DRIVEN-4

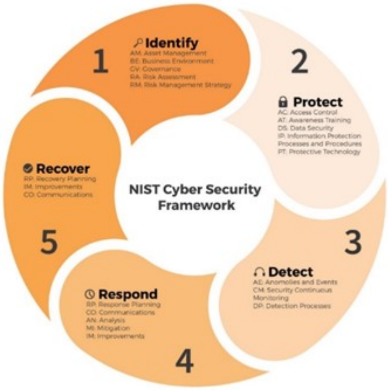
May 2018 Newsletter

Cybersecurity for Connected Products and Operations

As the world becomes more and more connected, cybersecurity is always top of mind. Organizations need to utilize an overarching framework, while utilizing technology, such as blockchain, to develop an organization that is aware, educated, prepared, preemptive and ready to take corrective action, if and when needed.

The NIST Cybersecurity Framework

The NIST Framework consists of a set of standards, guidelines, and best practices to manage cybersecurity related risk. The Framework utilizes the following steps:
Step #1: Identify: Includes the development of an asset management strategy, process and system, as well as, executing a cybersecurity risk assessment and developing a risk management strategy.
Step #2: Protect: Focuses on access control, awareness training, data security and protective technology selection.
Step#3: Detect: Is centered around anomaly and event detection and a continuous monitoring strategy.
Step#4: Respond: Develops the response planning, communication strategy and protocol, analysis and mitigation processes.
Step#5: Recover: Focuses on recovery planning, and operational improvement.



Blockchain Transforms the Manufacturing Industry

Manufacturers need to take blockchain from theory and put it into practice, identifying concrete business problems and opportunities that the technology can help address. For each use case, a manufacturer should:

- Determine key performance indicators that can be used to evaluate success and setting clear goals.
- Ensure the blockchain project addresses specific business problems or opportunities.
- Specify the actions needed for implementation. Assess the required resources, create a process map and develop an implementation guide.
- Explore a variety of platforms, including both permissioned and permissionless.
- Combine artificial intelligence with blockchain to increase the security of systems by placing key aspects of decision-making in the blockchain rather than individual machine learning systems.

Securing connected products – Internet of things (IoT) meets Cyber Security

Connected devices have become an increasingly attractive target for criminals. On these devices, 6 quick steps that can reduce the risk in the environment include the following:

- Control everything that connects into your network especially mobile devices. Be aware what's connected to your network by conducting scans and utilizing Network Access Control (NAC) appliances.
- Create security based on context and layers. Layered security or defense in-depth strategy creates many layers of defense making it difficult for an attacker to gain access into the environment.
- Centralize and segment the connected devices
- Update and patch baselines if at all possible. Updating all devices is crucial in closing vulnerability holes.
- If systems cannot be updated— conduct a risk assessment and put in place risk mitigation techniques.
- Always test your systems and maintain visibility. Conducting static code analysis on developed programs can identify poor coding practices and network weaknesses before they are introduced into production.

From our perspective, cybersecurity and the strategy, framework and technology your organization utilizes to defend your reputation, connected products and manufacturing environment, is not only a necessity but needs to be a top priority. The integration of these concepts within your people, processes and systems needs to be seamless in order to minimize any potential vulnerabilities. You need to constantly assess, develop and improve these core strength for your company, it needs to become a core competency in order to succeed in the connected world of today and tomorrow.

Coming in June: Augmented Reality Use Cases for Today's Organization