Cyber security for digital factories
Risk Advisory Deloitte
A new world of challenges and opportunities awaits us

The digital revolution is fundamentally changing the industrial landscape. More computing power, high-speed internet connectivity, the proliferation of "smart" devices, robotics, artificial intelligence and data analytics are transforming the operational technologies (OT) used by businesses, a transition that is often referred to as the fourth industrial revolution.

This revolution in OT and the digitalisation of industry control systems (ICS) is turning manufacturing enterprises into “digital factories”. It is providing them with a plethora of benefits – including shorter order fulfilment cycles, more sustainable production processes, higher product quality and lower costs.

However, these advances come with new challenges. The rapidly changing OT landscape poses a major cyber security concern for manufacturers. Many are now confronted with the reality of vulnerable legacy systems, putting them at greater risk of increasingly sophisticated and large-scale cyber attacks.

Furthermore, the OT ecosystem is expanding to include more third-party vendors and managed services providers, resulting in a larger attack surface because of the wider digital environment exposed to potential hackers.

The effort spent in running and protecting OT assets in today’s riskier security environment is holding many companies back from becoming front-runners in innovation, potentially leading to missed business opportunities.

To manage these risks while taking full advantage of the benefits of digital factories, adopting digital and organisational security measures is of paramount importance. As we embark on the fourth industrial revolution, a robust cyber security strategy will protect companies and allow them to pursue their business objectives.

Dana Spătaru
Partner
Digital is the new normal

Trends and developments

Growing number of connected devices
The number of OT systems connected to the internet has grown exponentially over the last decade.

Integrated OT and IT
Manufacturing companies can no longer afford to keep OT and IT separate due to the increase in data, connectivity, complexity and costs.

A plethora of business opportunities and solutions
Companies can now choose from a wide variety of technical solutions, hardware, software and communication protocols.

Expanding ecosystem of OT actors
A growing number of organisations are entering the OT ecosystem, including technology vendors, security providers and other third parties.

Adapted from: Top Trends in the Gartner Hype Cycle for Emerging Technologies, Gartner, 2018

Time to mainstream adoption:
- < 2 years
- 2 - 5 years
- 5 - 10 years
- > 10 years
Digital is the new normal

The concept of digital factories
Challenges for leadership
Protecting a digital factory
A typical transformation roadmap
Learning from others
OT security at Deloitte
Contact
The concept of digital factories

Merging physical and digital technologies, opening the doors to new business opportunities.

Manufacturing is on the brink of an extensive transformation as we enter the fourth industrial revolution. New and emerging technological trends, enabled by connected OT, are turning traditional factories into digital factories.

Digital factories can facilitate the technological transformation of manufacturing processes, a transition in which advanced production and operational techniques meet smart digital technologies. Companies now have to decide where and how to invest, which technologies better fit their needs and what opportunities to pursue. For example, a company might consider changing the way it works, improving safety, creating more sustainable production methods, instilling shorter product lifecycles and looking at options for setting up new revenue streams.

The result? An even broader concept, the “digital enterprise”, an enterprise that is interconnected, autonomous and has the power to analyse, communicate and use data to drive actions back to the physical world. Manufacturing processes in smart factories will embed connected technologies into their processes, people and assets, powered by breakthroughs in fields such as robotics, data analytics, artificial intelligence, additive manufacturing (3D printing) and digital twins (virtual models of a process or service).

Without a clear understanding of the changes and of the opportunities digital factories bring, companies risk losing ground.
Introduction

Digital is the new normal

The concept of digital factories

Challenges for leadership

Protecting a digital factory

A typical transformation roadmap

Learning from others

OT security at Deloitte

Contact
Challenges for leadership

Technological developments – including increased computing power, fast internet, artificial intelligence, digital twins and augmented reality – are accelerating digitalisation processes in factories. This brings numerous advantages to manufacturers, including shorter production times, a more sustainable production process, decreased manufacturing costs and decreased factory downtime.

However, in order to keep up with all these new developments, business leaders should pay close attention to managing cyber security risks in the OT domain – focusing on addressing a range of challenges relating to people, process and technology.

<table>
<thead>
<tr>
<th>Challenge</th>
<th>Deloitte’s approach</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Process</strong></td>
<td></td>
</tr>
<tr>
<td>Companies do not have an integrated approach to OT security. OT security is different from IT security; it follows different processes and requires different risk management.</td>
<td>We understand, rationalise and help execute the different processes to achieve a solid, unified view on security risks.</td>
</tr>
<tr>
<td>Security processes are technology oriented, rather than aligned with the business.</td>
<td>We operate with a business centric approach, in which business risks are translated to security risks, both technical and non-technical.</td>
</tr>
<tr>
<td><strong>People</strong></td>
<td></td>
</tr>
<tr>
<td>OT and IT staff do not always share perspectives or approaches and sometimes they follow different directions.</td>
<td>We bring together people and find a common ground to enable in-house relationships and sustainable cooperation.</td>
</tr>
<tr>
<td>OT security staff will eventually leave or retire, potentially leaving the company poorly protected in some critical areas.</td>
<td>We promote knowledge transfer and ensure continuity, supplementing the areas in which there may be a gap with professional services until stability is reached.</td>
</tr>
<tr>
<td><strong>Technology</strong></td>
<td></td>
</tr>
<tr>
<td>Companies have difficulties implementing effective security, as technology solutions are still relatively immature in the cyber area.</td>
<td>We act as an orchestrator and help identify suitable solutions, and where needed, advise on alternative controls.</td>
</tr>
<tr>
<td>As technologies are changing fast, companies struggle to keep up-to-date and design appropriate technical solutions.</td>
<td>We help companies remain up to speed in swiftly changing environments.</td>
</tr>
</tbody>
</table>

Additional external challenges include, evolving threat landscape, remaining transparent, accountable and responsive; and increasing regulatory pressure.
Introduction

Digital is the new normal

The concept of digital factories

Challenges for leadership

Protecting a digital factory

A typical transformation roadmap

Learning from others

OT security at Deloitte

Contact
Protecting a digital factory

As more devices are connected to the internet, organisations are exposed to more cyber risks

<table>
<thead>
<tr>
<th>Top challenges facing digital factories</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>The ever-increasing attack surface</strong></td>
</tr>
</tbody>
</table>
| • Increase in the number and complexity of automation system, tools, as well as communication channels in the OT landscape.  
  • Emergence of communication channels for monitoring between previously independent objects.  
  • Expanded opportunities for criminals to plan and execute attacks. |
| **The growing interest of cyber criminals in industrial enterprise** |
| • Cyber criminals are finding it harder and less profitable to attack many traditional IT targets which is pushing them to search for new targets in OT.  
  • There has been a growth in the number of espionage and terrorist attacks on industrial enterprises. |
| **The underestimation of general threat levels** |
| • A lack of access to information about security threats means that many industrial companies underestimate the problem. |
| **The misunderstanding of specific threats and a poor choice of protection options** |
| • In industrial cyber security, companies often lack sufficient understanding of the OT threats and are misled by high profile incidents reported by the media.  
  • Security software is often based on artificial scenarios than on real life and may therefore not work as expected during a real incident. |
To address cyber security challenges in OT environments an end-to-end security transformation programme is required. No two companies are alike and therefore no silver bullet exists to address your security concerns. The goal is to develop the capabilities required to reach a mature state of security, a state in which cyber security is aligned with business objectives and adds real value to your daily operations. A transformation programme and the implementation of solutions should be based on industry practices in areas such as corporate governance, network architecture, security monitoring, regulatory readiness, incident response and forensics.

Protecting a digital factory

Threat landscape on OT malicious objects

![Evolving threat landscape](source: Kaspersky Lab - ICS-CERT, Threat landscape for industrial automation systems: H1 2018, 2018)

![OT security annual spend forecast](source: Gartner, Competitive Landscape: Operational Technology Security, 2018)
A typical transformation roadmap

**Current and target state for OT security defined**
Risk management and compliance capabilities are established, including the evaluation of OT risk and identification of procedures to minimise it.

**Deloitte services:**
- Security assessment
- TIBER (Threat Intelligence-based Ethical Red Teaming)
- Compromise assessment
- Vulnerability assessment and penetration testing

**OT asset inventory, security training and incident response**
Inventory of OT assets is made continuously available, and vulnerability management is in place. An incident response plan is implemented. OT security trainings are also kicked off in this phase.

**Deloitte services:**
- GICSP (Global Industrial Cyber Security Professional) exam preparation
- Vulnerability management
- Incident response

**TOM Governance & Roadmap**
OT security governance and operations architecture are designed according to the defined target state. The implementation of the security capabilities is prioritised into a roadmap.

**Deloitte services:**
- OT TOM
- OT Roadmap
- OT Governance establishment

1 of 2 pages
Introduction

Digital is the new normal

The concept of digital factories

Challenges for leadership

Protecting a digital factory

A typical transformation roadmap

Learning from others

OT security at Deloitte

Contact
Learning from others
Cyber transformation: In a snapshot

Holistic solution to face challenges today and tomorrow

**Situation:**
A large Dutch multinational company producing health, nutrition and other products in more than 100 production sites worldwide needed to improve the security of its industrial control systems.

**Approach:**
Given the complexity of the assignment and the variety of stakeholders, Deloitte created a security programme for the company that was divided into four attainable work streams, amalgamating the following compliance-based and risk-based approaches:

- **Industrial cyber security services:** workshops and discussions were set up to align views on the threat landscape, risk appetite and how the risks should be managed.
- **Standards and practices:** standards and guidelines were written for all relevant OT-related topics and supporting tools for all production sites across the globe.
- **Training:** a training curriculum was created for both ordinary OT users and OT security personnel.
- **Site assessments:** a site assessment approach was created to test the security of the company's OT systems.

**Value:**
The use of technology accelerators and a multi-disciplinary team containing change management, programme management, cyber strategy and OT cyber security professionals meant the company was able to implement effective cyber security controls across the globe.
Learning from others
Cyber transformation: In a snapshot

Our cyber security transformation programmes typically combines a variety of activities, including:

- **Incident Response**
  Combination of team and tools to handle incidents and get back to business-as-usual.

- **Security & Awareness Training**
  A comprehensive curriculum to train your team.

- **In-depth Security Assessment**
  Methodology and team to understand your OT environments inside-out.

- **TIBER**
  Threat Intelligence-Based Ethical Red-teaming (TIBER) for OT environments.
Handling incidents rapidly and with the correct approach is an important part of getting back to business-as-usual. This case study of an international corporation explains how an appropriate and immediate response to a worldwide OT security incident had a positive outcome. We take care of all aspects of incident handling – including business continuity, investigations, corporate communications, legal and technical matters. Our approach is based on industry best practices and many years’ experience dealing with global incidents for clients.

**Client situation:** An international transport company with offices in 130 countries and around 88,000 employees contacted us for help after a virus had infiltrated its networks and systems and disrupted its global operations.

**Approach:** The challenge was immense, requiring a variety of competencies and services. We used a global response team covering cyber security, forensics and crisis management to handle the incident. This team of 130-plus from across Europe came together as “One Deloitte”, working around the clock to get the organisation back up and running. We worked closely with the client’s staff, joining forces as one team operating together, enabling us to take responsibility and rectify the situation.

Working in 24/7 shifts we rebuilt the client’s entire IT organisation in five weeks, including 65,000 laptop builds and a company-wide operating system upgrade. We also restarted its OT operations in nine days. While we restored systems, our international Deloitte colleagues reverse-engineered the virus and provided security intelligence, giving an insight into what could be done to stop the virus spreading.

**Value:** Our intervention played a critical part in protecting the client from bankruptcy. Our support helped restore its business operations and ensured its network was safeguarded against similar malware attacks in future.

Achieving a good knowledge of OT environments is harder than it looks. We can gain an insight into the cyber security position of a company’s manufacturing sites where IT and OT domains interact. Our assessments cover the full width of the OT cyber security spectrum, following industry-recognised standards, and covering topics such as governance, risk management, network architecture, identity management, incident response and forensics.

**Client situation:** A global manufacturing company with numerous production locations across the world asked Deloitte to assess its overall OT security posture.

**Approach:** We carried out assessments in six locations with a team of local and international specialists, specifically geared towards the different environments. Our approach – a combination of interviews, active testing, documentation assessments and questionnaires, covering the whole spectrum of OT security controls – involved an efficient and fruitful interaction with the client’s local teams.

**Value:** The multi-disciplinary, international team from Deloitte brought a fresh perspective that resounded well with both the client’s management team as well as the production locations’ personnel. Our insights and recommendations were valued by the client who described them as “great input for the cyber resilience improvement plan”.

Incident Response

In-depth Security Assessment
Skilled people form the backbone of a company’s security. Our training covers the whole range of OT cyber security topics – from deep technical topics, such as PLC (programmable logic controllers) testing, infrastructure testing and hardware hacking, to high level strategic risk management. In addition to preparatory courses for professional certifications, we can also develop a bespoke curriculum with clients, focused on their specific training needs.

**Client story:** We were approached by a company that wanted to build a network of internal OT cyber security experts.

**Approach:** By using our database of training material alongside client-specific materials we had collected, we set up and implemented a training programme that provided both general technical knowledge on OT security and client-specific content on recommendations that needed to be implemented in factories.

**Value:** As a result of training these experts, the company was able to further roll out and implement their worldwide OT cyber security programme. We ensure not only that our clients have skilled people in their security team, but also that they can create a domino effect of “training the trainer” to scale up and rapidly improve the entire organisation’s security position.

The European framework for Threat Intelligence-Based Ethical Red-teaming (TIBER) enables companies to make effective, real-time decisions about the security risks it faces. It combines red-teaming, OT knowledge and cyber threat intelligence to emulate the tactics, techniques and procedures of threat actors that are most likely to target a particular organisation. This enables companies to make effective, real-time decisions about cyber security risks.

**Client story:** A global chemical company asked Deloitte to test its core operations network, which included IT, OT and an “in-house bank” as part of the critical assets. The client had taken various security measures in recent years, but wanted to understand how resistant the in-house bank would be to a targeted cyber attack.

**Approach:** Together with the company, and based on the latest threat intelligence it faced, we used the TIBER framework to develop and execute a small set of holistic cyber attack scenarios. These scenarios included physical, human and cyber elements. The engagement highlighted the strengths and weaknesses of the in-house bank’s security posture and led to key recommendations on improvements that should be made.

**Value:** We helped the client implement appropriate controls to protect its high-risk assets. We made additional improvement suggestions regarding IT security, monitoring and incident response, while also highlighting the strong controls already in place.
OT security at Deloitte
Our practice

Accredited in the following technical certifications: GICSP, CISSP, CISM, GSCP, ITIL, CEPP, CEH, and more.

Continuous investment in cyber innovation.

Our organisational certifications include: ISO27001, ISO22301, PCI, SOC 2 Type II.

Extensive set of best practices, use cases, and client references across all industries.

Global alliances with multiple cyber technology vendors.

End-to-end cyber risk services across the four main cybersecurity domains: Cyber Strategy | Secure | Vigilant | Resilient.

Regions Professionals
North America > 4,500
EMEA > 2,000
Asia Pacific > 2,500
Rest of the World > 1,500

Our practice

Contact
Introduction

Digital is the new normal

The concept of digital factories

Challenges for leadership

Protecting a digital factory

A typical transformation roadmap

Learning from others

OT security at Deloitte

Contact
Introduction
Digital is the new normal
The concept of digital factories
Challenges for leadership
Protecting a digital factory
A typical transformation roadmap
Learning from others
OT security at Deloitte

Contact
Dana Spătaru
Partner
dspataru@deloitte.nl
+31 88 288 66 23