May 6, 2022

Ms. Vanessa Countryman
Secretary
U.S. Securities and Exchange Commission
100 F Street N.E.
Washington, D.C. 20549

Re: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure; 17 CFR Parts 229, 232, 239, 240, and 249; [Release Nos. 33-11038; 34-94382; IC-34529; File No. S7-09-22]
https://www.sec.gov/rules/proposed/2022/33-11038.pdf

Dear Ms. Countryman:

I respectfully submit this comment letter in response to the Securities and Exchange Commission's (the "Commission") proposed rules.

> "If one has a hammer one tends to look for nails…" Silvan S. Tomkins, Princeton University from the conference paper collection Computer Simulation of Personality: Frontier of Psychological Theory, in Chapter 1, Page 8, presented June 1962.
>
> "I suppose it is tempting, if the only tool you have is a hammer, to treat everything as if it were a nail." Abraham H. Maslow, The Psychology of Science, page 15, 1966

Summary

The proposed cyber security rules are like a "hammer" looking for a "nail."

- The proposed rules apply the "hammer" -- methods of internal control over financial reporting (ICFR) – to the "nail" of cyber security and warfare
    - Considering cybersecurity to be a "nail" like ICFR is a category error and structural flaw
    - It is a category error and structural flaw because ICFR is a linear stable system
    - In sharp contrast, cyber security and warfare are complex dynamic and more adversarial systems
- The risk assessment-heavy approach reinforces this error because its emphasis is outward, rather than balanced with the internal system
    - In ICFR this might be a reasonable assumption because the system is linear and stable
    - In cyber security and warfare, this assumption is false

- The proposed paperwork-based approach may work for ICFR. But a paperwork-based approach cannot:
    - Create a winning restaurant or sports team
    - Cause world leaders to acknowledge the threat of Putin's aggression before he attacked
    - Strengthen cyber security – it has harmed cyber security

In revising the proposed rules, it would be helpful to reconsider the objective.

- By way of analogy to Putin's aggression, is the objective to enable litigation against the Biden Administration for failing to convince world leaders to do more to deter Putin? Or is the purpose to shape the conditions to make it as easy as possible for the Biden Administration to do everything possible for global security?
- In cyber security and warfare, the opportunity is to encourage the use of Critical Thinking, Systems Thinking, Design Thinking and Zero Trust strategies to make companies more secure to contribute to national and global security
- If the proposed rules are not revised, then they would become the root cause of incidents and breaches

After an explanation of this summary, resources are provided on how the proposed rules can be revised by taking advantage of how Critical Thinking, Systems Thinking, Design Thinking and Zero Trust strategies are already used in the U.S. Government and beyond.

Managing risk is all about understanding the system

Successfully managing risk requires 1) thoroughly understanding "how it works" – the nature of the system, 2) discovering the real problem, 3) asking, "What if?" 4) to solve the real problem. This is fundamental to systems thinking and applies from cooking to driving a car through a storm to ice skating to kinetic warfare to new products management to forestry.

The integrity of information reported to the SEC's EDGAR system is entirely different from cyber security and warfare.

- Financial reporting is about **reasonable assurance** of the accuracy of the financial **consequences** of tangible transactions (e.g., payment for raw materials) that happened in the **past** in a **linear, stable system** -- general ledger. A high-end threat is detecting fraud or a bribe paid. Debates about accounting treatments happen within the confines of rules and professional guidance. Errors and omissions are addressed with routine methods. Thus, confidence in error ranges and predictability are relatively high.
- Cyber security and warfare are about managing **risk in unfolding situations** in a **complex dynamic system** in an unpredictable, **emerging future**. Cybersecurity is more adversarial. High-end threats include disabling a power grid, contaminating water supplies, halting logistics, or turning off infusion pumps in hospitals. While scenarios can be imagined using creative, film-script style methods and wargaming, a company faces an emerging future as do President Biden and world leaders facing Putin's aggressive war. Law enforcement revelations about hacking gangs like LAPSUS$ reinforce the nature of the system and the future.

In short, because of these differences in the nature of the system, it would be a structural flaw and the "wrong tool for the job" to apply linear stable system methods to a complex dynamic and highly adversarial system.

Consequences of the proposed rules – a category error

The proposed rules use the term "controls" broadly. While "control" can be applied in many senses, simplifying here into just two.

- Those in the accounting tradition previously termed "checks" that are "to do" lists with origins in ancient Egyptian grain accounting. They are best for linear, repetitive tasks. They are the nature of the "policies and procedures" disclosures listed in the proposed rules, beginning on page 12.
- Those in the mechanical/automated tradition, with origins in ancient animal traps now found in steam engines, air conditioning, consumer electronics, avionics and more. These are designed with specific ranges, tolerances and service lifetimes – look at the back of your laptop power supply.

Reliability and use are strikingly different, especially in the complex dynamic system of cybersecurity. For example, please see the CISA page for the SolarWinds compromise https://www.cisa.gov/uscert/remediating-apt-compromised-networks. To better understand the mechanical/automated approach in the context of systems for cybersecurity, please see https://csrc.nist.gov/publications/detail/sp/800-160/vol-1/final

More, the ICFR approach defocuses and distracts from actions to strengthen security and reduce business losses.

Consider a restaurant. It could have the most hygienic kitchen. It could have the finest ingredients – far beyond certification standards for organic. It could have the happiest staff. Yet will those actions cause a "5-star" rating across the categories of presentation, experience and taste of food?

Consider further:

- Does the method for checking the cash box at a sporting event make a team win?
- Does the method for checking for a pilot's hotel bill make a safe flight?
- Does the method for checking the cash box at a circus ensure animal welfare?

More, consider the structural flaw of applying ICFR-based methods of managing risk to cyber security and warfare.

- By that same logic would the SEC apply ICFR-based methods to other business disciplines – new product management, marketing, logistics or IT systems response time on "Black Friday." Those disciplines have decades of proven and practical math and methods.
- By that same logic would the SEC apply ICFR-based methods to all aspects of a business – including industrial operations and transportation? Would it override the guidance of the CSB or NTSB for public companies and replace that guidance with ICFR-based methods?

Creating causes of action or solving the real problem?

More, the proposed rules would reinforce an error in the application of Section 404 of the Sarbanes-Oxley Act. Too often, ICFR-based methods used for the linear, stable system of financial reporting are applied to the complex dynamic system of cyber security and warfare. Too often, the root cause of an incident is bad math and method used by the cybersecurity team – often based on ICFR-based methods. The proposed rules could be construed to legitimize those common errors.

The paperwork nature of the proposed rules gives rise to problems:

Paperwork is not always bad. Aviation, medical procedures, auto repair and more have detailed documentation. But those are for linear tasks. Flight safety or military success in complex dynamic systems comes from thinking and practice – flight simulators or years of experience in tumor removal. The crash of Air France Flight 447 is a tragic reminder.

The focus on paperwork – policies, procedures and assessments -- over solving the real problem…

- Defocuses from understanding the nature of the system and solving the real problem
- Causes companies to reach for the SEC's preferred tools rather than the right tools
- Causes companies to double-down on what they perceive will protect from enforcement actions and private causes of action, rather than what improves security for customers, employees and the United States

Consider the error of focusing on risk assessments instead of focusing on understanding the nature of the system and "how it works." Reflect on this winter's snowstorms that clogged freeways and electric vehicles that lost power on those freeways becoming roadblocks. The owners failed to understand the limitation of the system that was their car.

The proposed rules cite the NIST Risk Management Framework, without realizing that the Framework (which isn't a framework as it is not comprehensive) states "However, the variety of ways in which the Framework can be used by an organization means that phrases like "compliance with the Framework" can be confusing."

The cumulative effect of this path would be to create vulnerabilities that become incidents that become breaches.

In sum, the errors and flaws would put the SEC at the root cause of incidents. This is the opposite of the objectives of the Biden Administration.

Regarding cybersecurity expertise on boards of directors, the real question is, What expertise?

- If it is more ICFR-based expertise, then that would reinforce the structural flaw of using ICFR-based methods for cyber security and warfare. It would also reinforce the problem of having cybersecurity overseen by audit committees.
- All board members should be encouraged to bring their personal and professional backgrounds in critical thinking, systems thinking and design thinking to best oversee and guide management

in creating authentic Zero Trust strategies. For more on Zero Trust, please see https://www.cisa.gov/sites/default/files/publications/Final%20Draft%20NSTAC%20Report%20to%20the%20President%20on%20Zero%20Trust%20and%20Trusted%20Identity%20Management.pdf Many disciplines include design thinking and systems and root cause analysis – cooking, information technology, architecture, biology and assembly line design. Board members should be encouraged to bring their "whole self" experience in root cause analysis and design expertise to cybersecurity discussions – not feel excluded.

- The "expert" needs to bring strength in critical thinking, systems thinking and design thinking – especially in a technology context – to draw out the strengths of other board members and guide the asking of smart questions of management to improve company and national security.

References for proposed rule revisions

Alternative approaches are available to the SEC. The references below are to critical thinking, systems thinking and design thinking as used elsewhere in U.S. Government. Some references are in the context of cybersecurity and some are other complex dynamic systems where these approaches have been successful.

The point is that these thinking types apply to complex dynamic systems that are the environment of cyber security and warfare. This is more effective than the assumption in the proposed rules of an ICFR-like linear stable system.

With these approaches to "thinking," the SEC can revise the proposed rules to be less likely to cause vulnerabilities and breaches in regulated companies.
Using approaches appropriate to complex dynamic and highly adversarial systems would avoid the error of applying ICFR-based methods that are only appropriate for linear stable systems.

Zero Trust Strategies

- President Biden's Executive Order including Zero Trust https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
- NSTAC Report https://www.cisa.gov/sites/default/files/publications/Final%20Draft%20NSTAC%20Report%20to%20the%20President%20on%20Zero%20Trust%20and%20Trusted%20Identity%20Management.pdf

Critical Thinking

- https://files.eric.ed.gov/fulltext/EJ1143316.pdf
- https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4216424/
- https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4235550/
- https://www.dol.gov/sites/dolgov/files/odep/topics/youth/softskills/problem.pdf
- https://leb.fbi.gov/articles/perspective/perspective-need-for-critical-thinking-in-police-training
- https://emilms.fema.gov/is_0453/groups/46.html
- https://www.dhs.gov/publication/media-literacy-and-critical-thinking-online

- https://humancapital.learning.hhs.gov/e-blast/eblast201904.asp
- https://appel.nasa.gov/course-catalog/critical-thinking-and-problem-solving-appel-ctps/
- https://psnet.ahrq.gov/issue/developing-critical-thinking-skills-delivering-optimal-care

Systems Thinking

- https://csrc.nist.gov/publications/detail/sp/800-160/vol-1/final
- www.ntsb.gov
- www.csb.gov
- https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3940421/
- https://www.dhs.gov/publication/st-operations-and-requirements-analysis-overview-fact-sheet
- https://www.dhs.gov/science-and-technology/ora
- https://apps.dtic.mil/sti/citations/AD1045468
- https://www.airforcemedicine.af.mil/News/Display/Article/1089321/afms-uses-systems-thinking-to-keep-everyone-on-the-same-team/
- https://archive.epa.gov/ged/tutorial/web/html/index.html
- https://www.fs.usda.gov/treesearch/pubs/60063

Design Thinking – please notice use in military

- Department of Defense Joint Special Operations University https://www.youtube.com/channel/UCL7hOd0ihWzmJlga_Y4wCJg
- https://www.dyess.af.mil/News/Features/Article/2552100/afgsc-design-thinking-course-leads-to-dyess-afbs-first-sbir-phase-3/
- https://www.dhs.gov/sites/default/files/publications/OCIO%20Strategic%20Plan.Dec2018.pdf
- https://www.secnav.navy.mil/agility/assets/documents/WCD%20Fac%20course%20version%2020200830.pdf
- https://junior officer.army.mil/turn-your-meetings-into-intrapreneur-workshops/
- https://www.nist.gov/blogs/manufacturing-innovation-blog/five-hottest-innovation-tools-0
- https://www.cdc.gov/pcd/issues/2018/18_0128.htm
- https://www.acf.hhs.gov/ofa/report/creating-solutions-together-design-thinking-office-family-assistance-and-3-grantees
- https://www.ed.gov/sites/default/files/documents/stem/cybersecurity-slides.pdf
- https://niccs.cisa.gov/training/search/skillsoft/prototyping-design-thinking
- https://assets.section508.gov/files/Copy%20of%20Universal_Design_%20White%20Paper_vFinal_0.pdf

Brief summary of the above

- www.thinkdesingcyber.com

Very respectfully submitted,
Brian Barnier