Deloitte.

The future of consumer sector

Cyber everywhere. Go anywhere.

2020

Introduction

Technologies will drive a myriad of business operations and processes in the manufacturing and retail industry. The accelerated pace of technological innovation will also prompt many trends that may prove consequential in keeping businesses agile and sustainable. Smart technologies will help build smarter homes, with engaging products for consumers. Different Industrial Control Systems (ICS) will utilise the latest technologies to control high-risk manufacturing processes. Consumer product companies are continuously developing proprietary technology to drive innovation and growth. Furthermore, manufacturers and retailers will also technologically invest in their products, manufacturing processes and industrial ecosystem relationships so that they can compete in a changing global marketplace.

Key trends

Artificial Intelligence (AI)/ Machine Learning (ML)

As the volume of data increases, so will the necessity to extract measurable insights from the available data. This is where AI and ML will help the manufacturing and consumer-goods sector to establish an infrastructure that drives greater efficiency, faster response-time and also help in creating new business opportunities. AI can be used to provide a seamless customer journey by curating personalised experiences and simplifying the shopping process. In the manufacturing sector, AI can provide insight into bottlenecks and pain-points by using predictive analytics. A supervisor would be able to have a work-flow view of the plant in real-time and need not physically supervise the entire manufacturing floor.

Workforce of the future

While digitisation is changing the manufacturing and consumer goods landscape, it is also important for the organisation to see how they employ talent who can stay abreast of the fast-paced digital transformations happening in the industry. Therefore, the role of cyber-security professionals will also change, not just in scope, but also in scale.

Internet of Things (IoT) expansion

Manufacturers are increasingly adopting the use of IoT to empower making strategic and informed decisions. In a recent study , 63 percent of participants from the manufacturing industry, believed that IoT will have a significant impact on the future. IoT expansion helps achieve three key goals: improved safety, increased efficiency and cost reduction, and assists with garnering real-time, crucial data for product maintenance and innovation. IoT will also be of immense use to the consumer sector; an apt example here is household electronic appliances, which could be connected with the help of centrally-enabled electronic personal assistants such as Amazon Echo, Google Home, etc. With the roll-out of 5G close at hand, there will be reduced latency, so a vast array of devices could be controlled remotely.

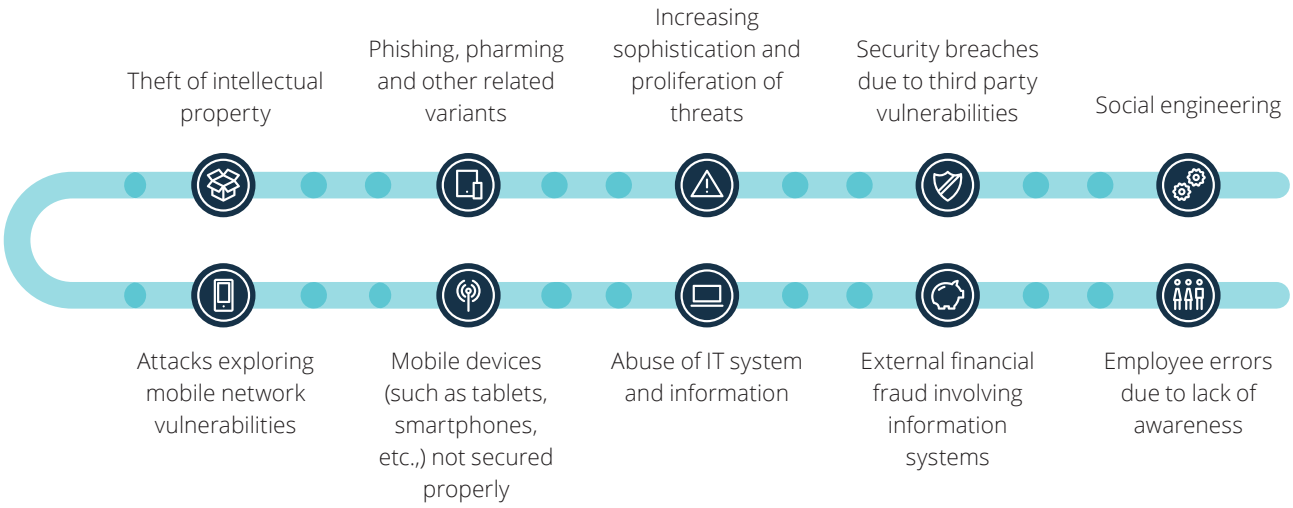
New patterns of personal consumption

With a large amount of data available at your fingertips, consumers are always looking for the next best thing in the market. This calls for continuous innovation and research and development (R&D) to be undertaken by the organisations, to ensure they remain on top of the sustainability graph. Technologies like big data and predictive analytics are being used by companies to sift through and analyse information faster, helping build personalisation at a large scale, to cater to the growing demand for better customer experiences.

Threat landscape

The existing technology footprint, along with expected changes in the digital ecosystem, will have a considerable impact on the entailing cyber risk exposure in the future.

In a report by International Data Corporation (IDC), the number of connected IoT devices is said to increase to 41.6 billion by 2025, which would generate 79.4 zettabytes of data.



Our solutions

The retail and manufacturing industries will need to bank heavily on the value addition that emerging technologies will bring; while, at the same time, they must work towards increasing their cyber security posture, should a cyber-breach occur. They should remain secure, vigilant and resilient. We, at Deloitte, understand the risks brought forth by digital transformations, and can help institutions secure their digital perimeter effectively, so that they can better defend themselves against such attacks. Here is a brief overview of our services:

Priority

- Security of industrial automation
- Ensuring availability
- Identity and access management

Priority

- Internet of Things (IoT)
- Digitalisation and industry 4.0

Sources:
https://www2.deloitte.com/us/en/pages/manufacturing/articles/cyber-risk-in-advanced-manufacturing.html
https://www2.deloitte.com/content/dam/Deloitte/fi/Documents/risk/Cyber%20Secure%20Manufacturing%20in%202021.pdf
http://mpi-group.com/wp-content/uploads/2016/01/IoT-Summary2016.pdf
https://iot.electronicsforu.com/headlines/promising-numbers-for-the-growth-of-iot-devices-by-2025/

Key contacts

Anthony Crasto
President, Risk Advisory
Deloitte India
acrasto@deloitte.com

Abhijit Katkar
Partner, Risk Advisory
Deloitte India
akatkar@deloitte.com

Kamaljit Chawla
Leader – Cyber Operate
Risk Advisory, Deloitte India
kamaljitc@deloitte.com

Tarun Kaura
Leader – Cyber Advisory
Risk Advisory, Deloitte India
tkaura@deloitte.com

Anand Tiwari
Partner, Risk Advisory
Deloitte India
anandtiwari@deloitte.com

Anand Venkatraman
Partner, Risk Advisory
Deloitte India
anandv@deloitte.com

Chintan Matalia
Partner, Risk Advisory
Deloitte India
chmatalia@deloitte.com

Deepa Seshadri
Partner, Risk Advisory
Deloitte India
deseshadri@deloitte.com

Manish Sehgal
Partner, Risk Advisory
Deloitte India
masehgal@deloitte.com

Muthukumar Karuppiah
Partner, Risk Advisory
Deloitte India
mkaruppiah@deloitte.com

Praveen Sasidharan
Partner, Risk Advisory
Deloitte India
psasidharan@deloitte.com

Vikas Garg
Partner, Risk Advisory
Deloitte India
vikasgarg@deloitte.com

Deloitte.