# Assessing and Improving the People Aspect of Cybersecurity

## David A. Wagle Northcentral University

TIM-8301: Principles of Cybersecurity Dr. Bill Souza

April 25, 2021

# Introduction

Understanding the Impact of Cybersecurity

* Large companies are large targets

1. Uber, Facebook, Financial companies and others have lost control of billions of customer records in recent years (Zadeh et al., 2020). Between the cost of lost data, fines, lawsuits, and identity theft monitoring costs of impacted customers, the cost to organizations can be in the hundreds of millions of dollars.

# Introduction

Understanding the Impact of Cybersecurity

* + Large companies are large targets
  + Cybersecurity breaches have multi-factorial negative impacts

1. Uber, Facebook, Financial companies and others have lost control of billions of customer records in recent years (Zadeh et al., 2020). Between the cost of lost data, fines, lawsuits, and identity theft monitoring costs of impacted customers, the cost to organizations can be in the hundreds of millions of dollars.
2. Cybersecuirty breaches reduce customer and investor trust, negatively impact market value, negatively impact share price, and have the potential to negatively impact customer revnue. A 2014 report estimated that the cost to an institution averages $201.21 (Zureich & Graebe, 2015).

# Introduction

Understanding the Impact of Cybersecurity

* + Large companies are large targets
  + Cybersecurity [breaches](#_bookmark34) have multi-factorial negative impacts

## Legal implications can be severe

1. Uber, Facebook, Financial companies and others have lost control of billions of customer records in recent years (Zadeh et al., 2020). Between the cost of lost data, fines, lawsuits, and identity theft monitoring costs of impacted customers, the cost to organizations can be in the hundreds of millions of dollars.
2. Cybersecuirty breaches reduce customer and investor trust, negatively impact market value, negatively impact share price, and have the potential to negatively impact customer revnue. A 2014 report estimated that the cost to an institution averages $201.21 (Zureich & Graebe, 2015).
3. Successful litigation against companies found to have suffered preventable data breaches have taken a variety of forms: shareholder suits to recover losses in stock value; securities fraud class action suits; class actions suits by those who’s data was compromised; and enforcement actions by government regulatory bodies (Hooker & Pill, 2016).

# Data Breach Causes

How We Lose Control

* + There are a variety of factors that contribute to data loss

1. While this is by no means an exhaustive list, it is helpful to think of the potential threats to our data security as a multidimensional surface. Each “face” of that surface represents an additional potential attack vector. The total surface area is the “attack surface” that exposes us to risk which must be mitigated. The ability to address each area of the key areas in organizational, process and technology spaces combines to establish the over-all risk exposre of the organization.

The examples under each sub-heading above are not exhaustive, but are merely examples of the types of components that reside under each category (Dolezel & McLeod, 2019). The overall threat model is the combined impacts of all the surfaces exposed to attack through one or more means.

# Data Breach Causes

How We Lose Control

* + There are a variety of factors that contribute to data loss

### Organizational Factors

* + - * IT Budget
      * Security Culture
      * Vendor Selection Process
      * Employee training

1. While this is by no means an exhaustive list, it is helpful to think of the potential threats to our data security as a multidimensional surface. Each “face” of that surface represents an additional potential attack vector. The total surface area is the “attack surface” that exposes us to risk which must be mitigated. The ability to address each area of the key areas in organizational, process and technology spaces combines to establish the over-all risk exposre of the organization.

The examples under each sub-heading above are not exhaustive, but are merely examples of the types of components that reside under each category (Dolezel & McLeod, 2019). The overall threat model is the combined impacts of all the surfaces exposed to attack through one or more means.

# Data Breach Causes

How We Lose Control

* + There are a variety of factors that contribute to data loss

### Organizational Factors

* + - * IT Budget
      * Security Culture
      * Vendor Selection Process
      * Employee training

### Business Process Exposure

* + - * Number and Complexity of Systems
      * Networking Topology
      * Size of Enterprise

1. While this is by no means an exhaustive list, it is helpful to think of the potential threats to our data security as a multidimensional surface. Each “face” of that surface represents an additional potential attack vector. The total surface area is the “attack surface” that exposes us to risk which must be mitigated. The ability to address each area of the key areas in organizational, process and technology spaces combines to establish the over-all risk exposre of the organization.

The examples under each sub-heading above are not exhaustive, but are merely examples of the types of components that reside under each category (Dolezel & McLeod, 2019). The overall threat model is the combined impacts of all the surfaces exposed to attack through one or more means.

# Data Breach Causes

How We Lose Control

* + There are a variety of factors that contribute to data loss

### Organizational Factors

* + - * IT Budget
      * Security Culture
      * Vendor Selection Process
      * Employee training

### Business Process Exposure

* + - * Number and Complexity of Systems
      * Networking Topology
      * Size of Enterprise

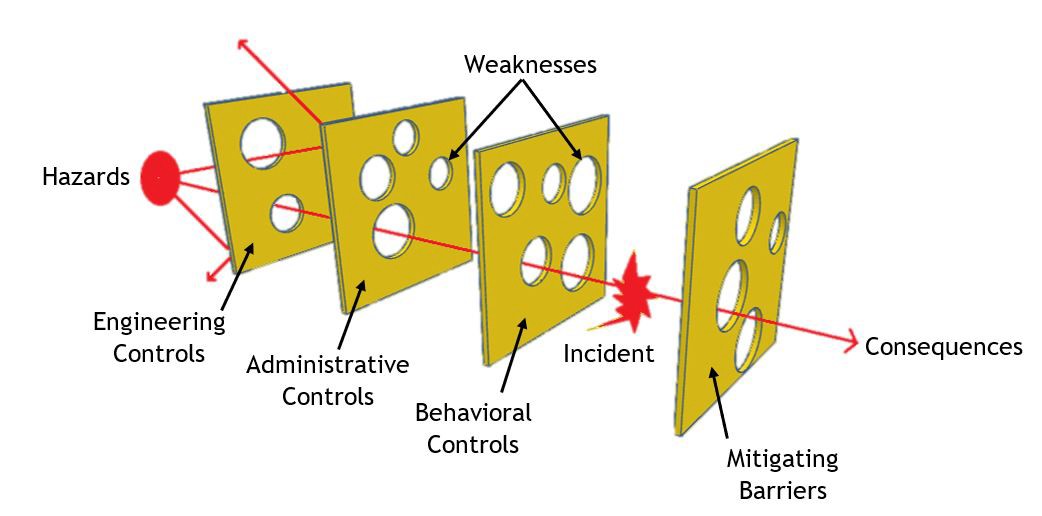
### Technological Level of Security

* + - * Authorization and Authentication Protocols
      * Data Storage and Encryption Standards
      * Threat Detection Maturity

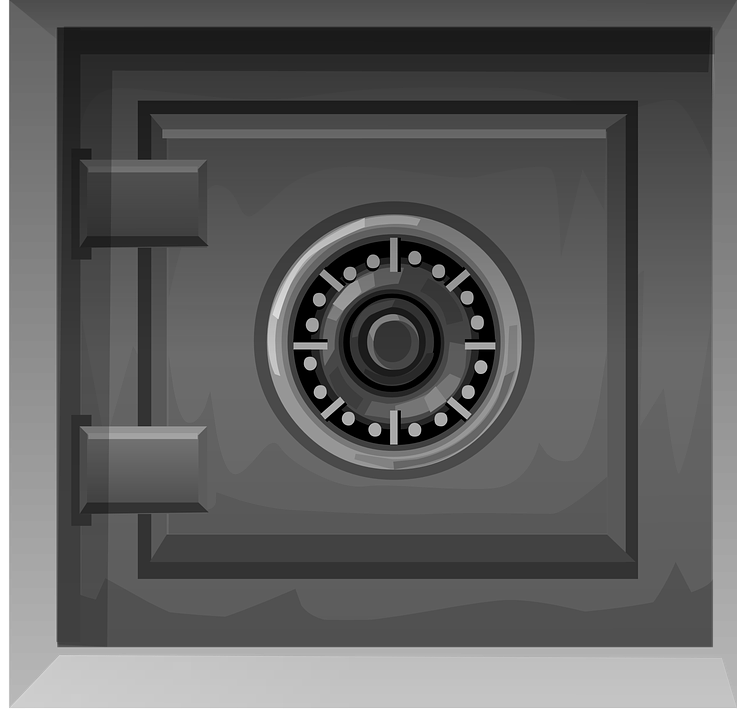
1. While this is by no means an exhaustive list, it is helpful to think of the potential threats to our data security as a multidimensional surface. Each “face” of that surface represents an additional potential attack vector. The total surface area is the “attack surface” that exposes us to risk which must be mitigated. The ability to address each area of the key areas in organizational, process and technology spaces combines to establish the over-all risk exposre of the organization.

The examples under each sub-heading above are not exhaustive, but are merely examples of the types of components that reside under each category (Dolezel & McLeod, 2019). The overall threat model is the combined impacts of all the surfaces exposed to attack through one or more means.

# What We Want



Versus What We Have

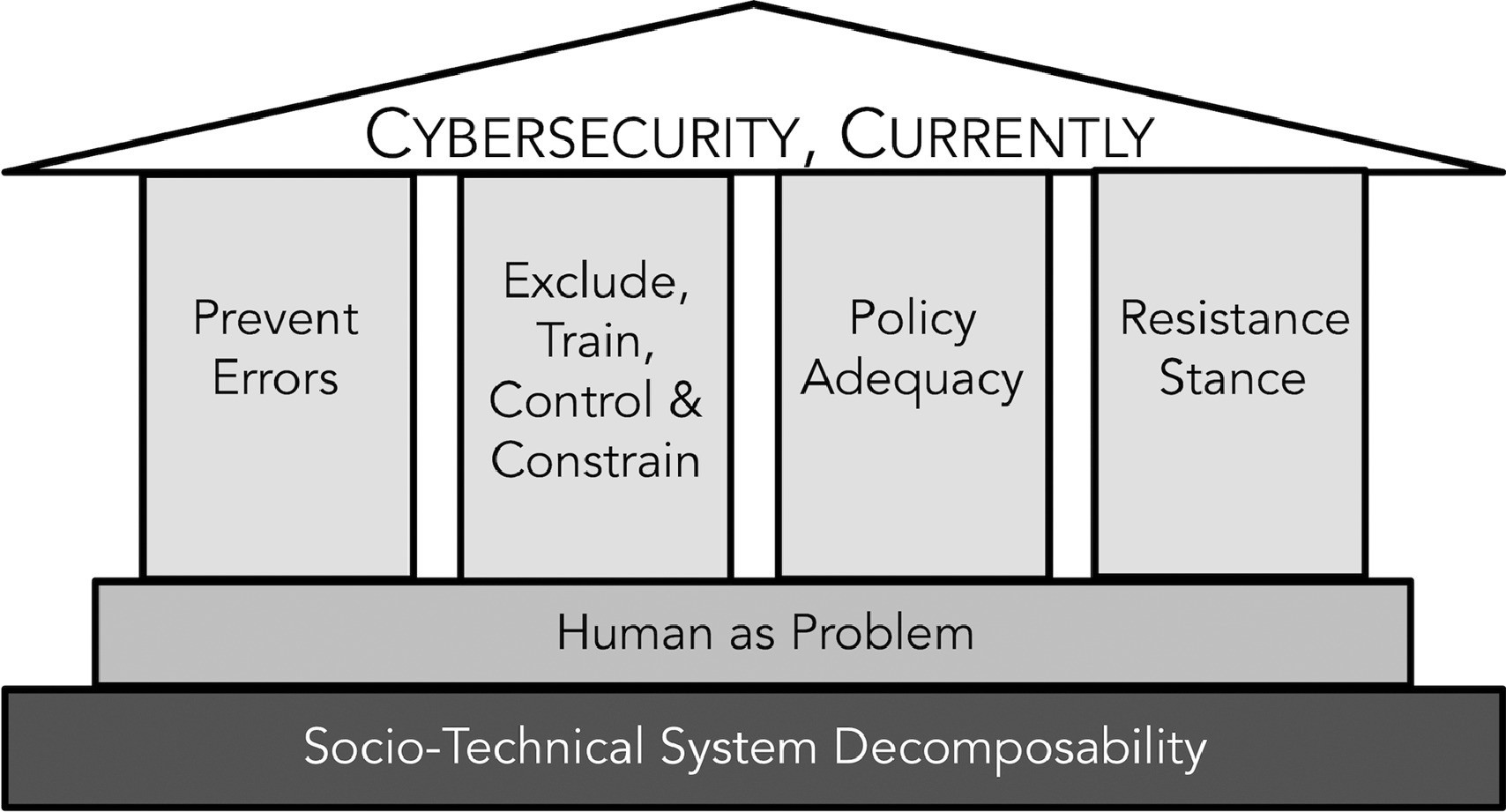
What we think of as security

What security actually is

Security in a complex computer environment is an inter-layering of imperfect solutions. None of these security solutions is capable of stopping all, or even most attack vectors. And the larger the attack surface, the more such layers are necessary. Perfect security is an unattainable myth if we wish to retain a usable system capable of producing business value. Instead, our cybersecurity is dependent upon ensuring that each of the multiple layers of our defense-in-depth is as robust as is reasonably possible (Jander et al., 2018), and that we focus on the weakest areas the most to achieve the greatest security posture.

# What Prevents Perfection

Are We Stuck Here?

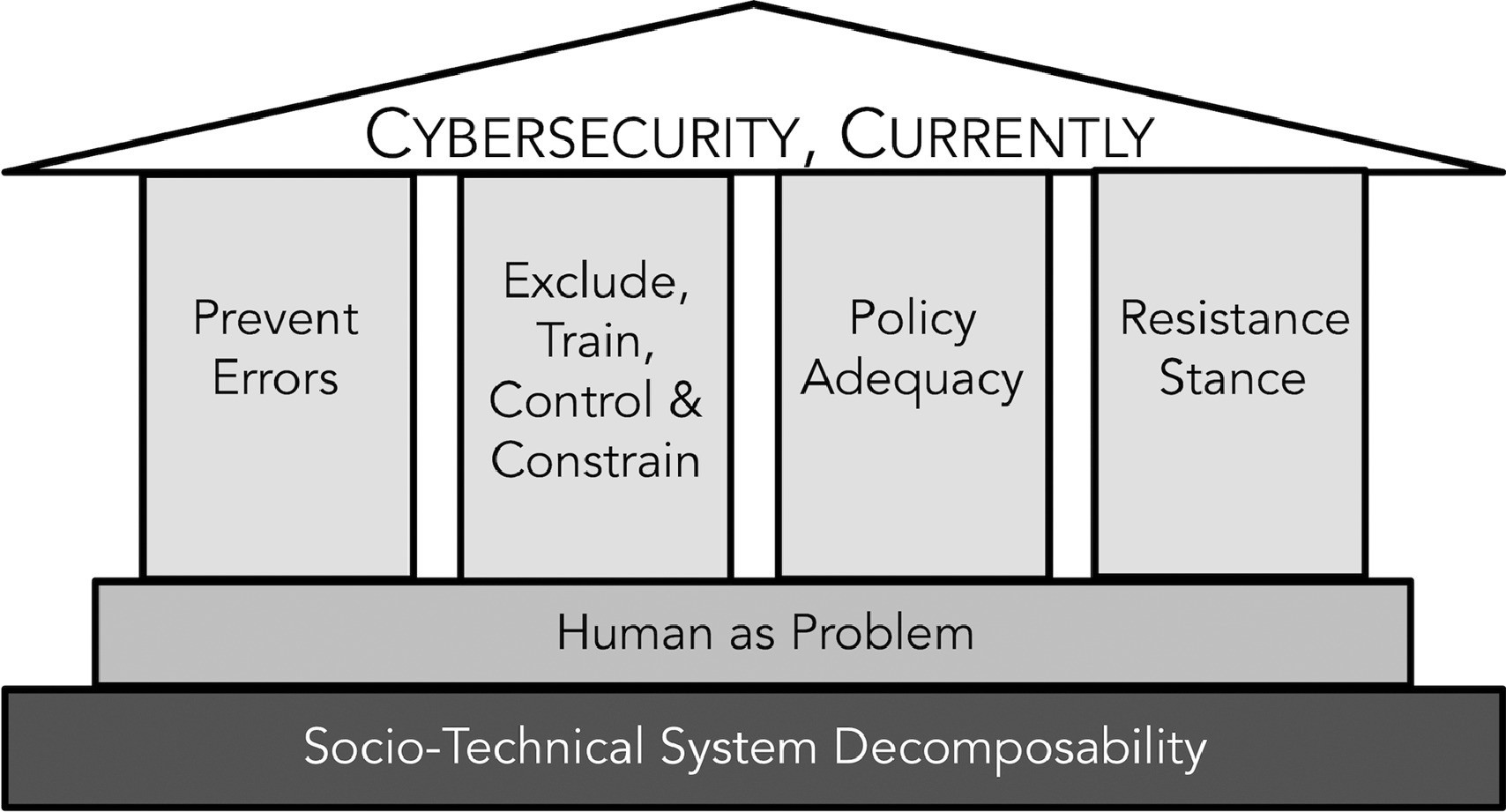
* People are the Common Factor

1. Within every domain of Cybersecurity people play a key and decisive role for ensuring success or failure. Bacchi (2012) suggests that within any policy discussion, the proposal itself is a “prescriptive text” that frames and represents an underlying problem in a particular way. Policy is how we constitute the problem. In cybersecurity people appear in several places within the framing of the problem: as the attackers seeking to subvert the controls and protections; as those attempting to prevent attacks by implementing countermeasures and security policies; as those who may inadvertently empower attacks by violating policy or subverting countermeasures; and as intentional internal bad actors. People are a common factor. As this illustration from (Bracchi, 2012) suggests.

# What Prevents Perfection

Are We Stuck Here?

* + People are the Common Factor



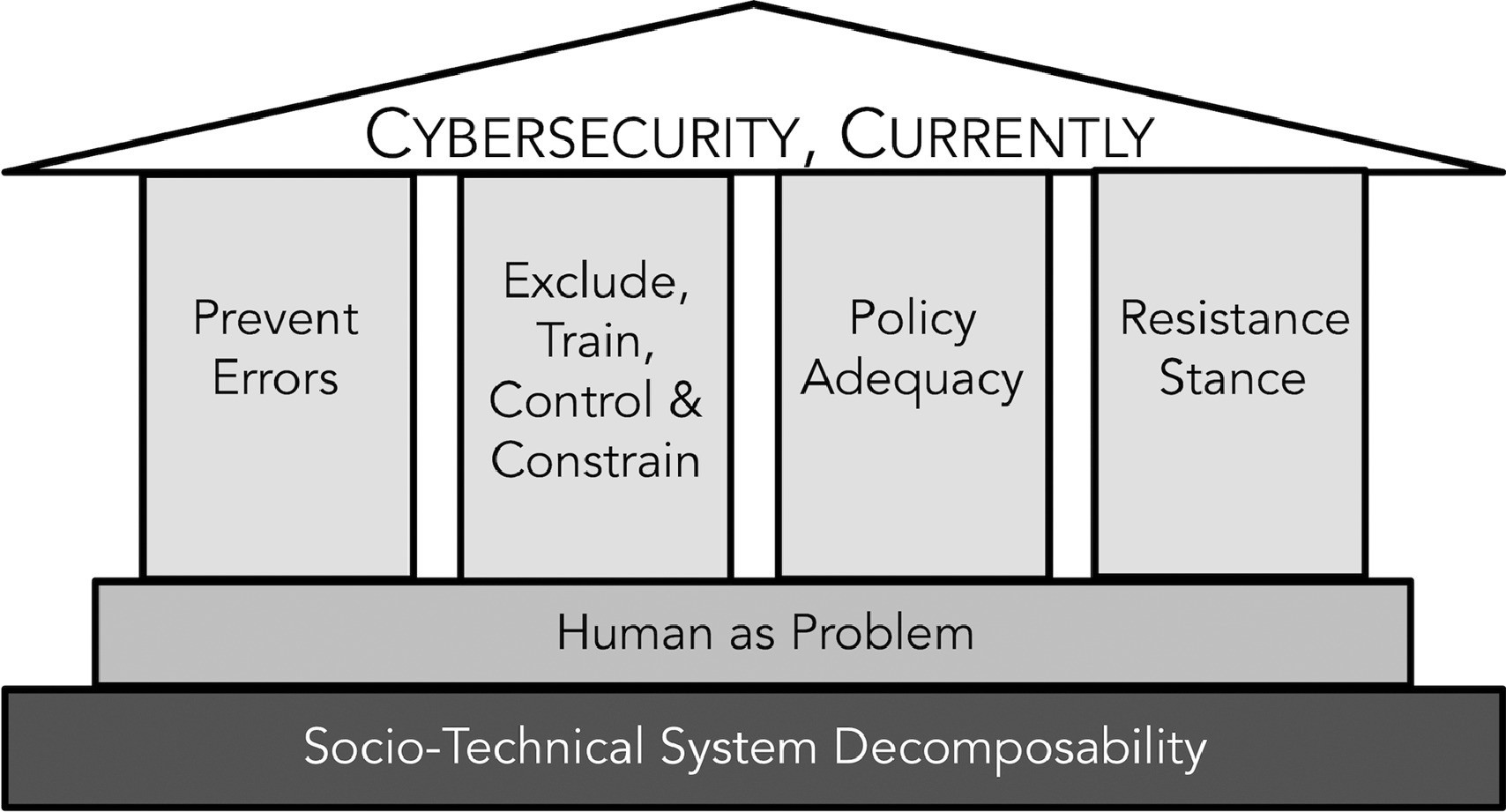
* + Are People the Common Solution?

1. Within every domain of Cybersecurity people play a key and decisive role for ensuring success or failure. Bacchi (2012) suggests that within any policy discussion, the proposal itself is a “prescriptive text” that frames and represents an underlying problem in a particular way. Policy is how we constitute the problem. In cybersecurity people appear in several places within the framing of the problem: as the attackers seeking to subvert the controls and protections; as those attempting to prevent attacks by implementing countermeasures and security policies; as those who may inadvertently empower attacks by violating policy or subverting countermeasures; and as intentional internal bad actors. People are a common factor. As this illustration from (Bracchi, 2012) suggests.
2. As nearly, if not all, issues in cybersecurity involve human actors in various roles; it follows that human actors are the most plausible solution to addressing cybersecurity problems (Zimmermann & Renaud, 2019).

# What Prevents Perfection

Are We Stuck Here?

* + People are the Common Factor



* + Are People the Common Solution?

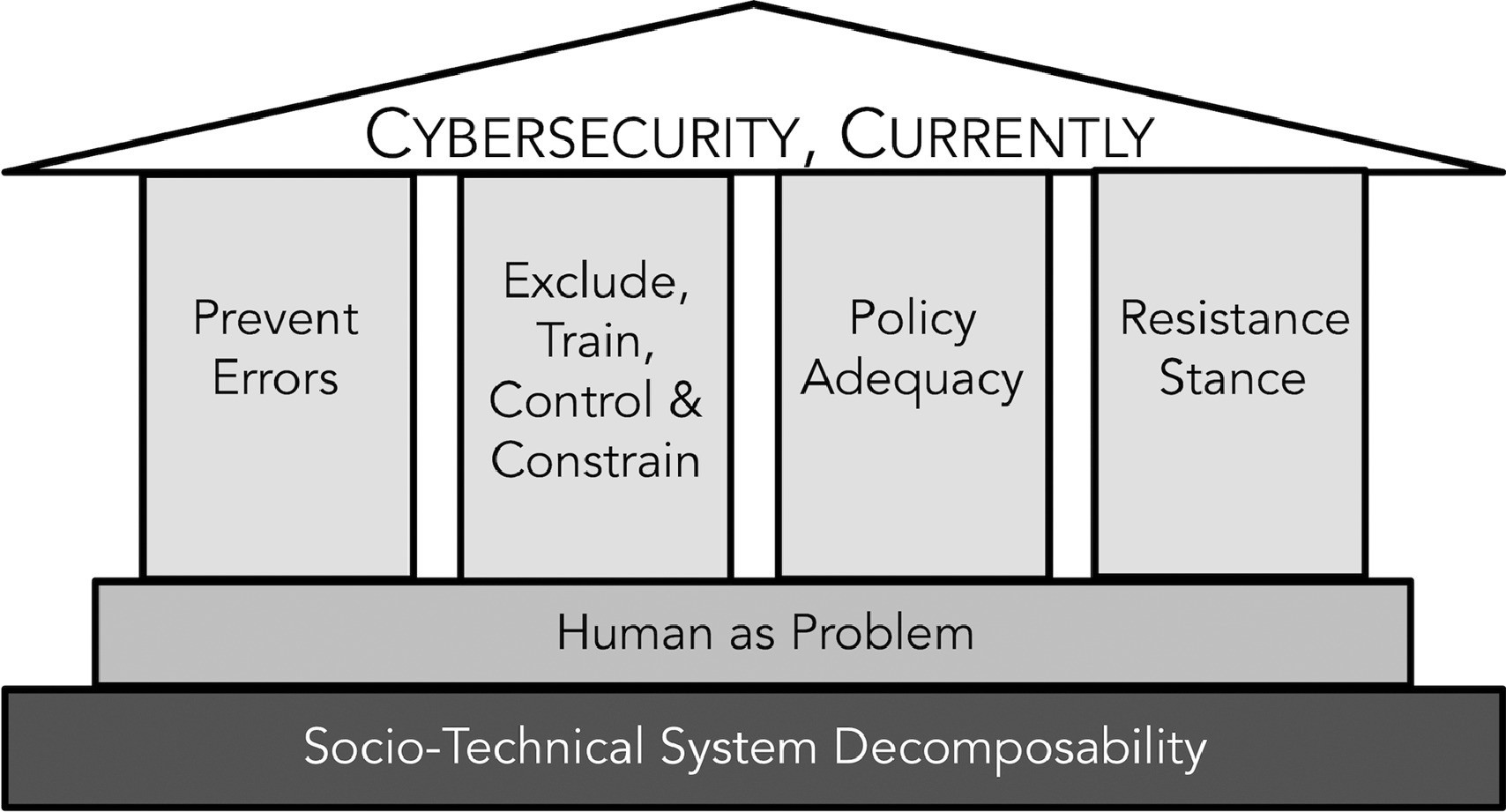
## People in the plural, not Person in the Singular

1. Within every domain of Cybersecurity people play a key and decisive role for ensuring success or failure. Bacchi (2012) suggests that within any policy discussion, the proposal itself is a “prescriptive text” that frames and represents an underlying problem in a particular way. Policy is how we constitute the problem. In cybersecurity people appear in several places within the framing of the problem: as the attackers seeking to subvert the controls and protections; as those attempting to prevent attacks by implementing countermeasures and security policies; as those who may inadvertently empower attacks by violating policy or subverting countermeasures; and as intentional internal bad actors. People are a common factor. As this illustration from (Bracchi, 2012) suggests.
2. As nearly, if not all, issues in cybersecurity involve human actors in various roles; it follows that human actors are the most plausible solution to addressing cybersecurity problems (Zimmermann & Renaud, 2019).
3. Historically, individual mistakes, laziness, apathy, ignorance, and other characteristics best collectively addressed as moral judgements have been considered the underlying cause of cybersecurity failure. Very few studies focused on broader questions of human behavior generally or the social psychology of cybersecurity (Renaud & Flowerday, 2017).

# What Prevents Perfection

Are We Stuck Here?

* + People are the Common Factor



* + Are People the Common Solution?

## People in the plural, not Person in the Singular

* + The Problem may not be People, but Perception

1. Within every domain of Cybersecurity people play a key and decisive role for ensuring success or failure. Bacchi (2012) suggests that within any policy discussion, the proposal itself is a “prescriptive text” that frames and represents an underlying problem in a particular way. Policy is how we constitute the problem. In cybersecurity people appear in several places within the framing of the problem: as the attackers seeking to subvert the controls and protections; as those attempting to prevent attacks by implementing countermeasures and security policies; as those who may inadvertently empower attacks by violating policy or subverting countermeasures; and as intentional internal bad actors. People are a common factor. As this illustration from (Bracchi, 2012) suggests.
2. As nearly, if not all, issues in cybersecurity involve human actors in various roles; it follows that human actors are the most plausible solution to addressing cybersecurity problems (Zimmermann & Renaud, 2019).
3. Historically, individual mistakes, laziness, apathy, ignorance, and other characteristics best collectively addressed as moral judgements have been considered the underlying cause of cybersecurity failure. Very few studies focused on broader questions of human behavior generally or the social psychology of cybersecurity (Renaud & Flowerday, 2017).
4. If we understand people as external entities who have to work both with and within the environment, then our approach to cybersecurity must change, and with it the resulting outcomes. If we perceive individual failures as the underlying cause of cybersecurity failure, we can’t examine the possibility that our problem definition is structured poorly. What if the problem isn’t individual training, apathy, competence, and so forth, but social attitudes and perceptions?

# What Prevents Perfection

Are We Still Stuck Here?

* + Root Cause Investigations are Insufficient

1. The common approach to cybersecurity incidents is to search for root cause(s) of the failure in order to remediate the presumed point of failure. As noted early, this choice of problem framing is filled with assumptions. The assumption that the failure can be remediated. The assumption that the failure is from a single or simple number of causes. The assumption that the system can be adequately decomposed to independent causal agents and more. These assumptions prevent the industry from moving beyond the notion of root cause and on to preventative action.

# What Prevents Perfection

Are We Still Stuck Here?

* + Root Cause Investigations are Insufficient
  + Other High-Risk Industries Do It Differently

1. The common approach to cybersecurity incidents is to search for root cause(s) of the failure in order to remediate the presumed point of failure. As noted early, this choice of problem framing is filled with assumptions. The assumption that the failure can be remediated. The assumption that the failure is from a single or simple number of causes. The assumption that the system can be adequately decomposed to independent causal agents and more. These assumptions prevent the industry from moving beyond the notion of root cause and on to preventative action.
2. In the aviation industry, after an incident or accident, an investigative body looking into the causes of an aviation incident are not looking for a single cause, but a chain of causality. It is presumed that there would be multiple places where an accident or incident could have been prevented. There is rarely a single “root cause,” rather there is a complex tapestry of multiple, interleaving events and actions that lead to an event. While ultimate responsibility will generally fall on the last person or persons in the chain who could have prevented the event, that doesn’t stop the investigators from noting how many others were in positions to change the outcome along the way. Further, the governing boards provide that “It is not the function of the Board to assign fault or determine civil or criminal liability, but the Board shall not refrain from fully reporting on the causes and contributing factors merely because fault or liability might be inferred from the Board’s findings ... No finding of the Board shall be construed as assigning fault or determining civil or criminal liability.” (Dempsey, 2010).

# Thinking Differently

Acknowledging the Illusion of Control

* + When Security Focuses on Compliance, Complacency Ensues

1. It is a well-understood phenomenon of social psychology that when rules are instituted, the perception of responsibility for the outcome is transferred from the person engaged in the actions covered by the rules to the rule-makers. If a problem is seen, the person acting will assume their perception is flawed because otherwise the police writer would have covered the situation. A personal sense of ownership and accountability for outcomes is lost and the burden to act with full responsibility is shifted away from the actor (Pham et al., 2017).

# Thinking Differently

Acknowledging the Illusion of Control

* + When Security Focuses on Compliance, Complacency Ensues
  + Parallels in Phsyical Safety

1. It is a well-understood phenomenon of social psychology that when rules are instituted, the perception of responsibility for the outcome is transferred from the person engaged in the actions covered by the rules to the rule-makers. If a problem is seen, the person acting will assume their perception is flawed because otherwise the police writer would have covered the situation. A personal sense of ownership and accountability for outcomes is lost and the burden to act with full responsibility is shifted away from the actor (Pham et al., 2017).
2. When physical safety research started, command and control attempts to direct human behavior were tried and failed repeatedly. Systems were tightly coupled and unpredictable with emerging behaviors that rule makers could not predict. Management teams focused on safety empowered employees not merely to react to changing conditions and situations but to be responsible for them. Systems were created that were highly redundant, highly flexible, and expertise was valued over compliance to process and procedure. A social culture of shared ownership, demarcated by a “no-blame” atmosphere where learning from errors was more important than punishing error makers resulted in significantly higher safety rates (Zimmermann & Renaud, 2019). In his famous book on the topic, Dekker (2014) characterized this shift as people moving from a “problem to control” and on to “a solution to harness.”

# An Already Solved Problem

Agile Security

* + Command-Control and Process/Policy Based Knowledge Work Considered Harmful

1. Knowledge workers first appeared in a work by Drucker (1952). While Drucker used it to mean people who create knowledge, it has come to encompass any employee who possesses a hgh level of professional knowledge and who engages in the creation, transfer, or practical use of knowledge as part of their role (Surawski, 2019). Knowledge workers are effectively those employees who’s tasks include complex communication skills and critical thinking. A definition that covers most very office worker and modern manufacturing machine operator in American industry today. Practical experience in multiple arenas has shown that command-control structures over such workers reduces their effectiveness, efficiency, engagement, morale, and the overall quality of outputs (Abrashoff, 2012; Lencioni, 2002; Marquet & Covey, 2013).

# An Already Solved Problem

Agile Security

* + Command-Control and Process/Policy Based Knowledge Work Considered Harmful
  + Empowerment is a Solved Problem

1. Knowledge workers first appeared in a work by Drucker (1952). While Drucker used it to mean people who create knowledge, it has come to encompass any employee who possesses a hgh level of professional knowledge and who engages in the creation, transfer, or practical use of knowledge as part of their role (Surawski, 2019). Knowledge workers are effectively those employees who’s tasks include complex communication skills and critical thinking. A definition that covers most very office worker and modern manufacturing machine operator in American industry today. Practical experience in multiple arenas has shown that command-control structures over such workers reduces their effectiveness, efficiency, engagement, morale, and the overall quality of outputs (Abrashoff, 2012; Lencioni, 2002; Marquet & Covey, 2013).
2. Given that command and control structures don’t work, what structures do? Experience in the industry shows that using principles of business agility and leadership, which effectively amount to pushing decisions to the lowest possible level, allow employees to make such decisions without fear, trusting in their competency, and creating a safe, learning organization focused on continuous improvement, knowledge worker engagement, efficiency, and quality all tend to increase (digital.ai, 2020; Reifer, 2002). Of course such methods still require discipline around execution and commitment to sound working principles, but the issue of being able to create a learning organization of empowered, engaged knowledge workers is a problem with a known working solution.

# An Already Solved Problem

Agile Security

* + Command-Control and Process/Policy Based Knowledge Work Considered Harmful
  + Empowerment is a Solved Problem

## Security Can Follow This Model. But Needs Leadership!

1. Knowledge workers first appeared in a work by Drucker (1952). While Drucker used it to mean people who create knowledge, it has come to encompass any employee who possesses a hgh level of professional knowledge and who engages in the creation, transfer, or practical use of knowledge as part of their role (Surawski, 2019). Knowledge workers are effectively those employees who’s tasks include complex communication skills and critical thinking. A definition that covers most very office worker and modern manufacturing machine operator in American industry today. Practical experience in multiple arenas has shown that command-control structures over such workers reduces their effectiveness, efficiency, engagement, morale, and the overall quality of outputs (Abrashoff, 2012; Lencioni, 2002; Marquet & Covey, 2013).
2. Given that command and control structures don’t work, what structures do? Experience in the industry shows that using principles of business agility and leadership, which effectively amount to pushing decisions to the lowest possible level, allow employees to make such decisions without fear, trusting in their competency, and creating a safe, learning organization focused on continuous improvement, knowledge worker engagement, efficiency, and quality all tend to increase (digital.ai, 2020; Reifer, 2002). Of course such methods still require discipline around execution and commitment to sound working principles, but the issue of being able to create a learning organization of empowered, engaged knowledge workers is a problem with a known working solution.
3. Just as Dekker (2014) showed that physical security and safety can be better solved by engaging employees as partners in the solution rather than regulating them to the being the subjects of command and control, new theories about cybersecurity suggest that the best way to address the complex dynamic

cyber-environments that give rise to security issues is to move away from command-control, regulation, and governance as the primary driveres of security and instead focus on the social engagement and empowerment of people to be the drivers of solutions (Zimmermann & Renaud, 2019). To do so however, requires industry leadership at multiple levels. First and foremost, leaders at the industry level must make compliance with strict prescriptive acts not be a reason in and of itself to fail external audits. Second, internal policies and procedures must focus on empowering SMEs to find, address, and react to issues without fear of reprisal. Lastly, companies must focus on building a culture of shared social accountability and awareness for cybersecurity.

# Specific Opportunities

Security as value-less add-ons

* + CISSP Domains and Have Limited Stand-alone Value Delivery

### Security and Risk Management

* + - Asset Security

### Security Architecture and Engineering

* + - Communications and Network Security

### Security Assessment and Testing

* + - Security Operations

### Software Development Security

1. The key point to notice about each of these items is that none of them by themselves is something that produces value to the organization if viewed through the lens of being a command and control function that must be “bolted on” to products and services that an organization provides.

# Specific Opportunities

CISSP Security and Risk Management as Customer delight-ers

As an exmaple of how focusing on security as value provides opportunities

* + We ensure you can always do what you need to as a customer

## We focus on establishing trust between users, systems, suppliers, business partners, and our employees

* + We ensure no one has access to your data without your explicit permission

1. Switching the focus from being about what we as a company do to comply with CISSP or NIST or any other standard, to what we provide to our stakeholders as a value proposition changes the conversation from security as a bolt-on afterthought to security as a feature adding customer value. Apple is masterful at this (Apple, Inc, 2021). Consider the messaging from Apple: “Privacy is a fundamental human right.” Apple isn’t selling security, they aren’t selling a product. They are protecting their customer’s human rights! Who wouldn’t want to be part of that equation? By changing access management from an audit mandated extra to a customer-centric feature, Apple creates value and increases revenue.

# Specific Changes to Leverage Security as a Value Opportunity

## Agile organizations requires new paradigms of leadership, Particularly around governance issues

* + Every employee is accountable to always be learning how to do security better

## Security must be a cultural touchstone

* + Every employee must be empowered to do security better

## Policy must follow sound practice, not dictate it or constrain it

* + Leadership must be about results not process

1. Switching the focus from being about what we as a company do to comply with CISSP or NIST or any other standard, to what we provide to our stakeholders as a value proposition changes the conversation from security as a bolt-on afterthought to security as a feature adding customer value. Apple is masterful at this (Apple, Inc, 2021). Consider the messaging from Apple: “Privacy is a fundamental human right.” Apple isn’t selling security, they aren’t selling a product. They are protecting their customer’s human rights! Who wouldn’t want to be part of that equation? By changing access management from an audit mandated extra to a customer-centric feature, Apple creates value and increases revenue.

# Specific Risks to Be Addresseed

Risks

* + Every employee is accountable to always be learning how to do security better
  + Security must be a cultural touchstone

## Every employee must be empowered to do security better

* + Policy must follow sound practice, not dictate it or constrain it.

## Leadership must be about [results](#_bookmark49) not process

1. Every employee being accountable for security may take time to become normative. The risk is that in moving to this model, security issues may develop because employees are not fully aware of their own accountability.
2. Cultural chanCultural change is hard and takes time. Getting employees to fully embrace security as a cultural element will require a significant effort.
3. Empowerment to make changes in how security is approached will require constant communication, transparency, and support, not to mention training for some many people.
4. Getting employees to think holistically about best practices takes time, which means that policy can’t simply be disregarded. Further, some policies will have to remain enforced due to external regulatory requirements.
5. There is a risk that existing bonus and evaluation paradigms will not readily facilitate the desired behaviors, and could drive anti-patterns.
6. Moving from human as issue to human as solution is a major cultural change. Such changes always carry risk (Yeganeh, 2020). While the risks and costs of cultural change must be managed, the need to move from a perspective of people needing to be controlled and managed to people being a company’s most important security asset presents a real opportunity to move ahead of the security curve (Zimmermann & Renaud, 2019).

Abrashoff, C. D. M. (2012, October 9). *It’s your ship: Management techniques from the best damn ship in the navy, 10th anniversary edition* (10th Anniversary Revised & Updated edition). New York, Grand Central Publishing.



Apple, Inc. (2021). *Privacy*. Apple. Retrieved April 25, 2021, from <https://www.apple.com/privacy/>



Bacchi, C. (2012). Why study problematizations? making politics visible. *Open Journal of Political Science*, *02*(01), 1. <https://doi.org/10.4236/ojps.2012.21001>



Dekker, S. (2014, June 23). *Safety differently: Human factors for a new era, second edition*. CRC Press.



Dempsey, P. S. (2010). Independence of aviation safety investigation authorities: Keeping the foxes from the henhouse. *Symposium at SMU on Air Law, 2010*, *75*(2), 223–284. Retrieved April 24, 2021, from [http://proxy1.ncu.edu/login?url=https:](http://proxy1.ncu.edu/login?url=https)



//search.ebscohost.com/login.aspx?direct=true&db= ofs&AN=502157119&site=eds-live

digital.ai. (2020). *State of agile survey*. Retrieved April 24, 2021, from <https://stateofagile.com/>



Dolezel, D., & McLeod, A. (2019). Managing security risk: Modeling the root causes of data breaches. *The Health Care Manager*, *38*(4), 322–330. <https://doi.org/10.1097/HCM.0000000000000282>



Drucker, P. F. (1952). Management and the professional employee. *Harvard Business Review*, *30*(3), 84–90.



Hooker, M., & Pill, J. (2016). You’ve been hacked, and now you’re being sued: The developing world of cybersecurity litigation. *Florida Bar Journal*, *90*(7), 30–40. Retrieved April 24, 2021, from [http://proxy1.ncu.edu/login?url=https:](http://proxy1.ncu.edu/login?url=https)



//search.ebscohost.com/login.aspx?direct=true&db= a9h&AN=116410271&site=eds-live

## Jander, K., Braubach, L., & Pokahr, A. (2018). Defense-in-depth and role authentication for microservice systems.



*Procedia Computer Science*, *130*, 456–463. Retrieved

## April 24, 2021, from

[http://proxy1.ncu.edu/login?url=https:](http://proxy1.ncu.edu/login?url=https)

## //search.ebscohost.com/login.aspx?direct=true&db= edo&AN=129273669&site=eds-live

Lencioni, P. (2002, April 11). *The five dysfunctions of a team: A leadership fable* (1st edition). San Francisco,



## Jossey-Bass.

Marquet, L. D., & Covey, S. R. (2013, May 16). *Turn the ship around!: A true story of turning followers into leaders* (1st edition). Portfolio.



Pham, H. C., Pham, D. D., Brennan, L., & Richardson, J. (2017). Information security and people: A conundrum for compliance. *Australasian Journal of Information* *Systems*, *21*. <https://doi.org/10.3127/ajis.v21i0.1321>



## Reifer, D. (2002). How good are agile methods? *IEEE Software*, *19*(4), 16–18.



<https://doi.org/10.1109/MS.2002.1020280>

## Renaud, K., & Flowerday, S. (2017). Contemplating



human-centred security & privacy research: Suggesting future directions. *Journal of Information Security and Applications*, *34*, 76–81. <https://doi.org/10.1016/j.jisa.2017.05.006>

## Surawski, B. (2019). Who is a ”knowledge worker” – clarifying the meaning of the term through comparison with synonymous and associated terms. *Management (1429-9321)*, *23*(1), 105–133.



<https://doi.org/10.2478/manment-2019-0007>

Yeganeh, H. (2020). Salient cultural transformations in the age of globalization: Implications for business and management. *International Journal of Sociology & Social Policy*, *40*(7/8), 695–712. Retrieved April 26, 2021, from [http://proxy1.ncu.edu/login?url=https:](http://proxy1.ncu.edu/login?url=https)



//search.ebscohost.com/login.aspx?direct=true&db= edb&AN=144205396&site=eds-live

Zadeh, A. H., Jeyaraj, A., & Biros, D. (2020). Characterizing cybersecurity threats to organizations in support of risk mitigation decisions. *e-Service Journal*, *12*(2), 1–34. <https://doi.org/10.2979/eservicej.12.2.01>



Zimmermann, V., & Renaud, K. (2019). Moving from a ‘human-as-problem” to a ‘human-as-solution” cybersecurity mindset. *International Journal of Human-Computer Studies*, *131*, 169–187. <https://doi.org/10.1016/j.ijhcs.2019.05.005>



## Zureich, D., & Graebe, W. (2015). Cybersecurity: The continuing evolution of insurance and ethics. *Defense Counsel Journal*, *82*(2), 192–198. Retrieved April 24,



2021, from [http://proxy1.ncu.edu/login?url=https:](http://proxy1.ncu.edu/login?url=https)

## //search.ebscohost.com/login.aspx?direct=true&db= bth&AN=102363112&site=eds-live