HOFFMAN NEWSLETTER

Leadership in Cybersecurity: A Conversation with Professor Georges Ataya on the 6 Key Steps to Building Organisational Resilience

March 2025

In an era where digital threats are constantly evolving, cybersecurity has become a crucial concern for organisations across all sectors. I recently had the opportunity to speak with Professor Georges Ataya, a renowned expert in digital governance and cybersecurity, to discuss the essential steps leaders should take to protect their businesses. Our discussion highlighted six key factors in the field of cybersecurity, outlined below.

We began our discussion with Georges by addressing "the concept of the 'Knowledge Paradox', which suggests that less knowledge of cybersecurity risks often leads to overconfidence. This can result in an underestimation of risks during digital transformation efforts."

Cybersecurity Facts

Fact 1: Cybersecurity Myths

According to Georges, companies often struggle to strike the right balance between adequate cybersecurity spending and reasonable protection. All expenditures on tools, protection systems, and defence methods are only fully productive if they are based on a risk analysis validated by management. When examining incident statistics, this sought-after balance does not seem to be achieved in most organisations, from the largest to the smallest. Indeed, there are several common myths about cybersecurity, such as considering it solely as a technical problem.

Fact 2: Security Debt

Like Technical Debt, Security Debt is an accumulation of deficiencies in a company and its IT architecture elements, including business processes and technologies. The cost of Security Debt corresponds to recurring payments caused by poor planning and implementation of protections, as well as the absence of a security-by-design approach. It has both commercial and technological dimensions.

Fact 3: The Need for Governance

Cybersecurity Governance, like Digital Governance, defines processes that enable efficient decision-making and actions. Risk optimisation and resource optimisation must aim to achieve strategic objectives while optimising the balance between risks and expenses.

Our discussion continued on what business leaders should do. Based on his extensive and widely recognised experience, Georges summarised it all by proposing six key steps:

The Cybersecurity Leaderhip Checklist

Step 1: Business Risks

Leaders must identify and assess security risks related to the business, beyond the concerns of the IT department alone. "We've been led to believe that cybersecurity involves spending money primarily to protect the IT department," says Georges. Indeed, companies with low maturity confine cybersecurity activities to the IT department.
In short, "the return on investment of expenses incurred to mitigate business-related cybersecurity risks is better estimated when comparing the costs of additional protections to the loss of reputation, customer service, and financial impact."

Step 2: Technological Risks

This step involves assessing existing technological protections and aligning them with business priorities. It covers the examination of Technical, Organisational, Human, and Physical protections.

Step 3: Cybersecurity Roadmap

Digital transformation aimed at protecting the business leads to the launch of a set of construction and implementation programmes and projects. This involves developing a comprehensive roadmap that prioritises implementation projects based on risk mitigation. It involves implementing new or improved technologies, modifying business processes, raising employee awareness, contracting an external service, a major change in the company's architecture, or simply signing an insurance contract.
Implementation projects are prioritised based on the risks they are intended to avoid. These risks have a high or low impact and can be assigned a high or low probability. Prioritisation involves selecting a good balance between protections that mitigate the most likely and impactful risks. This could result in an annual investment of 2 to 5% of the company's total operating budget, depending on the Technological Debt. As an anecdote, NATO countries spend no less on their own defence.

Step 4: Cybersecurity Dashboard

Given the level and importance of the budgets involved and the risks to be avoided, a dashboard is an essential tool for monitoring this strategic transformation. It will offer real figures and status reports of various risk postures, project progress, financial data, and any other elements necessary to guide the various stakeholders. Georges and his team have developed a four-dimensional model, based on the "Balanced Scorecard" practice, applied to cybersecurity management needs. The four dimensions are Finance, Business Process, Customers, and Learning and Growth.

Step 5: An Effective Cybersecurity Leader

Georges emphasises the importance of clear managerial responsibility for cybersecurity activities, even in small businesses. While insisting that there is a critical need for multiple skills,

often going well beyond the capabilities of a "single person". In this regard, the HTP Group offers a rather unique proposition, supporting its clients with various cybersecurity leadership models, from permanent talent placement to "as a service".

Step 6: Engaging in a Cybersecurity Programme

This step underlines the need for involvement at all levels of the organisation, including the Board of Directors, CEO, business managers, technology leaders, and the CISO.

Conclusion

When I asked Georges what he would advise companies to do, in a very concrete way, he did not hesitate to emphasise the importance of conducting an audit to determine the potential value and improvements that a comprehensive cybersecurity programme could bring. These structured assessments have been developed for small, medium, and large companies and allow them, at a very limited cost, to achieve complete basic cybersecurity hygiene.

How can the HTP Group help you

The HTP Group offers a rather unique combination of services, ensuring that our clients' needs are fully covered, from defining and implementing comprehensive digital governance, to conducting an audit and assisting companies in meeting all DORA, GDPR, NIS2, ISO27001, and other regulatory and standards requirements. But also by supporting its clients with various cybersecurity leadership models, from permanent talent placement, interim, or "as a service".

Do not hesitate to contact us for an exploratory discussion.

Georges Ataya, Founder & Member of the Board
ga@atayapartners.com
Michel Grisay, Partner, Hoffman
mg@hoffman.be