IDC Analyst Perspective

Sponsored by: **IBM Nordic**

Author: Jan Horsager,
Research Director, IDC
Nordic

Cyber Resiliency: A Recipe for Digital Trust?

September 2018

You can almost hear business people holding their breaths and imagine them crossing their fingers whenever the talk turns to IT risks. Add continuity or the organization's ability to get not only IT but all business back on track after an incident, and the tension ratchets up even higher.

In boardrooms and CxO suites all over the world, there is a very clear understanding of the need for action on risk, security, and continuity. According to the findings of an IDC survey on digital transformation in Europe, 89% of organizations have digital transformation as a business priority. That is huge, and with this comes risk. But how can you mitigate IT, security, and continuity risks — quickly and all at the same time? Will this have a negative impact on the expected benefits that digital transformation is supposed to deliver to your company?

IDC's global security experts highlight a trend in which we are moving from IT security to digital trust. In this Analyst Perspective, we explore IBM's concept of cyber resiliency from a Nordic perspective but in a global context — and whether cyber resiliency is a recipe for digital trust.

Digital Trust and the Threat Landscape

Moving from IT security to digital trust means moving away from the concept of making your IT — hardware, software, and services — 100% secure. It means establishing trust around your digital solutions and services, and ensuring that the entire organization is doing everything it can to keep data safe, protect digital services, and constantly be able to restore and get the business back on track in the event of an attack.

How can you mitigate IT, security, and continuity risks — quickly and all at the same time?

Every January, before the world's top leaders meet in Davos for the World Economic Forum, the organization publishes its Global Risk Report. The report lists all serious global risks in a classical two-by-two grid, and then plots the risks according to their likelihood of happening (on the x-axis) and their impact (on the y-axis). In the 2018 edition, cyberattacks were in the upper right corner, behind only natural disasters and extreme weather events.

Cyberattacks and data breaches really emerged as a boardroom issue in 2017, in the wake of the WannaCry, Petya, and NotPetya attacks. In the Nordics, the threats became very real after Maersk, a global leader in shipping and one of the largest Nordic enterprises, was hit by NotPetya. IT systems were locked by ransomware for days, and ended up costing the organization between €174 million and €254 million.

In IDC Nordic's *Next-Generation Security Survey 2017*, 45% of organizations said they have experienced a security breach that negatively impacted customer relations. Safely managing customer and client data is central to building trust as a business.

The Maersk attack was an eyeopener for many executives, and the threat of the business coming to a total standstill was real. More importantly, for business leaders, the attack highlighted the importance of assessing their ability to get the business up and running and digital back on track after an attack — business continuity.

To gain digital trust, leadership must focus on:

- IT security solutions and services: investors and employees need to be reassured that the organization can tackle a constantly evolving threat landscape with the fewest possible attacks and the least possible impact on the business.
- Data management: customers and clients need to know that you respect personal data and can buy and sell data in an orderly fashion, ethically and economically.
- Business continuity: you need to show that you can bring the organization back to full digital capacity as soon as possible and restore data management immediately.

Like most digital issues, the important levers are not technology but organization and process design. The board of directors and the members of the executive suites have the responsibility to establish the foundation by executing the decisions that will make digital transformation happen.

Cyberattacks span from trespassing to terrorist attacks.

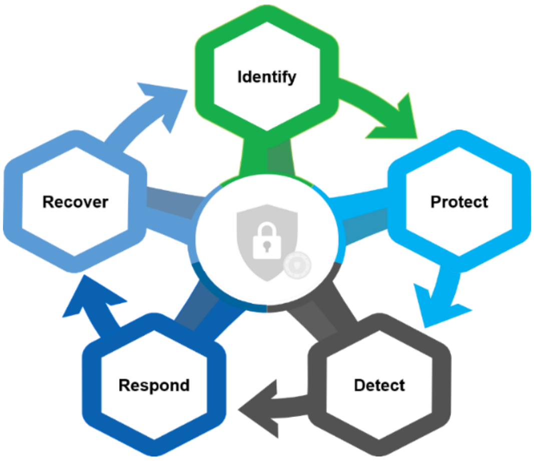
What is Cyber Resiliency?

Felicity March used to be a hacker. Now she is a cyber resiliency specialist for IBM in Europe. In between, she moved from development into selling solutions. She sees a perfect storm emerging in digital. "Cyberattacks span from trespassing to terrorist attacks," she said. "The light bulb moment is that organizations will be attacked — and what do you do then? How do you keep the store open — not necessarily with transactions but with a website that's accessible? It is different states and tasks in different situations."

IBM has introduced cyber resiliency over the past couple of years. This started as a concept with tools to prevent security incidents by protecting and detecting and responding when incidents happened, and has moved on to a framework including risk identification and recovery to normal operations.

Some of the thinking behind IBM's cyber resiliency is based on the National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity.

Figure 1
Cyber Resiliency is a Team Sport — Combining Security, Business Continuity, DR, and Networks



Source: IBM

March defines cyber resiliency as the ability of a company to maintain its core purpose and integrity in light of a cyberattack.

Cyber resiliency needs an end-to-end approach that brings together three critical areas:

- Information security
- Business continuity
- Network resilience

IBM's cyber resiliency offering includes assessments, tooling, and services covering these three areas, and at the same time explaining this in a managerial way for line-of-business leaders, CxOs, and board members. In future, March sees integrated resiliency. Automating processes plays an important role in this future integration — especially the fail-over elements that enable existing services to continue from another location, versions of software, and so on.

> *"You need to train. Firemen do drills most of the time, and the resiliency blueprint is like the fire escape plan."*

"Then you need to train," March says. "Firemen do drills most of the time, and the resiliency blueprint is like the fire escape plan."

Cyber Resiliency at Work

A retail company wanted IBM to test the security of its branches and see if it could hack them and gain access to the datacenter and sensitive data. IBM quickly showed that it could compromise the branch WiFi and take control of the POS systems. From there it could gain access to the datacenter, including the details of over 5 million credit card transactions, all unencrypted. The benefit for the customer was in identifying its vulnerabilities and pinpointing the data that could be accessed.

In June 2017, a global consumer goods company was the victim of an attack that rendered inoperable all its internally delivered IT services that were reliant on Microsoft operating systems, including its disaster recovery (DR) solution. All business ceased, globally. Crisis and continuity management was challenging, exacerbated by loss of communications and contact information. DR took weeks instead of hours and the business impact ran to tens of millions of euros, not including the impact on the share price.

IBM assessed the client's response to the cyberattack and reviewed the existing DR remediation project to identify issues and make recommendations. IBM then developed a crisis and continuity framework and plans, and provided a road map for implementation.

For the past decade, in IDC Nordic surveys, IT security has ranked first or second in terms of the most important IT priorities.

On June 27, 2017, worldwide operations at a global transportation conglomerate were hit by the NotPetya cyberattack. The malware infection started midmorning, infecting the client's businesses globally in the first hour, and spread exponentially in a couple of hours. In three hours, more than 6,000 Windows servers and more than 50,000 workstations were infected. AD and DNS servers were destroyed, impacting all global business applications and halting all global shipping operations.

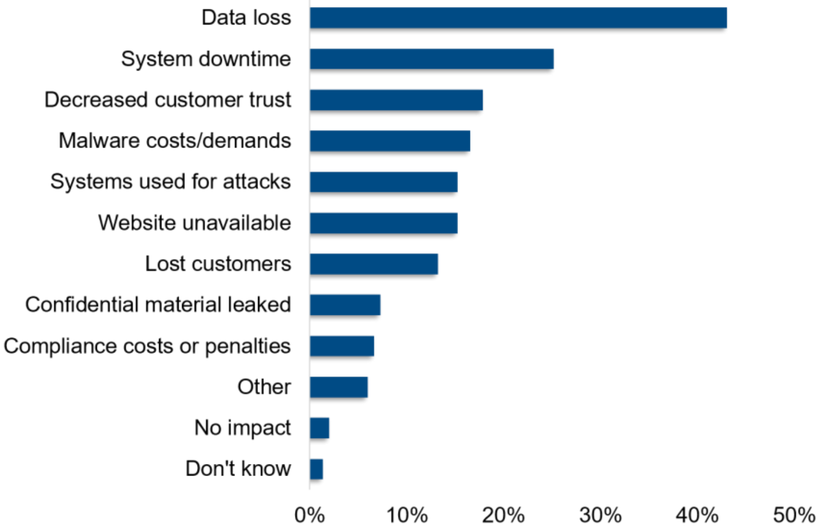
IBM used its X-Force IRIS cyber incident response resources to tackle the issue. The IRIS team deployed tools to assess the extent of the breach, and worked with the client on restoration activities. Within three days, 95% of business functionality was restored, 100% of the Linux/AIX server estate was online and available, 84% of Production Windows servers were restored, and over 180 applications were restored. IBM Security Services was awarded a $9 million, 51-month contract for managed endpoint detection and response services, to detect future malicious activity and prevent propagation.

Nordic Leaders' Experiences With IT Security

The World Economic Forum's Networked Readiness Index and the European Union's Digital Economic and Society Index rank Nordic countries at the top in terms of digital readiness and IT use. Although there are very different business structures in Denmark, Finland, Norway, and Sweden, the similarities in the region have made the Nordics a testbed for advanced technology use.

According to IDC Nordic surveys, IT security has consistently ranked number 1 or 2 in most important IT priorities. The number of security breaches, however, has grown and the impact has worsened. IDC Nordic's *Next-Generation Security Survey 2017* showed that local organizations typically experience a breach every six months, while 7% of organizations said they have had more than 10 breaches in the past two years.

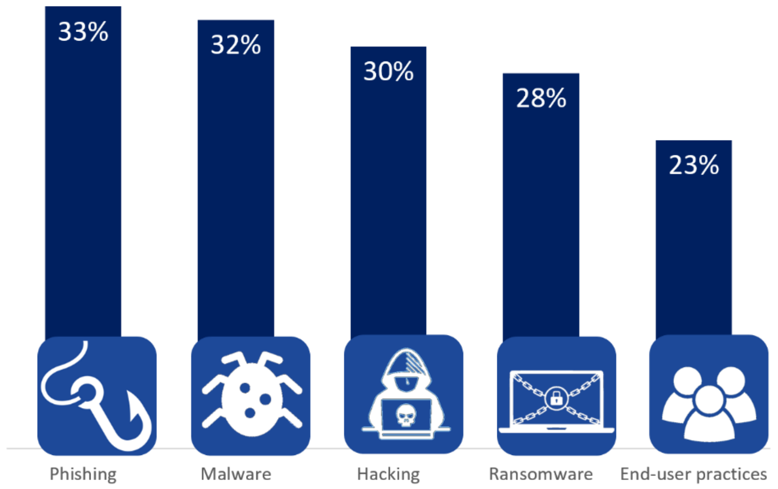
Figure 2
The Business Impact of Security Breaches



Source: IDC Nordic, *Next-Generation Security Survey*, 2017 (n = 202)

The biggest threat experienced by Nordic organizations is phishing. This reminds us that the human factor is still very important when it comes to establishing trust and resiliency around digital transformation, even when most of the attention is focused on threats like malware, hacking, and ransomware.

Figure 3
Top 5 Most Dangerous Security Threats to Nordic Organizations



Source: IDC Nordic, *Next-Generation Security Survey*, 2017 (n = 202)

Key Takeaways

IT security has been an important IT priority for years in the Nordics. Because of the growing and ever-changing threat landscape, IT security and business continuity after an incident should be permanently on the agenda of boards and C-level management.

All organizations need to create digital trust to stay relevant. The cyber resiliency framework from IBM enables IT professionals to work with security in full, from risk management and prevention, to detection and responding to attacks, and to the recovery of operations.

It is a recipe for trust, but one that is only as good as the way it is executed. Although the framework is complex, seasoned leaders will have the business acumen to understand it. Trust and resiliency are still very much about people, even when a large part of the underlying processes are automated.

The human factor is still very important when it comes to establishing trust and resiliency around digital transformation.

Recommended Actions

Start by considering what will happen when your organization is attacked. What will you do then?

Get IT security and business continuity onto your corporate agenda, as this will instill some urgency to take the actions needed to build trust and resiliency.

Involve all parts of the organization to create a digital trust network in your organization — one that will lead by example.

IDC Nordic

Bredgade 23A, 3.
DK-1260 Copenhagen K

www nordic.idc.com

company/idc-nordic

@IDCNordic

IDCNordic

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.