A RIVEW ON THE NEED OF CYBER SECURITY IN INDUSTRY

Tushar Pillai, Anup Bongirwar, Anmol Sharma, Ankit Panchbudhe

Students , Mechanical Engineering, G.H.Raisoni. Collage of Engineering, Nagpur Maharashtra

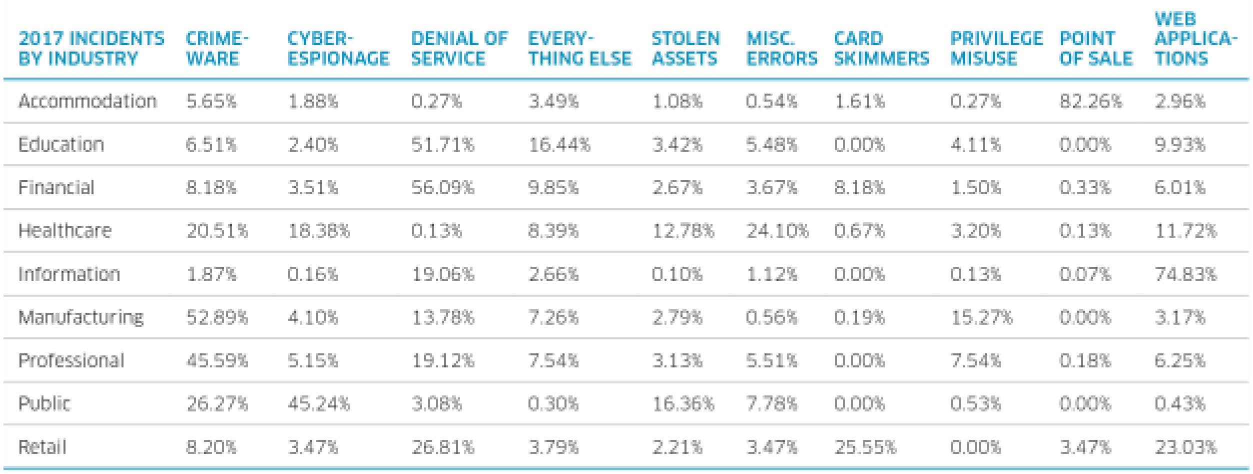
Abstract

At this era the industrial sector become the target for threats, it can be proofed by recent attacks on industries in 2015. To look for these threats, cyber security is the measure we have to take, to defend our industrial systems from the threats that are integrating industrial control processes and the industrial system with the internet produces.

Keywords: *industrial sector, threats, cyber security.*

What is Cybersecurity and Why is it Important?

Cybersecurity focuses on protecting computers, networks, programs, and data from unauthorized and/or unintended access. Cybersecurity has become increasingly important recently as governments, corporations, and people collect, process, and store vast amounts of confidential information and transmit that data across networks. Data breaches have become almost commonplace in recent years. Over the last few years, high-profile cases of cyber hacks have increased the demand for sophisticated software and security products. Companies across the globe are growing more aware of the potential threat, which is leading to a greater allocation of resources towards companies that help mitigate such risks.



2017 INCIDENTS BY INDUSTRY	CRIME-WARE	CYBER-ESPIONAGE	DENIAL OF SERVICE	EVERY-THING ELSE	STOLEN ASSETS	MISC. ERRORS	CARD SKIMMERS	PRIVILEGE MISUSE	POINT OF SALE	WEB APPLICA-TIONS
Accommodation	5.65%	1.88%	0.27%	3.49%	1.08%	0.54%	1.61%	0.27%	82.26%	2.96%
Education	6.51%	2.40%	51.71%	16.44%	3.42%	5.48%	0.00%	4.11%	0.00%	9.93%
Financial	8.18%	3.51%	56.09%	9.85%	2.67%	3.67%	8.18%	1.50%	0.33%	6.01%
Healthcare	20.51%	18.38%	0.13%	8.39%	12.78%	24.10%	0.67%	3.20%	0.13%	11.72%
Information	1.87%	0.16%	19.06%	2.66%	0.10%	1.12%	0.00%	0.13%	0.07%	74.83%
Manufacturing	52.89%	4.10%	13.78%	7.26%	2.79%	0.56%	0.19%	15.27%	0.00%	3.17%
Professional	45.59%	5.15%	19.12%	7.54%	3.13%	5.51%	0.00%	7.54%	0.18%	6.25%
Public	26.27%	45.24%	3.08%	0.30%	16.36%	7.78%	0.00%	0.53%	0.00%	0.43%
Retail	8.20%	3.47%	26.81%	3.79%	2.21%	3.47%	25.55%	0.00%	3.47%	23.03%

CYBER SECURITY IS THE BIGGEST DISRUPTOR TO THE TECH INDUSTRY:

- Cyber security was the most talked about topic in technology last year due to the announcement of a number of high profile hacks on the World Anti-Doping Agency's database (WADA).
- Due to a high proportion of cyber security risks arising through a company's own staff, there is also a requirement for companywide education on cyber security practices. A recent study by Intel Security

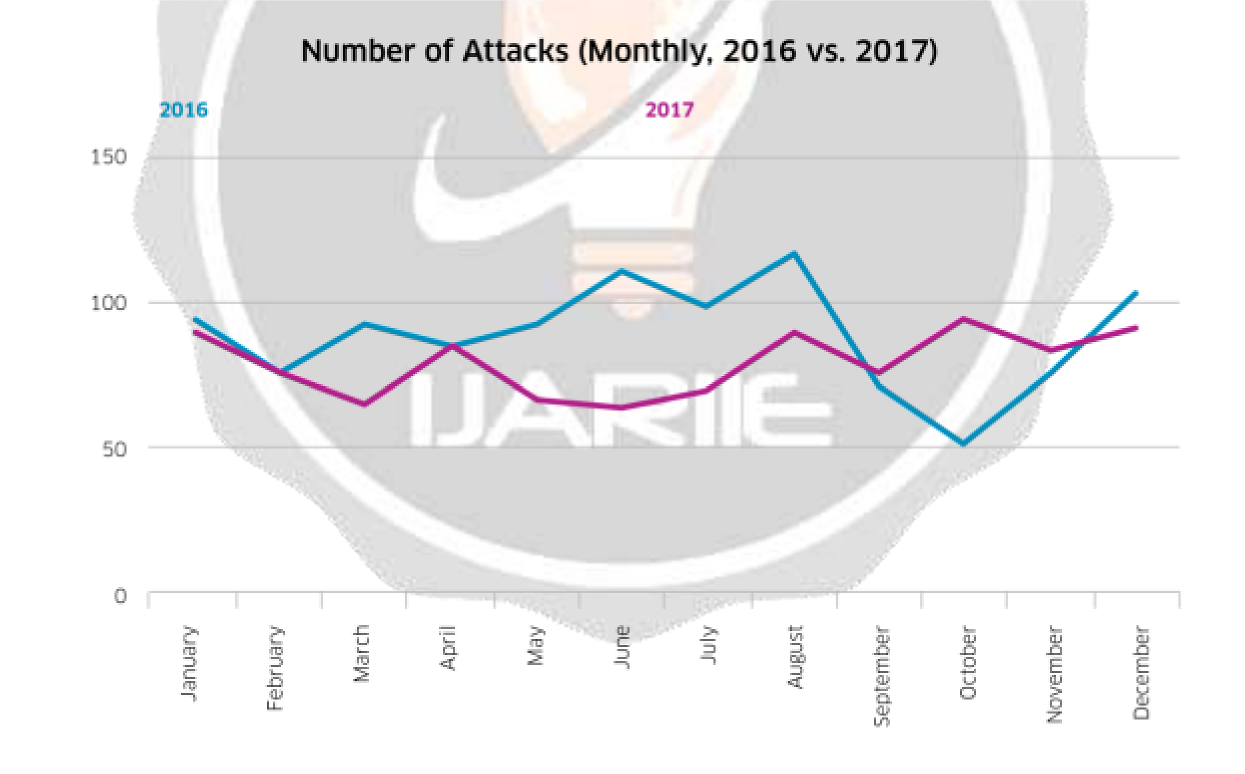
found that a large proportion (43%) of data breaches and security hacks are caused internally by employees acting irresponsibly or unwittingly meddling with the company's data and systems. This can have huge implications on the reputation of the company as their use of data is slandered on the news.

- Cyber security beat other hot technology innovations such as IoT (40%), Big Data (40%), automated technology (39%) and 5G (26%) as well as political/policy changes (42%) to take the top spot as the biggest disruptor.
- The increase in security threats caused by the Industry 4.0 technologies and its innovative services must be addressed

CYBER-SECURITY THREATS OF INDUSTRY 4.0 TECHNOLOGIES:

Massive interconnection of machines, Operators and the product itself.The main concerns are the attacks perpetrated against their availability, due to the scarcity of resources (CPU, memory or battery).

Processing of information retrieved by IIoT devices, cloud-based manufacturing. The most common attack goes against its availability, by means of a Denial of service (DoS) attacks against the infrastructure. Confidentiality problems arise when putting trust in the service provider, who hastotal access to the stored data. Data analytics with the information extracted from the industrial network to optimize operations and identify anomalies • Difficult to ensure the security of all components and nodes • Confidentiality and Integrity of data are threatened if appropriate measures are not applied, which is frequent in this context to improve efficiency.



Virtualization :

Virtual representations of machines for simulations and AR/VR devices to interact with the production chain. The main challenge is the secure information exchange between the physical assets and their virtual representations .Authentication issues exist with the dissemination of information over multiple vulnerable platforms (e.g., smartphones).

INTRUSION DETECTION IN INDUSTRY 4.0:

Requirements for the design, deployment and management of intrusion detection systems(IDS):

Coverage:

• All interactions and elements of an Industry 4.0

• Easily upgradable with new detection algorithms.

Holism:

• Users, configurations, potential points of failure and cascade effects are taken into account

• They must be familiarizedwith the cooperative nature.

Intelligence: Behavioral analysis and informationcorrelation to consider the existence of more advanced attacks

Symbiosis: Close interaction with other protectionmechanisms, such as prevention systems and forensics, as well as the Industry 4.0 services.

The state of the art on IDS for the current industrial ecosystems does not fully cover the previouslymentioned requirements.

Conclusion:

Today's highly automated and connected smart factories (Industry 4.0) were born out of yesterday's steam engines that mechanized manufacturing (Industry 1.0); mass-production lines expanded with the advent of electricity (Industry 2.0); and then IT-enabled manufacturing plants ushered in the era of connected industrial control systems with programmable logic controllers (PLC).hence cyber security is an important factor to consider in our industrial system.

Reference's:

- www.networkerstechnology.com/VoW_CyberSecurity_Disruptor
- www.critis2017.org/Presentations/OralPres43.pdf
- business.nasdaq.com/marketinsite/2018/GIS/Cybersecurity-Industry-Report-Investment-Case.html