Picture credit: Detertech

CRIME WITHOUT BOUNDARIES

Gary Higgins *looks inside the evolving world of serious acquisitive crime*

When a van full of tools disappears overnight or copper cable worth thousands vanishes from wind farms or national network rail infrastructure, it is easy to chalk it up to the work of opportunistic thieves striking lucky. However, there is something much larger going on. DeterTech crime analysts, who have a data sharing agreement with all 43 police forces in England and Wales, have identified a concerning, ongoing spike in serious organised acquisitive crime. Proven to be driven by networks of professionals, these groups are working across the country to thoroughly plan and carry out targeted attacks across all sectors, including rail, renewables, construction, retail and more. Attacks on wind farms have surged 200 percent and tool thefts totalled a shocking £40-million in 2024 alone.

These aren't all random crimes. Many are co-ordinated attacks, conducted by organised groups with pre-established disposal routes for stolen tools, assets and materials. Therefore, police, sector professionals and communities are being forced to rethink current methods of site security to combat these threats.

Serious organised acquisitive crime (SOAC) refers to coordinated theft or attacks that are planned, often cross-regional, and motivated by financial gain. These groups move from site to site to target specific valuable goods such as copper, power tools, site equipment or branded retail goods such as perfume, clothing, bags and designer products. These stolen goods are then quickly resold to make a hefty profit.

We can see changes in both the scale and sophistication of SOAC attacks. DeterTech's intelligence teams, who analyse national data from police forces and private organisations, note how these groups operate to remain undiscovered. Organised crime groups exploit supply chain weaknesses and gaps in site security, as well as relying on the strain police are under to respond to every incident (specifically in the case of retail and tool theft). Increasing economic pressure adds fuel, with the cost-of-living crisis intensifying and global commodity prices rising, items like copper, tools and site equipment are more valuable than ever, intensifying the reward over risk factor for many criminal groups.

Retailers have a renewed focus on deterrence using forensic marking such as SmartWater

DeterTech shares key live crime intelligence to the police and public to help identify sectors and regions across England and Wales under significant threat, whether that be retail, construction, energy, rail or others. Each faces its own unique challenges, but they are all connected by the presence of serious organised acquisitive crime, which is becoming increasingly harder to catch due to the nature and volume of attacks. This therefore calls for the increasing need for smarter, collaborative prevention methods.

The UK's transition to renewable energy has created vast new infrastructure networks, from solar farms and wind turbines to energy storage sites, but this has also meant an increased opportunity for organised crime. Copper theft has long been a problem, but has evolved drastically into complex, coordinated operations that threaten energy sites across the country.

Between January and August 2024, DeterTech recorded over 70 offences against solar farms, with an estimated 750km of copper cable being stolen. This year, the North-West of England saw a major rise in reported incidents of copper and cable theft identified as orchestrated by organised crime groups. These attacks include the loss of almost £500,000 of copper cable from a Bolton site, significant loss of string cable from a solar farm in Preston impacting local power supply, and theft from Wigan rail network costing the UK economy an estimated £1-million.

Additionally, DeterTech's analysis indicates a 300 percent year-on-year increase in attacks, with offenders often working in small, coordinated teams to strip valuable components and materials from multiple turbines in a single night. This can have a major negative impact on surrounding towns, cutting energy supplies to key infrastructure including hospitals, telecommunications and public services. Replacement and repairs can take months and is extremely costly.

These cases are not rare and renewables sites across the UK are being increasingly targeted. Likely due to a number of reasons, the most prominent being the difficulty of securing these often desolate, remotely located sites. Many solar and wind farms are in rural areas that are difficult to establish a strong and secure perimeter. However, DeterTech's work with police and operators shows that strategic prevention works. Forensic marking cable to make it traceable, remote 24/7 monitoring systems, and overt deterrents such as signage and lighting have proven to reduce theft dramatically – in some cases by up to 89 percent. Their intelligence also reveals that sites visibly marked and registered as protected are far less likely to be re-targeted.

The construction and trade industries remain among the most heavily targeted by organised crime groups. Tool theft is now estimated to cost UK businesses more than £40-million each year and impacts many key infrastructure development projects. Not to mention the detrimental impact these thefts have on tradespeople's livelihoods and mental health who are often victimised at their place of work or homes.

Vans and construction sites are particularly vulnerable, typically attacked overnight or during weekends when few people are around and the risk of being caught is particularly low. Additionally, DeterTech data reveals that once a site is targeted, it is extremely likely to be targeted again – sometimes multiple times. This makes it imperative that security upgrades are made immediately following an attack to ensure repeat victimisation is avoided.

Tools are particularly attractive due to their high value and portable nature, as well as being notoriously hard to track or mark, making them easy to resell. A single stolen van can represent tens of thousands of pounds in lost assets, project delays and replacement costs, on top of the mental toll it takes on the victims.

TECH AND INTELLIGENCE ARE CRUCIAL FOR PREDICTING RATHER THAN REACTING TO CRIME

In the UK the long-anticipated Equipment Theft Prevention Act is considered a flagship moment in deterring the theft and resale of tools and equipment. Yet, almost two years on we are still awaiting the secondary legislation that will allow mandatory forensic marking and registration by manufacturers to come into force. Even then it will only apply to new equipment and not to items that people already own. Of course, there's nothing stopping individuals from taking matters into their own hands. Why wait for legislation when forensic marking is a quick and simple measure that offers instant benefits and that anybody can carry out for themselves?

When it comes to the protection of construction sites themselves these are notoriously recognised as difficult to secure due to their temporary nature, as well as the constant arrivals and departures of delivery drivers and workers. DeterTech's intelligence stresses the importance of establishing unified state protocols including secure storage containers, tracking and identification methods like forensic marking and physical surveillance and security personnel. Temporary 24/7 monitored alarm systems are also ideal options for reducing blind spots and deterring repeat offenders from striking again, particularly for worksites that only require short-term surveillance and security.

Retail has been one of the hardest-hit sectors, experiencing a surge in thefts of all product categories. Over 530,000 shoplifting occurrences were recorded in the year to March 2024, up 20 percent from the previous year. This is symptomatic of deeper systemic issues, yet a significant component is groups targeting high-value goods to resell for a profit on the black market. Some of the most commonly targeted categories include cosmetics, fragrances, alcohol, tech and designer goods. These offenders are often highly mobile, moving throughout towns or regions to avoid recognition and they frequently exploit the lack of resources many retailers face when combatting theft.

Retailers are responding with a renewed focus on deterrence and intelligence, combining a range of solutions in a layered approach. One way is through clear signage of forensic marking such as SmartWater as well as CCTV, facial recognition, asset tagging, real-time monitoring, physical security and local data sharing partnerships.

ORGANISED CRIME GROUPS EXPLOIT SUPPLY CHAIN WEAKNESSES AND GAPS IN SITE SECURITY

Crucially, collaboration is key and initiatives like the National Business Crime Solution (NBCS), data and incident information shared between retailers and police forces can reveal repeat offenders, behaviours and methods, and resale hubs, helping to disrupt organised theft at its source. DeterTech evidence shows that when retailers participate in shared intelligence networks and deploy forensic deterrents, repeat incidents can fall by over 60 percent.

Sadly, the problem goes beyond losses in profit; persistent organised theft can have a detrimental impact on workers' morale and feeling of safety in the workplace. There are over 2,000 incidents of violence or abuse per day against retail workers, up from 1,300 the previous year, highlighting the impact on workers. This makes it imperative that retailers take necessary steps to protect workers and customers by deterring crime and reducing the reward over risk temptation.

As serious organised acquisitive crime continues to evolve, one thing is clear; it's no longer a localised or isolated problem, it's a national threat that cuts across industries, regions and communities. Whether it is high street retailers, tradespeople, large construction sites, energy sites, rail or other critical infrastructure, the methods adopted by offenders are becoming increasingly sophisticated, networked and professional.

DeterTech's intelligence shows that these organised criminal groups operate best when their activity goes under the radar, so data sharing and collaboration between those on site and police forces is critical. Important to note, effective crime prevention doesn't always mean high-cost infrastructure, but intentional, smart solutions installed for each individual situation. From live 24/7 monitoring and forensic marking to intelligence sharing between sectors, the most successful crime reduction models are built on visibility, partnership and proactivity.

Businesses can no longer simply rely on basic CCTV solutions or on workers to correctly identify and stop criminals; technology and intelligence are crucial for predicting rather than reacting to crime. Through recognising trends early and targeting repeat offenders through shared data, patterns can be detected and criminal activity can be disrupted before it escalates. Businesses that make an active effort to engage with intelligence networks see measurable drops in theft and repeat victimisation.

It is important to remember that prevention is not just about protecting assets, but also people. Each theft affects staff morale, customer trust and public confidence in local infrastructure. Through embedding crime prevention into daily operations, businesses are committing to protect the people impacted by acquisitive crime. Ultimately, tackling organised acquisitive crime requires a collective effort from all involved. The proof is clear, when intelligence is combined with smart technology solutions designed to deter, we collectively move from reacting to crime to redefining how it can be prevented entirely ●

Gary Higgins is Director of Security and Risk at DeterTech.

The most successful crime reduction models are built on visibility, partnership and proactivity

Picture credit: Detertech