Complexity of Organizational Cybersecurity Capability Development

Mohammad Jalali, PhD
Research Scientist, MIT Sloan School of Management
jalali@mit.edu

2016 MIT Information and Communication Technologies Conference
April 20, 2016
Welcome to MIT! So, let’s start with a quiz! 😊
Welcome to MIT!  So, let’s start with a quiz! 😊

What percentage of the breaches had patches available for more than a year?

What percentage of cases go undiscovered for months?
Welcome to MIT! So, let’s start with a quiz! 😊

What percentage of the breaches had patches available for more than a year?

over 80%

What percentage of cases go undiscovered for months?

about 75%

Based on Verizon Data Breach Report
A common news:
Yet another hospital got infected with a ransomware...

Just during the last few weeks, many hospitals in the US got hit with ransomware.
A common news:
Yet another hospital got infected with a ransomware...

In the case of *MedStar Health Network* (operating 10 hospitals in MD and DC)

• The US gov’t, Red Hat, and others issued urgent warnings about the security flaw in **Feb 2007, Mar 2010** and again **Apr 2016**!

• Fixing the problem involved:
  • installing an *available* update, or
  • manually deleting *two lines* of software code.
Why do we continuously see such behaviors in organizations?
Cybersecurity, a complex system

No doubt about the complexity of cybersecurity, with various sub-systems that are interconnected, forming feedback loop mechanisms, and potential delays... which create non-linear behaviors in the system.

➡️ How can we better understand such complexity?
Cybersecurity, a complex system

Research already shows that making a decision drawn from a complex web of causal pathways joint with delays is a task that the human brain is not well-equipped to do.
‘Systems Science’ can help

There are already quite a few systems science projects to help simulate and understand the complexity of a cyber attack.

Their common *(claimed)* objectives:
- measure the ability of an organization to respond to a cyber attack
- train employees with effective preventive practices
- help them make decisions with limited information
However, the majority of current research projects focus on the technical aspects of cybersecurity.

What’s missing is the focus on ‘organizational and strategic’ aspects of cybersecurity, particularly on cybersecurity capabilities development.
MIT-(IC)³ Approach

In a series of projects, we focus on organizational cybersecurity and use Systems Science, particularly System Dynamics Modeling to:

- understand ‘unfolding’ of situations,
- eliminate limitations of linear logics,
- anticipate & predict modes of the system,
- explore the range of unintended consequences
Developing simulation models that are

Simply complex!
  • As simple as possible, but no simpler!

Educational to help managers understand:
  • feedback loop mechanisms, and
  • potential delays in the systems
Example: a dynamic model

(simplified version for presentation to illustrate the main feedback loops)
Building cybersecurity (CS) capabilities

CS capabilities

*Examples:*
- Organizational changes
- Security culture
- Awareness training
- Technical infrastructure
- etc.
Managers often have bias in perceiving the level of organizational CS capabilities.
Management bias and perception

Managers often have bias in perceiving the level of organizational CS capabilities.

Results from (IC)^3 surveys help estimate this bias.
Observed shortfalls in CS capabilities
Observed shortfalls in CS capabilities

In a neat decision making scenario, managers compare their perception with the organization vision (if any) and realize a shortfall...
Motivation for CS capabilities development

Once they perceive a Shortfall in CS capability, they are motivated and are willing to invest in CS capability development.
Motivation for CS capabilities development

Once they perceive a Shortfall in CS capability, they are motivated and are willing to invest in CS capability development.
Motivation for CS capabilities development

Once they perceive a Shortfall in CS capability, they are motivated and are willing to invest in CS capability development.

This is virtuous cycle which results in filling out the gap between the perception and organizational vision.
Return of investment, a potential barrier

However, the story isn’t that simply good!

A stronger driver of managers’ motivation to invest in CS capability development is ROI!

But they usually can’t observe the ROI of security spending.
Return of investment, a potential barrier

However, the story isn’t that simply good!

A stronger driver of managers’ motivation to invest in CS capability development is ROI!

But they usually can’t observe the ROI of security spending.
However, the story isn’t that simply good!

A stronger driver of managers’ motivation to invest in CS capability development is ROI!

But they usually can’t observe the ROI of security spending.
Cyberattack and uncertainty

• Managers often make decisions based on beliefs concerning the likelihood of ‘uncertain’ events such as cyber-attacks.

• But, overall, humans are not good in understanding **low probability, high consequences** scenarios.

• Behavioral economics as well as judgement and decision making research already show that managers rely on a set of heuristics—to make decisions in ‘uncertain’ situations—which can potentially cause systematic errors.
Cyberattack and uncertainty

• The intuitive assessment of probability is often based on perceptual quantities (e.g., distance, scale, or size);

  Example: the more sharply you can see the object, the closer it appears to be. But what if the visibility is poor... don’t you underestimate the distance?

• In dealing with improbable gains, managers are often risk seeking, but in dealing with ‘unlikely losses’, they are risk-averse.
Return of investment, a potential barrier

Psychologically, if nothing happens, what’s the motivation to invest in security?

- Hence, many managers often don’t envision the risk properly.
Return of investment, a potential barrier

Psychologically, if nothing happens, what’s the motivation to invest in security?

- Hence, many managers often don’t envision the risk properly.

*Remember?*

Over 80% of the breaches had patches available for more than a year!
75% of cases go undiscovered for months!
Return of investment, a potential barrier
Cyber attacks, from onset to impact your systems
How CS capabilities affect your business
A very common scenario

Due to delays in capability development and misunderstanding of the risks, if managers start investing in capability development after detecting an attack:

- they are not able to **recover properly in time**
- they are in danger of **facing with other attacks in near future**
A very common scenario

cyberattacks

Profits (M$)
It’s not rocket science! Right?
It’s not rocket science! Right?

Check out how many more organizations fall into this trap!
Discussion

• Finding the sweet spot in the level of investment in CS capability development isn’t an easy task!

• Nonlinearities and tipping points may exist due to inertia and path-dependence in systems.

• Similar experiments in capability development in other fields also show that the majority of managers fail to grasp this insight.
Thank you!

jalali@mit.edu

@msjalali

@MIT_IC3