

## CYBERSECURITY

*Is your network protected against costly cyber attacks?*

Manufacturing and industrial plants house complex IT networks with vast amounts of data collected and communicated between devices. These large connected networks are major targets for cyber attacks, enticing criminals to steal valuable data and impact a company's bottom line. In order to protect this wealth of data, security assessments and testing should be performed to identify potential weaknesses and work to strengthen the overall network.

***Fact: Security***

- More than 80% of manufacturing and industrial executives in the medium-large sector anticipate a security breach in their enterprise.
- Moving and sharing data outside of the plant floor to the cloud or hybrid cloud creates risk and opportunity for a breach.
- To a hacker, a smart device is a vulnerable, exploitable device.

*Denison's security professionals are experienced in continuously addressing potential breaches throughout the design, build and network management process.*

***Fact: Vulnerability & Risk***

- Cyber security incidents are on the rise, particularly in the manufacturing and engineering sectors.
- In 2015, U.S. companies lost an estimated \$61.3 billion in revenue due to a cyber attack.
- Data is vulnerable to all kinds of threats regardless of type, industry, location or protection mechanisms in place.

*Denison can conduct a thorough security audit, suggest risk mitigations and offer recommendations to strengthen and implement security changes required against malicious intrusions/cyber attacks.*

EMAIL US:

[info@denisonconsultinggroup.com](mailto:info@denisonconsultinggroup.com)

FOLLOW US ON:



in



## ***Fact: Governance, Risk & Compliance (GRC)***

- GRC tackles an organization's management, risk management and compliance strategies to help the organization reach its overall goals.
- Addressing cyber security is a critical part of any effective risk management program, particularly in the industrial and manufacturing sectors.

*Denison conducts vulnerability and risk assessments to identify potential flaws or weaknesses in a network and will work to eliminate them, strengthening the overall enterprise architecture.*



## ***Fact: Penetration & Intrusion Testing***

- Penetration and intrusion testing simulate an attack on a network, looking for security vulnerabilities or opportunities to break into a system and steal its data.
- By mimicking the mindset of a potential cybercriminal, security experts are able to remain steps ahead of costly security breaches.

*Denison analyzes the strength of each network by performing penetration and intrusion testing to spot potential faults in a system, thus stopping cyber attacks before they are able to be carried out.*

## ***The Denison Difference:***

- ✓ Technical strength with proven track record of large-scale clients
- ✓ Partnership with world-class product vendors
- ✓ Agility and flexibility
- ✓ Financial strength
- ✓ Managed services
- ✓ Focus on quality and continuous improvement
- ✓ Industry leadership and vision, with a focus on future solutions
- ✓ Members of NAM, ISA, CSA, IEEE, IETF, WBENC and other key industry groups