CORPORATER

Digital Transformation

Is cyber threat really the greatest risk of all?

Owe Lie-Bjelland,
Director - Program Management GPRC, Corporater

ARTICLE

Digital transformation

Is cyber threat really the greatest risk of all?

Having worked with governance, risk and compliance from a technology and business perspective across different industries and countries for more than 20 years, I have witnessed and been part of the birth of the cloud, the success of SaaS, the maturation of cybersecurity, and the exponential growth in technology outsourcing. This evolution has triggered a seismic shift in the mindset of enterprises when it comes to information - and cybersecurity, compliance, governance, and assurance. Among business leaders, we have seen a shift from ignorance to fear, we are witnessing a shift from fear to awareness, and now we would like to see a shift from awareness to confidence.

No doubt, technology will continue as a trendsetter in the outsourcing market, businesses will continue the digitalization trend, cyber threats will not vanish, many companies will rise and fall, and industries and markets are becoming more and more regulated. The question I wish to answer in this article is this:

In a myriad of new risks, which is the number one most significant risk related to digital transformation?

Introduction

In the late '90s, cyber and information security was in its infancy. So was I, I was in my mid-twenties and my aspiration was to leverage the new web technology to deliver enterprise-grade applications over the internet. I was the technology guy and the co-founder of one of the first SaaS providers in Norway.

As a SaaS provider handling some of the most business-critical information for the global oil & gas industry, information and cybersecurity were paramount to building our business due to the risk of negative reputation and legal consequences that obviously would have caused great loss and possibly bankruptcy for our boutique SaaS business. This is not to mention the ethical responsibility we took on to protecting our customer's data. I remember my partner once said, *"if we get hacked, the financial consequences are so big we can just go home, and we don't even have to lock the door behind us"*.

I started working on what would turn out to become a success, and what would give me great insight. It was hard work; however, my main challenges were not related to the complexity of establishing and maintaining an internal management system or keeping up with regulatory and legal requirements. My main challenges were firstly to make the board understand the potential loss and ROI for our negative and positive risks, resulting in dollars in my budget, and secondly to make the internal and external auditors understand our digital business.

> **"if we get hacked, the financial consequences are so big we can just go home, and we don't even have to lock the door behind us."**

History of risk assessment for information security management

In the early days of information and cyber risk, back in the era of ISO 27001:2005, risk assessments were conducted focusing on the infrastructure components and the deployed software. Consequence and probability were assessed using a qualified approach, also considering the component's vulnerability to calculate the risk level. This approach was good enough for the IT department to reduce the risk to a perceived acceptable level, however, it only got us so far. Problems arose when trying to enhance security further as we realized we painted ourselves into a corner. The work we produced was great for communicating internally among peers who understood the technical and security-related domain, however, it was not something we could easily share with top management to argue for doubling the security budget in the coming year.

With ISO 27001:2013, we saw a shift to align information security management more with enterprise risk management and the insistence on understanding the business context for correct implementation. This, along with digitization, led to a shift to place more emphasis on the assets i.e. actual information and information containers. The risk assessment methodology was enhanced to a semi-quantitative approach where intervals were used to decide the consequence. This was a step in the right direction, however, due to the nature of an interval scale, you cannot do any calculations when trying to aggregate and consolidate risks across departments and up the chain. This approach was still not optimal for communicating effectively outside an IT and security context. The challenges so far were very much related to digitization. However, when a company wants to disrupt its business model through digital transformation, new risks are introduced.

> **The risk assessment methodology was enhanced to a semi-quantitative approach where intervals were used to decide the consequence.**

Digital transformation comes with greater risk exposure

Digital transformation results in a merger of business context and digital context. The two worlds meet causing a reaction on bringing the new knowledge into the board room, blended with the expectation from the board that assurance and operations will add additional value to the business.

Where is the value?

Let's start with a common denominator; any business needs to properly manage its assets. With digital transformation comes the need to assess and manage a business' digital assets. These assets are the same assets security staff are protecting and enabling.

However, assets are still very much out of sight or given less priority as initiatives, processes, infrastructure, cloud, and applications. Reading risk and assurance reports, I seldom see anybody focusing on assets. In a press release from 2017 [i], Gartner says that "*the value of an organization's information generally cannot be found anywhere on the balance sheet*". In the same press release, analyst Douglas Laney says that "*anyone properly valuing a business in today's increasingly digital world must make note of its data and analytics capabilities, including the volume, variety, and quality of its information assets*". Further, Gartner predicts that "*by 2022, organizations will be valued on their Information portfolios*". If you think about it, how big a proportion of your company's assets are digital? You might be surprised to learn that they could easily add up to over 80%.

With digital assets becoming a vital part of the business, it is a key figure when assessing the value of the business in an M&A setting, and it is increasingly important in an insurance context. The CFO office includes the current value of business-assets on the balance sheet [ii], but what about the digital assets? Digital companies' M&A valuation is currently not reflected on their balance sheet, but this does not change the fact that a digital asset has a value. Have you ever stopped to consider the relationship between the inherent risk of a digital asset and the cyber insurance value? Surely, that's one good reason to keep track of the inherent risk.

Digital transformation comes with greater risk exposure and requires proper governance, management, and protection. Greater risk also means a greater risk of opportunities, not only the negative consequence of risk. A positive risk will potentially add value to your business – that is why we pursue the opportunity risk of digital transformation. Strategy, tactics, operation, and data must be seamlessly integrated and holistically governed to understand the real value of the business on its journey through digital transformation.

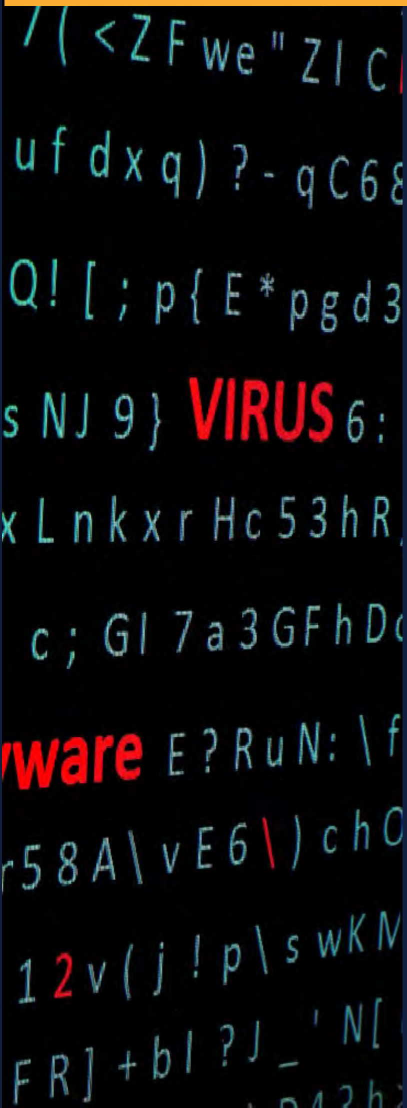
> **"Have you ever stopped to consider the relationship between the inherent risk of a digital asset and the cyber insurance value? Surely, that's one good reason to keep track of the inherent risk."**

Brakes make a car go fast; great brakes even faster

In our boutique business, I quickly realized that risk management was the key to staying ahead of threats, making prioritizations, communicating with stakeholders, and aligning operations to our strategy. I have learned to think of risk management as an enabler for a business to perform better. To give you an analogy; the defensive way of thinking about the purpose of brakes is to make the car stop.

Offensive thinking flips this around and emphasizes the benefits of having brakes – for the car to go fast. The better the brakes, the faster you can go. Keeping in mind that risk can be offensive, we're witnessing an unparalleled opportunity to put digitalization on the board's agenda to stay ahead of the game – and I mean really put it on the agenda, not by checking in on the progress of digital transformation as the last item before lunch. Running a digital business requires a different mindset, different tools, different skills, and a different way of communicating. Businesses need to know that digital transformation is not about introducing tablets and providing board papers as PDFs – that is called digitization. It is a seismic shift in how to value your business, how to measure performance, and how to manage your risks. My personal statement is, "*the greatest risk in digital transformation is the lack of effective communication between the board, executives, and managers*". In a cyber context, the potential impact of this risk alone can be devastating to the company and individuals on the board.

> **"The greatest risk in digital transformation is the lack of effective communication between the board, executives, and managers."**



Assurance might hold the key to remediation

A company's assurance function is experiencing challenges in adding value to its stakeholders. Executives seek greater value in the assurance function, especially when it comes to regulatory compliance, third-party relationships, cybersecurity, business continuity, emerging markets, and IT governance. The internal auditors in many companies are stuck between a rock and a hard place due to this communication gap. How do you effectively audit a company in digital transformation where security staff and business are not aligned? If there's a misalignment internally, how can we effectively assure that 3rd parties are aligned with the business context – after all, they might be managing or accessing some of our digital assets?

The assurance function has a great opportunity to add value to their stakeholders by advising on how to remedy this communication gap, running scenario-based threat assessments, assessing the processes and technologies exploiting the digital assets, aligning protection efforts with asset value, reducing compliance cost by holistically assessing compliance across multiple business domains and regions, working more effectively by getting insight into holistic and integrated risk & compliance data, leveraging RegTech, AI and analytics to streamline audits, and prioritizing the assets that matter the most. The 2018 Global Chief Audit Executive Research Survey Results states that: "*failure to act will see risk and change outpace internal Audit*"[iii].

From ignorance to fear

In human psychology, if you don't understand the consequence of a probable event, if you're not able to apply the impact to your own life or to another's life, you will enter the state of ignorance. However, after witnessing somebody in your immediate proximity getting impacted, or if you experience it yourself, you will find you enter the state of fear. Security managers have seen the threat exposure to digital assets for years, however, some have not been able to speak the language of executives, and some have not seen the potential business impact. The executives on their side have been in a state of ignorance, some have not understood the potential ramification for the business, their customers, the market, and even the economy.

With the recent incidents highlighted in the news impacting companies all around the globe with regards to data privacy, ransomware, information leakage, breaches and more, businesses have entered the state of fear. Cybersecurity vendors are aware of this, and they drive a lot of the news, emphasizing areas of fear where their products are specifically targeted. Their objective is to influence executive conversations in corporations about cybersecurity, using the executives state of fear and the lack of a realistic risk profile. The cybersecurity vendor marketplace is growing so crowded that some companies are even lying about security emergencies and threatening to expose insignificant breaches to the media. If the company's risk profile cannot be understood and trusted, it is very hard for managers, and not to mention executives and the board, to relate to the current trend.

At the top, performance goals and strategic initiatives are very often quantified. Anything executives believe can impact their objectives will get their attention. However, the more red/super-high risks on a heat map, the more frustrated they become. Semi-quantitative heat maps/risk cubes are not effectively communicating a realistic risk profile. They might even resent the idea of dealing with the risk. At this point, both parties are in a state of fear. The security managers are afraid of not conveying the message, and the executives are afraid they will not understand how to make the right decisions. This easily leads to frustration, stress, and conflicts. To move on from the state of fear to a state of awareness and eventually into confidence, executives must drive effective communication as part of their digital transformation.

The more red/super-high risks on a heat map, the more frustrated they become.

From fear to fair

How do we get from a state of fear to a state of awareness? We need a way of communicating risk effectively. Executives are seeking a way of quantifying their cyber risks, similar to their traditional enterprise risks, and, they are seeking to understand cyber and the risk it poses to the business to make better and faster decisions to perform and confirm. Managers, on the other hand, seek to understand the business context and successfully communicate the risk profile to executives to get their support for mitigating and pursuing the risks.

Effective communication around risk management and digital asset management can be achieved by introducing a couple of tools:

The first tool is to have a uniform way of quantifying risks; An example of a method used for establishing a uniform communication for cyber risk is Factor Analysis of Information Risk (FAIR) [iv]. FAIR has emerged as the standard Value at Risk (VaR) framework for cybersecurity and operational risk. The result of a FAIR approach is easily understood by the board and executives. FAIR will also educate security staff to align their thinking to the business context. As you will estimate the value at risk, you need to identify the value for e.g. your digital assets.

The second tool is to integrate a siloed risk space. In 2017, Gartner introduced the concept of Integrated Risk Management (IRM). This can be leveraged to bridge the communication gap in combination with FAIR to establish the fundamental structure needed.

Effective communication around risk management and digital asset management can be achieved by introducing a couple of tools.

From fair to awareness

Directors need to ask the right questions to bridge the communication gap, and security managers need to be able to answer what they might perceive as irrelevant and very difficult questions.

- How secure are we as a company?
- What are the residual risk values compared to the inherent values for our digital assets?
- What's our current threat level?
- Are we spending the right amount of money?
- What is the ROI for cyber risk reduction (CR3OI) initiatives?
- What's the expected loss for a ransomware attack scenario?
- How do we compare to our peers?
- What are our options for mitigating the risks?

Thinking of risk in an integrated, holistic and quantitative manner will enable security staff to answer the above questions.

Speaking the same language, where to start?

Important actions to take are:

- Ensure leadership commitment (yes, they are ready for it)
- Identify the correct best practices for the cyber and information security management or overall GRC needs in your industry and market
- Have an effective strategy and visualization of performance goals, objectives, and risks across the organization
- Work on awareness and have everybody speak the same language when interfacing different groups in meetings using a quantitative language
- Evaluate your existing risk tool's ROI
- Agree on how to measure the effectiveness of a holistic GRC program
- Establish a baseline of Inherent risk for your digital assets
- Determine how much cyber insurance you need?

You can't manage what you can't measure

The current situation in many organizations is a siloed operation in digital coexistence, often lacking a unified tactical approach to risk management, which in turn drives performance, regulatory and organizational compliance management, legal management, audit management, third party risk management, digital risk management, and business continuity management. Peter Drucker's famous quote "*you can't manage what you can't measure*" is a key to solving this situation. However, the CEO of Corporater, Tor Inge Vasshus, once said "*you can't manage what you can't describe*" to help executives complement their metrics and get a deeper understanding of their business. To bridge the communication gap for cyber risk, you must start describing your digital assets, assigning responsibilities, valuing them, risk assess them using a VaR approach, and then add a comment from an SME to complement your metrics. Here are a few examples of metrics you should consider monitoring holistically:

- The ability to recover from a cyber attack expressed as cyber resilience[v] in a BCM context
- The value of your assets
- Risk exposure
- Effectiveness for risk and compliance management
- Effectiveness for assurance

> "You can't manage what you can't describe."
>
> - Tor Inge Vasshus

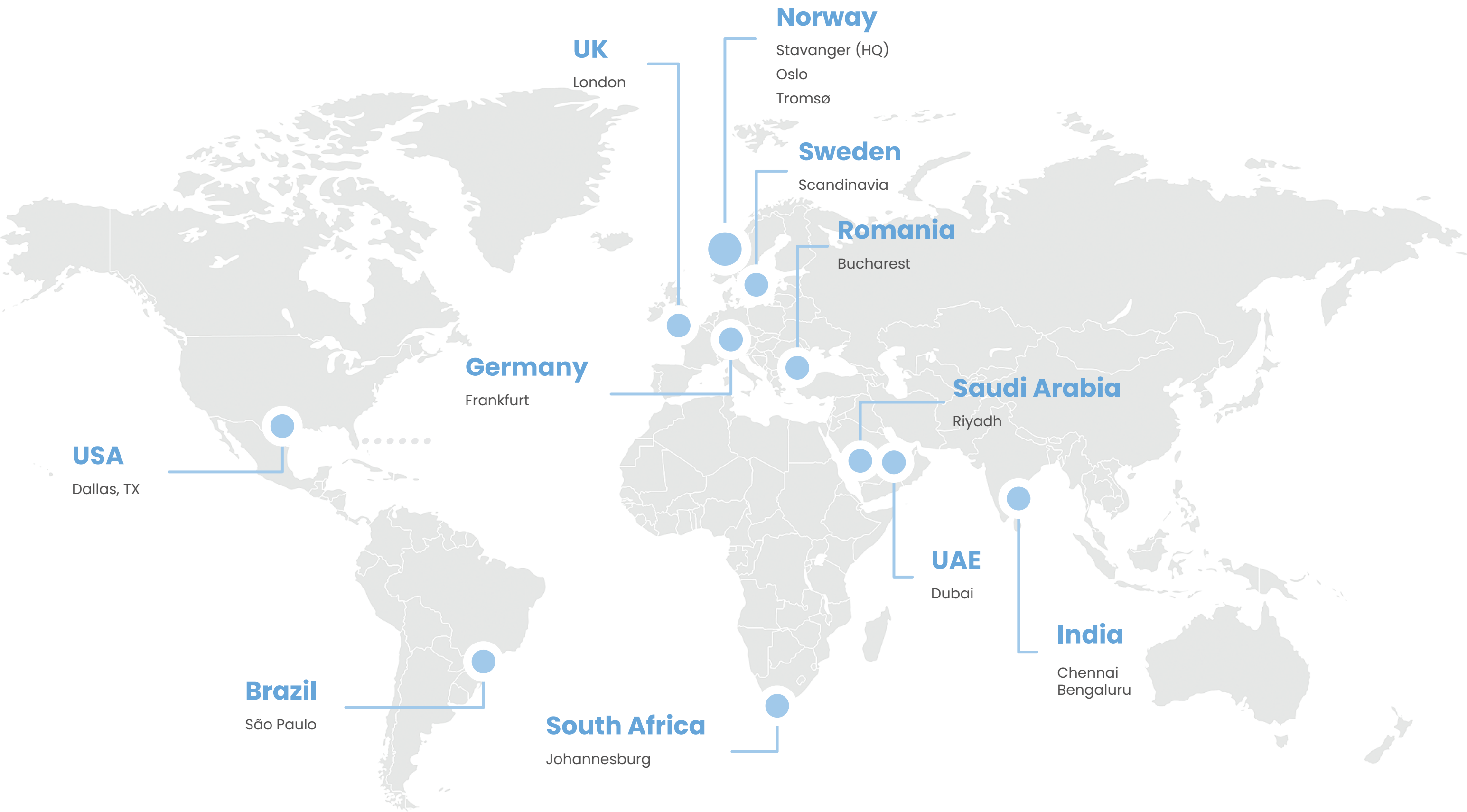
Conclusion

In conclusion, to answer the question in the title to this article, in my opinion the greatest risk of all is in fact not cyber threat in itself but an inability to communicate internally in the organization in a common language which allows meaningful decisions and actions to be taken, amongst these to reduce the cyber threat to an acceptable level.

This article first appeared in SIRK 1/2019 published by IIA Norway.

About Author

Owe Lie-Bjelland has his background from the software technology industry as the co-founder, CTO, and CEO of Xait. He has more than 20 years of international GRC experience in business management, software innovation, cyber & information security, legal & financial compliance, and data & information governance from working as a trusted vendor, management advisor and consultant for several fortune 500 companies across different industries in Europe, USA, and Latin America.



Corporater is a global software company that empowers medium and large organizations worldwide to manage their entire business on a rapid solution configuration business management platform that adapts to their unique business model. We use our gains to make a social impact.

Corporater BCM software solution provides a digital platform to holistically govern, manage and assure the organization's business continuity program according to international best practices.

CORPORATER

Contact us for demo at
www.corporater.com/requestdemo
info@corporater.com