tapestry NETWORKS

EGAN SUMMARY OF THEMES

Access to capital, crisis simulation, cybersecurity, and scenario planning for resilience

October 2024

The European Growth Audit Network (EGAN) met in London on September 17 to discuss:

- **High-Growth Companies and Access to Capital** with Matt Harold, Private Markets Sustainability Specialist, Independent
- **Crisis Simulation: Cybersecurity Lessons** with Paul Robertson, UK Cyber Resilience, Preparedness and Response Partner, EY and Andrew Hobbs, EMEIA Center for Board Matters Leader and EMEIA Public Policy Leader, EY
- **Scenario Planning for Resilience** with Mats Persson, Strategy and Transactions Partner, EY

For a list of meeting participants, see Appendix 1 (page 8).

This *Summary of Themes*[1] provides an overview of the following discussions:

EY Building a better working world

High-Growth Companies and Access to Capital

Securing capital is critical for companies seeking to grow. Matt Harold met with members to discuss strategies for securing capital in the current economic climate. Key themes included:

- **Recent global events have made it difficult to access capital.** *"It's been called a poly-crisis—multiple crises occurring simultaneously, creating a situation that is more severe than the individual crises combined,"* observed Mr. Harold. He outlined recent and concurrent disruptions, including a volatile global economy, war and conflict, high energy prices, nationalistic trade policies, inflation/recession, and the cost-of-living crisis. All have made capital raising more difficult. *"Most notably, the central banks raised rates, and that was the end of free money,"* said Mr. Harold. He highlighted two key events that added pressure to banks: *"First, leading banks were having trouble cleaning up their balance sheets by moving debt into secondary markets. The most notable example of this was the US$13bn Morgan Stanley, Bank of America, Barclays, and four others put forward for the Twitter take-private in late 2022. Well into 2023, these banks were still trying to offload this debt, even at a discount. The second event was the collapse of Silicon Valley Bank. This caused ripples across the different financial markets,"* he explained, adding, *"The IPO window closed and shuttered across various public markets, and M&A volumes dropped by half from 2021 to 2023."*
- **Investors are more cautious and are seeking sustainable value creation.** EY's François Langlois noted, *"Historically, investors prioritized either speed or scale—choosing a larger payout for scale or a quicker exit for speed. Now, however, it appears to be the same journey for all."* Investors are now emphasizing economic value creation, which goes beyond near-term returns–investments grounded in long-term sustainability, operational resilience, and tangible business impact. Companies are increasingly evaluated on their ability to create lasting value for stakeholders—customers, employees, and the community—rather than just maximizing short-term profits.
- **Sustainability can both hinder and boost fundraising.** *"I believe investors are becoming more sophisticated regarding sustainability, but its influence on fundraising and capital allocation is waning in some jurisdictions. In the US, we're seeing polarization and the weaponization of sustainability,"* Mr. Harold said. He nonetheless advised companies to seize opportunities to get ahead of competitors: *"Think strategically. For many B2B businesses, like manufacturing, you'll need access to more sustainable raw materials to align with evolving customer sentiments. But these materials are often in limited supply. Companies that focus on a long-term strategy to build resilient supply chains to secure these resources will gain a competitive advantage. If market trends shift in this direction, they will reap the rewards while competitors struggle to catch up."* A member added, *"The more sophisticated investors are the ones thinking about the future."* Another underscored the sentiment, *"It's very important to get green financing."*
- **Opportunities to go public are again emerging, but terms may be less attractive.** *"The IPO window is opening, with activity in the first half of 2024 double what it was in the first half of 2023 and quadruple the activity levels in the first half of 2022."* noted Mr. Harold. But preferences are shifting. A member observed, *"A lot of companies feel undervalued in public markets. They believe the share price doesn't accurately value the business."* Another noted, *"When I started in business, everyone*

aimed to take their companies public. Now, we see businesses growing larger and remaining private for longer."

- **Funding for growing companies is coming from nontraditional sources.** Companies have adopted new funding strategies. Joint ventures have emerged as a promising avenue for securing capital while sharing risks and resources. One member noted, *"Big groups are coming together to accelerate access to markets and capital."* Other observations included:
  - **The use of private credit is increasing.** *"While banks have been struggling with their balance sheets, private credit is now a US$1.5 trillion market, up fifty percent from 2020,"* noted Mr. Harold. *"Most estimates suggest this figure could nearly double by 2028 to US$2.8 trillion, indicating an increasing amount of money and products in the market."*
  - **Syndicated lower-risk deals have replaced unilateral lenders.** A decline in risk appetite and tighter balance sheet constraints have made it more challenging to secure funding from a single source. *"I've observed a strong resurgence in portfolio companies, primarily leveraged by partners and owners, who syndicate low-risk deals,"* said Mr. Harold. *"Many portfolio companies are restructuring and refinancing original loans from acquisitions made a few years ago by syndicating new loans. This involves multiple parties and banks collaborating, creating a crowded decision-making environment—but that may be necessary in the current climate."* A member agreed that syndicated loans are a solution to risk-averse investors but noted that managing multiple relationships can be challenging: *"The company where I serve on the board is seeking financing from various shareholders, each with different interests—some are eager to invest, while others don't want to risk dilution. This creates a real conflict. The only solution is through syndicated loans. But this is a new experience for the company in managing both relationships and reporting requirements—it's a concern."*
  - **Growth in M&A activity and private equity transactions is on the horizon.** *"Forty six percent of private equity-backed assets under management are four years or older, surpassing the typical holding period of three-to-five years. General partners are feeling pressure from limited partners for distributions, and significant work remains to exit these older investments as the markets heat up,"* noted Mr. Harold. *"Additionally, there is US$2.6 trillion in committed but uncalled capital, which suggests we can expect a surge in M&A and private equity transactions as the deal environment becomes more attractive."*

Crisis Simulation: Cybersecurity Lessons

EGAN members took part in a simulation led by EY's Paul Robertson. Members were presented with a fictional company that had been subject to what looked like a large-scale cyber intrusion, with hackers demanding a ransom. The cyberattack was followed by a second crisis: the CEO experienced a serious medical issue and was hospitalized, out of action. Members discussed how to approach the dual crisis,

grappling with some challenging decisions, including whether to pay a ransom to the hackers. Lessons from the simulation included:

- **Understanding the severity of a cyberattack takes time and involves navigating ambiguity.** Cyberattacks are complex, and threat actors continue to evolve their tactics and technologies. It is often difficult to quickly discern whether technical issues are the result of a cyber incident or another operational problem. *"Cyber events are inherently ambiguous. It often takes time to identify an attack and even weeks to fully understand what occurred,"* said Dr. Robertson. *"The board should set clear expectations of when they will be informed of any incident. The initial information about the extent of infiltration and impact is often unclear, making informed decision-making extremely difficult*," Dr. Robertson explained. He added, *"As humans, we dislike ambiguity and prefer to manage consequences. Uncertainty can create a psychologically challenging situation for all involved across the organization."*
- **An overall response plan for crisis situations is critical**. Crises unfold quickly. Having protocols around when to implement the plan, designated roles and responsibilities, and detailed response procedures for different crisis scenarios can help manage the situation more effectively. Other important aspects discussed include:
  - **A communications plan is a vital part of the response.** In any crisis, scrutiny from external and internal stakeholders can be unrelenting, with constant demands for updates and clarity about the situation. This is particularly challenging when circumstances are persistently unclear. Pressure to communicate transparently but accurately complicates effective oversight of an incident. Some jurisdictions require rapid disclosures to regulators or other government bodies, and in some cases to the public. Dr. Robertson explained, *"The scrutiny and interest extend beyond the media to include shareholders, investors, employees and regulators, such as in the US SEC cyber incident disclosure rules and the EU's Cyber Resilience Act. This will also be true for the forthcoming UK's cybersecurity bill."*
  - **Frequent review and scrutiny of the response plan.** *"The threat environment is constantly evolving—not just in terms of technology, but also in how people use it,"* said Dr. Robertson. He advised frequently reviewing and updating cyber incident management strategies. He encouraged members to *"ask your management team: When was the last time executives stress-tested the plan? How far was the plan and capability to respond pushed? Did it reach breaking point? At what point does the organization break under pressure from cyberattacks? And at what point was escalation to the board done or needed?"* He added, *"Often, we see exercises which choose disruptions that are more of an annoyance than strategically challenging—make sure the plan focuses on the showstoppers."*
  - **Balancing urgency with caution.** *"The initial rush to action followed by pulling back can be risky,"* said Mr. Hobbs. *"There may already be a plan in place that needs to be examined more carefully. In the US, rushing in can lead to SEC violations. As a nonexecutive, it's important to stay on the right side of the fence—both to avoid regulatory breaches and to ensure good governance."*

- **Build current relationships with external resources you may need in the future.** Driven by increased regulation, European companies are increasingly adding experts in fields like cybersecurity and sustainability to their boards and executive teams. But these specialists are in high demand and require competitive compensation. Strong external support thus becomes even more crucial. Dr. Robertson advised engaging with such support before a crisis occurs and stressed the importance of investing time to develop the relationship. *"In times of need, you'll rely on someone, such as a cybersecurity expert or legal counsel."* he said. *"Build relationships with the right people to avoid bringing in someone whose working style or agenda doesn't align with yours, especially in high-stress situations. Ensure you have a partner you know and trust."* A member agreed and emphasized: *"It should be someone the board trusts completely. Even if you don't follow their advice, you'll still appreciate it."* Dr. Robertson summed it up: *"The best responses stem from pre-existing relationships."*
- **Ongoing board efforts.** Mr. Langlois asked, *"What about board readiness? What role will the board play in a crisis, and what role should it not play?"* One member responded, *"We need to empower and support management."* The group highlighted several ways to do so:
  - **A deep understanding of risks and company operations helps boards respond in a crisis.** *"The board must be educated on a variety of subjects, and cyber is particularly challenging due to its fast pace,"* Dr. Robertson said. He recommends gaining a strong understanding of company operations as a foundation for informed decision-making. In high-growth companies, where board members are often more hands-on, this approach is especially beneficial. He said, *"It's important to both grasp how systems operate internally and understand the external threat environment. The most engaged and effective boards are those that seek to understand situations deeply, not just to make decisions but to truly dive into the context, which stems from a place of wanting to learn."*
  - **Understand the right questions to ask.** Effective oversight requires being armed with the right questions. Dr. Robertson recommended reviewing the UK Cyber Governance Code of Practice[2] for a list of questions to ask the management team. He said, *"It offers a practical checklist for leaders, consisting of a series of questions for each proposed domain—risk management, cyber strategy, people, incident planning and response, assurance and oversight—on whether your organization adequately manages cyber risk and how."* He asked, *"As board members, how confident are you that you could answer those questions?"*
- **Factor in other crises that may emerge.** Members discussed how the second crisis event influenced their decision making regarding the cyberattack. *"This scenario, where the CEO has a heart attack, presents governance challenges, such as who steps into the role. In real situations, we've seen senior executives involved in fraud during a crisis response, misreporting financial misconduct, or potential embezzlement."* Dr. Robertson said. *"The goal isn't to focus solely on the CEO's health but to ask: what else could be happening that influences decision-making? While the board addresses the cyber incident, there may be complexities arising from other business situations."* A member concurred and shared her experience: *"I've seen it happen. You deal with one crisis, only to discover that the root problem is something entirely different, which can be shocking. As you start to dig deeper, unexpected issues often emerge."*

Scenario Planning for Resilience

While resilience is top of mind for high-growth companies, members said that they are devoting limited resources to scenario planning, as opposed to growth strategies and tactics. But all companies need to be able to anticipate and manage risk, diversify, and adjust so that they remain agile in a rapidly evolving environment. Well-structured scenario planning allows boards to anticipate potential challenges and continue to grow in the face of disruptions.

Mats Persson joined members to discuss the insights from the dual crisis simulation and to explore scenario planning appropriate to high-growth companies. Key observations included:

- **Proactive scenario planning can help high-growth companies stay agile and operational in a crisis.** As Mr. Persson put it, *"Scenario planning is no longer nice to have, it's essential."* Fast-growing companies are accustomed to responding to crises with speed and agility; scenario planning can help them remain operational while making informed decisions. *"When you build your scenario plan, you'll have pre-agreed actions linked to a trigger, so you can react quickly,"* said Mr. Persson.
- **Planning involves broader thinking with multiple potential outcomes.** ***"****The world has moved to the point where we have to think about a range of options instead of singular outcomes,"* said Mr. Persson. He emphasized his point with an example: *"In March 2022, the Bank of England concluded there was a five percent probability of inflation hitting and peaking nine percent in the UK. Only a few months later, inflation was 9% and later peaked at eleven percent. This outcome that wasn't in the ninety-five percent chance of probability materialized within six months."*
- **Planning for a broad range of events can be difficult.** *"I understand the value of scenario planning, but how low in probability should I go when considering possible scenarios?"* asked a member. *"For example, who would have thought the entire world would go into lockdown and survive? Scenario analysis needs to be efficient; evaluating every unlikely scenario isn't practical. How do you weigh probabilities when deciding which scenarios to consider or avoid?"* The group explored several strategies:
  - **Focus on what is material.** *"Some events, like cyberattacks and supply chain disruptions, are foreseeable—you know you'll eventually face one; it's just a matter of when and how severe,"* Mr. Persson said. He advised a focus on what is material for the company: *"You need to view the world through the lens of your entire business—not through functional silos—and identify what truly drives value. This means prioritizing customers and understanding what impacts your bottom line."*
  - **Identify what can break the system.** Mr. Hobbs recommended reverse stress testing the scenarios. He explained, *"Reverse stress testing involves focusing on what could break a system rather than assessing every potential risk. For example, consider significant operations in specific higher-risk regions—how might the company approach planning from that angle?"*
  - **Prepare for high-probability scenarios and adapt as needed.** Proactive planning can help reevaluate existing processes and vulnerabilities. For example, before the COVID-19 pandemic, many companies recognized that their supply chains were overly reliant on long-distance logistics

and that their focus was mainly on cost efficiency. When the pandemic struck, they faced significant delays and shortages. Mr. Persson noted, *"Planning for scenarios like a pandemic is worthwhile if it aligns with other ongoing challenges."* Those that had prepared for supply chain disruptions were better equipped to handle the pandemic because they could apply their prior scenario planning. He emphasized, *"Pandemics should be included in every risk register, but active planning should only occur if it supports other initiatives. For example, I wouldn't advise planning for World War III as it would likely be catastrophic for everyone. But scenario planning for supply chain disruptions, for example, often overlaps with multiple concerns such as geopolitical shocks, trade wars, and energy transitions. Focus on scenarios where actionable steps can align with existing plans."*

- **Scenario planning can help identify no-regrets moves for risk mitigation.** Safeguarding assets and remaining resilient for companies where resources are limited, require an approach that starts with lower risks. Mr. Persson outlined three categories of risk mitigation: *"A 'no-regrets' move, the first category, is a low-investment strategy that provides significant impact and serves as a hedge. The second category involves a more substantial hedge, and the third is full mitigation—going all in to counter risks. For instance, some companies moved before knowing the Brexit outcome, and some are currently completely relocating out of China due to perceived risks."* He added, *"We can't achieve one hundred percent risk aversion, but the goal is to understand the risks and their impact as much as possible. Draw out as much information as you can and consult widely to identify 'no-regrets' moves."* Dr. Robertson added, *"These no-regrets moves are often actions that would be good business sense to implement now, regardless."*
- **Cost-efficiency and security must coexist.** High-growth companies must strategically balance their resources. This applies for scenario planning and risk mitigation. *"Duplicating the supply chain can be expensive. It's important to weigh the materiality and investment involved: do you want full insurance, including a complete duplicate supply chain, dual intellectual property, and full risk mitigation? That's costly. Instead, focus on what is justifiable based on probability and material impact—very few companies can afford full mitigation,"* said Mr. Persson. *"Companies often favor ultra cost-efficient supply chains because they are cheap, but these aren't necessarily secure. Both cost efficiency and security must coexist."* Dr. Robertson recommended investing in low-cost risk mitigation solutions. He said, *"If a high-impact event occurs, what low-cost options can we pursue to make a significant difference? For example, we might look for a local supplier or switch from air freight to truck shipping, reducing costs. If a UK supplier represents five percent of our business, having that option helps mitigate risks associated with slowing international trade. What optionality can we invest in now that will also benefit us in the future?"*

Appendix 1: Participants

The following members participated in all or part of the meeting:

Nadja Borisova, BlaBlaCar and Pomegranate Investment
Carolyn Dittmeier, Illy Caffè
Brenda J. Eprile, Atlantica Sustainable Infrastructure and Westport Fuel Systems
Christoph Hütten, Brockhaus Technologies
Linda McGoldrick, Alvotech, Compass Pathway, and Cranial Technologies
Carl Mellander, Tobii

EY was represented by the following in all or part of the EGAN meeting:

François Langlois, EMEIA Assurance, Managing Partner, Markets and Business Development, EY

Tapestry Networks was represented by the following in all or part of the meeting:

Beverley Bahlmann, Executive Director
Todd Schwartz, Executive Director
Hannah Skilton, Associate
Abigail Ververis, Project and Event Manager

Endnotes

[1] *Summary of Themes* reflects the network's use of a modified version of the Chatham House Rule whereby names of members and their company affiliations are a matter of public record, but comments are not attributed to individuals or corporations. Quotations in italics are drawn directly from members and guests in connection with the meeting but may be edited for clarity.

[2] UK Government, Department for Science, Innovation and Technology, "Cyber Governance Code of Practice: Call for Views," January 23, 2024.