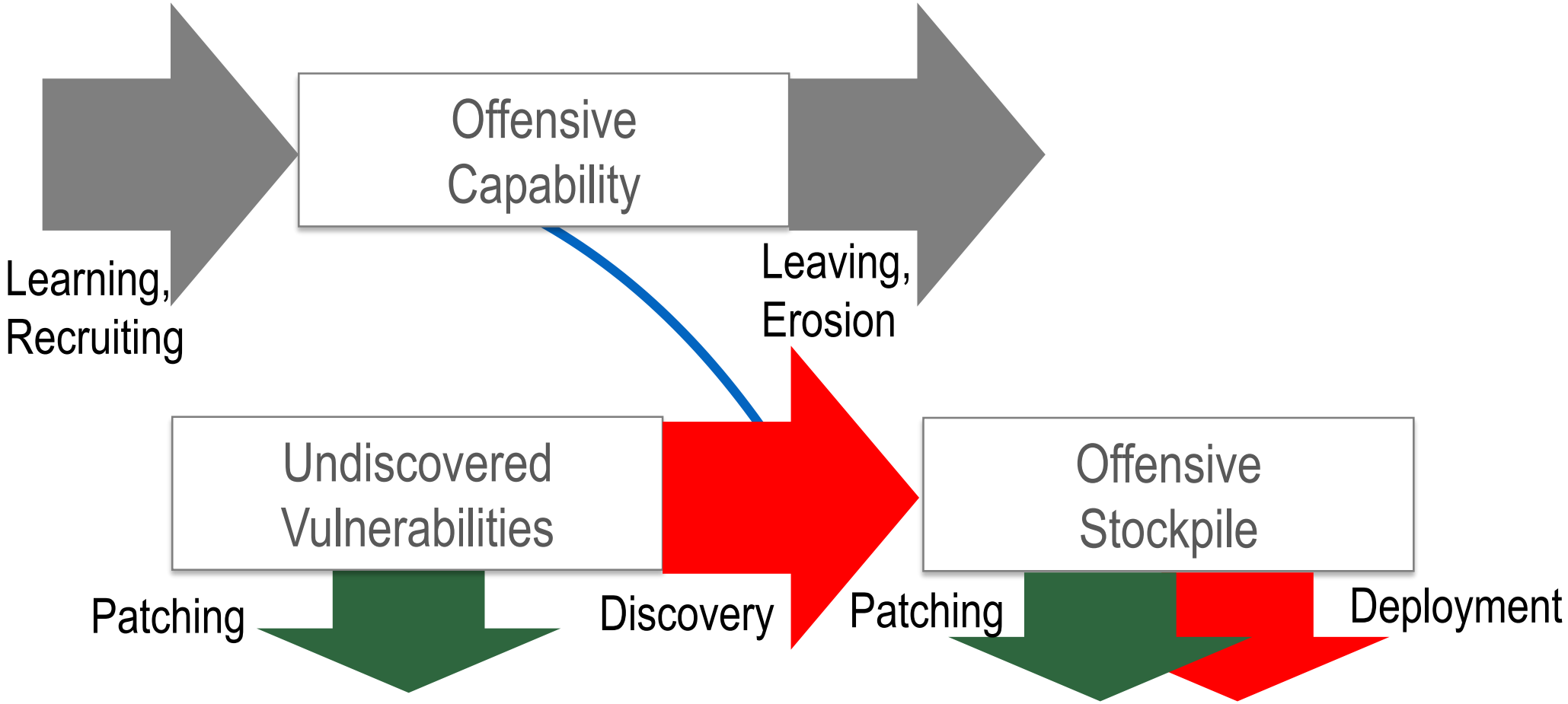
http://www.computerworld.com/article/3007305/cybercrime-hacking/united-airlines-waits-6-months-to-patch-critical-flaw-submitted-to-bug-bounty-program.html

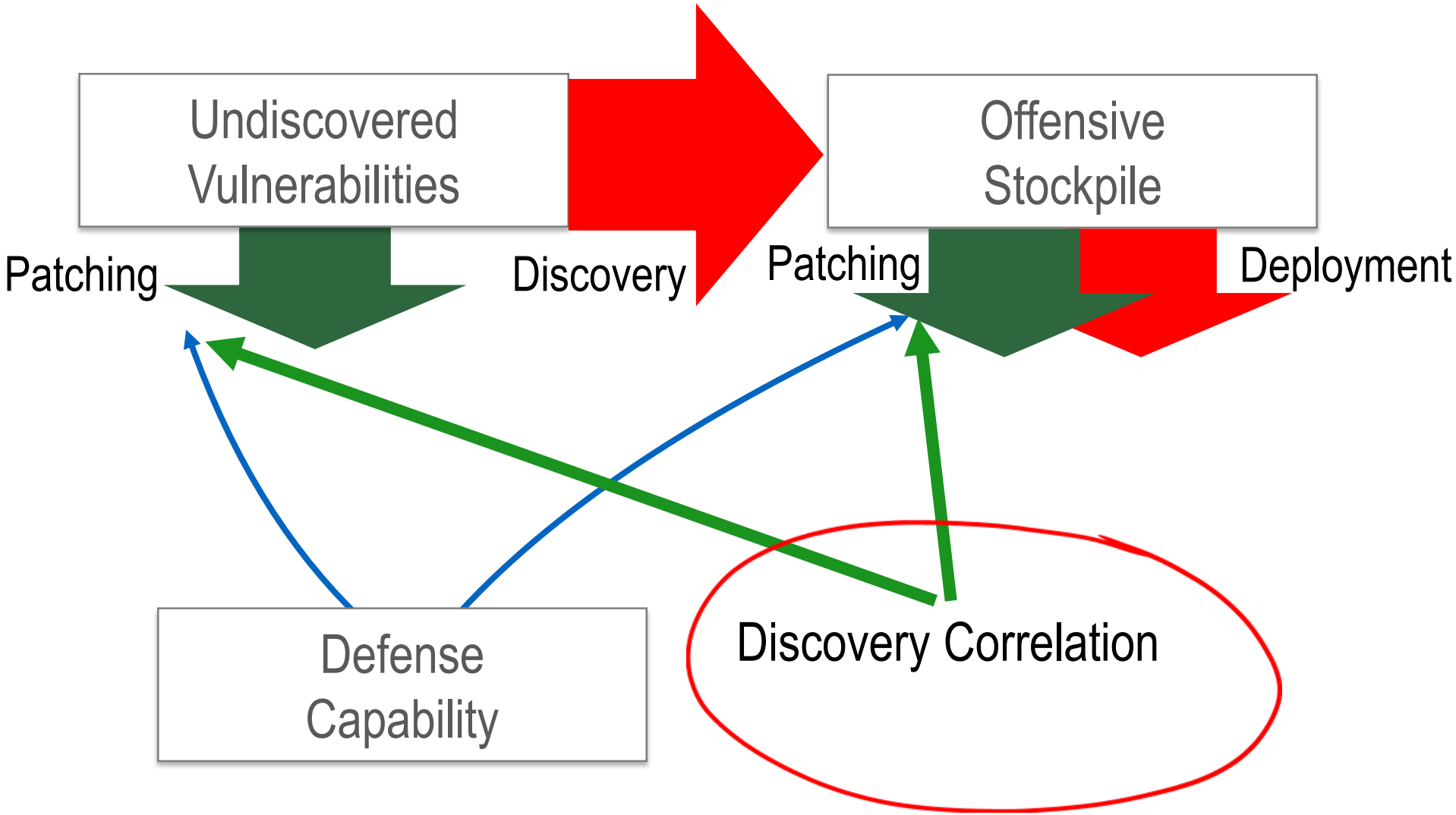
MAKING THINGS BETTER: A SYSTEMS VIEW OF CYBERSECURITY

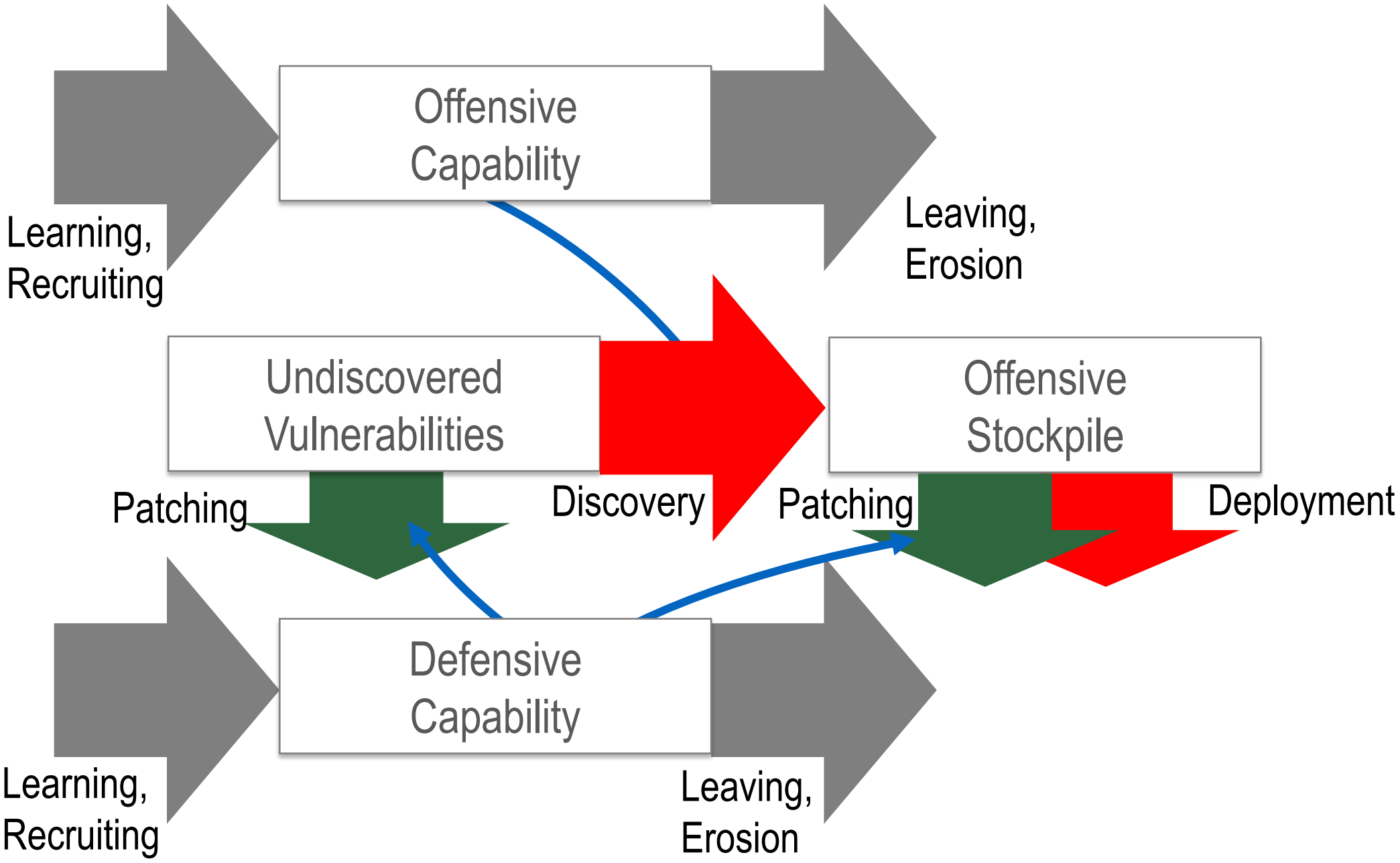
-REDUCING VULNERABILITIES: PLAYING BETTER DEFENSE


Undiscovered
Vulnerabilities
Patching

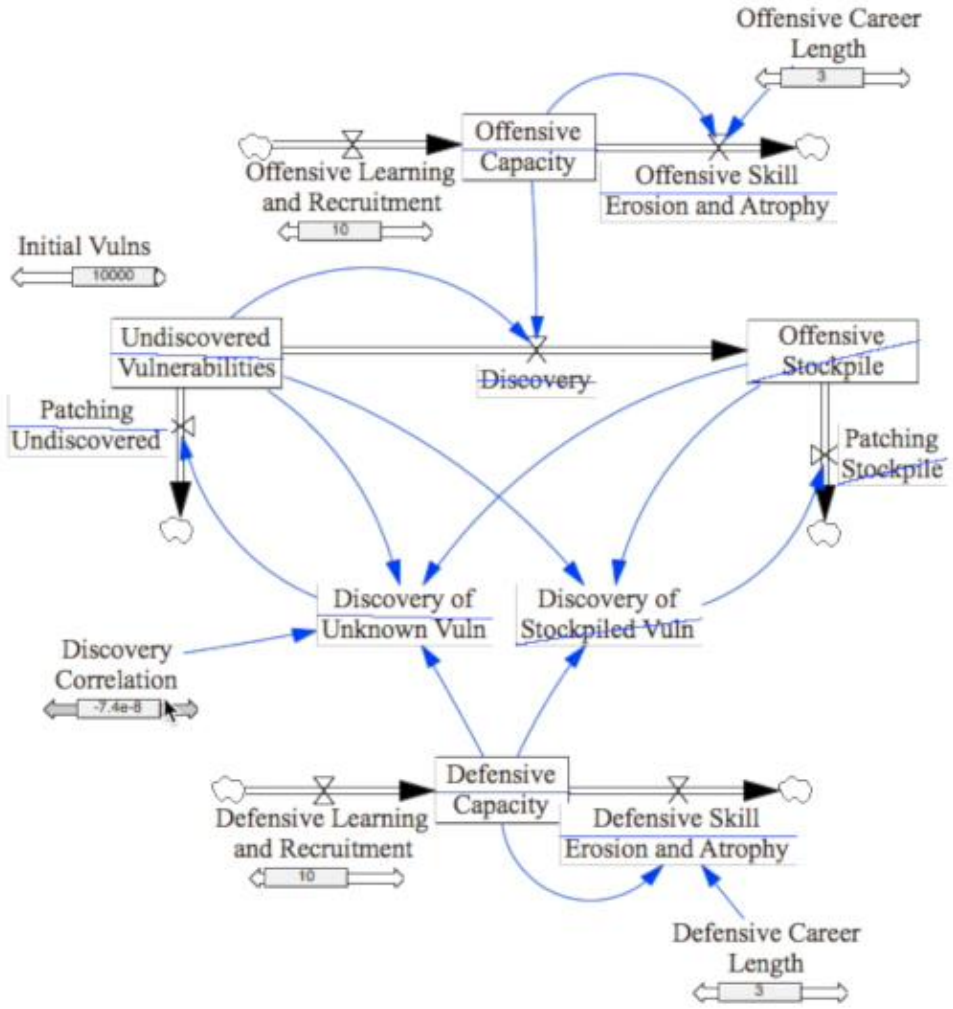

Undiscovered Vulnerabilities
Patching
Discovery
Offensive Stockpile
Patching
Deployment

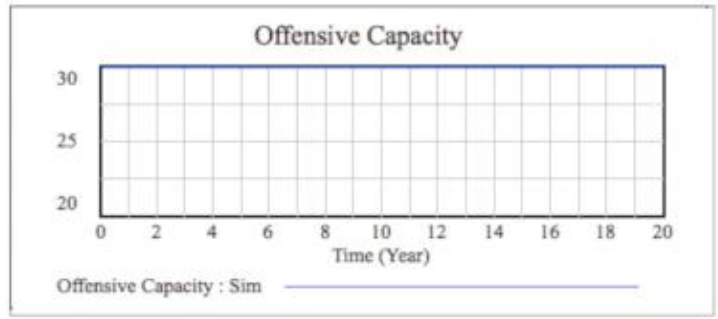

Offensive
Capability
Learning,
Recruiting
Leaving,
Erosion
Undiscovered
Vulnerabilities
Offensive
Stockpile
Patching
Discovery
Patching
Deployment

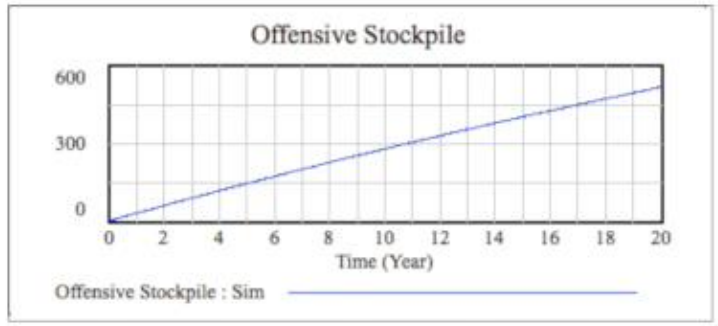

Undiscovered Vulnerabilities
Offensive Stockpile
Patching
Discovery
Patching
Deployment
Defense Capability
Discovery Correlation

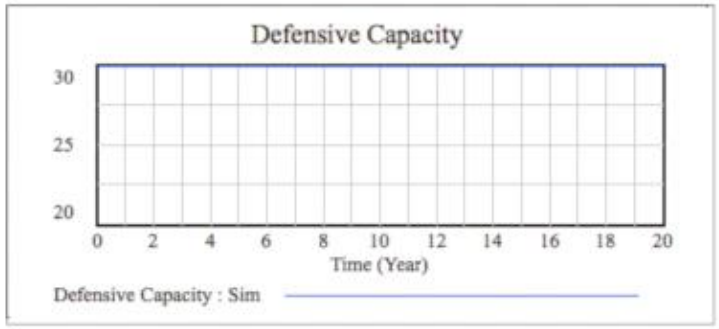

Offensive Capability
Learning, Recruiting
Leaving, Erosion
Undiscovered Vulnerabilities
Offensive Stockpile
Patching
Discovery
Patching
Deployment
Defensive Capability
Learning, Recruiting
Leaving, Erosion

THE 0DAY MARKET SYSTEM DYNAMICS MODEL





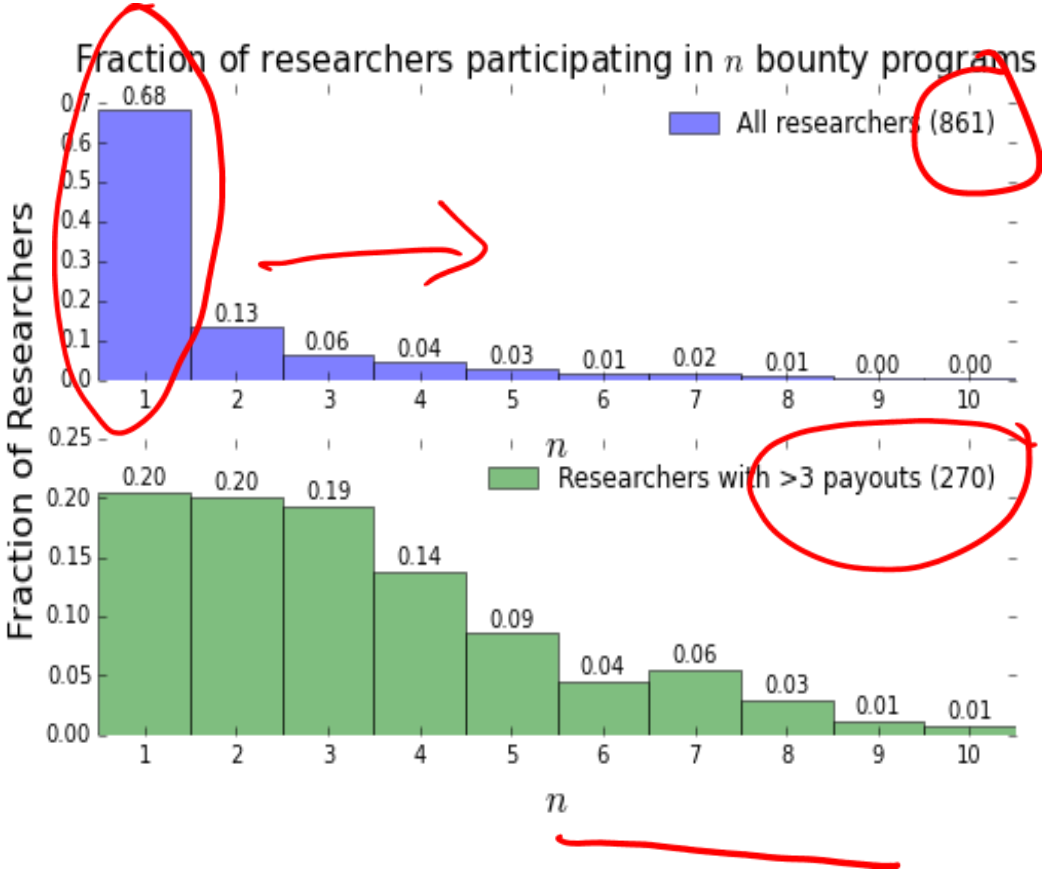


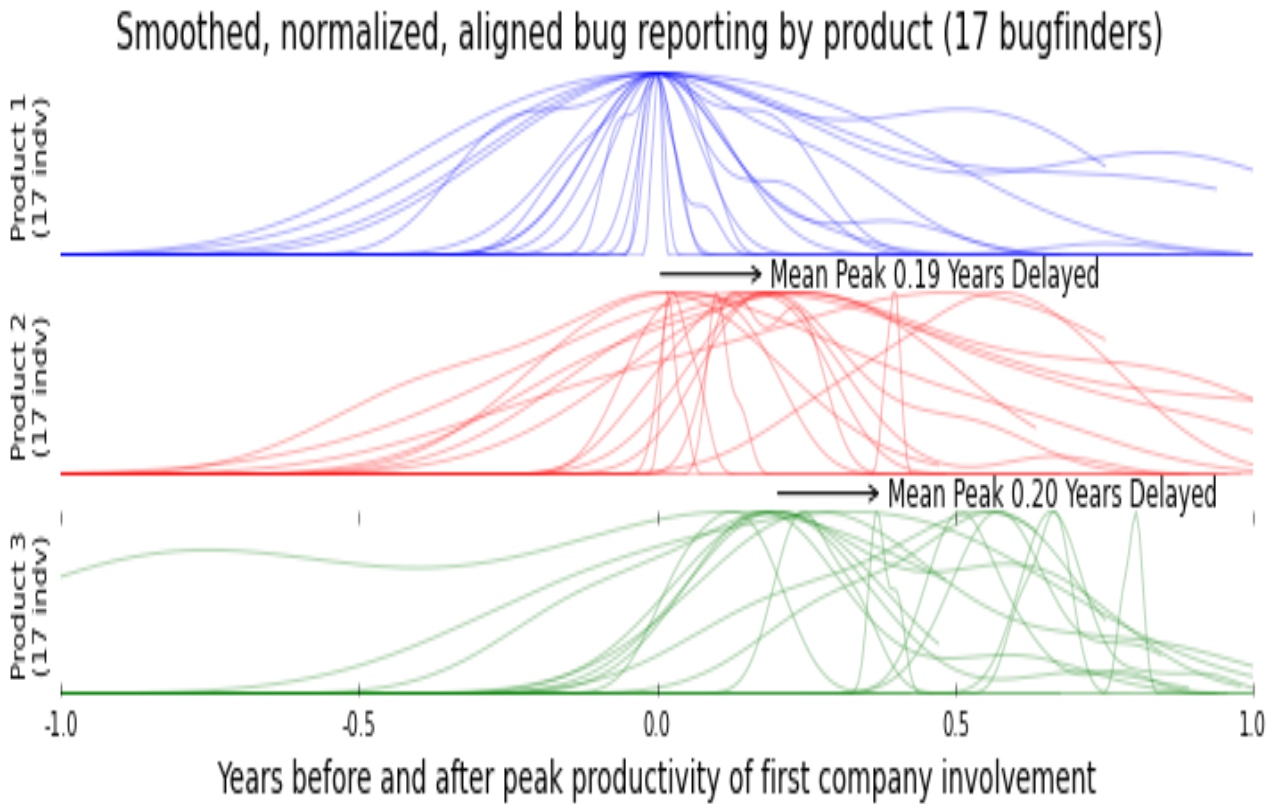


MAKING THINGS BETTER: A SYSTEMS VIEW OF CYBERSECURITY

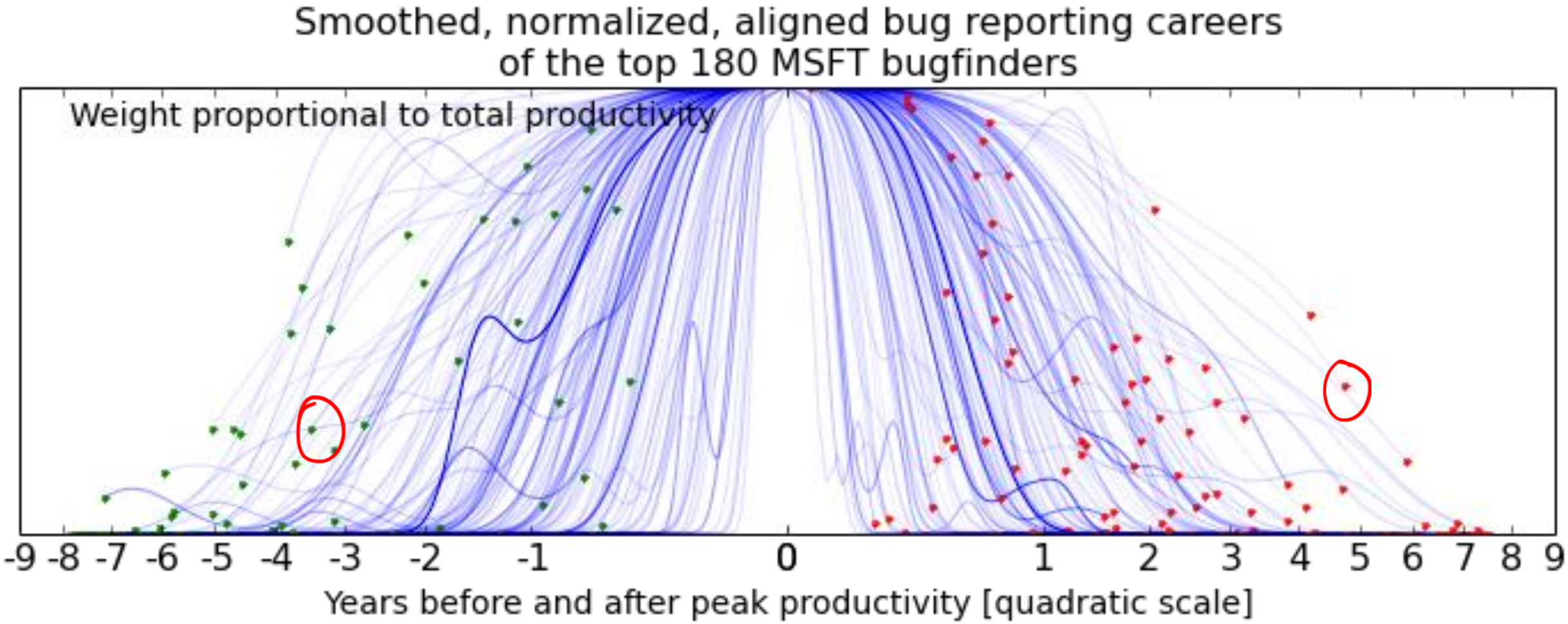
-THE WHITE HAT WORKFORCE

Defense Market Workforce : Bug Bounty Programs

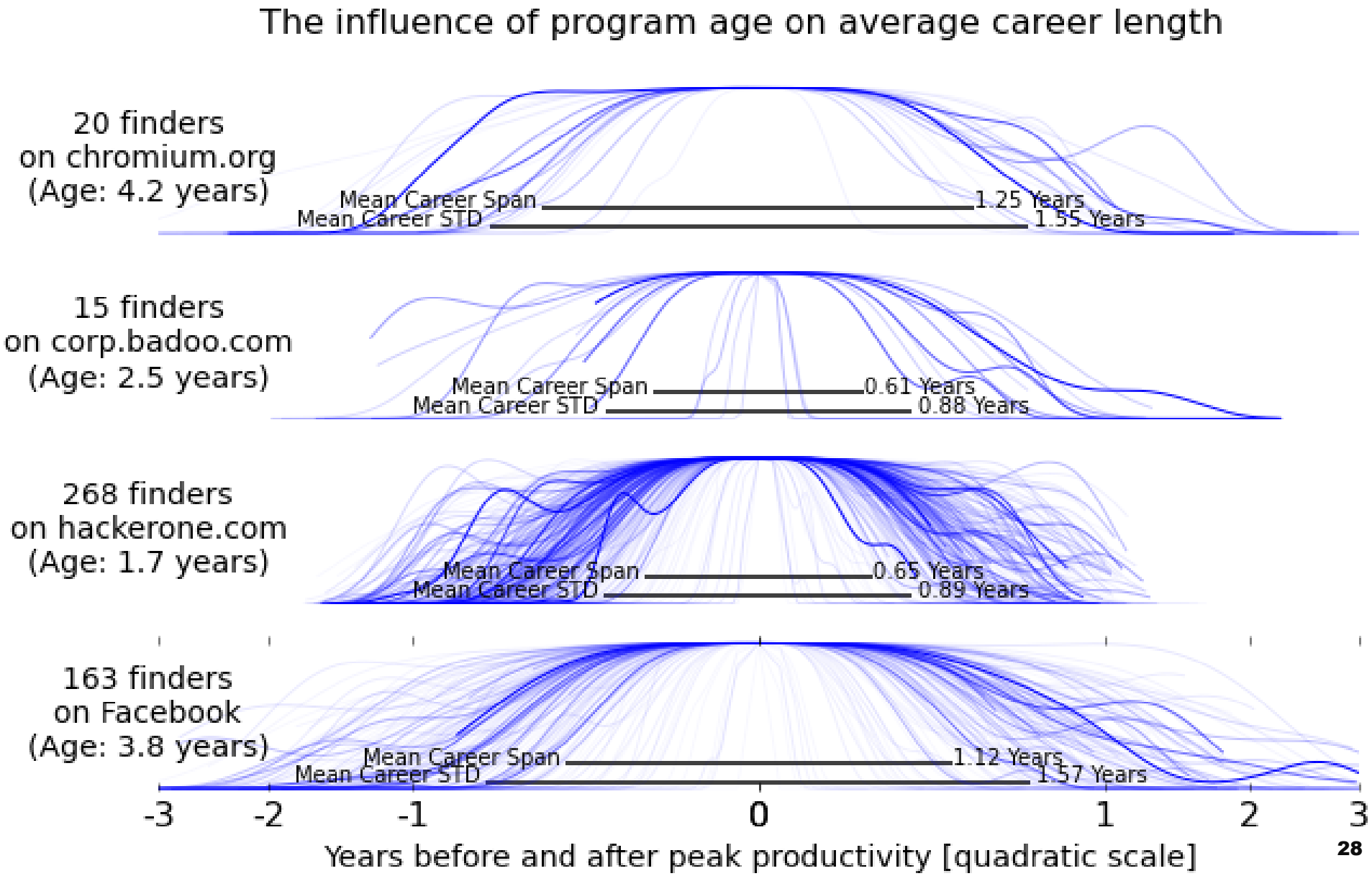




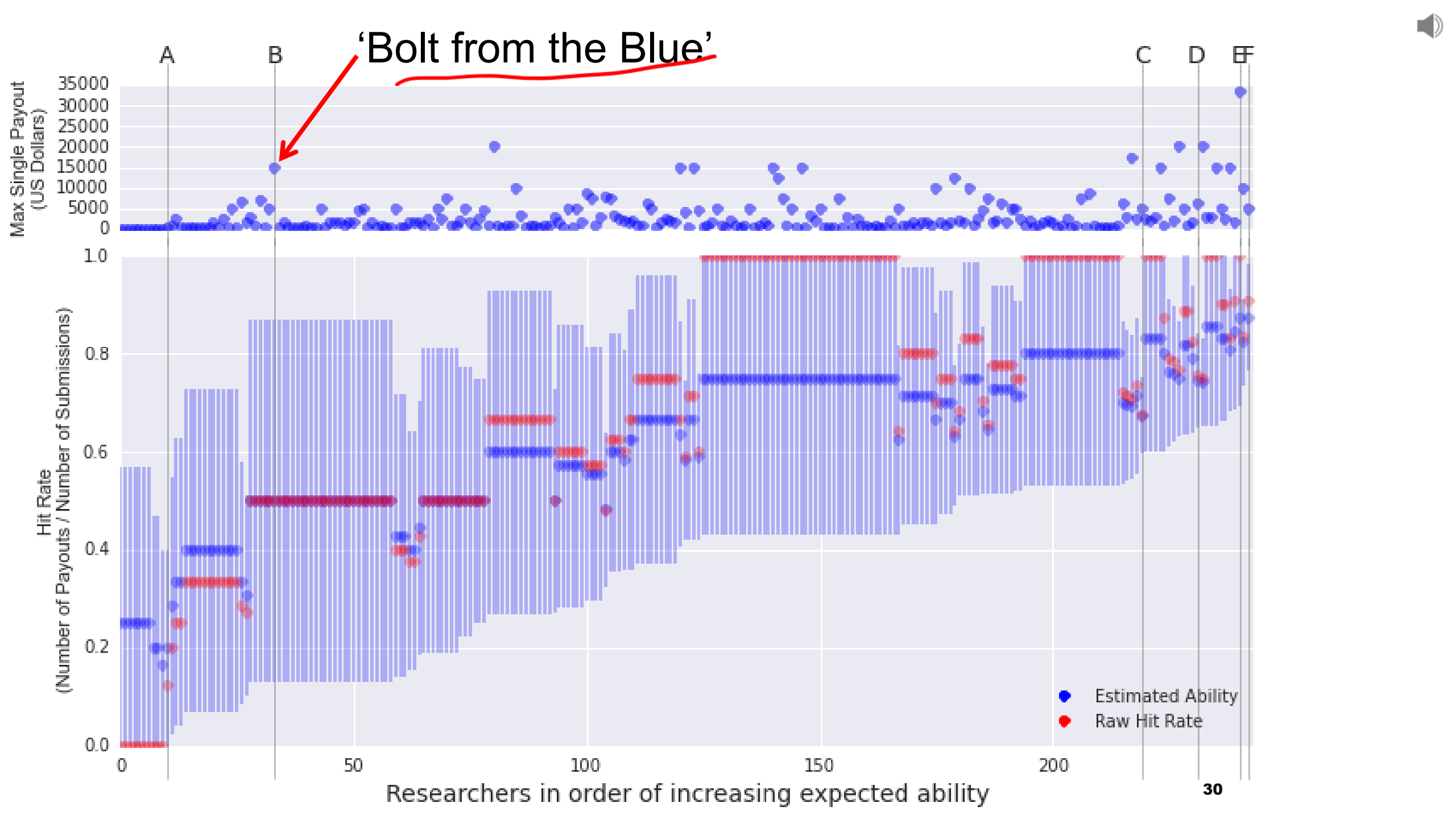
The Defense Market Workforce: Career Lifespan



Defense Market Workforce: Program Age vs. Career Lifespan

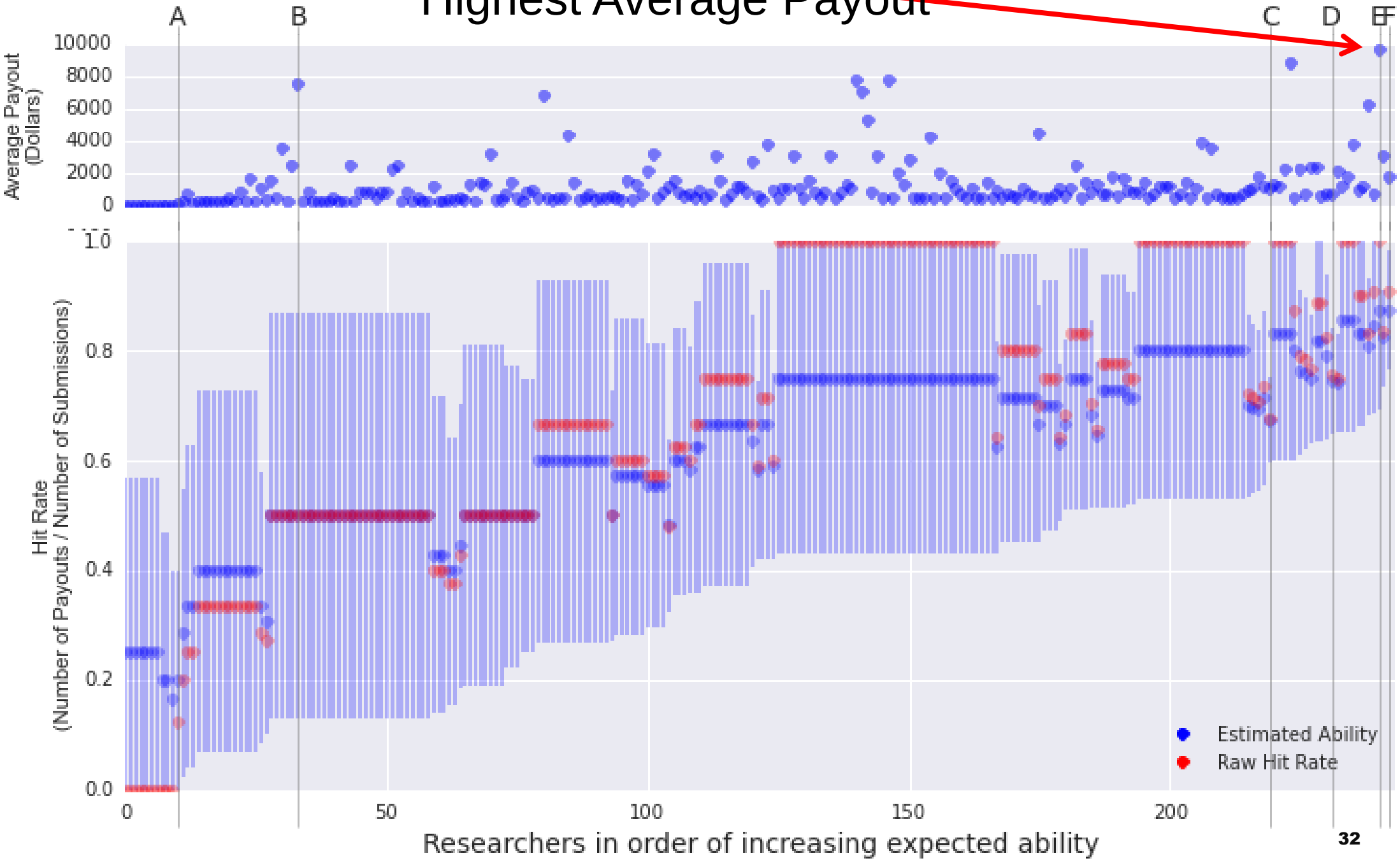



Lowest Expected Hit Rate
A
B
C
D
E
F
Number of Submissions
10^2
10^1
10^0
Hit Rate (Number of Payouts / Number of Submissions)
1.0
0.8
0.6
0.4
0.2
0.0
0
50
100
150
200
Researchers in order of increasing expected ability
Estimated Ability
Raw Hit Rate


‘Bolt from the Blue’
A
B
C
D
E
F
Max Single Payout (US Dollars)
35000
30000
25000
20000
15000
10000
5000
0
Hit Rate (Number of Payouts / Number of Submissions)
1.0
0.8
0.6
0.4
0.2
0.0
0
50
100
150
200
Researchers in order of increasing expected ability
Estimated Ability
Raw Hit Rate

Largest Number of Submissions

Highest Average Payout



Insights from a Systems View

- Understanding the tools and techniques of finding vulnerabilities helps to improve security
- Creating incentives for tools and techniques for vulnerability discovery is a more efficient way for defenders to drain the offensive stockpile
- Bug bounties are effective way to help find vulnerabilities, especially in less mature software
- Understanding the researcher/hacker/security workforce will help with defense and offense
- All organizations can learn from bug bounty programs

MAKING THINGS BETTER: A SYSTEMS VIEW OF CYBERSECURITY

-EXAMINING METRICS AND ROI

The Dynamics of Cyber Threats and Security

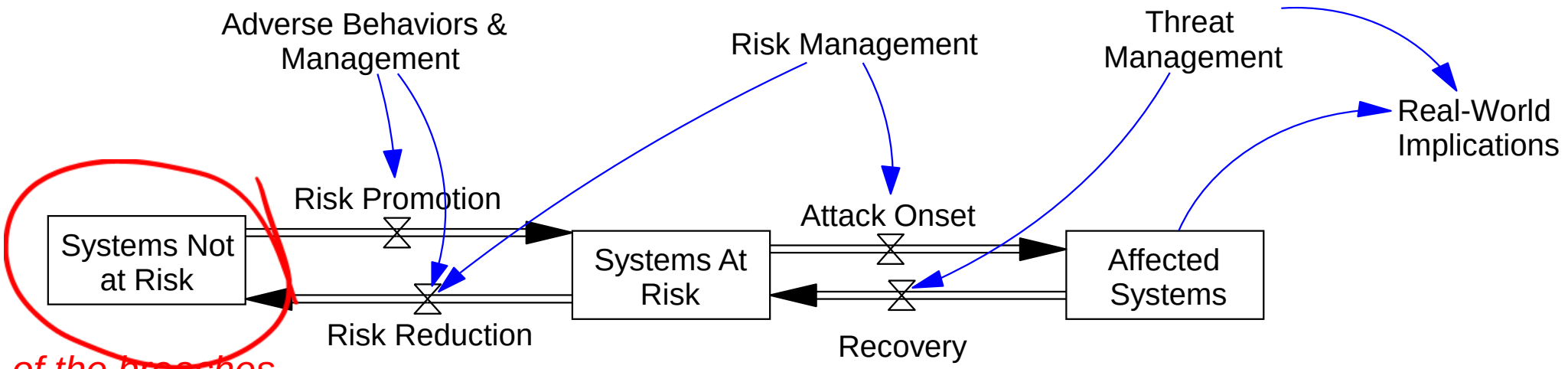
60% of all incidents were attributed to errors made by System Administrators

67% were aided by significant errors (of the victim)

170 Million malware attacks – 5 malware events every second

64% resulted from hacking

38% utilized Malware



Over 80% of the breaches had patches available for more than 1 year

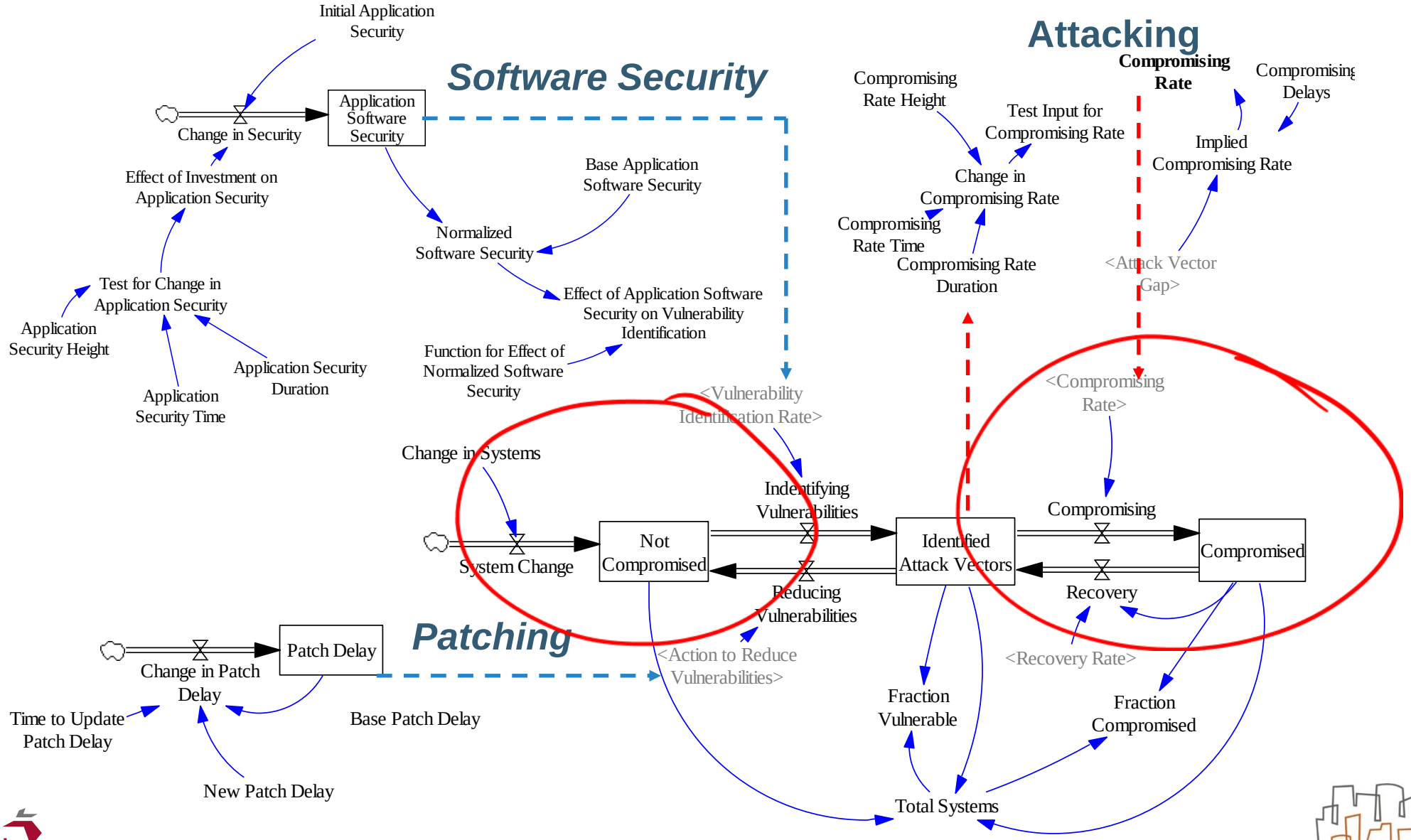
99.9% of the exploited vulnerabilities were compromised more than a year after the patch was available

75% of cases go undiscovered or uncontained for weeks or months

On average, *an attack is only discovered after it has been active 243 days*

- Verizon Data Breach Report 2009
- Verizon Data Breach Report 2015

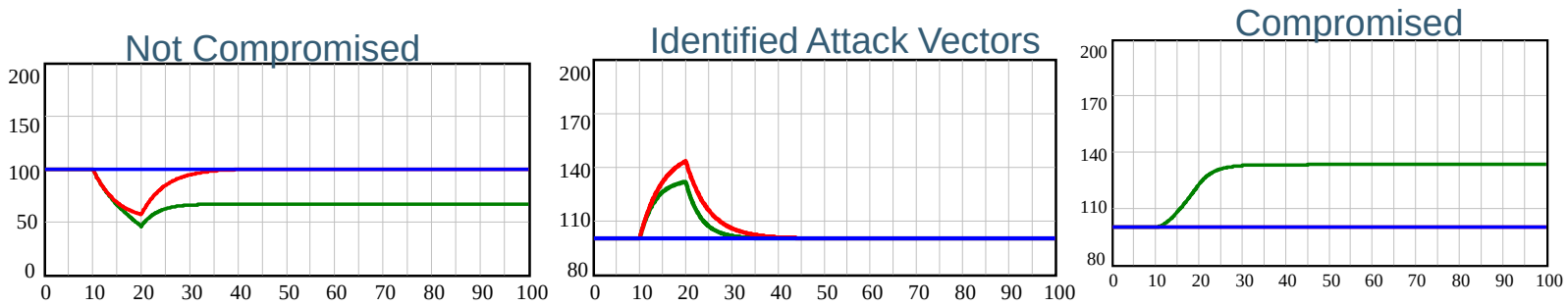
Modeling Software Quality and Patching Techniques



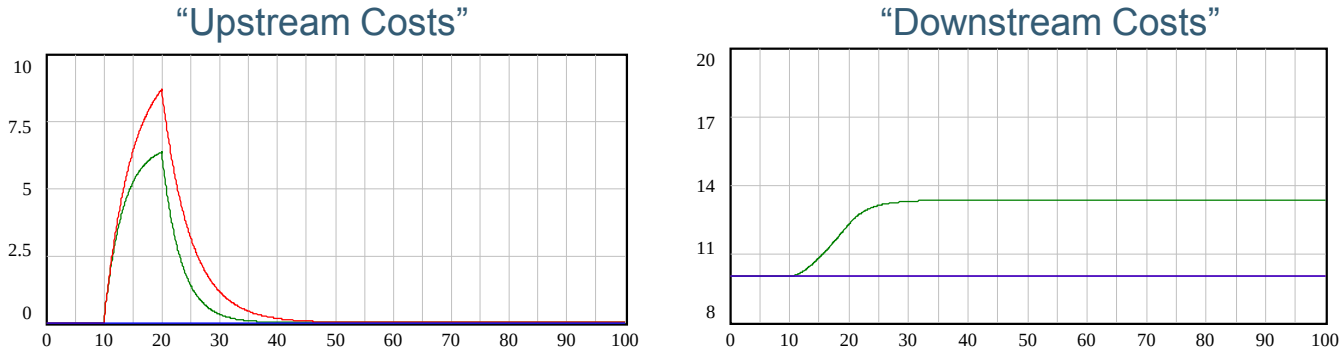
Cyber Risk Evaluation and Metrics – Examining ROI

Blue is base case; red case is patching with configuration standards; green is current case

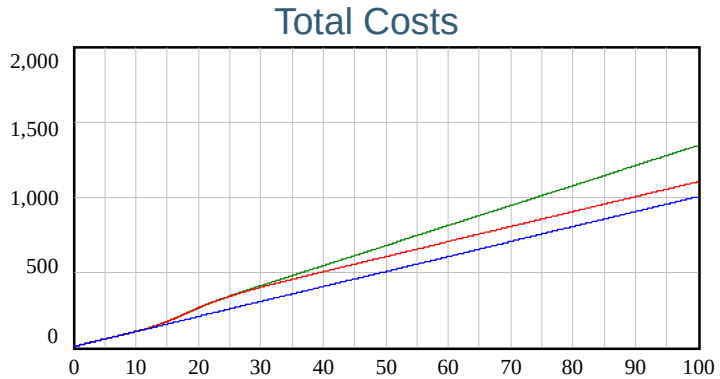
Technical



Managers



Senior Management (CIO)



MANAGEMENT AND GOVERANCE OF CYBERSECURITY

-EDUCATION
-CYBERSECURITY FRAMEWORKS

Management Level Cyber Education

	Topic	Description	Type of Session(s)
Cyber Security Background	Compliance, Security & Risk	What is the difference among these areas? How should a board view them? Prioritize them? Manage them?	Lecture
	Cyber Security as a System	Overview of Preventative, Detective and Response (Compensating) controls – and discussion of how they are necessary and work as a system.	Lecture, Exercise/Simulation
Fiduciary Responsibility	The Board & Executive Management	How often and how much time to spend on Cyber Security issues at the Board level. Composition of the Board. The Role of Board Committees. Reporting and executive staff interaction. Look at the issues, processes, etc. from both sides. Certification, Frameworks (NIST).	Case Study Best Practices
Management	Cyber Risk	Various approaches and frameworks that an organization might use to manage Risk issues related to cyber activity. Understand the strengths & weaknesses of the approaches, what to expect from management staff, etc.	Lecture Case Study
	Investment	Approaches to allocating investment (time and funds) across business and cyber security items – and also across various cyber security areas.	Best Practices
	People	Models for interaction between the Board, Executive Business Management, the Chief Information Officer and the Chief Information Security Officer.	Case study Best Practices

NIST CYBERSECURITY FRAMEWORK CORE

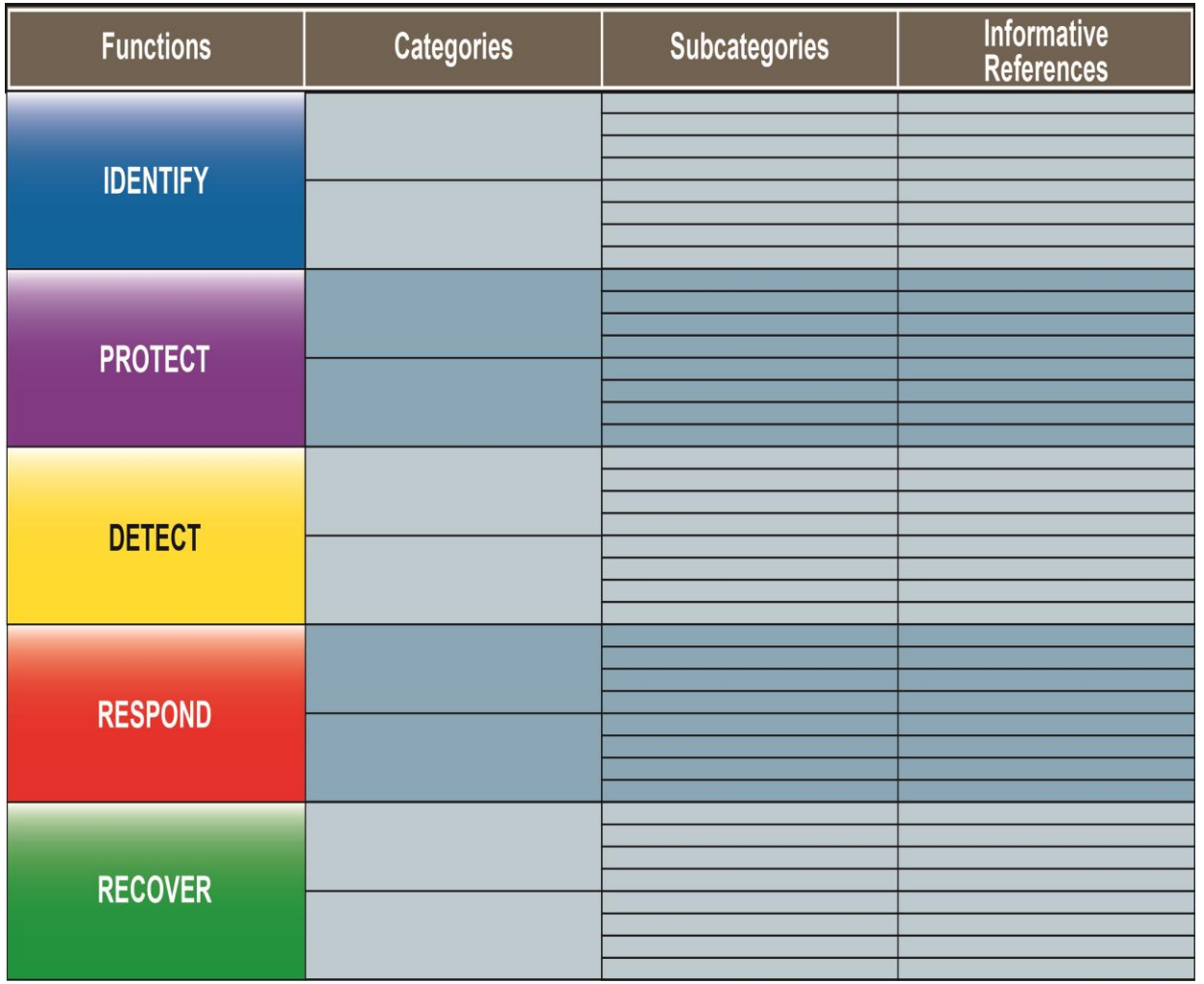
What processes and assets need protection?

What safeguards are available?

What techniques can identify incidents?

What techniques can contain impacts of incidents?

What techniques can restore capabilities?



http://www.nist.gov/cyberframework/

FRAMEWORK CORE SAMPLE

PROTECT (PR)	**Access Control (PR.AC):** Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are managed for authorized devices and users	• **CCS CSC** 16 • **COBIT 5** DSS05.04, DSS06.03 • **ISA 62443-2-1:2009** 4.3.3.5.1 • **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 • **ISO/IEC 27001:2013** A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3 • **NIST SP 800-53 Rev. 4** AC-2, IA Family
		PR.AC-2: Physical access to assets is managed and protected	• **COBIT 5** DSS01.04, DSS05.05 • **ISA 62443-2-1:2009** 4.3.3.3.2, 4.3.3.3.8 • **ISO/IEC 27001:2013** A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3 • **NIST SP 800-53 Rev. 4** PE-2, PE-3, PE-4, PE-5, PE-6, PE-9
		PR.AC-3: Remote access is managed	• **COBIT 5** APO13.01, DSS01.04, DSS05.03 • **ISA 62443-2-1:2009** 4.3.3.6.6 • **ISA 62443-3-3:2013** SR 1.13, SR 2.6 • **ISO/IEC 27001:2013** A.6.2.2, A.13.1.1, A.13.2.1

http://www.nist.gov/cyberframework/

CURRENT USES

The NIST Cybersecurity Framework is designed to use in business and cybersecurity operations:

- Self-Assessment, Risk Assessment, Gap Analysis, Budget & Resourcing Decisions
- Standardizing Communication Between Business Units
- Communicate Requirements with Partners and Suppliers
- Describe Applicability of Products and Services
- Identify Opportunities for New or Revised Standards
- As a Part of Cybersecurity Certifications
- Categorize and Organize Requests for Proposal Responses

The Framework also supports:

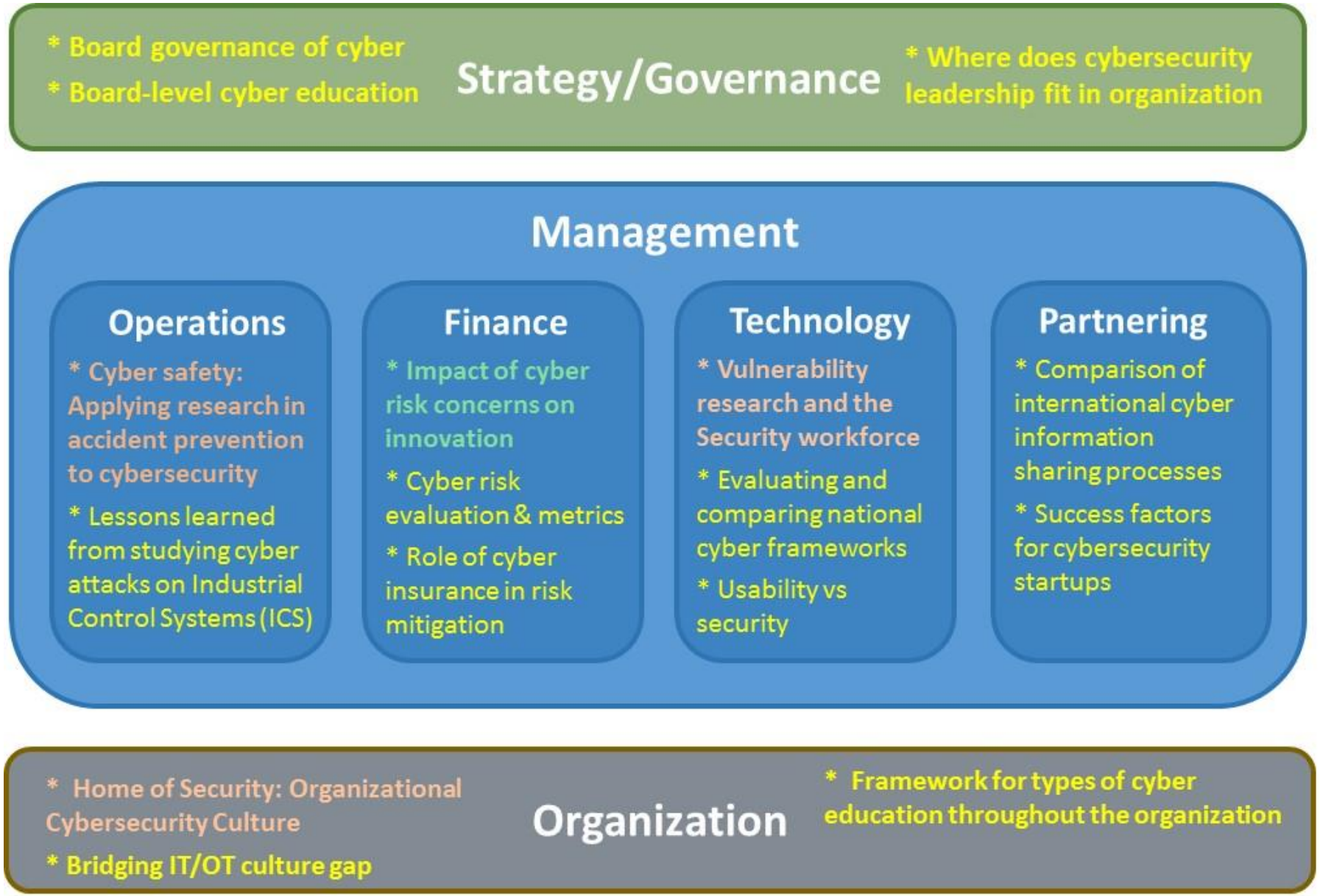
- Consistent dialog, both within and amongst countries
- Common platform on which to innovate, and identify market opportunities

http://www.nist.gov/cyberframework/

Additional Activities

- Analysis of offensive markets and security researchers
- Understanding offensive and defensive markets through the eyes of practitioners
- Policy analysis: Vulnerability markets and the DOD
- Analysis of threat sharing initiatives
- Publications, training and education

Current Active $(IC)^3$ Projects



INTERDISCIPLINARY CONSORTIUM for IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY

MIT Sloan MANAGEMENT

$(IC)^3$

*** Mature research (papers available)**
*** In-progress research (informal initial results)**
*** Start-up research**

For more information please contact:
msiegel@mit.edu
ic3.mit.edu

THANK YOU

Michael Siegel

Principal Research Scientist – Sloan School of Management