TRACTION Guest.

Physical security considerations for manufacturers.

Protecting the people and assets that make up the manufacturing facility

When it comes to possible risks, breaches, incidents, and personnel involved in physical security at a manufacturing facility, there are many competing concerns that security professionals are handling. Security professionals are responsible for protecting important assets and information, including:

- On-site staff
- Products produced
- Equipment used in manufacturing
- Customer and employee information
- Financial records
- Trade secrets, product information, and blueprints

With the increasing range of assets to protect, it leaves security teams struggling to determine how to prioritize their efforts without spreading the security team too thin.

In this document, we'll explore why physical security is critical to protecting the assets that make up the manufacturing facility, as well as the workforce, and why physical security to protect both can't be ignored by manufacturers.

We'll look at:

- Why physical security is often overlooked
- Managing the human risk element
- Vulnerability when dealing with multiple locations
- What can be done to combat the overwhelming physical security priorities

Physical security gets overlooked.

Security trends have been leaning towards focusing on cyber attacks. With the focus shifting away from physical security, manufacturers are leaving the server room door wide open, quite literally. All the best authentication tools and data encryption codes won't help prevent a security breach if a would-be attacker gets inside the server room. From there, they have access to the physical server, Internet lines, and all the data in that room. A strong cyber attacker could make quick work of the server's security features, rendering any cybersecurity measures put in place now useless.

There are also physical concerns regarding physical security, such as access control systems, including key card access. Employees and contractors are often given key cards to swipe into rooms, offices, and manufacturing floors. These cards can be lost or stolen, or in the case of a terminated employee, not returned, but still remain active. This leaves an open door, even when the door is closed, for a would-be threat to walk in undetected.

To combat the risks that come with access control to physical locations, manufacturers are adding additional layers to their security measures in order to gain access. This includes utilizing sign-in systems that screen watch-lists to check visitors against internal created watchlists, and third-party watchlists that screen local and international law enforcement lists, among others.

These physical security and access control measures are often overlooked as greater emphasis is being placed on cybersecurity measures to expel attackers from outside the location. Even when cybersecurity measures are enhanced, measures that pertain to physical security have to match those in the cyber world. When physical security measures that are put in place fail, even the best cybersecurity policy will fall flat. Manufacturers need to return to the basics of security and think about people physically coming inside.

Managing the human risk factor.

Physical security concerns arise because of human beings. Take away the bad actors, and there is no risk. Unfortunately for security professionals, bad actors can come from both outside the organization (contractors, uninvited guests, even family members of staff), or from the employees themselves.

To protect the physical assets inside the manufacturing facility, security needs to manage the human risk factor appropriately, depending on the type of person they are.

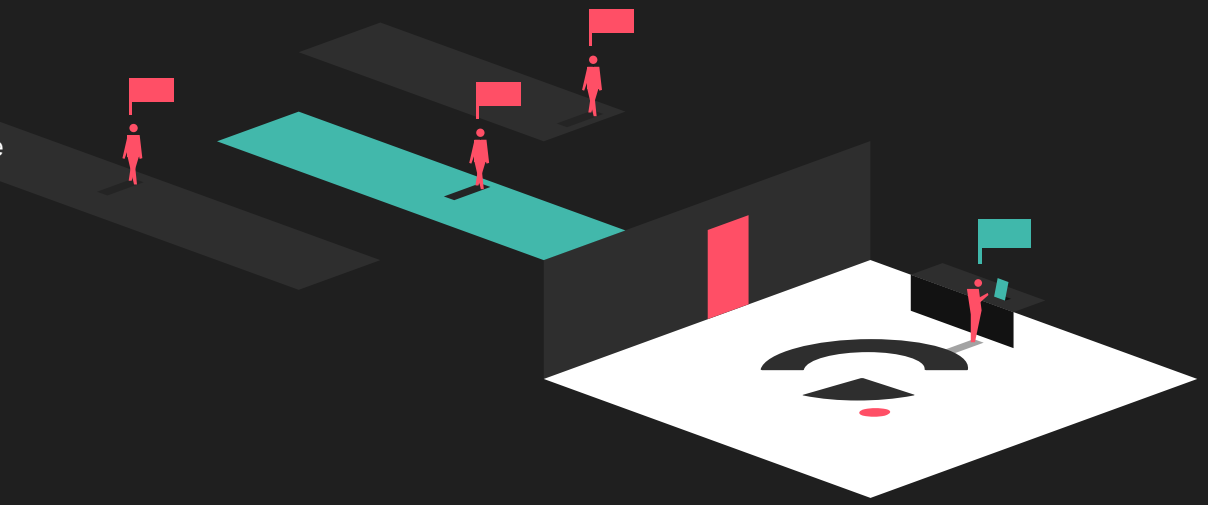
1. Theft and violence from outside actors

No facility is secure from outside actors. These external actors have a reason to be on-site and are given access every day, including specialty contractors, maintenance and repair workers, and associate business partners. There are also family members who visit, job applicants, coming in for an interview, and delivery drivers dropping off a package.

It's easy to turn a blind eye to these lone actors as they appear harmless to the facility's overall security. However, unauthorized visitors can be damaging to the operation of a facility if they can breach an access point and gain entry to sensitive areas. Often these outside actors have someone's trust, or they have been given a key card or access credentials, but they can cause physical harm to employees and steal valuable technical data.

Despite the relative safety of these outsiders, physical security measures need to be in place to protect all the facility's assets. It only takes one bad outside actor to cause millions of dollars in damage. A good visitor management experience can reduce the risk of these outside actors by checking internal and external watchlists and doing background checks against third-party systems. All while maintaining an experience that has them moving seamlessly to where they need to be with the added security knowledge of who they are and why they are on-site.

It's important that manufacturers treat outside actors as a constant threat, and put barriers, workflows, and systems in place to ensure security measures are met. While it may seem redundant to contractors to continue swiping in through a sign-in system, a proper visitor management system in place will streamline the entry process to ensure a fluid movement of authorization personnel into the facility.



2. Internal security threats

One might assume that those who you don't know—outside actors—would be more of a threat, but oftentimes those who you know are the greater risk. Employees have access to the manufacturing facility daily and have had their security checks already completed, but that hasn't stopped internal actors from stealing valuable information and assets from their employers.

According to the Verizon's 2019 Data Breach Investigations Report, 34% of data breaches in 2018 involved internal actors. Thinking of cyber breaches as a proxy for physical considerations, the employee cohort can represent a significant gap.

With greater access comes more significant concern from a physical security perspective. Employees have extensive knowledge of the facility, its layout, and its security measures. They often have access to video and monitors, internal and Intranet systems to remove records from, and they can occupy security personnel to carry out a crime.

Furthermore, employees have a better understanding of what data, assets, and equipment is valuable and where it is stored, as well as trade secrets on personal devices such as laptops and mobile phones. So, they can move faster than an outside actor can, directly to the source of the asset, cutting down time to commit their crime.

A way to combat the internal threat is to treat even employees as a possible risk, and put them through similar procedures as external actors. Requiring sign-ins through a visitor management system before using an access control system will give security a real-time view of who is actually on the premises. By using a scheduling or inviting system, it ensures that the people who are supposed to be there are allowed to come in, and employees that are not invited or scheduled to work, are denied access. This 'invite first' approach is especially relevant as organizations move to flexible/hybrid work arrangements and lose the sense of core-hours of the known staff cohort.

What can manufacturers do?

To maintain the highest level of security, manufacturers need to assess their risks, their needs, and what damages could be most devastating to their organization. They then need to install the physical security measures that will help them achieve their desired goals.

By having a clear understanding of all the risks and outcomes, manufacturing organizations can then design a security plan that suits their location and organizational policy to keep their people, assets, and technical data secure from outside and internal threats.

Manufacturing organizations need to modernize their approach to physical security and go beyond simplistic perimeter security. This new modern approach includes utilizing third-party watchlists, visitor management systems, access control devices, and workforce security Platform.

Articles of interest:

- StandardAero makes compliance consistent across global organization
- Veeco reboots it's operation thanks highly customizable security platform
- Bonduelle processes contractor entry through contractor integration

About Traction Guest.

Traction Guest ensures safety and security for employees, contractors, and essential visitors – wherever they work - through our Workforce Security Platform. The platform provides the most advanced enterprise visitor management system (VMS), health and safety controls, critical outreach and alerting, as well as analytics and auditing functionality.

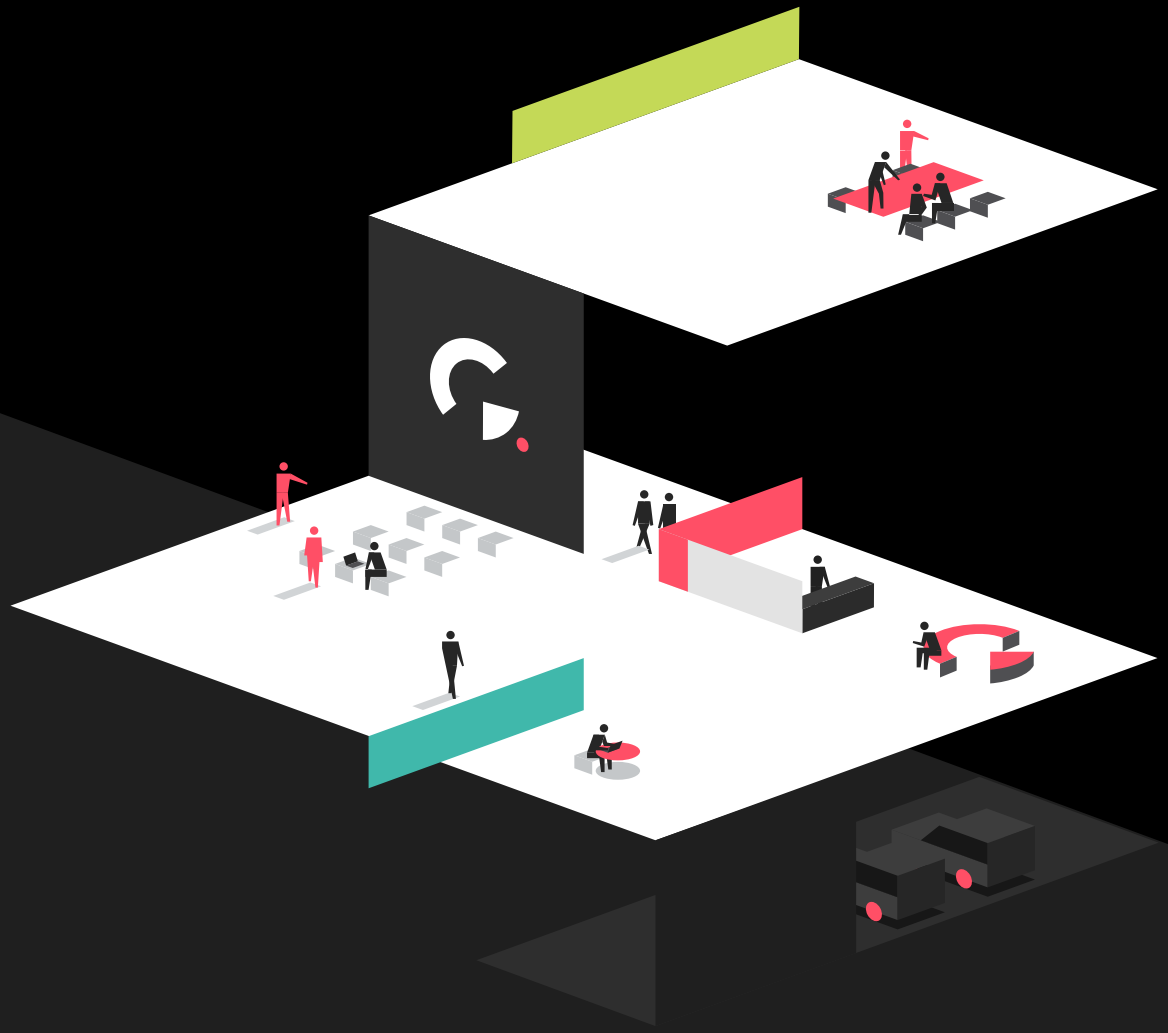
Traction Guest facilitates multi-layered screening and approvals so that security processes can be finely tuned for unlimited locations, types of workplaces, and roles. It's a robust solution to support duty of care requirements and keep people safe in a rapidly changing environment.

Centrally manage multi-location customizations

- Support employees and non-employees in a hybrid environment
- Standardize and codify compliance requirements
- Solve complex security and safety problems

Global brands across five continents and dozens of industries trust Traction Guest's highly customizable platform to mitigate risk and deliver unparalleled security through an intuitive, touchless, highly branded experience that supports compliance, employee engagement, and duty of care requirements.

TRACTION Guest.



tractionguest.com >

info@tractionguest.com >