LEADERSHIP IN CYBER SECURITY

10 REASONS YOU NEED A CYBER SECURITY ADVISOR

By Sorin Toma

Jan 2022

Read: 5 minutes.

REASONS | DRIVERS:

"It takes 20 years to build a reputation and few minutes of cyber-incident to ruin it." – Stephane Nappo

1. INDEPENDENCE

- An independent cyber security advisor is driven by your organization's interests alone.

2. REPRESENTATION

- Can effectively represent and advise on cyber security in executive forums and at board level.
- Will assist decision makers and engage key stakeholders.

3. THOUGHT LEADERSHIP

- Can assist the leadership team in developing new and innovative approaches and solutions for critical cyber security challenges.
- Advise on segmentation - providing different levels of protection for different assets according to risk profile.
- Innovative approaches to address:
  - Identity management (DigitalID),
  - Online security and customer safety whilst delivering an enhanced customer experience (usability labs).
- Software development/engineering (embedding security in software).

4. ENHANCED PROTECTION

- Can help to better protect your organization's reputation and brand.
- Will optimize cyber security operations to address critical risks and challenges and maximize benefits.

"As cybersecurity leaders, we have to create our message of influence because security is a culture, and you need the business to take place and be part of that security culture." — Britney Hommertzheim

5. Cyber Strategy Expertise

- A Cyber Security Advisor is an expert in developing and executing cyber strategy.
- Can help transform the cyber security function to address new market events (digital, pandemic/work from home).
- Can provide valuable insight on cyber security due diligence in a Mergers and Acquisition (M&A) scenario or post M&A consolidation.

6. Improve Resilience

- Verify incident response management policies and plan are in place.
- Advise board and the leadership team in case of an incident or attack.

7. "Unite and Conquer".

- Can bring all the relevant players together including Audit and Risk, Legal and Commercial, Operational Business Leaders/GMs, IT, and the Executive Team.

8. Holistic Coverage

- Provide end-to-end coverage of cyber security – broad expertise and experience.
- Provide oversight and advise on:
  - Leadership and building teams (structure and process and including recruitment),
  - Governance, compliance, and reporting,

We shouldn't ask our customers to make a tradeoff between privacy and security. We need to offer them the best of both. Tim Cook

- Risk management, legal and commercials (procurement and negotiations),
- Communications – presentations, whitepapers, webinars, executive and board reports,
- Online safety as part of Digital and Customer Experience,
- Drive cultural change – raise awareness,
- Stakeholder engagement, and
- Advanced technology (Internet of Things – sensors, Artificial Intelligence, Virtual Reality, Digital Twins, Big Data and much more…).

9. Understands your Organisation

- Focused on protecting and achieving benefits for your organization.
- Knows the staff and the business processes, policies, and systems.
- Understands your organization's risk profile and business strategy.
- Will align cyber security with your organization's operational risk exposure, and corporate strategies and direction.

10. Improve Maturity

- Across business processes, people, and technology.

"Act to secure your business and your future" www.Act2Secure.com