The security blindspot.

The non-employee risk manufacturers are ignoring.

When an employee walks onto the floor of a manufacturing facility, the security team has a very good idea of who that person is. Through the interview process, they have had the opportunity to vet that employee for possible security threats, such as legal troubles, previous criminal history, credit history, even going as far as to look at their social media accounts.

It's common practice now to perform background checks on employees coming into the facility every day to know exactly the type of person you are about to grant access to business information.

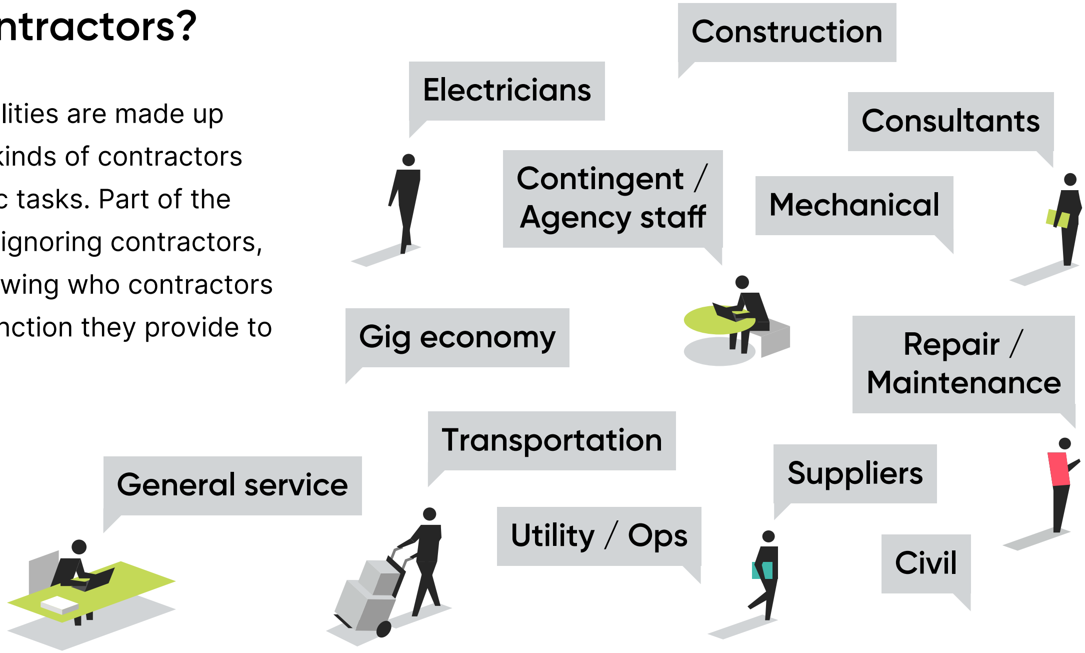
Yet, manufacturers don't do the same thing for visitors and contractors coming through their doors. This creates a security blindspot for security teams who should treat each person - whether an employee, contractor, or visitor - as a possible threat because they lack in-depth background information

"No company would ever hire someone without doing a background check or criminal history check because the risk and exposure would be too great," said McKay Johnson, Vice President of Sales with Indent Solutions. *"But manufacturers will allow hundreds, even thousands of people through their facilities every year and don't know anything about them."*

Screening procedures for many manufacturers don't generally include background checks on new job applicants coming to the facility, delivery personnel, maintenance crews for HVAC systems, and janitorial staff. They can pose a high-security risk like an employee, except that the security team is in the dark.

Who are contractors?

Manufacturing facilities are made up of many different kinds of contractors performing specific tasks. Part of the blindspot isn't just ignoring contractors, but rather, not knowing who contractors really are or the function they provide to the facility.



Construction

Electricians

Consultants

Contingent / Agency staff

Mechanical

Gig economy

Repair / Maintenance

Transportation

General service

Suppliers

Utility / Ops

Civil

Protecting people is just the beginning for manufacturers.

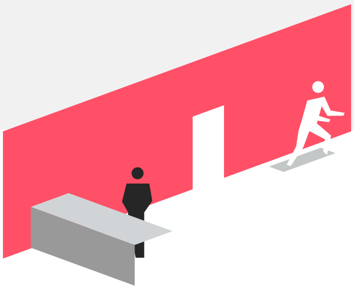
For every manufacturing security team, protecting people is just the beginning of their security strategy. They also ensure property security, including the physical locations and any equipment in those locations and intellectual assets. Protecting the workforce is of the utmost importance, but so is protecting the physical and intellectual assets of the organization.

"Every security team has one main goal, and that's the security of their people, their property, and other assets," said Johnson. *"But we have identified a clear gap in everybody's process. They know nothing about their visitors. We should ask ourselves, 'what do I know about the visitor I'm about to give access into our facility, into our people,' and should we be letting them in the first place."*

According to an Intel whitepaper, The Cost of a Lost Laptop, the value of a stolen laptop is not just the replacement cost of the physical laptop. But also the value of other cost components, such as replacement cost, detection, forensics, data breach, lost intellectual property costs, lost productivity, and legal, consulting, and regulatory expenses. Intel says that a stolen laptop has an average cost of $49,246 when factoring in the additional cost components.

Laptops, where the organization's intellectual assets are stored, can be stolen by non-employees. That is why Johnson believes it is crucial to understand every person coming into your manufacturing facility fully. Even a seemingly innocent theft can be costly and detrimental to a manufacturer's business.

"Something as seemingly insignificant as having someone come in and steal a laptop could be devastating to a manufacturing facility," said Johnson. *"The bottom line is, companies need to know who's coming in. It goes beyond compliance requirements, but also extends to understanding if someone has a pattern of behavior that puts the organization at risk."*



Greater concern for the lone actor.

Many believe that the most considerable threats to a manufacturing organization are large groups of possible attackers. However, Johnson said that it's often the lone actor that poses the greatest danger for a security team. That's because they can slip through security undetected.

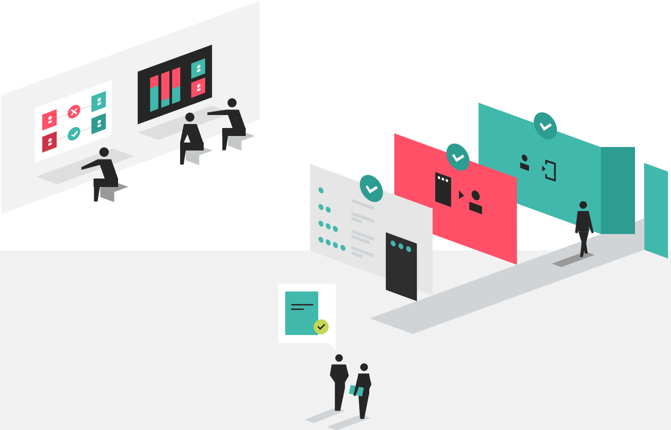
These individuals could have a past criminal history or qualifications that would warrant an escort or denial of entry to the building. However, due to a lack of screening and a policy to perform a background check on every individual coming in, a lone actor can be granted access to sensitive information, physical assets like laptops and servers. It also includes access to employees. All of which can result in potential security threats.

"The big concern is the one individual - the lone actor - which is hard to identify when you have a sea of people that you're dealing with," said Johnson. *"Even if it's 20 to 30 a day, or potentially hundreds of people, you're still in that mode of looking for a needle in a haystack."*

To reduce the impact a lone actor can have on a manufacturing organization, Johnson said security processes need to change. Systems need to look at every individual to see if there is something of concern. Having an automated screening process as part of a visitor management policy can properly screen any person coming into a facility. No individual should be able to pass through a security checkpoint without having a complete background check.

Employees have extensive screening completed during the hiring process, but lone visitors and contractors remain in a gap. Upon entry, everyone should be seen as the individual - and possible threat - that they are.

A lack of an automated system reduces the security team's ability to screen these individuals adequately, or it's a time-consuming process that creates a backlog in a lobby. It can lead to individuals that aren't employees being granted access with proper checks, as often they will only be inside a short period and won't pose a threat.



It takes an entire organization to remove a security blindspot.

To remove this security blind spot, the entire manufacturing organization needs to change its mindset regarding visitor management and security. Members of different departments, such as HR, marketing, sales, and operations, must have a zero-trust, security-first attitude when considering allowing individuals into a facility. It simply can't all be on the shoulders of the security team.

People don't think of the impacts or risks a dangerous actor could represent. The actual cost of replacing a stolen laptop, for example, goes well beyond the physical value of the asset and includes the intellectual property trade secrets, organizational procedures, and blueprints.

"People don't necessarily think that way, they think - we lost the laptop," said Johnson. *"Yes, you can replace a $2,500 laptop. But if that data gets out, that is intellectual property or a data breach, that's not replaceable. Many throughout the manufacturing organization may not see it that way, especially employees. So, it takes much effort to try and educate all employees about these types of measures because they can be devastating for an organization."*

An educational training program should be part of a new security effort to individualize visitors coming into the facility to address this mindset gap. This program includes training employees about the new level of screening their visitors, guests and contractors will have when they arrive. By making them aware of the risk lone actors present to the organization, it's more likely that the entire manufacturing organization will widely adopt increasing screening.

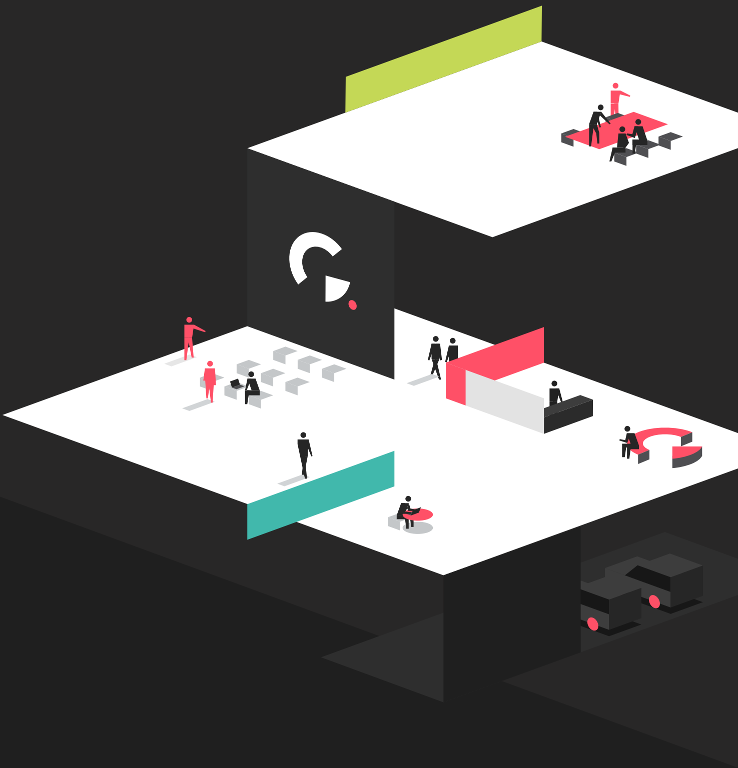
About Traction Guest.

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.



About Ident Solutions.

Ident Solutions was founded with one big idea, to make your world a more transparent place by disrupting the status quo. As technology pioneers we provide clear, honest, and instant background checks that help businesses make quicker, safer, and more informed decisions. We do this through a combination of agile engineering, dataology, and innovative technology that has never existed before.

tractionguest.com >

info@tractionguest.com >