Evaluative Thinking: Addressing Complex Adaptive Challenges in the Agricultural Cybersecurity Workforce

Samson Adeoye
sadeoye@vt.edu
Department of Agricultural, Leadership, and Community Education

This work was supported [in part] by the Commonwealth Cyber Initiative, an investment in the advancement of cyber R&D, innovation, and workforce development. For more information about CCI, visit development http://www.cyberinitiative.org.

VIRGINIA TECH

Session Agenda

"We ignore the human element of cyber threats at our peril" (Marble et al., 2015).

Note: Image from flickr.com

1. Cybersecurity and the Human Factor
2. Agricultural Cybersecurity
3. Evaluative Thinking and Adaptive Knowledge-worker
4. Cybersecurity Strategy: Building a Robust Culture
5. Capacity Building: Adaptive Evaluation and Adaptive Leadership
6. Questions & Comments

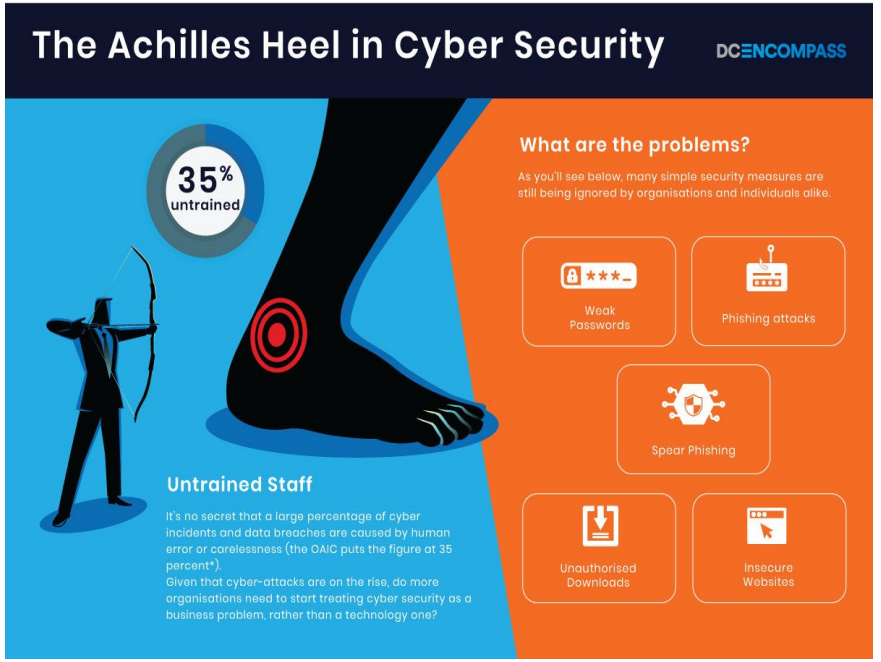
Cybersecurity and the Human Factor

- Cybersecurity is a growing high risk problem associated with everything an individual or organization does that is enhanced by the internet (Yusif & Hafeez-Baig, 2021)
- Challenges are complex, transboundary, emerging, and highly politicized (Carr & Lesniewska, 2020; Mezher & Mdool, 2022).
- Due to the adaptive nature, technical and rationalistic approaches are not sufficient (Archibald et al., 2018)
- Humans generally take actions they perceive as logical; not intending to set themselves for failure (Marble et al., 2015)

Note: Image from https://medium.com/@dvozen/social-engineering-cybersecuritys-achilles-heel-fb3cc5891231

Cybersecurity and the Human Factor

- Cyber attackers consider humans (workforce) as weak attractive exploit targets (Ani & He, 2018)
- Cyber tools are technically engineered
- “Continued reliance on engineered solutions to cyber incursions” is reductionist (Marble, 2015)
- Preventing attacks depends on humans’ understanding of emerging complexities (Marble, 2015)
- Humans are at the center of the NIST Cybersecurity Framework: identify, protect, detect, respond, and recover (Mahn, 2018)



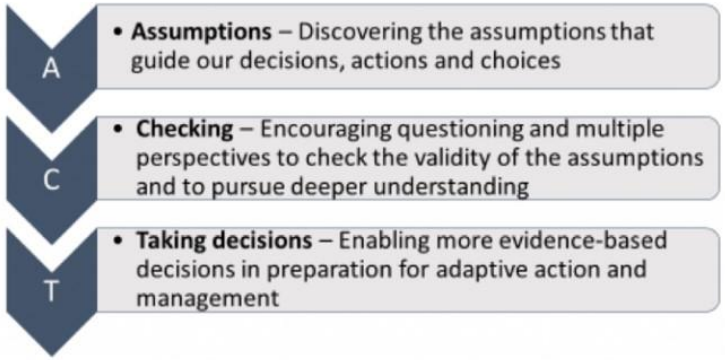
Note: Image from https://dcencompass.com.au/blog/untrained-staff-the-achilles-heel-in-cyber-security-and-it-infrastructure/

Why Agricultural Cybersecurity?

- Past technological revolutions began on the farm, but the digital revolution is sparked at multiple nodes along the agricultulture and food value chain (Schroeder et al., 2021)
- Heterogeneous technology and data requirements (e.g. robots, remote sensing, drones, farm management softwares, sensor networks, etc.) (Cheein & Carelli, 2013; Chi et al., 2017; Sontowski et al., 2020)
- Differential cybersecurity measures and strategies across the food and agriculture value chains
- Agriculture has not well adapted to the digital world, leading to many vulnerabilities in operational systems (Stephen et al., 2023)
- Threats to the fight against food insecurity, hunger, malnutrition, and sustainable food production (Murch & Drape, 2022; Duncan et al., 2019; Stephen et al., 2023)
- Data breaches and operations disruption in Ag have multiplier effects on other sectors like health, the environment, and our collective existence

Evaluative Thinking

Evaluative Thinking Process



Note: Image from Sharrock et al. (2017). https://aea365.org/blog/evaluative-thinking-as-a-way-of-doing-business-by-guy-sharrock-tom-archibald-and-jane-buckley/

"Critical thinking

applied in the context of evaluation,

motivated by an attitude of inquisitiveness and a belief in the value of evidence,

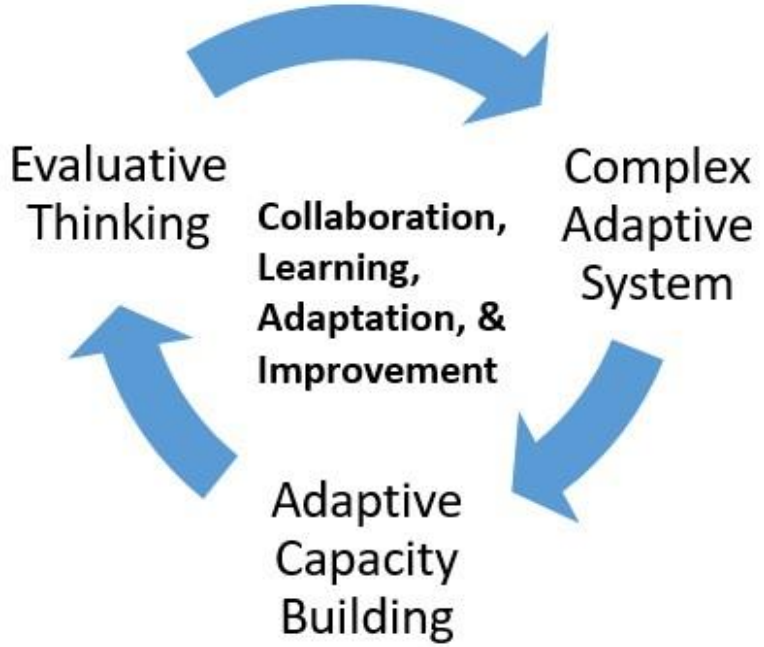
involves identifying assumptions, posing thoughtful questions, pursuing deeper understanding through reflection and

perspective taking, and informing decisions in preparation for action" (Buckley et al., 2015, p. 378)

Developing Adaptive "Knowledge Workers"

"Instead of simply executing technical processes based on predetermined plans, … practitioners can be "knowledge workers" who use evaluative thinking to promote collaboration, learning, and adaptation" (Archibald et al., 2018)

- Knowledge work transcends conventional, routine, linear, rationalistic work
- A "combination of convergent, divergent, and creative thinking" (Archibald et al., 2018)
- Complex adaptive system supports evaluation capacity building (Larenz et ai., 2018)



Developing Adaptive Knowledge Workers

Evaluative Thinking and Complex Adaptive Challenges

Evaluative Thinking

Reflects on and assesses information/situations

Identifies and defines problems

Promotes strategy development

Prioritizes evidence and analysis

Considers differing perspectives and interest groups

End goal is accurate judgment and decision making

Complex Adaptive Challenges

Dynamic, unpredictable, interrelated situations

Messy, ambiguous problems

Requires tailored strategies and feedback loops

Requires analysis and evaluation of strategies

Involves multiple stakeholders with conflicting interests

Requires targeted, adaptive actions to resolve

Ag. Cybersecurity Strategy: Building a Robust Culture

Collaboration

- Cybersecurity is polycentric and depends on collaborative efforts (Carr & Lesniewska, 2020)
- Collaboration and partnership are the life-blood of cyber and infrastructure security (CISA, n.d)

Learning

- Learning from incidents and responses promotes security strategy development (Ahmad et al., 2020)
- Reflective learning translates knowledge into beneficial cyber action (Trim & Upton, 2016)

Adaptation

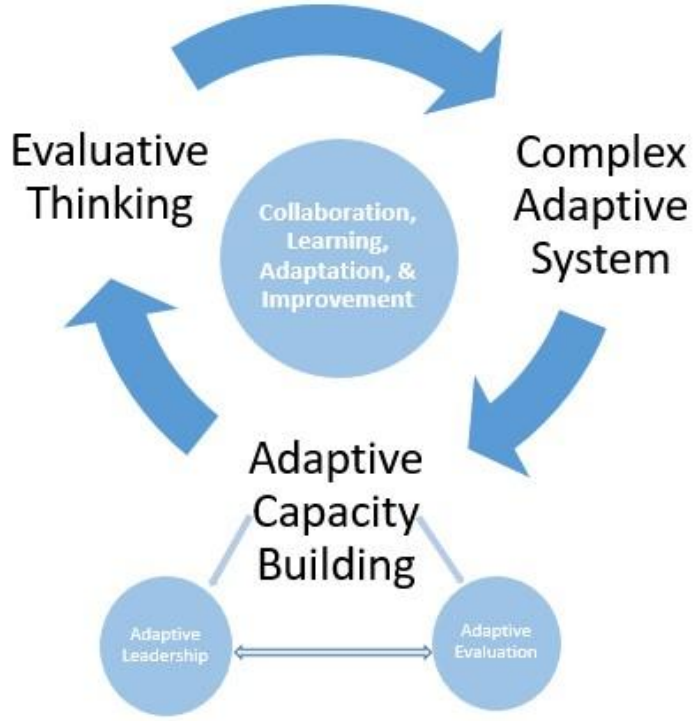
- Adaptation of systems operators and users an important element in risk assessment and management processes (Busby, 2017)
- Cyber strategies must adapt to organizational culture or vice versa (Haas, 2023)

Improvement (Continuous Measured Improvement)

- No one-size-fits-all strategy for cybersecurity (Baral, 2022)
- Technological change is ever-dynamic and can outpace man (UNCTAD, 2019)

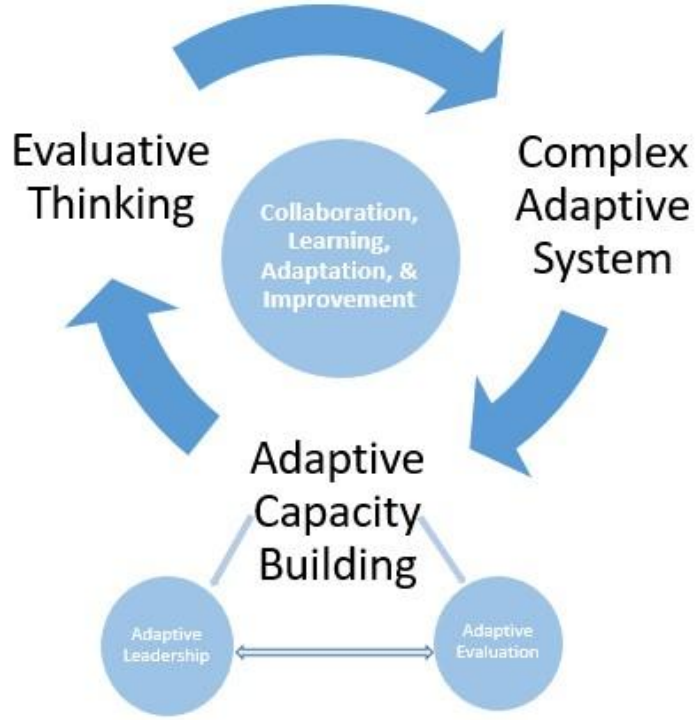
Capacity Building: Adaptive Evaluation + Adaptive Leadership

- Requisite resources and motivation to conduct, analyze, and use evaluations (Gibbs et al., 2002)
- Adaptive evaluation is complexity-based approach to systematic learning supporting innovation (Gokhale & Walton, 2022)
- Evaluation capacity building is hampered by organizational leadership (Preskill & Boyle, 2008)
- Adaptive leadership addresses required adaptation by people in response to changing environments (Heifertz, 2009)



Ag Cybersecurity Workforce Development Framework

Why does this Model Matter for Cybersecurity Strategy?



- Promotion of monitoring, evaluation, accountability, and learning (MEAL) (Archibald et al., 2018)
- Monitoring, evaluation, accountability influence employees attitude toward cybersecurity (Alqahtani & Braun, 2021)
- Constructive challenge of own assumptions and those of others to generate new wisdom (Britton, 1998)
- Human factor of cybersecurity are psychological and cognitive-based, drawing on heterogeneous factors (Yusif & Hafeez-Baig, 2021)
- Agricultural cybersecurity strategy development
- Transformation of the agricultural cybersecurity workforce from mere technical to adaptive and knowledge-working

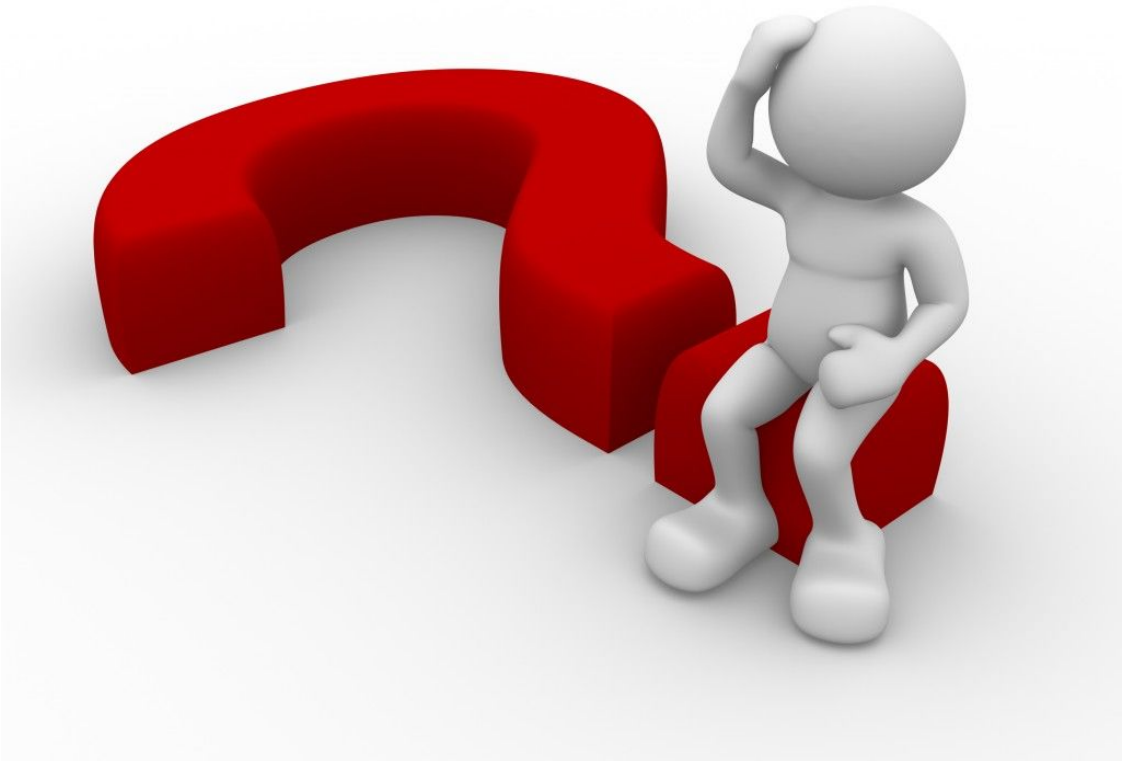
Key Takeaways

- Educators, practitioners, and researchers need to recognize and rise to the growing importance of cybersecurity within the agriculture sector, particularly the vulnerabilities in food and agriculture systems
- Agricultural organizations must stress the importance of implementing practical, human-centered cyber guidance to improve security and resilience of critical infrastructure
- Monitoring, evaluation, accountability, and learning (MEAL) are key to enhanced cybersecurity awareness, preparedness, and resilience in the agriculture sector
- Given the emerging nature of technology, evaluative thinking creates opportunities for integrating proactive and adaptive cybersecurity approaches in addressing vulnerabilities in the agriculture sector

Thank you!

VIRGINIA TECH™

Questions and Comments



Note: Image from Indra Consulting

References

Ahmad, A., Desouza, K.C., Maynard, S.B., Naseer, H., Baskerville, R.L. (2020). How integration of cyber security management and incident response enables organizational learning. *Journal of the Association of Information Science and Technology., 71,* 939-953.

Alqahtani, M. & Braun, R. (2021). Examining the impact of technical controls, accountability and monitoring towards cyber security compliance in e-government organisations. *Research Square.* https://doi.org/10.21203/rs.3.rs-196216/v1

Archibald, T., Sharrock, G., Buckley, J., & Young, S. (2018). Every practitioner a "knowledge worker": Promoting evaluative thinking to enhance learning and adaptive management in international development. In A. T. Vo & T. Archibald (Eds.). *Evaluative Thinking. New Directions for Evaluation,* 158, 73–91.

Baral, A. (2022). Continuous measured improvement: A new approach to meeting the municipal cybersecurity challenge. Bachelor's thesis, Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology.

Britton, B. (1998). *The learning NGO*. Occasional Paper Series Number 17. Oxford.

Buckley, J., Archibald, T., Hargraves, M., & Trochim, W. M. (2015). Defining and teaching evaluative thinking: Insights from research on critical thinking. *American Journal of Evaluation*, *36*(3), 375–388. https://doi.org/10.1177/1098214015581706

Busby, J.S., Green, B., Hutchison, D. (2017). Analysis of affordance, time, and adaptation in the assessment of industrial control system cybersecurity risk. *Risk Analysis, 17,* (7), 1298-1314. https://doi.org/10.1111/risa.12681

Carr, M., & Lesniewska, F. (2020). Internet of Things, cybersecurity and governing wicked problems: Learning from climate change governance. *International Relations, 34*(3), 391-412. https://doi.org/10.1177/0047117820948247

Cheein, F. A. A. & Carelli, R. (2013). Agricultural robotics: Unmanned robotics service units in agricultural tasks. *IEEE Industrial Electronics Magazine 7*(3), 48-58. https://doi.org/10.1109/MIE.2013.2252957

Chi, H., Welch, S., Vasserman, E., & Kalaimannan, E. (2017). *A framework of cybersecurity approaches in precession agriculture.* In A. R. Bryant, J. R. Lopez, & R. F. Mills (eds.). *Proceedings of the 12th International Conference on Cyber Warfare and Security.* pp. 90-95.

Cybersecurity and Infrastructure Security AGency (CISA) (n.d.). *Partnerships and collaboration.* https://www.cisa.gov/topics/partnerships-and-collaboration

Duncan, S. E., Reinhard, R., Williams, R. C., Ramsey, F., Thomason, W., Lee, K., Dudek, N., Mostaghimi, S., Colbert, E., & Murch, R. (2019). Cyberbiosecurity: A new perspective on protecting U.S. food and agricultural system. *Frontiers in Bioengineering and Biotechnology, 7*, 63. https://doi.org/10.3389/fbioe.2019.00063

Gibbs, D., Napp, D., Jolly, D., Westover, B., & Uhl, G. (2002). Increasing evaluation capacity within community based HIV prevention programs. *Evaluation and Program Planning, 25,* 261-269.

Gokhale & Walton, M. (2022, September 9). *Adaptive evaluation - A complexity-based approach to systematic learning for innovation and scaling in development.* IMAGO Global Grassroots.

Haas, T. C. (2023). Adapting cybersecurity practice to reduce wildlife cybercrime. *Journal of Cybersecurity,* 1-20. https://doi.org/10.1093/cybsec/tyad004

References

Heifetz, R. A., Grashow, A., & Linsky, M. (2009). *The theory behind the practice: A brief introduction to the adaptive leadership framework*. Harvard Business Press. https://www.hbsp.harvard.edu/product/3241BC-PDF-ENG

Lawrenz, F., Kollmann, E. K., King, J. A., Bequette, M. Pattison, S., Nelson, A. G., et al. (2018). Promoting evaluation capacity building in a complex adaptive system. *Evaluation and Pragram Planning, 69*, 53-60. https://doi.org/10.1016/j.evalprogplan.2018.04.005

Mahn, A. (2018, October 23). *Identify, protect, detect, respond and recover: The NIST Cybersecurity Framework*. Identify, Protect, Detect, Respond and Recover: The NIST Cybersecurity Framework | NIST

Marble, J. L., Lawless, W. F., Mittu, R., Coyne, J., Abramson, M., & Sibley, C. (2015). The human factor in cybersecurity: Robust & intelligent defense. In S. Jajodia et al. (Eds.). *Cyber Warfare, Advances in Information Security 56*, 10.1007/978-3-319-14039-1_9

Mezher, A. A. & Mdool, A. S. (2020). Relationship between continuous improvement and quality cybersecurity. *PJAEE, 19*(2),365- 377.

Murch, R., & Drape, T. A. (2022). *Leveraging cyberbiosecurity to safeguard agriculture and food* [White paper]. VTechWorks. http://hdl.handle.net/10919/112168

Preskil, H. l & Boyle, S. (2008). A multidisciplinary model of evaluation capacity building. *American Journal of Evaluation, 29*(4). https://doi.org/10.1177/1098214008324182

Schroeder, K., Lampietti, J., Elabed, G. (2021, March 16). *What's cooking: Digital transformation of the agrifood system.* Agriculture and Food Series, World Bank. http://hdl.handle.net/10986/35216

Sontowski, S., Gupta, M., Chukkapalli, S.S.L., Abdelsalam, M., Sudip, M., Joshi, A. et al. (2020). Cyber attacks on smart farming infrastructure. *IEEE 6th International Conference on Collaboration and Internet Computing (CIC)*, pp. 135-143. https://doi.org/10.1109/CIC50333.2020.00025

Stephen, S., Alexander, K., Potter, L., Palmer, XL. (2023). Implication of cyberbiosecurity in advanced agriculture. *Proceedings of the 18th International Conference on Cyber Warfare and Security, 18*(1), 387-393.- https://doi.org/10.34190/iccws.18.1.995

Tim, P. & Upton, D. (2016). *Cybersecurity culture: Counteracting cyber threat through organizational learning and training.* Routledge

UNCTAD (2019). *The impact of rapid technological change on sustainable development.* United Nations publication, UNCTAD/DTL/STICT/2019/10.

Yusif, S. & Hafeez-BAig, A. (2021). A conceptual model for cybersecurity governance. *Journal of Applied Security Research, 16*(4), 490-523. https://doi.org/10.1080/19361610.2021.1918995