Nordic CRM

Cyber Risk Management

Cybersecurity is an industry that is blooming with an estimated 3.5 million unfilled positions by the end of 2021, and a zero-unemployment rate in 2021, a number that had held constant since 2011 for experienced professionals.

These numbers should lead to the realization that there is an industry with an even bigger boom namely the cyber criminals. This is also supported by the expected growth in cybercrime damage prediction and with services like Malware-as-a-Service being made available.

Executive Responsibility

World Cyber Scene

"Consolidated Democracies covers less then 10% of the earth population and suffer a loss 1-2% of GDP per year to cyber incidents

International Economics are moving away from Rule of Law into a more Authoritarian World

Accelerated movement of Global Centers of Economic Political Power to China "

Danish Defense committee on Cyber Weapons

Operating an organization in todays World Cyber Scene leaves no doubt that the common shared international values are not in the favor of what the original purposes of the internet were.

As an C-level or boardmember the question to ask your organization should not be "are we secured against an attack, can they get in?" but rather "can we survive an attack?"

Similar for an investor, if an organization do not provide able attention on cyber security as part of an organizational focus areas, it must be assumed that if that organization is hit, any investment might be in danger.

The question that needs to be known within an organization are

What are the top financial Cyber Risk

What are the risk that will significantly alter the core business foundation if they are impacted?

Present day generalized security and maturity frameworks aims at making a common shared security denominator within an organization. Extending this approach with a key focus on top financial Risk allows for better utilization of scared security resources and prioritizing which areas critical attention.

What happens if an ransomware or other attack occurs

Are all systems categorized, structured and protected so they supports the decision on when to ride of an attack or accept the demands proposed by the threat actor, i.e. if a ransomware impacts a top financial risk scenario?

Within the organization are security enclaves created in such a way that they can financial absorb a lockdown of services for the required time until a successful restore have been accomplished?

Is a Cyber insurance in place that is justifiable as a strategical asset to mitigate financial loss of a cyber attack?

Who assume responsibility if an critical impact occurs

Are the lines of responsibility clearly defined within the organization?

Who takes the decision on accepting a risk, not going forward with mitigating activities or simply not identifying the risks initially?

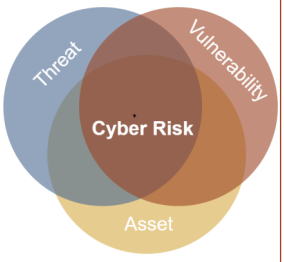
By utilizing risk based data driven decision making the responsibility can be diverted from individuals into a governance based framework. This supports both upper management but more importantly the managers with the day-to-day operation responsibility of key assets by providing transparency on identified issues throughout the hierarchy of the organization.

Nordic CRM

Enterprise Cyber Risk Management

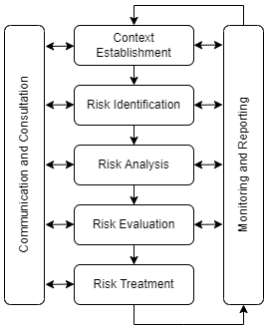
Cyber Risk

With contrast to classics Risk definitions a cyber risk is comprised by 3 factors: Threat, Asset and Vulnerability



ISO 31000

Process steps defined within the standard



Quantitative Risk

Allows for simulating Mutual Exclusion of risk that shares an attack map, incorporating elements like cyber insurance and financial caps

Attack Distribution

Financial impact distribution based on Risk attack type cluster

Nordic Cyber Risk Management bridges the highly matured and developed Quantitative Risk Management from the Engineering, Procurement and Construction (EPC) discipline unto the IT domain of Information Security.

The classics Risk Management is extended to be actor centric covering the full content of an Cyber Risk. Utilizing the foundational principles from FAIR extended with best practices from EPC Risk Management.

Engagement model

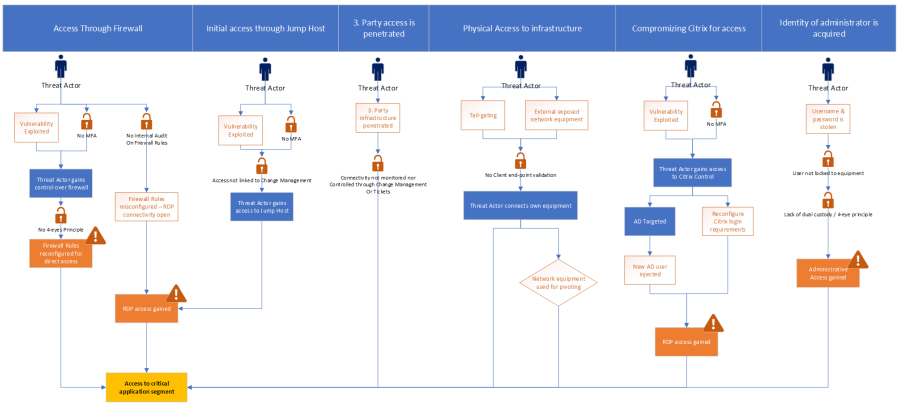
The service that Nordic CRM provides for an organization is a Cyber Risk Management framework that helps identify and evaluate the organizations top financial cyber risks. This is accomplished through an Engagement Model that adheres to the Risk Management principles defined in ISO 31000 to support the multitude of different Risk Management process within the company.

The process is initiated within the revenue generating business units and all data related to and identified within this process is owned by the individual business units. This enable the business units to give full disclosure of known issues and weak spots without being penalized during the process.

Data collections are managed through workshops aiming at answering:

Identifying Risk— discovery and documentation of key risk and their associated financial impacts. The property of doing Quantitative Risk evaluation supports aggregation of risk across business units with a shared communicative measurement.

Attack Vectors and Attack Maps— that justifies the risks are created together with the business illustrating missing controls in processes and systems. This supports the calculation of expected penetration times evaluating threat actors capabilities against the organization internal defense mechanism.



Threat Intelligence—based on the organizations existing threat landscape combined with Nordic RCM threat gathering and analysis process an statistically arrival frequency is calculated. The analysis is done evaluating clusters of threat actors against clusters of attack categories.

Quantitative Risk Model

The Nordic CRM model is based on cumulative risk distributions utilizing industry standard Palisade @Risk Monte Carlo simulation capabilities.

The model incorporate all the elements from the Engagement Model and provides a Cyber Risk Exposure that the organization is facing. The insight into the Top Financial Cyber Risk and the Cyber Risk Exposure enables management to evaluate if the identified risks scenarios are acceptable or not, producing a quantitative defined Risk Appetite baseline.

The output provides insight into the Risk Exposure based on key input parameters, like Attack Distribution based on the clustering of Risk, Financial accounts or threat actor

Nordic
CRM

Risk based decision making

From the Engagement Model and the simulated output a comprehensive report is produced that forms the finalization of the ISO 31000 Risk Evaluation phase.

The combination of visibility into the identified top financial Cyber Risks and associated vulnerabilities, attack maps and threat mapping supports the decision and prioritization moving forward for the organization.

At this point Nordic CRM has concluded the core service—providing insight and clear picture of an organization Risk Exposure and Risk Appetite.

Based on the Risk Appetite the organization may choose to accept current state and no further actions are endorsed and the engagement is concluded.

Governance and follow-up

If the organization decides to decrease the Cyber Risk Exposure the creation of a Treatment Plan is core for moving forward.

Nordic CRM supports setting up the required governance structure within the organization, either taking responsibility for execution or training and handover to relevant resources.

About Nordic Cyber Risk Management

Nordic CRM is a company founded with the vision of supporting organizations making risk based decisions in a rapid volatile cyber environment interconnected by the ever-growing Internet.

With yeas of experience within the highly matured Engineering, Procurement and Construction business Nordic CRM brings a mature approach for Risk Management into the immersive industry of Corporate Information Security.

Nordic CRM provides a maturity boost into the Cyber Risk Management discipline that are currently being defined within the less mature IT Domain.

Contact us at

Email: contact@ncrm.dk or visit ncrm.dk