Open Access License Notice

Invited Professional Paper

Envisioning Alternate Futures Will Change Our Thinking About Cybersecurity

Deep Kakkar and Lori Gordon

Abstract - The world is changing in new and profound ways. These shifts will substantially alter how the cybersecurity workforce will do its job in the future and will require innovative, shared thinking and decisions. Today, efforts to understand the future cybersecurity environment are focused on exercising known technological threats at the sector or organizational level. This is limiting and could too narrowly focus planning and decisions, as it is not reflective of broader, macro-level global shifts across social, economic, environmental, and political changes. An organizing construct is needed to understand how this broader risk environment may impact the future of cybersecurity. 'Alternate Futures' is a method within the broader discipline of foresight to consider a range of futures (e.g., probable, possible, preferable) twenty to thirty years from now across an organizational, cross-discipline, or global domain, and to create or alter our strategies, goals, plans, and actions to achieve desired outcomes. Alternate Futures is a method by which we: identify macro-level factors that will impact our world (e.g., social, technological, economic, environmental, political, legal), create scenarios for changes brought about by these factors (e.g., how will our world benefit or be worse off?), identify key drivers of change that could invoke these scenarios (e.g., changes in global interdependencies, government budgets, access to information, demographic shifts), and identify strategic needs that will ensure we are successful if any of these alternate futures unfold. Results from a small study we conducted of cybersecurity professionals across a range of roles aligned to NIST's Cybersecurity Workforce Framework indicated that they saw significant value in thinking more broadly and over a longer timeframe, as it would help to identify areas of risk convergence across multiple business functions, support CSO/CTO/CISO and governance board decision making processes, provide the cybersecurity community with a shared sense of direction and urgency to drive action toward meeting future needs, and ultimately to prepare the cybersecurity community for whatever challenges and opportunities the future holds.

To achieve these outcomes, we recommend creating cross-sector and cross-business line communities to facilitate thinking around Alternate Futures.

Keywords

cybersecurity, Alternate Futures, foresight, scenario, resilience, strategy, planning, sectors, social, technological, economic, environmental, political

1 INTRODUCTION

The world is changing in new and profound ways. In the past few decades, we've witnessed historic social, technological, and economic progress as people are more connected, and individuals, organizations, and states are more empowered. Despite this progress, we've experienced significant shocks, ranging from the 2008 Global Financial Crisis to the recent WannaCry and NotPetya cyber attacks, which created uncertainty, indecision, and instability across all sectors of society and infrastructure. In the next few decades we will undoubtedly experience similar events, and although our world will change in ways we can't fully predict, we can better prepare for the next WannaCry by being more deliberate about thinking farther into the future and considering a variety of scenarios in which the future could play out.

Currently, much of the discussion around the future of cybersecurity is focused on threats driven by *technological* factors, known threats, and the capabilities that will be needed to mitigate those threats. However, as the world is becoming more interconnected, interdependent, and volatile across social, economic, environmental, and political factors, these factors will increasingly impact the cybersecurity environment equal to or even more so than technological change. This is why it is critical that those in the cybersecurity workforce consider these broader global factors and the trends underpinning them across a range of alternate

futures, in order to make better decisions now that will prepare them for whatever future unfolds.

2 HISTORY OF ALTERNATIVE FUTURES

Foresight as a broader discipline was first conducted by the government after World War 2 to help agencies such as the U.S. Army understand the new world order, and specifically to help them with force planning, eliciting discussions about key assumptions, priorities, and choices.[1] [2] The concept of Alternate Futures was first conceptualized in the 1970's by Shell Oil economists in their "shift from precise data-driven prognostication to multiple futures and the use of various assumptions (e.g., discovery of new oil fields) to anticipate major changes." They explored how the future might unfold through best- and worst-case narratives.[3] Several government organizations such as the Office of the Director of National Intelligence (ODNI)'s National Intelligence Council (NIC) have embraced the concept and are using it to produce strategic assessments of how key trends might shape the world over the next 20 years to help senior leaders plan for the longer term.[4] While seminal work with Alternate Futures has been done in geospatial and space science, disruptive technologies are now shaping corporations and society. Today, this presents a significant opportunity for Alternate Futures to play a role in better understanding how IoT, autonomous systems, machine learning, data analytics and other technologies will impact industries including transportation, healthcare, industrial, technology, manufacturing, and finance.[5]

3 ALTERNATIVE FUTURES AND CYBERSECURITY

As these disruptive technologies are increasingly being integrated into the web of networks across interconnected and interdependent industries, this will introduce

[1] https://www.rand.org/pubs/monographs/MG219.html
[2] https://www.rand.org/pubs/papers/P7929.html
[3] http://www.nejm.org/doi/full/10.1056/NEJMp1704149?page=&sort=oldest&#article
[4] https://www.dni.gov/index.php/global-trends-home
[5] http://www.altfutures.org/pubs/PSFN/2015_Sanford_PSFN.pdf

both risks and opportunities in the field of cybersecurity. As such, cybersecurity practitioners would benefit from the use of Alternate Futures to better anticipate and prepare for future environments. A literature review, however, revealed scant evidence that the cybersecurity community is using Alternate Futures to assess how broader social, economic, environmental, and political trends as well as a range of future possible environments (looking 20-30 years from now and beyond) could impact cybersecurity. And in a study that we conducted of cybersecurity professionals,[6] half of the respondents indicated that they had not heard of the concept of Alternate Futures. Although more research is needed to understand why futures may not be prevalent across the cybersecurity community, it may be because of the expense and resourcing required, the need to prioritize near-term threats and to conduct time-consuming routine operations, or that executive management has not yet made the business case.

The cybersecurity community can benefit from Alternate Futures in ways similar to those that other communities are using it. For example, corporations and government agencies use Alternate Futures to better understand potential risks and distribute material to stakeholders communicating these risks. The US Congressional Budget Office[7] uses Alternate Futures to make long term budget projections. The US Department of Veterans Affairs uses Alternate Futures in enterprise risk management and planning decisions. In Singapore, the UK, and Finland, this process familiarizes leaders with the early signs of potentially disruptive

[6] We conducted a survey of cybersecurity professionals in November/December 2017 to understand the desire for Alternate Futures to help as a decision-making tool in the field of cybersecurity. The questions in the survey *Envisioning Future Worlds: What Global Trends Will Influence and Impact Cybersecurity?* were designed to gather information on participant demographics (e.g., job role/level in cybersecurity), familiarity with Alternate Futures, views on how Alternate Futures might help inform the future of cybersecurity, etc. Thirty-six percent of respondents to the survey identified as having roles in governance, strategy, and training, 18% risk management, 13% threat analysis, 13% system administration, and the rest operational planning, defense/response, or investigation/forensics. The executive, business, and operational level breakdown was 30%, 25%, and 45%, respectively. The industry, academia, and government breakdown was 76%, 11%, 11%, and 2%, respectively.

[7] "Long-Term Budget Projections". *Congressional Budget Office*. https://www.cbo.gov/publication/45308

change on the horizon.[8] Corporations, particularly those with long product development life cycles like the Shell Corporation,[9] use Alternative Futures in the development of their business strategies. The number of private and academic organizations conducting futures (more than 40 leading domestic and international research centers and programs according to Wikipedia) is indicative of its powerful role to inform business strategy and technology and workforce decisions.

Currently, government, industry, and academia are more focused on the here and now - on assessing near-term threats and risks to cybersecurity through exercises which range from multi-day, national and international-level exercises[10] to 15-minute state-level exercises.[11] Some tabletop and cyber range exercises look at a variety of cyber threats[12] and others are more focused on specific threats or specific sectors.[13] [14]

Discussions around the longer-term future of cybersecurity that are taking place are focused on how hackers could become more malevolent and identify new ways to penetrate networks or how the integration of emerging technology (AI, IoT) will introduce network vulnerabilities.[15] While important, this focus neglects larger macro-level trends that would enable us to identify significant gaps or needs borne from social, economic, environmental, or political trends. For example, it is imperative that the cybersecurity community consider the very real potential that increasing climate instability and natural disasters will require more congressional attention and funding, which could result in slashes to cyber range grants, thereby

[8] "Foresight in the Public Sector: 2017 Update". *AAI Foresight Inc.* October 10, 2017. http://www.aaiforesight.com/blog/foresight-public-sector-2017-update
[9] "Shell Scenarios". *shell.com*. Archived from the original on 2015-03-07. https://web.archive.org/web/20150307044027/http://www.shell.com/global/future-energy/scenarios.html
[10] https://www.mitre.org/sites/default/files/publications/pr_14-3929-cyber-exercise-playbook.pdf
[11] http://soc.wa.gov/resources/exercises
[12] https://www.cyberbit.com/cyber-attack-playbook-tabletop-exercise/
[13] http://www.nyba.com/wp-content/uploads/2016/05/PreConf_IncidentResponse_Part2-Exercise.pdf
[14] https://www.hsdl.org/?abstract&did=789781
[15] https://securityintelligence.com/the-future-of-cybersecurity/

impacting the ability of the cybersecurity workforce to maintain the required cybersecurity knowledge, skills, and abilities to counter threats.

The University of California Berkeley's Center for Long-Term Cybersecurity (CLTC) has published a set of robust, near-term scenarios that the field of cybersecurity could face in 2020.[16] [17] We believe that the development of *scenarios with a longer-term horizon* (2040 or beyond) is necessary as well (see Section V below), and that the identification of *drivers of change* and *strategic needs* as they relate to cybersecurity will help enable thoughtful discussions around what decisions and actions need to be made now to better prepare for alternate futures that might unfold (see Section V below). Finally, to launch these Alternate Futures discussions, we need an approach to establish the *cybersecurity communities* that would use Alternate Futures as a strategic planning tool (see Section 6 below).

4 CYBERSECURITY PROFESSIONALS BELIEVE THAT ALTERNATIVE FUTURES IS NEEDED IN THEIR FIELD

We conducted a survey of cybersecurity professionals across a range of roles aligned to NIST's Cybersecurity Workforce Framework[18] to understand the desire for Alternate Futures. Findings were as follows:

- When asked to rank how their role, function, and decision making in cybersecurity might be impacted by social, technological, economic, environmental, and political factors, they indicated that their role would be impacted most by technological factors and least by environmental factors, however, *when we provided scenarios that showcased how environmental factors could be impactful across a range of future outcomes, there was a slight uptick in their view of environmental factors impacting cybersecurity* (for example, if Congress was to shift funds to climate adaptation, this could reduce the amount of funding to cybersecurity).

[16] https://cltc.berkeley.edu/scenarios/
[17] https://cisac.fsi.stanford.edu/events/cybersecurity-futures-2020
[18] NIST's Cybersecurity Workforce Framework lays out work roles across 7 areas: Risk Management, System Administration, Governance, Defense, Threat Analysis, Operational Planning, Investigation/Forensics.

- When asked how their role, function, or decision making might change based on the scenarios provided, respondents indicated that the *most significant impacts would be that standards, regulations, or policies around what they do might change, that their role or activity might change, and that they would make different decisions*.
- Respondents indicated that Alternate Futures would help *identify strategic needs, enable a more effective operating environment, help enterprises assess areas of risk across multiple business functions, and enhance cybersecurity curriculum*. Other areas where Alternate Futures might help are in *hedging against uncertainty and avoiding strategic surprises, promoting information sharing across disciplines, understanding what changes may affect future cyber defense posture and response, and preparing and planning to more effectively operate in our future environment*.
- Half of respondents indicated that they had *not participated* in Alternate Futures discussions.
- *92 percent* of respondents indicated that they *'definitely'* or *'probably'* should do Alternate Futures.

One community that could benefit from Alternate Futures discussion is Cloud providers. As enterprises are migrating to cloud to leverage cost savings benefits and cutting-edge technologies such as Virtual On-demand Infrastructure, Microservices, Containers, Big Data, and Machine Learning, Cloud providers can leverage outcomes from Alternate Futures to explain to policy makers how Cloud adoption can help build economies, reduce carbon footprints, create cohesive societies, and boost startup industries. By looking through broader, global economic, social, and policy lenses, cloud providers could articulate the business case for how the technology can mitigate threats across these factors.

5 HOW TO CONDUCT ALTERNATIVE FUTURES FOR THE CYBERSECURITY COMMUNITY

A foresight capability is needed to understand the factors driving change in our world and to advance strategic thinking and planning in cybersecurity technologies, operations, and workforce. We recommend convening communities across

enterprise business lines and within or across sectors to conduct the Alternate Futures process. To demonstrate what this process might look like and what outcomes could result, we conducted Alternate Futures discussion with 10 individuals in the field of cybersecurity. We focused on how changes in global social, technological, economic, environmental, and political (STEEP) factors would impact cybersecurity, and what positive (pro) and negative (con) scenarios/outcomes could unfold across three industries: Energy, Government, and Emerging Technology. We also discussed what strategic needs are necessary to prepare and plan for these outcomes. Our process was as follows:

- **First, we identified key drivers of change** across macro-level factors (e.g., Social, Technological, Economic, Political, Security & Resilience) that will impact our world (e.g., changes in global interdependencies, access to information, demographic shifts). An exploration of the key drivers of change, including trends and emerging issues, will enable consideration of strategic needs to ensure we are planning and preparing appropriately for these future worlds.
- **Second, we created pro/con scenarios** for changes brought about by these factors (e.g., How will our world benefit? How will our world be worse off?). Scenarios enable us to imagine how converging trends might play out to change the future of cybersecurity. These are not all of the possible trends and implications that affect cybersecurity; they are a starting point for continued dialogue and analysis.
- **Third, we identified strategic needs** for how these alternate future scenarios might play out. Once the drivers have been identified and discussed relative to potential futures, cybersecurity professionals will be asked to identify strategic needs that will better prepare them for these alternate futures. It is critical that communities or groups obtain executive sponsorship to execute on the strategic needs to ensure they are prepared for a range of alternate futures.

5.1 Alternate Futures Discussions with The Cybersecurity Community

5.1.1 Energy

A significant *factor* shaping the future of the Energy industry and that will impact cybersecurity is the *advancement in common virtual electrical power grid technologies and critical infrastructure testing*. As the electric power system makes transformational changes in both supply and demand technologies, we will experience significant changes in the sources we rely on to generate electricity, the means by which we receive electricity, and even in the ways we consume electricity. The transition of communications and control systems from analog to digital, and from systems with a handful of control points at central stations to ones with potentially millions of control points, will provide areas of opportunity, but will also introduce risk. Driving these changes are the modernization of the electric power system, the centralized control on networks in the power distribution sector, and net metering technologies were the excess electricity generated by grid-connected renewable energy systems "turns back" electricity meter as it is fed back into the grid.

- Pro Scenario: The modern grid is more flexible, robust, and agile. It has the ability to dynamically optimize grid operations and resources, rapidly detect and mitigate disturbances, integrate diverse generation sources (on both the supply and demand sides), integrate demand response and energy-efficiency resources, and enable consumers to manage their electricity use and participate in markets.
- Con Scenario: Electrical power grids are more and more susceptible to cyber attacks. A series of recent hacker attacks not only compromised energy companies in the US and Europe but also resulted in the intruders gaining hands-on access to power grid operations—enough control that they could have induced blackouts on American soil at will. Hackers will increasingly be able to obtain operational access control of the interfaces power company engineers use to send actual commands to equipment like circuit breakers, giving them the ability to stop the flow of electricity into US homes and businesses.

To best leverage the opportunities and reduce risks in these alternate future scenarios, cybersecurity individuals must prepare and plan, and make decisions and choices on *strategic needs* which include the development of frameworks, standards, and regulations to mitigate risk; preparing the workforce to analyze various cyber attack incidents in power sector; and creating global information sharing and analysis centers that would provide common central information resource sharing platform.[19]

5.1.2 Government

A significant *factor* shaping the future of government and that will impact cybersecurity is the *growing prevalence of intergovernmental alliances in which member countries agree to mutual defense in response to an attack by any external party*. Driving this is an increasingly integrated world in which political conflict and instability, the movement of data and information, and health threats like pandemics, will move beyond borders. Countries are recognizing that cyberwarfare is an operational domain of war, just like land, sea and aerial warfare, and therefore partnering to share sensitive data with other governments to help mitigate threats to their infrastructure and political and social way of life.

- Pro Scenario: Mutual cooperation and trust prevails in nations partnering against external threats. They are sharing certain data highlighting the offending or malicious IPs (internet protocol address) with a central organization so that member countries at large can benefit and the entire digital ecosystem can be protected.
- Con Scenario: Collaborations between countries break down due to any one or more of the macro-level factors. Allies become adversaries. In economic or social challenges that will leave a country less stable – such as weak GDP growth, high debt in some segments of society, financial market volatility, and fewer dominant industries – it may proactively shut down its borders including virtual borders, which will shut down

[19] References: https://www.wired.com/story/hackers-gain-switch-flipping-access-to-us-power-systems/

intelligence sharing as well. Attacks to data centers are prevalent because adversaries now know their physical locations and IP addresses.

To best leverage the opportunities and reduce risks in these alternate futures (pro and con scenarios), cybersecurity individuals must prepare and plan, and make decisions and choices on *strategic needs* which include identifying new data wipeout technologies that automatically enforce policies and governance on sensitive data based on predictive modeling and context-based semantic modeling, and creating awareness in the workforce to prepare them for future scenarios.

5.1.3 Emerging Technologies

A significant *factor* shaping the future of Emerging Technologies that will impact cybersecurity are the *growing interdependencies across infrastructure*. Built on big data/cloud/mobile frameworks, these technologies will accelerate development and deployment, and also fundamentally transform infrastructure. Driving these increased interdependencies are the recognition that more points of interconnectivity will increase efficiency, enable scale, and precision/accuracy in commodity exchange. Networks that can host data-gathering IoT and the artificial intelligence that can process big data drives smarter decisions and uncovers new business value streams.

- Pro Scenario: Interdependencies across sectors will provide the opportunity to increase the speed and efficiency of data and information flow which will open the door to lucrative investment and returns in technology research and development – for example, in 4D printing, advanced materials, and blockchain, and in digital identity systems and increased sensory capabilities that can leverage these networks and integrated virtual platforms. These have the potential to increase security and resilience of infrastructure.
- Con Scenario: The pace of technological change may be counter-productive, given issues with price, security, and stability. And with biometrics and other emerging technology increasingly entering our lives, it is becoming more difficult to avoid this interconnected system, if privacy

is preferred. Geo-political tension and/or insider threats for critical infrastructure that is being managed at majority by a particular demographic in a geo-location. What if law changes that leads to a hostile situation for that demographic. How to protect that critical infrastructure in that case? How to protect intellectual property from getting stolen and/or leaked? They will have wide range of tools at their disposal and hacks can have fallout across industry, social networks, and national defense.

To best leverage the opportunities and reduce risks in these alternate futures (pro and con scenarios), cybersecurity individuals must prepare and plan, and make decisions and choices on strategic needs which include developing communities within the supply chain, across policy, technology, operations, or other functions, or across sector-specific communities (e.g., healthcare or finance) to enable understanding of needs; and influencing development of emerging, cybersecurity-relevant technologies.

6 ESTABLISHING CYBERSECURITY ALTERNATIVE FUTURES COMMUNITIES

To launch Alternate Futures discussions similar to the process above, we need an approach to promote the use of Alternate Futures as a strategic planning tool. We recommend establishing communities and partnerships; integrating into tools, models, and training; and building awareness.

Communities and Partnerships

- Develop communities within the supply chain, across policy, technology, operations, or other functions, or across sector-specific communities (e.g., healthcare or finance) to enable understanding of needs
- Develop cross-sector communities to identify areas of mutual need or convergence
- Partner with government, academia, industry to incorporate findings in testing & evaluation

Essential Capabilities

- Practice multi-directional knowledge sharing
- Infuse cybersecurity practices and skills across the entire educational experience
- Promote cybersecurity interoperability across all domains and infrastructure
- Build shared cybersecurity future vision with corporate plans and contingencies

Tools, Models, and Training

- Adopt new risk management tools and models to manage complex event consequences
- Incorporate scenario findings into sector and multi-sector planning processes

Awareness

- Broaden awareness of the Alternate Futures findings throughout the cyber community for integration into strategic and operational planning
- Work with standards organizations to integrate findings into cybersecurity standards
- Revisit regulations to ensure flexibility and incentives as they align to findings
- Influence development of emerging, cybersecurity-relevant technologies
- Integrate scenario findings into congressional requirements

7 CONCLUSION

Alternate Futures is an effective way to bring together the cybersecurity workforce community to discuss emerging global trends and how those may impact a range of futures that could shape the cybersecurity landscape. It is particularly needed because efforts to understand the future cybersecurity environment are currently focused on exercising current threats and assessing risks at the sector or organizational level, which is limiting and could misguide planning and decisions, as it is not reflective of broader, macro-level global shifts across other social, economic, environmental, and political changes that will significantly impact the cybersecurity environment, now, and in the future. We recommend creating cross-sector and cross-business line communities to conduct Alternate Futures to analyze major cross-cutting challenges, questions, issues, and opportunities with respect to cybersecurity operations and business practices. This approach will enable a cybersecurity community that is prepared for whatever challenges the future holds, and instill a shared sense of direction and urgency to drive action toward meeting shared future needs.

8 APPENDIX: SURVEY

The purpose of this survey is to better understand how emerging global trends influenced by social, technological, economic, environmental, and political factors might produce a range of Alternate futures that could impact and shape cybersecurity roles, functions, and decision making. Responses from cybersecurity professionals across all technical and non-technical roles are welcome and will be reflected (non-attribution) in a framework for cybersecurity futures planning that will be aligned to the NIST Cybersecurity Framework (CSF)[20] and the NIST NICE Cybersecurity Workforce Framework (CSWF).

1. Which most closely describes your role in cybersecurity? Please check one below.

   - ☐ Risk management, test/evaluation
   - ☐ System administration
   - ☐ Governance, strategy, training
   - ☐ Defense, response, vulnerability assessment
   - ☐ Threat analysis
   - ☐ Operational planning
   - ☐ Investigation, forensics

2. Which most accurately describes your role in your organization? Please check one below.

   - ☐ Executive Level
   - ☐ Business/Process Level
   - ☐ Implementation/Operations Level

[20] CSF

3. With which type of organization are you affiliated? Please check one below.

   - ☐ Industry
   - ☐ Academia
   - ☐ Government
   - ☐ Non-profit
   - ☐ Please indicate your sector (e.g., Finance, Healthcare, Information Services)

   _____

4. Imagine that it is the year 2040. Please rank how your role, function, and decision making in cybersecurity might be impacted by social, technological, economic, environmental, and political factors. Please pick LOW, MEDIUM, or HIGH for each, below:

DECISION	LOW, MEDIUM, or HIGH
Social (e.g., consumerism, social mobility)	
Technological (e.g., new discoveries, rates of obsolescence)	
Economic (e.g., business cycles, gross domestic product)	
Environmental (e.g., climate trends, corporate social responsibility)	
Political (e.g., government stability, regulation)	

5. Now imagine some scenarios that could play out in the future based on a mix of social, technological, economic, environmental, and political factors:

    - The increasing prevalence of severe weather has become the primary national security threat, significantly redirecting federal and state government resources from other national security risks
    - A more highly integrated world has exploded the number of nation-state conflicts and civil and regional instabilities; economic decline has resulted, squeezing budgets across all levels of government, increasing partisanship in political systems and delaying legislative action
    - Social networks and sharing economy start-ups have enabled individuals to play a greater role in shaping society, promoting innovative thinking and entrepreneurial risk-taking; as a result, new industries are more rapidly emerging and becoming obsolete
    - A new category of "virtual" critical infrastructure has emerged in which sectors are less distinct and operate on common networks to conduct distributed functions; while this enables spontaneous transactions and information exchange, it has triggered cascading consequences of failure

    Considering that these or a mix of other scenarios could play out in the future, would your role, function, or decision making in cybersecurity change? Check all that apply.

    - ☐ My role or activities would change
    - ☐ I would make different decisions
    - ☐ My management would make different decisions about my role or function
    - ☐ Standards, regulations, guidance, or policies around what I do would need to change or be updated
    - ☐ My role, function, or decision making would not change

Please list any updates or changes that might be needed to your role, functions/activities, or decision making processes

---

6. After reviewing the above scenarios, do you feel differently about the impact that social, technological, economic, environmental, and political factors could have on cybersecurity roles, functions, or decision making? Please pick LOW, MEDIUM, or HIGH for each, below:

DECISION	LOW, MEDIUM, or HIGH
Social (e.g., consumerism, social mobility)	
Technological (e.g., new discoveries, rates of obsolescence)	
Economic (e.g., business cycles, gross domestic product)	
Environmental (e.g., climate trends, corporate social responsibility)	
Political (e.g., government stability, regulation)	

7. In general, how do you think Alternate futures/scenarios could inform cybersecurity roles, functions, and decision making? Please check all that apply.

    - Identify strategic needs that will enable a more effective future operating environment
    - Enhance cybersecurity curriculum
    - Support CSO/CTO/CISO and governance board decision making processes (e.g., help determine risk posture)
    - Help link cybersecurity to other enterprise functions (e.g., business strategy, human resources, training)
    - Help enterprises identify areas of risk convergence across multiple business functions
    - Help inform cybersecurity standards and guidelines
    - Help avoid strategic surprises and hedge against uncertainty
    - Other (please specify)

    _____

8. Have you ever participated in Alternate futures/scenarios as it related to cybersecurity? Check all that apply.

    - Yes, in a formal, planned, or facilitated session(s)
    - Yes, in an informal, ad hoc, or anecdotal discussion(s)
    - No, I have not thought about Alternate futures
    - If you answered YES to this question, please provide more detail (e.g., organization or environment in which you participated)

    _____

9. When you think about Alternate futures/scenarios and its potential to influence cybersecurity roles, functions, and decision making, do you think of it as something that your organization should do? Check one below.

    - ☐ Definitely should do it
    - ☐ Probably should do it
    - ☐ Neutral
    - ☐ Probably not useful
    - ☐ Definitely not useful

10. If you would like to learn more about this research and receive an analysis of results/findings, please provide your contact info below - thank you!

    _____