International Journal of Applied Technology & Leadership
ISSN 2720-5215
Volume 2, Issue 1, January 2023
ijatl@org

Component Security vs. Cybersecurity: Defining Next Generation Cybersecurity

Ervin Henry Frenzel

Capitol Technology University (USA)

Ian McAndrew, PhD

Capitol Technology University (USA)

Abstract

While there are multiple versions of the Maconachy, Schou, Ragsdale or MSR model, most overlook technical component security breakouts in each of the primary cybersecurity countermeasures. Failing to break down and align countermeasures with existing the standards leaves many organizations and academia struggling to link other fields of study to cybersecurity efforts. Identifying how to incorporate other area specialists into cybersecurity, by first identifying and then training these experts in basic cybersecurity mechanics, incorporates key skills that are currently lacking within our cybersecurity workforce. Service outcomes should not be the initial look at the MSR cube, they should be the final objective. To fully integrate the next generation of not only the MSR model we must first identify in what state our data is in, then identify which countermeasure can be successfully engaged first and which countermeasures could be used as compensating as necessary, this then leads to the desired service outcome.

Key words*:* technical component security, non-technical component level security, Autonomic Self or Autonomous Identity

1. Introduction

So often, we are told something and believe it without question, but should we genuinely accept it blindly without questioning? The answer so many times should be maybe society should accept the suggestion blindly. For example, if I mention what my boundaries are, then yes, they should be taken as my boundaries. If, on the other hand, I speak from a position of non-authority about something I am not entirely knowledgeable about, then it should be questioned.

What is the cost of not questioning the status quo? In the case of cybersecurity, losses can amount to trillions of dollars a year, according to IBM [3]. In 2020, annualized US losses surpassed 6.7 trillion dollars, roughly 1/3 of the US gross domestic product [3][15].

2. Research Methodology

Research revealed seminal work describing three critical information characteristics by John McCumber; integrity, confidentiality, and availability, and three security safeguards; human factors, policy and practice, and technology [10]. Though a reasonably simplistic viewpoint by today's standards, it was an original attempt to model threats against digital business data.

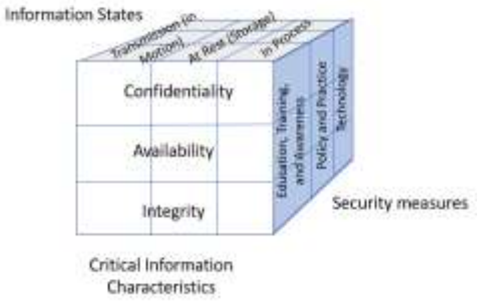


Fig. 1. McCumber Cube

The McCumber cube, however, became the judging standard for cybersecurity [10][8][14].

Later critical information characteristics were described as security services and, later added, authentication and non-repudiation. Finally, essential safeguards of cybersecurity transformed into security countermeasures. The model was transformed into Information Assurance as defined by Maconachy, Schou, and Ragsdale MSR during a 2001 IEEE conference on cybersecurity [8]. We call this reference model the MSR model.

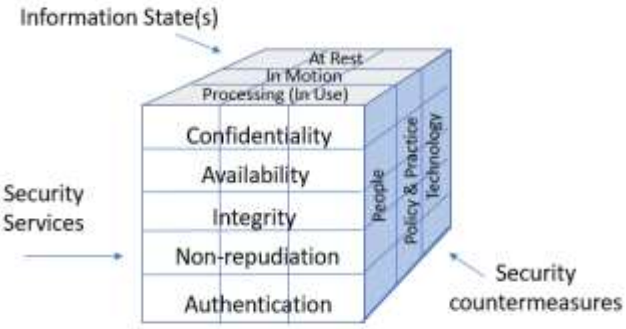


Fig. 2. Maconachy, Schou, Ragsdale or MSR model

The MSR model is the comparative baseline for other recognized security models, such as the Parkerian Hexad Model [11][8][13]. In the MSR model, the three sides would appear as component groupings known as security services, including countermeasures and information states. Countermeasures would seem much like this:

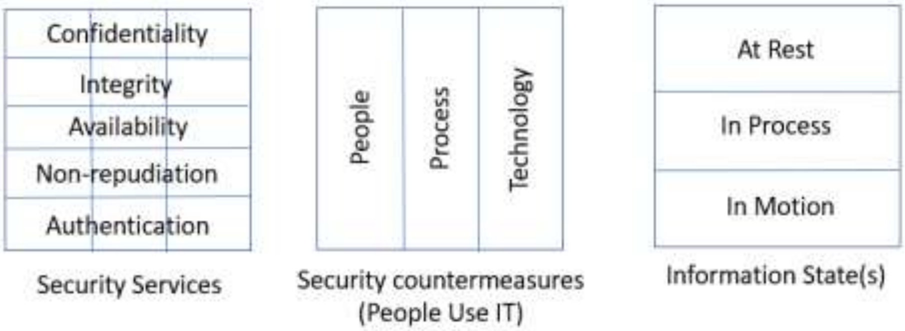


Fig. 3. Aspects of the MSR Cube

This model is what we now use to define cybersecurity. To simplify the MSR countermeasures, think of the countermeasures as encompassing people, processes, and technology or the holistic socio-technical system that represents people securely interacting with technology [1][6][8]. For example, previously made arguments argued that integrity should be the basis of information defense, not confidentiality [16].

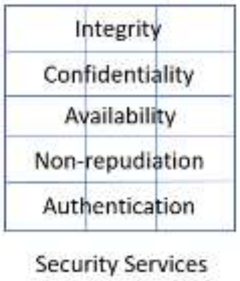


Fig. 4. Cybersecurity services of the MSR cube

3. Analysis results

Security countermeasures fall into one of the primary categories of people, processes, and technology. Therefore, a holistic cybersecurity protection system must include all security countermeasures to be considered complete [10][8][9][14][1].

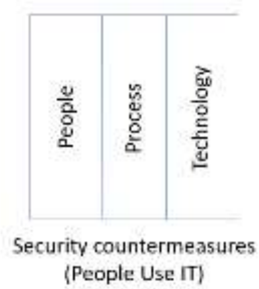


Fig. 5. Cybersecurity countermeasures of the MSR cube

An analysis of these countermeasures indicates existing knowledge that is ignored as simple terms when in fact, there is a great wealth of knowledge in each of these terms. Organizations should break down the complete technology countermeasure into one of the six recognized technology or component areas identified by one of the international communities, such as IEEE, ACM, and IFIP [4][12][7][5][2]. These areas include computer science, software engineering, computer engineering, information technology, information systems, and the newly recognized data science [4][12][7][5][2]. For simplicity, these can be aligned or stacked one above another to fit within the technology square of the people, process, and technology model [10][8][14][9].

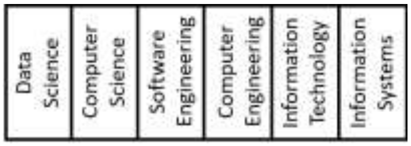


Fig. 6. Recognized IEEE and ACM technology components of the technical countermeasure

These technologies cannot exist by themselves; after all, this is about security [4][12][7][5][2]. Therefore, for lack of a better term, we will refer to this as technological component level security.

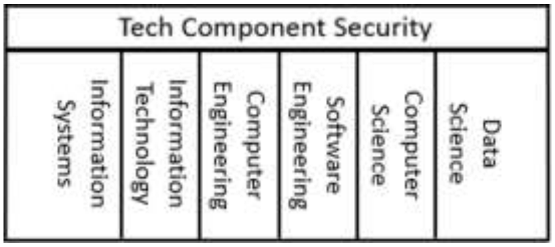


Fig. 7. Technical component security fields associated with the technical countermeasures field

While this part may seem self-explanatory, little thought is given to these as individual technical component-level security countermeasures. Still, component-level security countermeasures need to be addressed individually and as part of an organization's holistic cybersecurity strategy [1][6]. Specializations not commonly considered technology include processes and people-level security; however, specialized areas require specialized knowledge. These specializations each have a level set of security; we traditionally use these senses; however, we use technical component level security countermeasures [7]. Should we also not have people and process-level security?

It is the opinion of this author these specialized areas of security countermeasures should be considered technical proficiencies for the sake of security countermeasure training and development. Cakes are composed of ingredients; there are thousands of cakes. Much like a cake, different ratios of ingredients provide additional flavors to a cake. Therefore, combining all technical component-level security countermeasures makes up a specialized technical security cake or a complete cybersecurity cake.

The consideration of people and processes as technical component-level security countermeasures identify possible methodologies to approach the training of these specific countermeasure types [10][8][4][12][7][14][9][5][2]. For instance, the overlap of people and processes would be considered operational; in this case, a security scenario to cover this would be nominally called operational security or *OPSEC.* Therefore, training team members to understand the intersection of these countermeasures becomes critical to completing the holistic picture of an organization's Cybersecurity [1][6]. The standardized people, processes, and technology view now looks like this.

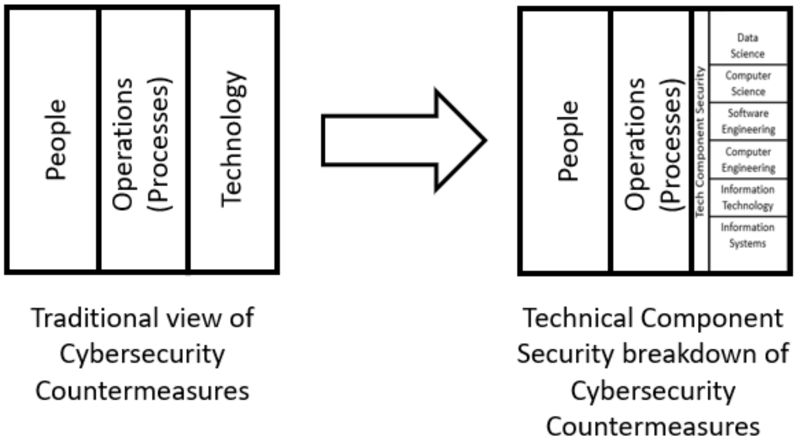


Fig. 8. Superimposing the technical component security fields into the technical countermeasure field of the MSR

To simplify and correct the current process of focusing on the outcomes before identifying how the countermeasures are engaged, this author views the MSR as follows:

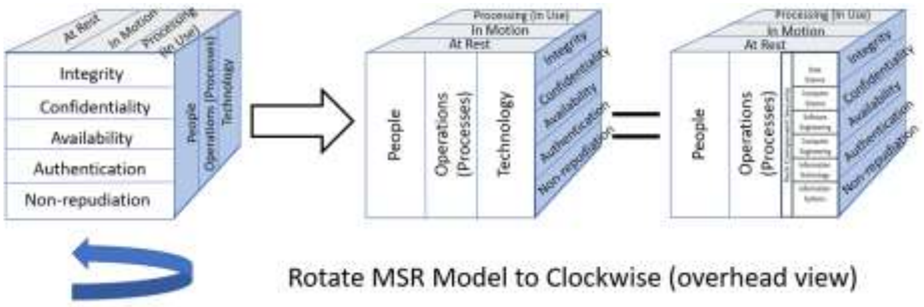


Fig. 9. Rotation of the MSR cube to bring the primary focus to the MSR countermeasures surface versus the final desired outcomes or services surface.

This change places the countermeasures up front where they become the focal point of the model versus hidden behind the service objectives. It then breaks down the technical component level security. However, this model drill-down is not yet complete.

Professionals should further break down the people and processes components. Like the technical component security of the technology countermeasure, both the processes and people countermeasures also have subcomponents; however, cybersecurity professionals need to recognize other fields of study contain experts in their respective fields [1]. Therefore, consideration should be made for the expertise of these field practitioners. Ensuring these professionals have a place within cybersecurity is critical to organizational success; more importantly, these professionals work to achieve a similar state of being without being formally included in defense of the organization.

Process experts typically align with project and enterprise organizational alignment, and a component level of cybersecurity is associated with processes; this cybersecurity component level security is known as operational security, often referred to as OPSEC. Operational security is the point where operations and people meet. Our countermeasures section now looks like this.

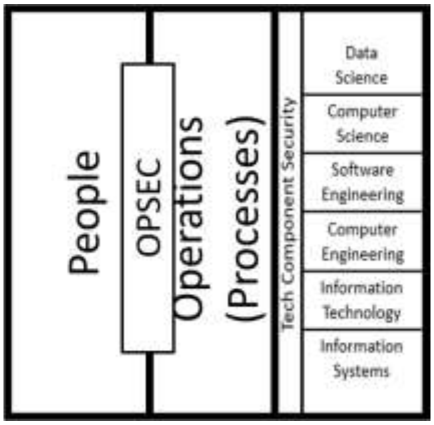


Fig. 10. Superimposing the operational processes component level security onto the operational countermeasure field of the MSR

More importantly, our version of the MSR now looks like this:

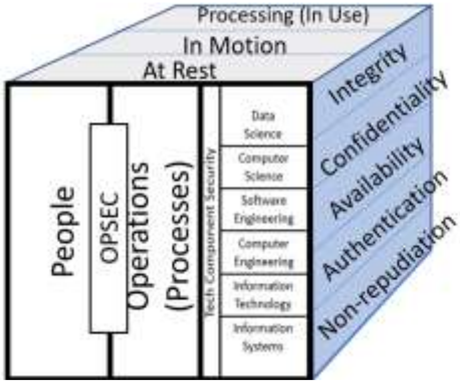


Fig. 11. The superimposed component level securities of the MSR (Processes and Technology countermeasures only)

Identifying technology component security and processes component security is critical to an organizational defense; however, the single largest asset is not accounted for. This asset is the people countermeasure [1]. This countermeasure has specialists who could be called technical component specialists. After all, a psychologist is far more technically competent when working with people than someone who works on firewalls day in and day out [7]. The firewall technician is more technically skilled when dealing with the firewall, a secure developer is far more competent than a hobby programmer, and a professional project manager is far more proficient when overseeing a program than an entry-level intern. A prudent conclusion might be an experienced leader will deal with employees and workers better than an entry-level technician. A possible method of breaking down not only desired social states in comparison to identity, but this author also refers to the identity proximity relationship as *Autonomic Self* or *Autonomous Identity* is shown below.

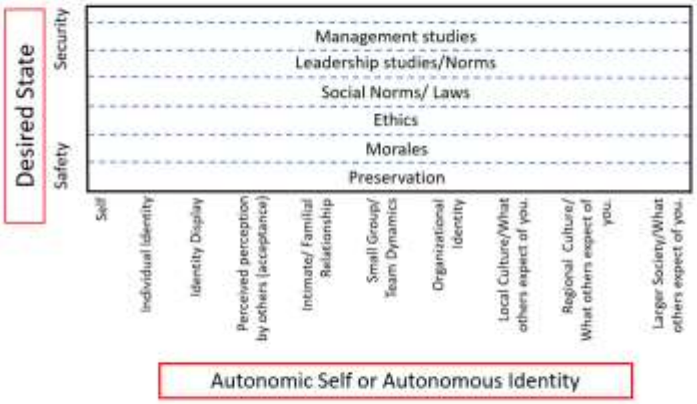

Desired State
Security
Safety
Management studies
Leadership studies/Norms
Social Norms/ Laws
Ethics
Morales
Preservation
Self
Individual Identity
Identity Display
Perceived perception by others (acceptance)
Intimate/ Familial Relationship
Small Group/ Team Dynamics
Organizational Identity
Local Culture/What others expect of you.
Regional Culture/ What others expect of you.
Larger Society/What others expect of you.
Autonomic Self or Autonomous Identity

Fig. 12. Possible breakdown of the Autonomic Self or Autonomous Identity, the "people" countermeasure component level security intersections of ethos and desired outcomes

Once we identify and break down the people technical component security pieces, we rotate the model 90 degrees clockwise and incorporate them into the existing model.

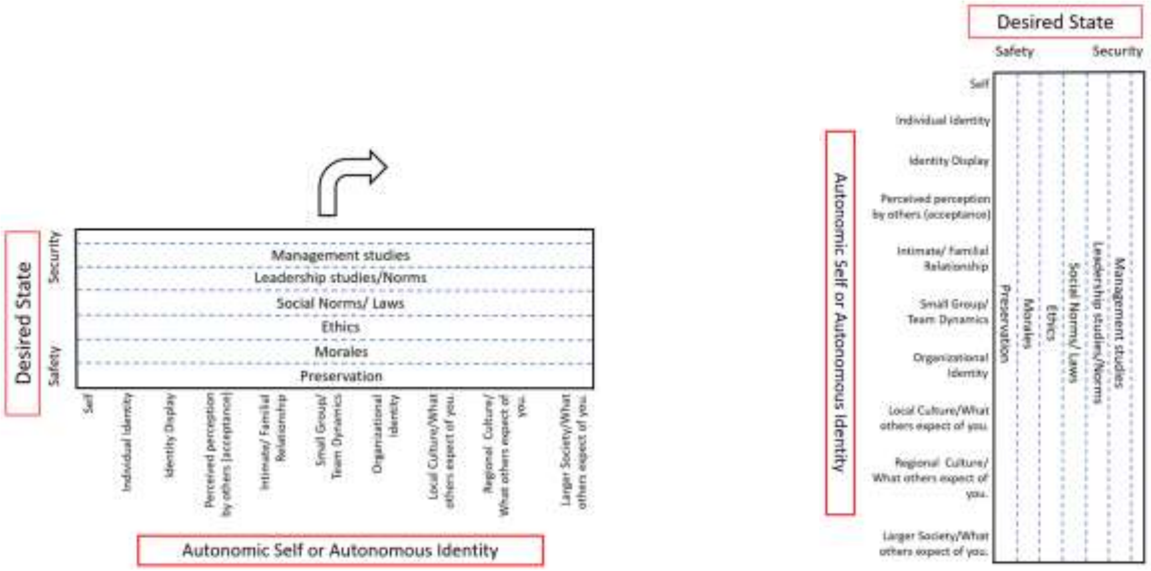

Desired State
Safety
Security
Management studies
Leadership studies/Norms
Social Norms/ Laws
Ethics
Morales
Preservation
Self
Individual Identity
Identity Display
Perceived perception by others (acceptance)
Intimate/ Familial Relationship
Small Group/ Team Dynamics
Organizational Identity
Local Culture/What others expect of you.
Regional Culture/ What others expect of you.
Larger Society/What others expect of you.
Autonomic Self or Autonomous Identity
Desired State
Safety
Security
Self
Individual Identity
Identity Display
Perceived perception by others (acceptance)
Intimate/ Familial Relationship
Small Group/ Team Dynamics
Organizational Identity
Local Culture/What others expect of you.
Regional Culture/ What others expect of you.
Larger Society/What others expect of you.
Autonomic Self or Autonomous Identity
Preservation
Morales
Ethics
Social Norms/ Laws
Leadership studies/Norms
Management studies

Fig. 13. 90-degree rotation of the Autonomic self-properties

This model now incorporates technical component securities in the people, processes, and technology countermeasure areas. This chart or one like it can be incorporated into the countermeasures process as:

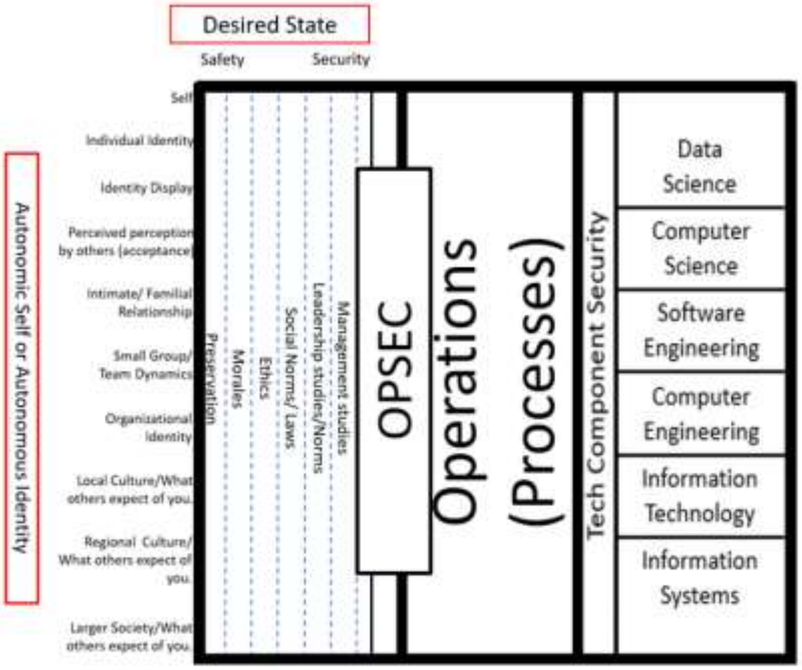


Fig. 14. Superimposing the Autonomic Self or Autonomous Identity component level security onto the "people" countermeasure component level security intersections of the MSR

The next update is something professionals have been addressing but the MSR has yet to address, which is understandable as businesses have significantly changed over the two decades since its first creation [8]. A data state needs to be addressed, a data state dealing with obtaining data from a third party or from an otherwise untrusted source. This author refers to this as *at Collection* as it seems MSR assumes data is in a clean state for usage [8]. In the past many organizations collected data for themselves, in the ever-changing business world of today many organizations opt to purchase data or worse. This data state exposes a completely vulnerable state that very little concern addresses, *the motion related to collection of data*. This translates to two additional states necessary to introduce data into an environment, an “at collection" and "collection motion". Placing these new additions in the order of engagement, from front to rear we now have; a) at collection, b) in motion, c) at rest, d) in motion, and e) finally in use.

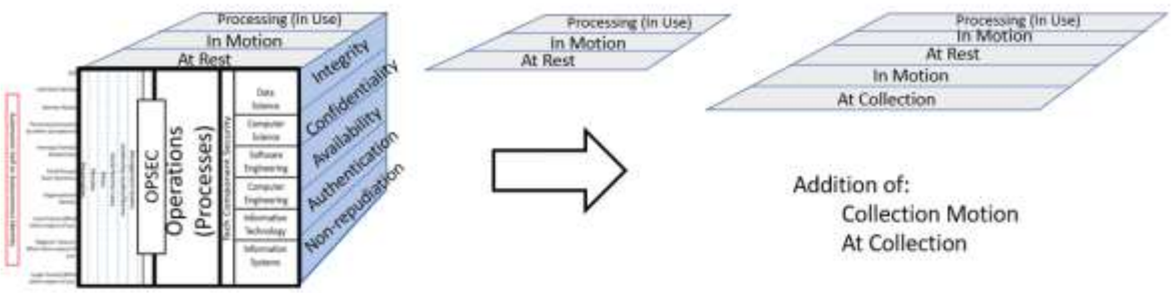


Fig. 15. The proposed addition of two data states to account for data gathering without absolute control of its source (third party source or partial control of initial in-transit motion)

When moving from our primary focal point of the countermeasures on the front and from front to rear of our model as we pass through our data states, our abreviated, updated, and combined model now resembles this:

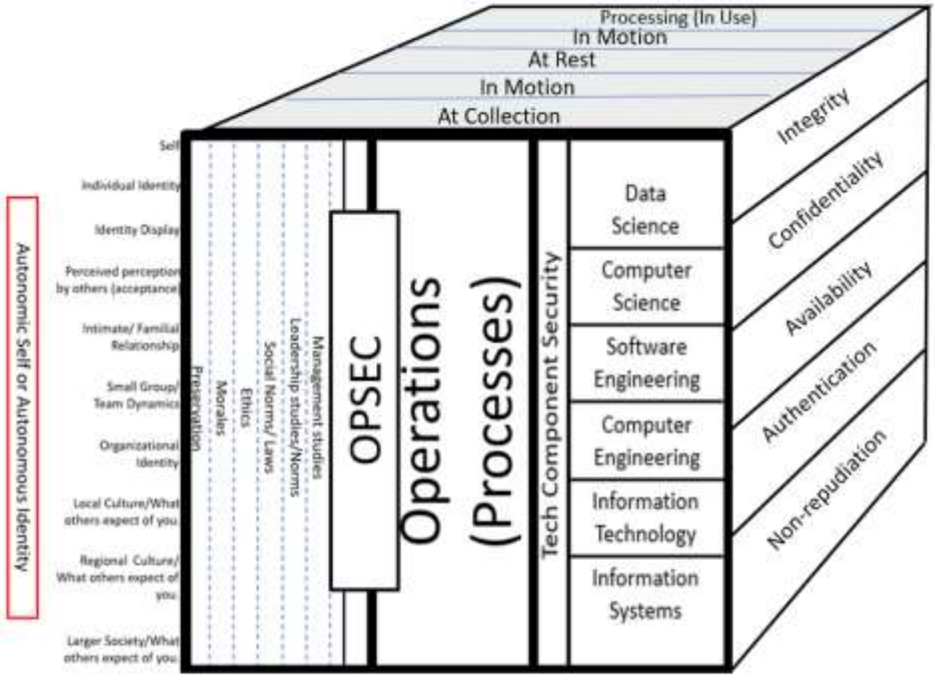


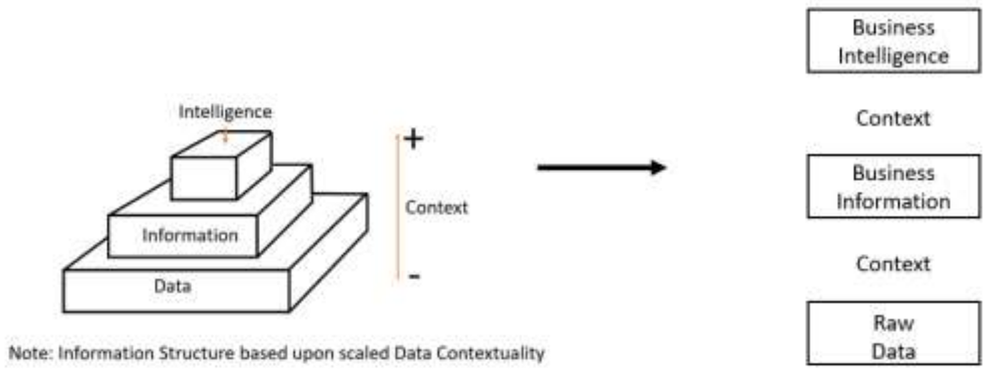
Fig. 16. The fully assembled cube after rotating the cube to add two additional data states, basing the services as an outcome instead of the primary focus, while basing the cube on integrity as the primarily needed service. Finally, breaking down the technical component level securities of people, processes, and technology

To fully address this usage evolution, practitioners must first recognize that this is a generational or evolutionary change in how observed cybersecurity is approached. To harness the full advantage of this expansion of the MSR cube and its components, cybersecurity practitioners need to approach the changes like a mathematical equation. First practitioners should determine in which data state they will perform their action, then they should identify which countermeasure will be the first to encounter the data in the predicted state. The first countermeasure encountered should be the primarily engaged countermeasure, with compensating countermeasures if the primary countermeasure is known to not completely nullify identify suspected threats. The final objective or security service should be viewed as the outcome and the last part of an equation to facilitate an understanding that it is not the beginning but rather an end. A formula might ressemble *Data State + Primary Countermeasure + Secondary Countermeasure = Desired Security Service* (as you can focus on which desired security service you want to build).

4. Process countermeasures component

Processes are the glue holding people to technology within the organization; it is a method in which people engage technology. Processes are native to every occurring thing, and the concepts are native to all persons; mastery, however, may not be. Therefore, it is essential to deconstruct processes for what they are, an action or set of actions moving toward a goal. The same is valid for technology, which automates people's actions to reduce the time spent performing activities to reach a goal.

If we once again consider data as the foundation of our action, we recognize data is the basis for action within the organization. Data must go through an act or series of activities to become usable information within an organization; it must then again go through an act or series of activities to become usable or actionable business intelligence. A simplistic way to embrace this is that information answers day-to-day or *operational* questions, while business intelligence often provides answers to long-term or *strategic* questions. As data works through these actions, the organization adds context to the individual data elements for the organization to function. The stack should be separated and context drawn between the layers to visualize this.



Note: Information Structure based upon scaled Data Contextuality

Figure 1. Data to information to intelligence relationship

The best method is to now place this framework within the people, process, and technology countermeasures. This simplified look clarifies the understanding of the nature of processes, which is an action or series of actions becoming the following contextual business product. At this point, the two lines represent boundaries and a*re a representative zone* separating the people from technological countermeasures. This space represents the processes interconnection of the people and technology countermeasures. The next step is to narrow the process countermeasure to represent a single set of actions to represent a single organizational activity. The model now resembles two rectangles sitting side by side. This line represents the contextualization between each business product, and it separates people from technologies, in essence, the *technology capability and people skills line*.

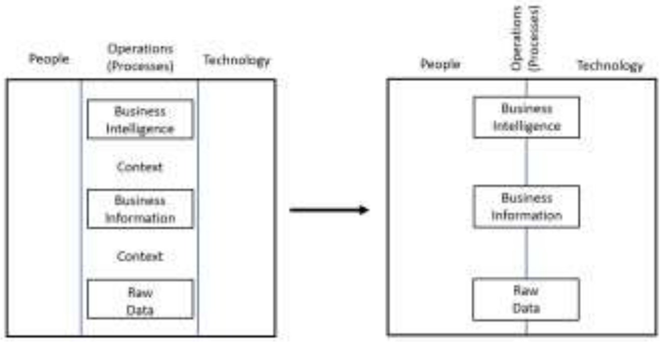


Figure 2. Single processes countermeasure line

Organizations have different capabilities for people and technology. This line is not straight but instead follows the technology capability and people skills line within the organization.

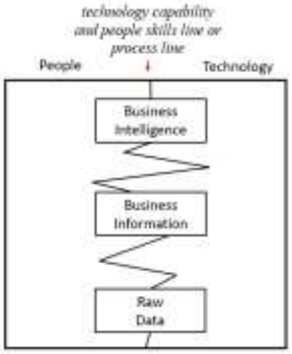


Figure 3. Example of process countermeasures line variations based upon organizational people and technologies variations.

This technology capability and people skills line represents many elements in many different organizational types, including process action component identification layers.

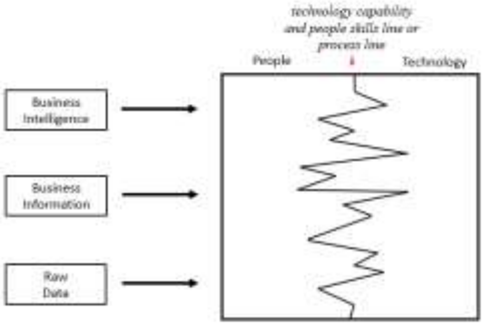


Figure 4. Visual explanation of phasing discrepancies between people or technology process operations

It is crucial to note experts will exist on both sides of the technical capability and people skills process line. Consider the technology or people countermeasure fields as a technology capability and people skills process line. Visualize this process line as a countermeasure component representative of several sub-components. These subcomponents might include experts in some of these fields: leadership alignment, work translation, efficiency, workforce alignment, portfolio management, program management, project management, process tasking, data processing, process engineers, process alignment engineers, or data collection. Many of these specializations already have national and international process accreditation [17]. The American national and international ISO/ANSI 17024 accreditation validates that these certifying organizations and skill sets meet standards predetermined for organizations meaning they are now ready to be professionally engaged (Frenzel & McAndrews, 2022). These roles may or may not exist based on organizational need, alignment, or even maturity.

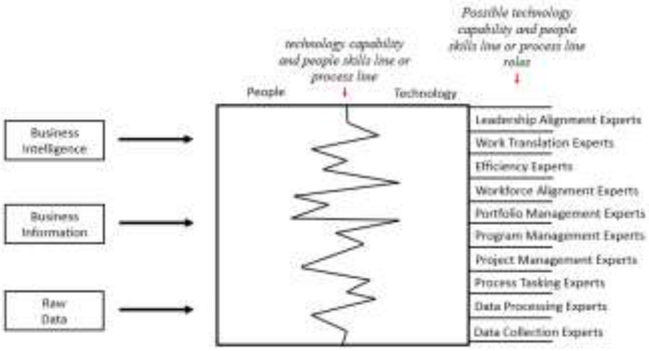

Possible technology capability and people skills line or process line roles
technology capability and people skills line or process line
People
Technology
Business Intelligence
Business Information
Raw Data
Leadership Alignment Experts
Work Translation Experts
Efficiency Experts
Workforce Alignment Experts
Portfolio Management Experts
Program Management Experts
Project Management Experts
Process Tasking Experts
Data Processing Experts
Data Collection Experts

Figure 5. Visual explanation of phasing discrepancies between people or technology process operations specialists and sample working job titles

5. Process countermeasures component security

Once again, understanding there are process specialists who start and align with technology or process specialists who align with people skills is key to understanding the concepts dealing with process countermeasure component security. This process is much simpler to explain than the processes understanding but may take much longer to master. It is weaponizing the people or technology process operation specialists via adversarial thinking [7]. Weaponization is the process by which professionals teach adversarial thinking to understand better how an outside entity would engage an organizational asset for an outside entity's gain [7]. This new organizational asset is an Operational Security or *OPSEC* specialist. Still, as previously shown, the specialist is now either a technologist component level security specialist or a people component level security specialist based upon their background. The combined MSR cube should now look something like this:

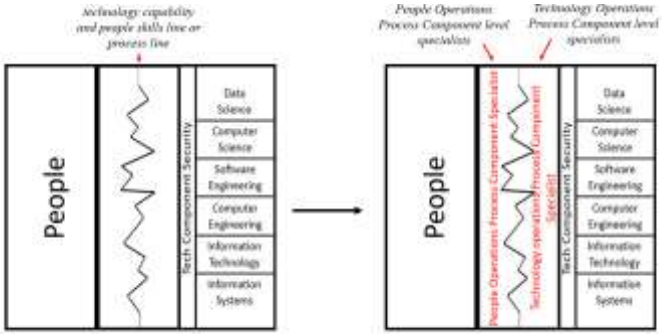


Figure 6. Evolved countermeasure face of the MSR cube following component identification for processes

Once we add adversarial thinking as a specialization for people or technology operations process component level specialists, these operations process component level specialists become technology operations process component level security specialization.

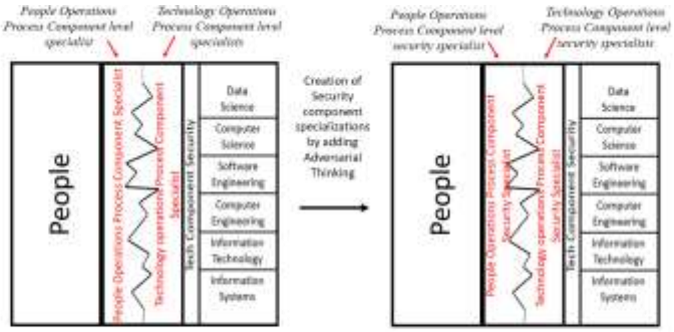

People Operations Process Component level specialist
Technology Operations Process Component level specialists
People
People Operations Process Component Specialist
Technology operations Process Component Specialist
Tech Component Security
Data Science
Computer Science
Software Engineering
Computer Engineering
Information Technology
Information Systems
Creation of Security component specializations by adding Adversarial Thinking
People Operations Process Component level security specialist
Technology Operations Process Component level security specialists
People
People Operations Process Component Security Specialist
Technology operations Process Component Security Specialist
Tech Component Security
Data Science
Computer Science
Software Engineering
Computer Engineering
Information Technology
Information Systems

Figure 7. Evolved countermeasure face of the MSR cube following component level security identification for processes

The final possible cube now resembles this.

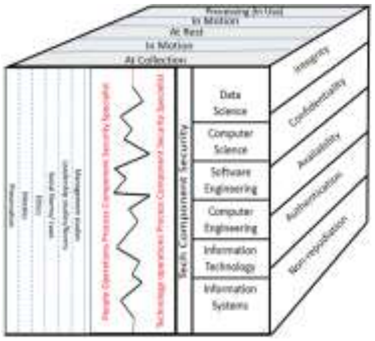


Figure 8. Final cube with all three countermeasures displayed with component level securities

6. Future Implications and call to action

Understanding the component security involved in the day-to-day operations of an organization is critical for the organization's continued defense. Organizations need to identify cybersecurity security specialists quickly, but not all cybersecurity countermeasure security specialists are equivalent. For example, a specialist in IT security is not a specialist in Computer Science or Software Engineering security, commonly referred to SecDevOps; the two would seldom, if ever, respond to a job announcement for one another without additional training. So why are entry-level security technicians placing terms such as cybersecurity technician on their resumes?

Would companies be better off searching for security specialists of a given specialization versus the mystical cybersecurity unicorn? Would it be better for these entry-level security specialists to identify their domain and play to that strength? It is time for organizations to realize their cybersecurity shortage is because they have failed to determine what they need: a technical security component specialist.

7. Conclusion

The Maconachy, Schou, and Ragsdale or MSR model covers many forms of component security if individuals or organizations simply take the time to understand and expand the technology component securities built into the model itself. The longer the fields of cybersecurity remain focused on outcomes without focusing on the pathways to achieve the outcomes, the longer the field will be delayed in implementing holistic solutions. To move from our current state of cybersecurity which focuses on modeling outcomes we must evolve to engage our data states and countermeasures first versus attempting to add these after the fact. We can evolve our cybersecurity through using data states and countermeasures to solve for our security service needs by simply expanding the MSR model. Additionally, there is a need to engage both technical and non-technical specialists, in their appropriate fields of study, from inside and outside the cybersecurity fields of practice.

References

[1] S. Back and J. LaPrade. (2019). The future of cybercrime prevention strategies: Human factors and a holistic approach to cyber intelligence. International Journal of Cybersecurity Intelligence & Cybercrime, 2(2), pp. 1-4. https://www.doi.org/10.52306/02020119KDHZ8339

[2] Cyber2yr2020 Task Group. (2020). "Cybersecurity curricular guidance for associate-degree programs," Association for Computing Machinery, New York, NY, USA. http://dx.doi.org/10.1145/3381686

[3] IBM Security. (2021). Cost of a data breach report 2020. https://www.ibm.com/security/services

[4] The Joint ACM/AIS MSIS 2016 Task Force. "Msis 2016 global competency model for graduate degree programs in information systems," Association for Computing Machinery, New York, NY, USA. 2016. https://doi.org/10.1145/3127597

[5] CC 2020 Task Force. "Computing curricula 2020: Paradigms for global computing education," Association for Computing Machinery, New York, NY, USA. 2020. https://doi.org/10.1145/3467967

[6] E. Tuorinsky, *The human factor in cybersecurity: Overcome human nature with a lock the door mentality.* September 2021. https://www.securitymagazine.com/articles/96009-the-human-factor-in-cybersecurity

[7] Joint Task Force on Cybersecurity Education. "Cybersecurity curricula 2017: Curriculum guidelines for post-secondary degree programs in cybersecurity," Association for Computing Machinery, New York, NY, USA. 2018. https://doi.org/10.1145/3184594

[8] W.V. Maconachy, C.D. Schou, D. Ragsdale, and D. Welch. "A model for information assurance: An integrated approach." *Proceedings of the 2001 IEEE, Workshop on*

Information Assurance and Security, United States Military Academy, West Point, NY, 5-6 June, 2001, pp. 306-310.

[9] M. Malatji, V.S. Sune, and A. Marnewick. Socio-technical systems cybersecurity framework. *Information and Computer Security, 2019. 27*(2), 233-272. http://dx.doi.org/10.1108/ICS-03-2018-0031

[10] J.R. McCumber. "Information systems security: A comprehensive model", *Proceedings of the 14th National Computer Security Conference.* National Institute of Standards and Technology. Baltimore, MD. October 1991, pp. 1-6.

[11] D. Parker. Fighting computer crime: A new framework for protecting information. Wiley Computer Publishing. 1998.

[12] A. Parrish, J. Impagliazzo, R. K. Raj, H. Santos, M. R. Asghar, A. Jøsang, T. Pereira, and E. Stavrou. "Global perspectives on cybersecurity education for 2030: A case for a meta-discipline." *In Proceedings Companion of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education (ITiCSE '18 Companion)*, July 2–4, 2018, Larnaca, Cyprus. ACM, New York, NY, USA, 2018. 19 pages. https://doi.org/10.1145/3293881.3295778

[13] R. C. Reid and A. H. Gilbert. "Using the parkerian hexad to introduce security in an information literacy class." *In 2010 Information Security Curriculum Development Conference (InfoSecCD '10).* Association for Computing Machinery, New York, NY, USA, 2010. 45–47. DOI: https://doi.org/10.1145/1940941.1940953

[14] A. Sosin. How to increase the information assurance in the information age. Journal of Defense Resources Management, 04/2018, Volume 9, Issue 1, 45-57. https://doaj.org/article/2dbbd0cb37444c0fb51d3df6d5c24cf5

[15] US Bureau of Labor Statistics. National compensation survey: Guide for evaluating your firm's jobs and pay. 2013. https://www.bls.gov/ncs/ocs/publications.htm

[16] E. Frenzel and I. McAndrews. "Cybersecurity: A brief introduction for grades k-12 instructors and non-practitioners," 2022. *Educational Leadership*. Submitted for publication.

[17] ANSI National Accreditation Board (2022). ANSI/ISO/IEC 17024 (Accredited). https://anabpd.ansi.org/Accreditation/credentialing/personnel-certification/ALLdirectoryListing

[18] E. Frenzel and I. McAndrews. "Component Security vs. Cybersecurity: Defining next generation Cybersecurity" 2022. *International Journal of Applied Technology & Leadership*. [Online]. 2(6). Available: https://www.ijatl.org/jr-paper_issue/?select_volume=2&select_issue=1