secior.
DIGITAL RISK MANAGEMENT

Digital Security Risk Management for data centres

Raymond Bierens and Sander Nieuwmeijer

New digital technologies are increasingly transforming the way organisations work. Data centres play an important role in this transformation and are therefore considered critical national infrastructure in a growing number of countries. Without data centres, online digital services as we know them are unavailable, digital devices cannot be operated without connectivity and big data cannot be exchanged. But, like any organisation, data centres are also undergoing the same digital transformation themselves, which makes it very important to map and manage the corresponding risks. What exactly is the impact of the growing connectivity in the control and operations of these data centres?

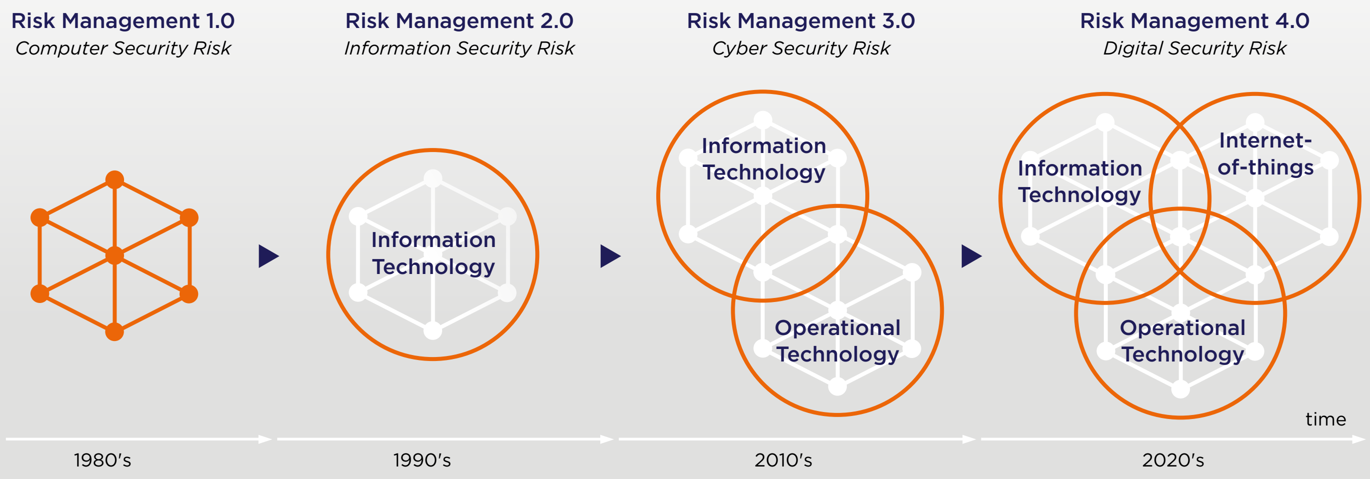

Diagram 1: Historical overview of the development to digital security risk management © Bierens 2020

The Netherlands a frontrunner in digital infrastructure

The Netherlands was the first country in the world linked up to the American internet as we now know it. As European initiator, and because of our favourable location, the Netherlands has always remained a frontrunner in digital infrastructure and is still a springboard to the rest of Europe. Because of its stable political climate and reliable power network, the Netherlands has an extremely favourable business climate for data centres. As a result, the Amsterdam Internet Exchange (AMS-IX) is one of the largest internet hubs in the world. This digital oasis also entails risks, however, which are still not always recognised or understood by everyone within organisations. The awareness of digital risks within organisations is therefore an important point for attention. Despite the fact that 63% of organisations are actively working on a digital transformation,[1] just 23% of the C-level devotes adequate attention to the digital risks arising from that.[2]

Growing risks for data centres

Cloud computing, growing automation and remote working have increased the possibilities of attack. Hackers have seized on this to carry out waves of cyber attacks, which means the risks for data centres have grown. Cyber attacks on data centre control systems can cause system outage, production loss, injury or even loss of human life and have a major impact on a data centre's reputation. The facilities infrastructures underlying the functioning of data centres are controlled using OT (operational technology). The OT ensures the proper functioning, security and availability of, among other things, the cooling equipment, power distribution and connectivity.

Merging the worlds of Iand OT

Diagram 1 provides a visual representation of the merging of the two previously distinct worlds of information technology and operational technology. With a view to efficiency, major steps have been taken by enabling IT and OT to communicate with each other. The Industrial Internet of Things (IIoT) is an expansion of the Internet of Things (IoT) for industrial applications.

[1] https://www.rsa.com/content/dam/en/white-paper/rsa-digital-risk-report-2019.pdf

[2] https://www.rsa.com/en-us/offers/rsa-digital-risk-report-second-edition

IIoT components are intended for machine-to-machine communication. IIoT is used in data centres and is at the cutting edge of IT and OT. The use of smart sensors and actuators has brought about drastic improvement in the monitoring and control of physical infrastructures, and in remote access and control. But the digital threats are also increasing and the security risk is greater than ever before.

In order to gain a good understanding of the impact of a data centre's digital transformation, the dependencies inside and outside the data centre must first be mapped out. This encompasses more than requiring that a supplier holds an ISO certificate. It involves obtaining a comprehensive overview of all the technologies that are directly or indirectly connected with each other. More than 98% of all processors can be found in embedded systems (OT), not in PCs or servers (IT).[3] OT is connected to IT and IT is connected to the internet. In a world where IT technology is used by a Network Operations Centre, where the (OT) cooling equipment, for instance, is controlled remotely and sensors are increasingly connected to suppliers, mapped out this attack area requires the first step of digital security risk management. After all, if something has an IP address, the digital risks must be managed. Attackers could activate sprinkler systems, for instance, and destroy thousands of servers, or deactivate or tamper with cooling and/or energy systems to cause a fire or explosion.

Once mapped out, the attack area provides a comprehensive overview of all the connected technology used in the data centre. The second step is how the providers of all these technologies can be managed. It was not for nothing that the NIST framework was expanded from v1.0 to v1.1 to include, among other things, the topic of supply chain management. At the same time, supply chain management is a term that corresponds to the outdated cybersecurity risk management, while digital risk management 4.0 assumes that this supply chain concerns many more dimensions. After all, every connected technology has all sorts of hardware and software components that have been purchased from different suppliers and put together. As the 2020 SolarWinds hack demonstrated, these days even security software modules are programmed based on material acquired externally, which means that corrupted software (updates) already arises in the programming phase. In the event of digital security risk, therefore, we no longer talk about a supply chain, but rather an ecosystem of suppliers, which have been mapped out behind each of the connected technologies in the first part of digital security risk management 4.0. Simply assigning these risk management responsibilities to the supplier has proved to be inadequate too often in the past.

Complex ecosystem as the starting point for digital risk management

Taking the ecosystem as the starting point for digital risk management also makes clear how quickly the risks grow as technologies become more connected with each other. An unmanageable architecture quickly arises from this, in which the digital security is much more difficult to guarantee, as became visible in May 2021 in, among others, the ransomware attack on Colonial Pipeline in the US. The rapidly growing number of devices in a network makes keeping a real-time overview of the dynamic attack area a necessary second part of digital security risk management. Good end-to-end network segregation and access management are essential parts of reducing the risks and their impact. This is easier said than done, because a segmentation within the data centre does not mean a segmentation of the suppliers of that connected hardware and software. It is precisely the growing desire on the part of suppliers for, among other things, energy efficiency and remote maintenance of operational technology that creates a risk for the continuity

[3] Cybervision 2025, United States Air Force Cyberspace Science and Technology Vision

of that same technology. The question is justified, therefore, whether organisations have sufficiently considered whether the cost advantages and efficiency improvements generated by connectivity outweigh the risks.

At the same time, the ecosystem has become so complex and contains so many interdependencies that an outage is increasingly likely if one of the components in the ecosystem is hit. Take the Kaseya software hack in July 2021, which forced all the Coop supermarkets to close, for instance. And what to make of the collateral damage, like that at Maersk in 2017 as the result of the hacking of the accountancy software used by the port in Odessa? Not to mention the acceptable number of programming errors in software before it is released.[4]

The final component that makes digital security risk management unique is the starting point that it not only defines defined risk appetite, but also makes the residual risk explicit in order for it to be managed. What are the residual risks that could cause the operations to come to a standstill and what mitigating measures can be come up with to counter those? Because the fact that it will happen is a statistical certainty, the only question that remains is whether the data centre itself has given this enough thought in advance.

Conclusion

Data centres pose a double risk in terms of digital security. Firstly, for the organisation's own operations, which are increasingly connected internally and externally, as a result of its own digital transformations. Secondly, for the growing dependencies of the users of these data centres who will see their operations come to a standstill without the data centre. For this reason alone, data centres can and should be expected to set an example when it comes to digital security.

Points in conclusion

- Approaching risk management from the perspective of a dynamically evolving ecosystem connected internally and externally to the organisation, in combination with explicitly identifying and managing residual risks, makes digital security risk management uniquely suited to the business operations of data centres.
- Through early adoption in this regard, data centres can distinguish themselves within their own sector and provide clients with a higher degree of continuity assurance.
- Waiting too long will only make the risk of outage more likely, resulting in societal disruption, so there is no time to lose.

[4] Steve McConnel – Code Complete 2 (A Practical Handbook of Software Construction)

Cybersecurity
for Datacenters

DIGITAL RISK MANAGEMENT

Boeing Avenue 254
1119 PZ Schiphol-Rijk
The Netherlands

T +31 85 273 6036
info@secior.com
www.secior.com