One of the key topics in today's discussion of risk is the concept of cyber risk. Executives and politicians worry and start acting on cyber risk – some more deliberate than others, and some actions are taken almost blindfolded.

However, I claim that cyber is not **a** risk ("a" implicitly meaning one). There is no "one cyber risk", which companies can start mitigating or buying insurance for – instead, there is plethora of risks which are based on the worlds increasing use of computers and internet – both in terms of numbers and degree of advancement.

Just like there is no one "reputation risk" – but a range of risks, which may affect your reputation.

Hence – "cyber risk" is a category of risks containing a number of bigger and smaller risks to the organisation.

Furthermore – there is another issue, which often derails the discussion of cyber risks. These are not IT risks, but business risks … related to the use of IT. This means that the IT team only rarely causes these risks, but very often have the tools to mitigate them. In this case, the IT organisation is to cyber risk what firefighters are to fire:

- Firefighters actually do sometimes initiate a fire … but does this in a controlled and deliberate manner to practice and/or enable more effective fighting of other fires. IT teams may hack systems to find weaknesses.
- Firefighters work a lot with pre-emptive measures to reduce the likelihood and impact of a fire. For IT teams and cyber related risks, this goes all the way from having systematic back-up procedures to deploying business processes to protect data integrity.
- Firefighters train and maintain their equipment diligently to ensure it will work as planned, when the need arises. For IT teams, this includes "fire drilling" key cyber attacks as well as ensuring safety software and processes are kept fully up to date.

Some companies are further in the development of this than others, yet some companies are more relying on IT and hence more vulnerable to cyber related risks than others.

Understanding cyber related risks

To understand cyber related risks, one can group these by type of consequences they may have on the company/business. These can be issues like:

- Loss of vital data or data accuracy, which may hamper operations.

  This could be deleting operational data by accident – or as an attack, as well as changing data to something which is wrong – but will not be easily detected, and hence may lead to wrong actions/decisions.

- Leak of confidential data, which can deplete competitiveness. This includes confidential data owned by business partners, who may stop collaboration because of this.

  This can be product launches, key strategies, as well as a host of other issues.

- Loss/failure of key IT supported processes, which includes attacks on processes (DOS etc.)
- Loss of systems platform.

To specific companies there can be others which are even more important.

Furthermore, one can look at the source of the risk … how/why it happened, and here we need to look at the source and how "deliberate" this risk was invoked.

To keep things simple, the risk instigator may be:

- The IT system/platform itself as this is flawed by some built-in inconsistency. One may argue these are failures/problems rather than risks – but they are here seen as risks, as they materialize somewhat at random … years after being "created".

  Such risks can and will generally be handled through systematic and comprehensive testing – which has to be done at the time of development and prior to full implementation. This is not seen as IT risk management, but as system quality assurance.

- Internal staff/employees – who for several types of cyber related risks are the key instigators.

  Here the key to handling is driven by training and having defined procedures, access control, password safety systems, monitoring use of IT systems, etc.

- Staff/employees at business partners. These may be upstream partners (vendors), downstream partners (customers) or just business partners (e.g. consultants, distributors)

  These are harder to control for the company, as people are employed by someone else. Key measures are collaboration between the two companies and agreeing on IT safety approach.

- External, i.e. people who do not normally interact with the company or its systems/data. This group includes cyber criminals

  Here no level of training will help or be even remotely plausible. This is where firewalls and IT security processes, password protection, and other methodologies comes into place. This is an area, which has been and is of growing concern, and where IT organisations need to be diligent and holistic in their proception approach. A case in point is a company who was hacked through the IT based control of their air conditioning system.

Finally, one may look at risk instigation (making it materialize). This may also be grouped as means of response differs:

- Accidental, i.e. actions taken (or more often, not taken) without any consideration of doing any harm to IT systems, processes or data. These are most often based on internal sloppiness to safety procedures and disregard of data confidentiality.

  Statistically, this constitutes the bulk of the risks that materializes, but rarely the most impactful ones. They happen "all the time". In parallel to employee health and safety – these risks rarely, if ever, kill anyone – but they include a lot of trip/fall bruises.

  They are often handled through some level of training and procedures, including "you have to hold on to the handrail when using the stairs" or "you are not allowed to look at your cell-phone while walking" and the like.

- Deliberate, i.e. actions deliberately taken – but not for the purpose of doing harm to the company. This includes "drive by shootings" where the action taken was aimed at something else than your company. A case in point was the Maersk Group being hit by the Notpetya attack.

These risks are A LOT rarer than the accidental issues – but that does not mean they are rare. It is commonly known that when it comes to being or having been hacked there are two types of companies. Those that have been hacked, and those that do not know, they have been hacked. Often the damage is so small the hacking is not even noticed – but as in the case of Maersk, it can be quite damaging.

As the company is not targeted, most existing mitigations like firewalls etc. will work, unless superseded by people's ignorance and sloppiness.

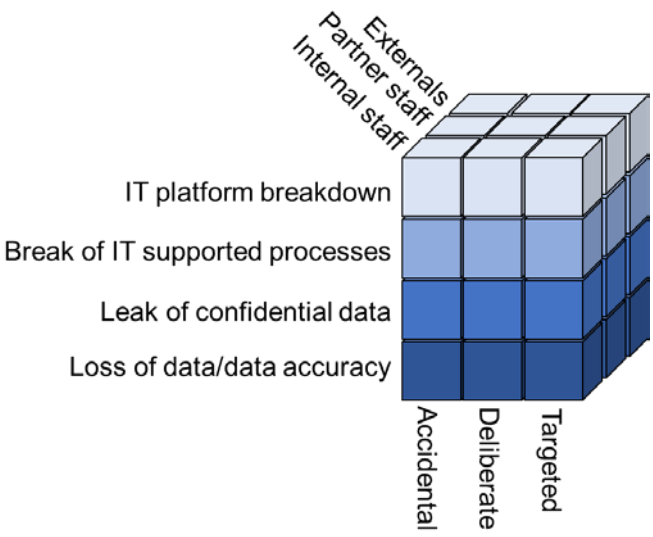
- Targeted, i.e. action taken to deliberately hurt your company. These risks are – to most companies – extremely rare, but generally also very damaging should they materialize. This group includes most cyber-crime, where criminals hack your company for money or some other benefit.

  These are generally criminal offenses, and can and will be investigated as such. One problem though is, that the approach may be so subtle and discrete, that the attack rolls for an extended period of time without anyone knowing it.

In total, we get some kind of cube of cyber related risks. I am certain others could add other equally valid dimensions to this making it very impossible to draw up.

The idea of making this cube is to create some platform from which company specialists – not just IT people, but also legal, operational, managerial and other relevant specialists can identify risks more tangibly and hence more relevant to actually address and act upon.

Some of these "little cubes" will be totally or next to irrelevant – but "nice to know" that here is an area of cyber related risks, we do NOT have to deal with.



Others may be absolutely pivotal – and acting is an absolute must to have an acceptable level of protection and security around the company's use of data and IT. As one example – protection against "mass hacking" of the autonomous vehicles which in a few years will be roaming the streets must be a key priority for those developing the hardware/software/communication platform of these vehicles – at least, I cannot imagine it would not be.

Managing cyber related risks

As stated in the beginning, the IT team is not "driving" the cyber related risks, but in a lot of instances, the IT organisation has the key tool to mitigate these. As such, IT is part of the solution rather than a part of the problem. However, not everything can be solved by the IT team.

Some handling/mitigation is done proactively or preventively and seeks to minimise the likelihood of a cyber related risks materialises.

- Some, a lot in mere numbers, can be effectively managed through training programs – ensuring that people know what they are doing, when they do, what they do. This includes "cultural training" of what is/is not good conduct.

  This type of mitigation is a business mitigation, and whereas the IT function may be involved, they need not be the driver of this.

- A parallel type of business mitigation is establishing and controlling procedures as to how to enter/update/delete data in the IT systems. Having precise process descriptions, and monitor that these are followed is a standard auditing process – which here reaches into the use of IT systems and handling of company data.

  This may also include access control whereby individuals are restricted only to handle data they are trained in- and certified to handle. Many companies have such programs, but in my experience, these are often not diligent enough to be effective as people changing jobs do not lose access to handling data they no longer need to handle, and/or managers are given the possibility to handle "everything" simply because they are managers.

- A lot is handled reasonably effective by use of firewalls, procedures, monitoring, and controls ensuring that (especially) externals do not get into and tamper with data/systems. However, as criminals are about as creative as firewall manufacturers – and vastly outnumber these – it cannot be avoided being a cat & mouse chase … and the problem is, that the company may have several/many mice running around, and every mouse that is not caught by the cat may present a problem.

  One also has to face that whereas most externals are individuals, some are organisations and, being professionally paranoid, even government agencies from some countries. These can be powerful adversaries to battle against.

  This kind of security is often expensive, and the company must strike the balance between how much they wish to do, and how much risk they are prepared to take.

All of these pre-emptive actions may and will serve to vastly reduce the likelihood of being hit by a cyber related risk – just like locking your car when parking reduces the likelihood of theft. However, at some point in time, the company will be hit by a cyber related risk … and then what?

The first issue is to actually know you are being or has been hit. In many instances, this can be tricky to discover, and some companies will have to make quite substantial efforts to be able to detect materialization. Then one could say "OK, but if we cannot see it – how important is it anyway" – well it need not be, but a hit may develop like a cancer, and if allowed to grow – can be fatal. Not all cyber related risks hits like breaking a leg.

The company needs to be able to handle a risk materializing. This includes having "disaster recovery plans" addressing how we effectively get over this – as well as "business continuity plans" addressing how do we run the company while recovering. Developing such plans should be a collaborative effort where people from risk, security and business work closely with IT to develop strong and viable plans – which are then described, trained and drilled to ensure effectiveness when the "fire hits".

Most companies have fire drills, where they ensure people know what to do, and how to get out of the building when the alarm sounds. Alarmingly few companies have something similar when it comes to any other forms of risks – including cyber related risks – and this can be absolute devastating. As a case in point, the Notpetya virus attack which hit the Maersk, had severe business and performance impact – despite Maersk having action plans in place.

On top of all this, no company is fully end-to-end, and hence any company may also need to see itself as a link in a chain – and ensure adequate protection of the other links in that chain. These or those partner data, which we need to operate – may not be essential to us, but may be life & death issues to a business partner. If our protective actions are inadequate, we may lose the business due to a collapse of the partner.

The same goes for the end consumers. Today there are regulations in the EU (the GDPR) to drive data safety for personal data. Whereas the company may not deal directly with end consumers, they may still be subject to mandatory actions to comply with GDPR. One has to be aware that GDPR protects criminals and non-criminals alike – and may make it harder to spot cyber based crime or criminals.

Closing comments

The issue of cyber related risks is complicated, and with the rapidly growing use of digitalization and computers – now into Artificial Intelligence – the severity as well as the complexity grows at an alarming rate. Still, there is no alternative to dealing with this effectively.

To provoke – if/when everything the company does and every process it applies uses IT – every risk it takes is or includes a cyber related risk. That does not mean that IT security should be overruling everybody and everything.

The paranoid can imagine a lot of (perfectly valid) risks and initiate a vast amount of pre-emptive and reactive actions – costing the company a lot of money, focus and resources. Each company has to define and apply a balance – bearing in mind, that if/when any given risk hits, possibly even harder than expected, management will always be blamed for not having done more, especially if the type of risk was known to the company.

Managing cyber related risks is not about risk aversity as this would lead to loss of competitiveness in the market due to resource drain and costs incurred. It is about intelligent risk taking – of knowing what risks to take, and how to deal with what is not acceptable.

The first step is to break the elephant into tangible and manageable pieces and deal with these systematically – some with more, others with less effort.

Hans Læssøe
AKTUS
hl@aktus.dk
www.aktus.dk