Cyber security in a disruptive paradigm shift

av John Wallhoff (CISA, CISM, CISSP)

Cyber security is more than a new name for IT- and Information security. It is a disruptive paradigm shift digitalisation have brought upon us, a paradigm shift that require a new approach and capabilities to meet opportunities and threats of today and tomorrow.

We are living in fascinating times where digitalisation changes how we act and interact, a time with opportunities but at the same time it affect us in a negative way. It is in this context the concept of cyber security is emerging, with its roots in IT- and Information security, but with new prerequisites and expectations. We are in a paradigm shift where the most severe mistake we can make, is to face cyber security with an out-dated approach and capabilities.

Today we don’t know what cyber security is, there are simply too many definitions. We have also taken an approach based upon how we used computers in the 1980-ies, a world that in many aspects looked different. Maybe our only option is to face the threats of today with the approach we have had for more than 30 years, just like we do now. At the same time there is an insight within the security industry about its failure. Weaknesses in cyber security have in many surveys indicated to be much more severe than ever before.

In several discussions I have seen that management teams acknowledge and are truly concerned about risks related to technology and digitalisation with its impact on the organisation. Still with this concern it is not unusual that efforts in cyber security is underestimated and unfortunately in some cases neglected.

If we reflect upon what may have an impact on our capability to act digitally, ”Advanced Persistent Threat” has emerged as a new type of attacks. It is about an attacker that uses several techniques and methods, while having patience in the attack. This might be the major reason why we need to address cyber security with much more sensitivity and better responsiveness than what we are used to, and that is also the essence of why cyber security is in a disruptive paradigm shift. We are forced to move our focus from prevention to response, as a consequence of our increased dependency on technology while it has become cheaper and easier for attackers to do their work.

What to be worried about

The picture of threats is mostly about that we have become so dependent on our technology, to be able to do our daily activities and generate value for our organisations. When technology ceases to work, we loose the capability to do our work and cannot generate this value. In some situations it is still possible to recover from a disaster or disruption, but the magnitude of work needed is so huge that in reality it is not possible.

There is also a threat related to privacy, where legislation will require more from organisations, to protect information that can be related to each and everyone. These requirements are becoming contradictions, where we tend to accept being exposed to a larger extent when we are acting digitally. The impact is razor-sharp of what is ethically and morally acceptable, where a mistake in how an organisation acts, can have a tremendous impact on the confidence in the organisation.

For organisations it is still important to keep some information confidential, but with the increase in speed of change, it need to be put into its context instead of being handled in a static manner. Very often we only need to protect information in a short period of its lifetime, and then reduce the level or protection. This assumption drives costs when you don’t have the capability to adapt the level of protection to its context or undermine the understanding of protecting information because it is too difficult.

The downside of value generation

Our technological evolution is driven by incitements of economics, with requirements on profitability and generating value. At a start it was achieved by using computers for administrative procedures such as accounting, invoicing and payroll. Since then a lot have happened and today it is about digitalisation, a change in how we act and interact where financial trading robots and digital coworkers are helping us with translations as some obvious examples. We have in other words gone from economies of scale to generating value.

When digitalisation is discussed, ”disruptive innovation” need to be included in the discussion, where cyber security is an obstacle that may prevent these innovations to become real. If you as a leader do not understand weaknesses related to cyber security in products and services, you risk loosing your competitiveness when the attack is a reality.

Primarily large organisations with global presence are exposed for risks related to cyber security, but this is a misconception based upon how we face the threats of today with an out-dated approach. Every organisation is exposed, no matter the size or industry, where it is about when you are attacked and not the probability of it. The paradigm shift is disruptive, through a new population of threats entering the market and acting in a way we have never seen before. Today it is possible with limited means to initiate a large scale and very precise attack and where knowledge about how to do it is shared in hyper speed.

About John Wallhoff

With more than 15 years of experience in IT and Information security, Cyber security have emerged a key topic. He works as advisor in Scillani Information AB where he also works with issues related to Fraud & Corruption, Analytics and IT Service Management.

What is new

How we look at it is the key difference compared with IT- and Information security, where the digitalisation is the essence of it. The transformation is about how digital technology has become a part of our daily life, where we move from a focus on what assets we use to how it is used.

Another difference is how we move from using IT to support our worklife to enable IT to become our digital co-worker. Fiction with robots like R2D2 and C-3PO in Starwars does no look like what we see in our reality where services are provided to navigate, translate and other activities that can be done digitally.

Technology is the epicentre of cyber security, where our focus needs to be. By addressing cyber security in products and services when we design and develop them, we will gain advantages for the organisation. First and foremost providing us better capability of deliver to meet customer demand. At the same time it is necessary that processes are both redesigned and improved, to be able to face opportunities and limitations in technology. In this context we are not only talking about processes within the IT department, we are taking about processes throughout the organisation, where digitalisation have a significant impact or is critical to generate value.

There are several forces driving digitalisation, where the increase in use of services via Internet (cloud services) is one of the strongest. It is today possible to develop and test new business ideas and concepts with a lower financial risk than before, where the organisation expects the service provider to deal with questions about capacity, availability and not the least cyber security.

Three steps on the cyber security journey

The first step – Open your mind

To undertake cyber security, we have to let go of what we have learned in the past and move forward. It is not about forgetting what we have experienced, instead it is about having a focus on the business, its processes and the value generated through digitalisation. It is also important to talk the language of the business and not make it harder for us talking the language of the security industry.

In practice it is about processes completely digitalised and designed for the consumer of a service. You see this in the financial industry but also in other industries. It is also about processes where humans interact with technology to generate value, like we do in the healthcare industry where technology is used for monitoring of patients. In this context we leave life defining decisions to humans (doctors and nurses) supported with the digital co-worker (the machine).

Open your mind is about putting what we deliver in focus and assess how we can do that with good quality and predictability. In many cases it is about function, i.e. to be able to do his or her job with pride.

The second step – Start with the basics

The capability to manage cyber security need to be built from bottom up and not with excuses that you need management commitment before you can make it happen. The speed of change is so much faster today, than what it was 30 years ago and that require the affected individual to act and take initiatives. This capability can be enabled by understanding limitations and use this to gradually identify and manage what may have a negative impact on digitalisation. Management do no longer set or run the agenda, it has to be observed and re-mediated in the field by the individually affected co-workers. Management have instead a role to support the agenda through a strategy and allocate resources to manage cyber security.

In practice this can be accomplished in many ways, from traditional training of all employees, to developing sophisticated technology to capture and mitigate attacks. It needs to be supported by an enhanced capability to combine function with dysfunction when products and services are developed, based upon sound security architecture.

Start with the basics is about enabling the capability to manage negative impact on business processes and where it is possible pre-empt it. Management need to change its way of working to be able to respond faster upon changes in the surrounding world and to recognise that all organisations are exposed.

The third step - Adapt

We cannot avoid the future, so we need to embrace and adapt to it. Threats changes continuously and it is not possible to build a protection that is static. It also require us to monitor how the technology we use in our digitalisation, can be used in a manner we want to avoid.

In practice it involves more focus to capture and analyse events that affect digitalisation and re-mediate the root cause of those events, but also to create a security architecture that can reduce the impact from an attack. To be able to investigate negative events, a capability is required to think like an attacker and how weaknesses are exploited, where you have the skills to follow the whole attack through. It involves more than technical skills, where communication and legal aspects are relevant to understand and use.

To adapt throws traditional long term planning and strategies over board, like it is necessary in a disruptive paradigm shift. It will have an impact on how specialists have been taught to manage IT-security, i.e. the approach based on previous experiences. It also has an impact on how different departments need to work together, managing negative events that have an impact on digitalised processes.

Were are we today

There are several initiatives to define what cyber security is, but mostly it is based upon old perceptions, experiences and expectations. Standards and frameworks have been given a new layer on top of everything else or parts of those standards and frameworks have been remodelled slightly. One thing is certain though; ”Cyber Security” is a new phenomenon to us and what it is about is being shaped right now.

One of the oldest definitions was published in 2008 by the international teleunion ITU, a special agency within UN:

> Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user’s assets.
>
> Organization and user’s assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user’s assets against relevant security risks in the cyber environment.

Other definitions have followed and in 2012 ISO/IEC defined “Cyber Security/ Cyberspace security” and “Cyberspace” as:

> Preservation of confidentiality, integrity and availability of information in the Cyberspace x).
>
> x) complex environment resulting form the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, whick does not exist in any physical form.

The work to manage cyber security have in 2014 resulted i in a publication by the US standardisation institute NIST, where “Cyber Security” is defined as:

> The process of protecting information by preventing, detecting, and responding to attacks.

Since then cyber security has been addressed in 2014 by the independent organisation ISACA6 with a definition of “Cyber Security” as:

> The protection of information assets by addressing threats to information processed, stored and transported by internetworked information systems.

We can now see a change in how cyber security is addressed, where “Cyber Resilience” instead of ”Cyber Security” is defined in the best practice publication Reslia:

> The ability to prevent, detect and correct any impact that incidents have on information required to do business.

In Sweden it has also been the topic for a public inquiry, where they combined the definition of information security with cyber security.

All together we see several initiatives about cyber security, where the fragmentation of definitions are so wide, that we can conclude that we really do not know what cyber security is. At the same time it is an indication that we are in a phase where it is evolving into a new context.

Resilia Foundation

Cyber Resilience Best Practice, Reslia™, is designed to help commercial and government organizations around the world prevent, detect and correct any impact cyber attacks will have on the information required to do business. Active cyber resilience is achieved through people, process and technology.

The Resilia™ Foundation course starts with the purpose, key terms, the distinction between resilience and security, and the benefits of implementing cyber resilience. It introduces risk management and the key activities needed to address risks and opportunities. Further, it explains the relevance of common management standards and best practice frameworks to achieve cyber resilience. Subsequently, it identifies the cyber resilience processes, the associated control objectives, interactions and activities that should be aligned with corresponding ITSM activities. In the final part of the course, it describes the segregation of duties and dual controls related to cyber resilience roles and responsibilities.

Audience

The Resilia™ Foundation course audience includes all teams across the IT and Risk functions, including:

- IT Service Management
- Business Analysis och Design
- Development
- IT Project& Programme Management
- Risk and Compliance

Prerequisites

There are no prerequisites for this course.

Place and date

Is provided together with our partners

RESILIA™ is a trademark of AXELOS Limited. The Swirl logo™ is a trademark of AXELOS Limited. www.axelos.com