REVEALRISK
SECURE YOUR BUSINESS
Cyber Security, Privacy, and Risk Management Consulting
RevealRisk.com

The CxO Business Executive and Security Leadership’s Guide to Cyber Security Harmony

By: Aaron Pritz – CEO and Co-Founder, Reveal Risk

Let’s face it: The relationship between many cyber security leaders, broader business executive leaders, and their boards at companies are not ALL exactly thriving. Despite a lot of industry discussion, tactical use of FUD (fear, uncertainty, and doubt), and an endless media barrage of breaches, there is still a *major* disconnect between business leaders, boards and cyber security leaders.

Some of the vocal narrative I’ve heard on both sides of the leadership equation include:

The Frustrated CxO (CEO, CFO, COO, CRO, CMO, CIO, CPO etc.)**:**

- “We’ve spent a lot of time and money on compliance, and security has likely been covered in that (re: Sarbanes Oxley). We need to minimize the volume of more controls and distractions from our core business as we just don’t have the time or resources.”
- “We aren’t in financial services or the defense industry: our focus on cyber security should be minimal.”
- “We didn’t focus heavily on this at the last company I managed, and we were fine, so I don’t think we need to go overboard here.” *(e.g. I’m willing to take the risk without understanding the risk)*
- “We don’t have intellectual property”
- “We aren’t / won’t be a target”
- “IT or the CIO will handle it”

The Frustrated CISO/Cyber Security Leader:

- “We shouldn’t tell them anything that we don’t want their help and intervention on”
- “We need to show our status as all ‘green’ because that reflects on our personal effectiveness as a team”
- “They (the CxO) just doesn’t / won’t understand the deep complexity of all of the IT tooling that is required to manage a good cyber security program, so we need to shield them.”
- “We should make significant progress implementing technical solutions before we get too much into risk management and measuring / stating program maturity: Otherwise, we are not going to look good here.”
- “We should minimize the number of times we have to interact with the board. It takes too much time to prepare for them.”

The truth is that all these statements, perceptions, and poor leadership behaviors are rooted from some experience or set of experiences the leader previously had that has driven them to think and operate the way that they do. ***You aren’t going to fix this overnight.*** Let’s look at some potential root causes.

<u>The CxO's Common Issues:</u>

The day where cyber security can be solely managed within the dark basements of IT are no longer a reality for most companies. Many CxO leaders know this, but they often struggle to translate this into action. I've observed various strategic/political and motivational/capability root causes result in lack of appropriate executive action and involvement:

- **Strategic/Political**: If a CxO is strategically avoiding cyber security, it usually stems from a deeply rooted philosophy or leadership culture where you can't be blamed for what you've not had a hand in or been made aware of. This is known as "putting your head in the sand." It is more common that one would think regardless of industry or company culture.
- **Motivational/Capability**: Lack of motivation and/or capability of a CxO to engage can stem from a number of factors that are likely more of the true root cause: burn-out, fear, or aptitude to draw the right insights out of subordinate leaders can often be. This usually results in leaders talking past each other or information getting lost in translation.

The CxO and board must proactively take action if he/she wishes to address the common problems that plague cyber security teams today. They need to remember in a hierarchical structure, it often takes the right engagement level, attitude, humility, and empathy to get the most out of subordinate leaders that are often nested layers beneath them. Not leveraging these soft skills plus a foundational approach (that this guide provides) can silo and disconnect key leadership interactions. These ten proactive themes and questions can help focus the engagement on both sides of the table and maximize the value of the time that must be spent on cyber security to obtain the desired executive understanding, action, and harmony.

The CxO's Solutions:

While this playbook is designed for the CxO, it can be used by security leaders to proactively engage with executive stakeholders and achieve harmony.

1. **BUSINESS RISK:** ***What are our most critical risks to our specific business and operations?***
   - Where could we see maximum damage and business impact if our company was faced with a cyber security event or if an insider acted maliciously?
   - Does our organization and functional leaders know what is most critical and where they need to be focusing?
   - Do you need any help or insights in ratifying these top business risks so I can help you focus?
   - Have we evaluated cyber risk in the context of enterprise risk?

2. **THREAT LANDSCAPE:** ***What are our most concerning threats that we are seeing right now?*** (Note: You want to focus on the current state and slightly into the future because there is no crystal ball.)
   - Has the threat landscape changed since our last discussion?
   - Is our current program focus still aligned to the threat landscape?
   - How do our top business risks correlate to our top threats we face?

3. **CURRENT STATE MATURITY:** ***Where are we right now in our IS (Information Security) program maturity journey?***
   - How do/will we link maturity measurements to business risk reduction to ensure optimized focus? How do we get to appropriate scale with our solutions?
   - How did we evaluate our current maturity? (Against a framework? Using an independent external party or internal team? If internal team, how did you mitigate internal bias?)

4. **FUTURE STATE MATURITY:** ***What are we striving to achieve in our IS program journey over time?***
   - How will this future state target translate to reducing critical business risks?
   - What are the major milestones and outcomes we are targeting? (push your cyber leader beyond tools and technologies being implemented and toward business risk reduction)
   - How are you splitting your focus and the focus of your team across people, process, technology efforts?
   - What organizational roadblocks (beyond IS and IT) do you see now or in the future? And how can I help?

5. **MEASUREMENT OVER TIME:** ***How will we measure progress towards our goals of getting from our current state to our desired future state outcomes?***
   - How do we measure progress towards our goals?
   - How will we ensure consistency of the measurement of progress over time, various leaders, and changing organizational structures?
   - What scorecard, metrics (KPIs/KRIs – key performance indicator / key risk indicators) do you need me to focus on so I'm ensuring I'm helping you and the program to the greatest extent possible?

6. **INTERNAL PARTNERING:** ***How are we partnering across cyber security, physical security, IT, legal, compliance, and privacy for both efficiency as well as risk coverage?***
    - What partner organizational roadblocks or points of friction exist (beyond IS and IT) now or potentially in the near future and how can I help?
    - How could we increase efficiency amongst these teams for both the benefit of the functions themselves as well as the organizations they support?
    - What governance structure or leadership sponsorship could enable this?

7. **EXTERNAL PARTNERING:** ***How is the cyber security team connected to cross-company sharing groups or individual relationships?***
    - Is your team part of any external information exchange forums? (E.g. ISAC – Information Sharing Analysis Center)
    - Can I make any introductions to company leaders that I'm connected know or boards that I sit on?
    - Is your organization growing their skill set enough to evolve in this space?

8. **CISO'S BIGGEST CONCERNS:** ***What most concerns you about the current state of cyber security at our company?*** (Sometimes this is phrased as "what keeps you up at night" but I've seen some awkward answers to this question because it varies across egos and sleeping habits vs asking it more forward to the true intent).

    - If you could wave a magic wand – what would you want to fix most?
    - Is there anything that we could change to alleviate this concern, influence change, or expedite progress towards resolving it?

9. **EXECUTIVE SUPPORT:** ***What help do you need from the company and executive team?*** *(financial, organizational change/sponsorship, governance, making decisions)*
    - What can I do to help you and your team?
    - Where can I recognize great efforts of your team? (only where doing so will truly motivate your team)
    - Is there anything that I or the executive leadership team are doing that is a barrier to your progress?

10. **Workforce Awareness and Engagement:** ***How is the organization engaging around information security and what is cultural maturity?***
    - What are the most critical workforce awareness and behavior change needs across the organization that would minimize security risk?
    - Are there any specific groups of workforce members or roles that we have a need for special additional focus on because of risk?
    - What workforce related interventions are currently planned or planned for the near future to minimize our risk?
    - How do we measure engagement and organizational change around critical security needs, behaviors, and goals – connected to critical business impacts?

Leaders need to treat this discussion playbook truly as a guide vs a script. And as with any important initiative, it cannot be a onetime discussion. Conversations should be dynamic, and people still need to use their analytical and conversational acumen. However, if more company leaders were having this level of conversation and action (even 80%), cyber security would be in a completely different state of control and transformation. Think about the big publicized breaches and how many leaders were caught off guard, not in the right loop, and blamed specific people or things when the problems were truly holistic.

***

Do you have any other key questions or ways that you focus these leadership engagements? Feel free to leave a comment and this playbook will be updated as needed to maximize the value for all. Also share your feedback if you found this helpful.

At Reveal Risk, we evaluate, design and deliver strong processes and results in cyber, privacy, risk that work efficiently, are fit-for-purpose, and are sustained. If you find that you want assistance in building your company's cyber security strategy, governance, and plan towards desired state maturity, please don't hesitate to connect with us at info@revealrisk.com.

REVEALRISK
SECURE YOUR BUSINESS

info@revealrisk.com
317.759.4453

About the Author

Aaron Pritz is senior IT/Security/Privacy/Risk leader with over 20 years of experience including at a large pharmaceutical company in the Midwest. Aaron co-founded Reveal Risk in 2018 after seeing significant corporate leadership and "execution of strategy-to-operations" capability gaps in the cyber security and privacy consulting industry. Aaron is a creative thinking strategist that brings strategies to life through engaging approaches and teamwork. He is an active industry influencer and speaker on the topics of business-driven risk management, insider theft, and cyber security in healthcare, and is no stranger to helping companies progress both before and after incidents/breaches (ideally the former!).