Deloitte.

Circular economy driver strengthens resiliency after successfully repelling a cyberattack

Rapid threat response provides path to a broader transformation

Energy, Resources & Industrials	Incident Response
Industry	Service

Cyber Stories

The starting point

The circular economy is growing, enabled by companies such as TOMRA. Founded in Norway in 1972, the organization has steadily grown worldwide as an industry leader that is helping to shape the future of the planet while continuing to innovate on the digital front – offering collection, sorting, and other sustainability-focused solutions to clients in industries such as mining and food production.

But as TOMRA's global profile and digital capabilities have grown, so have the potential cyber risks. One recent summer, those risks came into sharp focus after the company endured a cyberattack. The event forced TOMRA to proactively shut down services and disconnect sites to contain the attack, while shifting to manual workarounds to seamlessly continue operations as the company determined its next steps.

More than responding to the attack, company leaders understood that they needed to go a step beyond. They needed to plan for the evolution of the business and the cyber landscape—and become a more resilient, cyber-ready organization.

Factors in focus

- ✓ Growing digital business processes across the organization, including operations in 100+ countries
- ✓ A cyberattack that forced the company to pursue manual workarounds
- ✓ The need for long-term cyber readiness, response, and recovery capabilities

The way forward

The threat actor had infiltrated TOMRA's systems, installed a backdoor, and then moved across the company's cloud and on-premises systems possibly preparing for a ransomware attack. TOMRA specialists swiftly identified the incident and contained the attacker—isolating affected systems, limiting the attack's impact, and protecting the company's data. But what should happen next?

To ensure that the threat had been thoroughly eradicated, to reduce additional risks, and to position the company for long-term cyber success, TOMRA leaders enlisted the help of Deloitte. Leveraging Deloitte's Cyber Incident Readiness, Response, and Recovery (CIR3) services, TOMRA was able to address a broad array of needs, helping the company become more resilient across its business.

Building on TOMRA's initial response, Deloitte collaborated with the company to create joint teams that included Deloitte forensics and legal professionals, as well as technical architects and other specialists. An initial technical investigation team began work at six locations in five countries, focused on understanding how the attack had happened and taking steps to fully remediate it.

Joint teams also established processes for engaging with TOMRA customers, vendors, and others—focused on providing timely, transparent and relevant communication, and bolstering trust among stakeholders.

Insights to inspire

Keep communicating with customers. Proactively and regularly informing stakeholders about your response to a cyber incident can increase levels of trust and generate valuable feedback for your cyber strategy.

Rebuild for the future. A cyber incident is not simply a problem to fix. It can be an opportunity to transform your digital environment, reimagine your business processes, and create a more resilient organization from end to end.

At the same time, teams were working together to rebuild TOMRA’s landscape of IT and digital business processes to create a new minimum viable company that could securely continue operations for the company’s most important processes. Within 60 days, TOMRA and Deloitte created a new technology landscape for multiple critical business processes, restoring operations that included new cyber tools and controls for improving security and resilience.

To help TOMRA recover from the initial cyberattack—and develop a more comprehensive approach to cyber readiness—Deloitte brought in professionals across its global network to do the hands-on work as well as strategic planning.

The ongoing cyber transformation for TOMRA has helped put the company on a more solid foundation. In addition to reducing systems complexity and increasing security for cloud,

TOMRA’s journey has given leaders greater visibility into the company’s digitally enabled processes, provided processes and tools to prevent and handle cyberattacks, increased cyber awareness, created a more resilient organization, and bolstered customer trust.

The journey will continue, improving cyber security posture and making TOMRA excel and be able handle future cyber threats.

The achievements

Reduced complexity and increased visibility across digital business processes

Improved security tools, controls, and awareness—enabling greater readiness and resilience to prevent and handle cyber incidents

Elevated trust among customers, vendors, and other stakeholders

New capabilities and architecture for supporting a Zero Trust journey

Let’s talk cyber

What will your organization do when the next cyberattack happens? How will you rapidly respond to and recover from an incident—while building trust in your business?

Discover how Deloitte’s Cyber Incident Readiness, Response, and Recovery (CIR3) services can help your organization face the future with greater strength and resilience. Contact us to get the conversation started.

www.deloitte.com/cir3
www.deloitte.com/cyber

Deloitte.

Contacts

Bjorn Jonassen
Partner, Risk Advisory
Deloitte AS
bjojonassen@deloitte.no

John Gelinne
Global Cyber Incident Readiness, Response, and Recovery Leader
Managing Director
Deloitte & Touche LLP
jgelinne@deloitte.com

Kevvie Fowler
Global Cyber Incident Response Leader
Partner
Deloitte Canada
kfowler@deloitte.ca

About Deloitte
Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms, and their related entities (collectively, the “Deloitte organization”). DTTL (also referred to as “Deloitte Global”) and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see http://www.deloitte.com/about to learn more.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms or their related entities (collectively, the “Deloitte organization”) is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and Independent entities.

Copyright © 2024 Deloitte Development LLC. All rights reserved.