

Picture credit: DeterTech

HEAVY METAL

Mark Kubis Law *outlines why cable theft is back on the rise and how sites can fight back*

Copper and cable theft has become prevalent across multiple sectors and regions: it is having a detrimental impact across energy, rail, telecoms, water, and renewables sectors. DeterTech's crime intelligence team, which monitors metal theft trends, is seeing site operators report a resurgence of site trespass and theft, and the driver is simple economics. As copper prices climb and reach an all-time high, so does the incentive to steal it regardless of the wider implications it has on national power, communications and transport networks.

Cable theft was believed by many to be a solved problem, with the Scrap Metal Dealers Act 2013 introduced to ensure all scrap dealers are licensed, cash-in-hand sales are banned and valid ID is required for every sale. Following this, there was a dramatic decrease in rail-related cable theft and the delays it caused fell dramatically.

Yet, metal theft has always tracked commodity prices closely and in the last 18 months, copper prices have risen dramatically. Earlier this year copper hit an all-time high of over $14,500 a tonne according to the London Metal Exchange, a level that has pushed related crime firmly back up the risk register. The knock-on cost to the UK economy is estimated to be around £480-million a year, according to a report by the All-Party Parliamentary Group on metal, stone and heritage crime.

The pattern is visible across almost every sector that relies on exposed cable and DeterTech's crime intelligence analysts have been monitoring closely as it develops. Six significant incidents hit the North-West of England in a matter of weeks last autumn, spanning energy, transport, utilities and renewables sites, reported by DeterTech's crime intelligence team. Thieves in Bolton made off with 33kV copper cable worth close to £500,000. A solar farm near Preston lost around 40 percent of its output after string cable was stripped out, putting local power supply at risk and a rail incident in Wigan is estimated to have cost the UK economy more than £1-million in disruption.

Renewables have been significantly targeted. This is often due to sites being located in remote, quiet areas that are vast and extremely difficult to secure. Wind farms recorded 43 reported cable theft incidents by November 2025, against a typical historical figure of around five for the whole year. Losses across renewable sites from theft and associated downtime are estimated to be a minimum of £8-million for 2025 alone.

The rail industry is facing very similar issues: British Transport Police figures have long shown incident numbers rising and falling in step with copper values, with disruption often resulting in tens of thousands of minutes of delays a year. Now that copper prices are elevated again and there are a range of major infrastructure projects underway, it has become an opportune time for organised crime groups (OCGs) to take advantage of sites across industries.

The South of England has felt this most recently. Crime intelligence gathered by DeterTech points to a renewed cluster of offending across Hampshire this spring, with water, electricity, communications and transport sites all affected and the corridor between Winchester and Andover flagged as a particular hotspot. Two incidents were recorded there in April 2026 alone, at a site that had also been targeted the previous September.

Worryingly, cases like Hampshire's point to the wider problem with this type of acquisitive crime. Repeat victimisation is a significant problem when discussing metal theft; OCGs will scope out all vulnerabilities of a site and return to locations repeatedly because they know the layout, the gaps in coverage, and roughly how long they have before anyone responds. DeterTech crime intelligence teams report that a site attacked once is commonly retargeted within weeks, which is why a security review carried out immediately after a first incident matters far more than one done on a routine annual cycle.

There is a timing pattern too. Offences cluster around specific days and hours, commonly evenings and weekends, when sites are unmanned and response times are at their longest. This points to reconnaissance rather than pure opportunism, and increasingly to organised groups working across multiple sites and regions rather than lone offenders.

Additionally, sites also can be easy to take advantage of due to sharing similar characteristics such as generators, cable runs or substations being frequently located away from main buildings and out of easy sightlines. For many offenders, this combination is the whole appeal – the low chance of being disturbed and access to tens of thousands of pounds of cable make the rewards appear to outweigh the risk.

Across industries, security professionals are recording the same trends of being targeted and more than once. The ways in which they combat these issues, however, differ site-to-site depending on independent needs and threats recognised. It is important for site security operators to get a comprehensive site security assessment, for example, DeterTech conducts free site assessments across Europe to assess threats and weaknesses.

There are many options available to secure sites, including SmartWater forensic marking, which means cable and other high value assets can be invisibly marked, making them completely traceable to their original site. Additionally, visible signage about forensic marking is particularly effective as it highlights that a site is protected, acting as a proven effective deterrent to thieves. SmartWater also proves extremely useful in cases that do end in theft. When copper arrives at a scrapyard, it would have previously been untraceable, however copper seized from offenders can be traced back to the original site it was stolen from and can result in a conviction.

Offences cluster around specific days and hours when sites are unmanned and response times are at their longest

SPEED OFTEN DECIDES THE OUTCOME ONCE AN INTRUSION HAS BEEN SUCCESSFULLY DETECTED

Temporary security is filling a gap too, especially for sites that are vulnerable, but not yet fixed in their layout. For example, DeterTech PID360 deployable detection systems can be moved onto a site within hours rather than weeks, putting a visible, active presence on construction sites, substations or newly identified hotspots while permanent security is planned or installed. The point isn't to record a theft as it happens, it's to deter it from happening at all: a rapidly deployed, clearly signalled system tells an OCG that a site is no longer the easy, unmonitored target it was, closing the window before a return visit can be planned. This is especially important following a first incident, as this is when a site is statistically most at risk and needs immediate security and protection.

Beyond these, operators are increasingly investing in rapid alarm verification and dispatch (cutting the time between an intrusion being detected and someone actually responding), and in feeding what they see back into shared intelligence networks so patterns across regions and sectors can be spotted earlier. No single measure solves the problem alone, but combined they start to close the gap that organised groups have been exploiting.

For infrastructure operators and site managers, an effective response is layered; no single measure does the job alone.

Identify and understand risk. Start with the entry points an offender would actually use on foot and by vehicle, rather than treating the whole perimeter as equally vulnerable. It rarely is.

Strengthen and review site security. Check fencing regularly. Damage or cutting is often a precursor to further intrusion and a sign a site is already on an organised group's radar. Where a site has been targeted before, a security upgrade delivered quickly matters more than one

delivered months later, given how fast repeat offending tends to follow.

Communication and deterrence. Make it obvious that security is in place (cameras, alarms, forensic marking, clearly signposted). A deterrent nobody is aware of is not much of a deterrent. Briefing staff and the local community on what to look out for and who to call adds a further layer, provided everyone understands the rule: report, do not confront.

THE POINT ISN'T TO RECORD A THEFT AS IT HAPPENS, IT'S TO DETER IT FROM HAPPENING AT ALL

Surveillance that covers the right assets. CCTV pointed at a building entrance is of limited use if the generator at the rear of the site is the actual target. Coverage needs to include cable runs and substations specifically and it needs to be visible so its value is in putting offenders off before they act, not only in capturing footage afterwards. On sites that change shape over time, such as construction sites, cameras that can be redeployed as works progress tend to outperform fixed installations.

Rapid, verified response. Once an intrusion is detected, speed often decides the outcome. The gap between an alarm triggering and a response being dispatched is frequently the difference between a deterred attempt and a completed theft. Some monitoring centres now aim to review, verify and escalate a triggered alarm in under a minute.

Asset protection through forensic marking. Marking cable and other high value materials so they can be traced back to a specific site and making that visible, discourages theft and improves the odds of a successful prosecution if theft happens anyway. It is a large part of why roughly 1,000 miles of rail cable have been marked nationally already.

Reporting and intelligence-sharing. Report every theft, attempted theft and sighting of a suspicious vehicle promptly, not just to the police but into sector-wide intelligence networks where possible. The fuller the picture built up across operators, the better placed police and security teams are to spot patterns and disrupt organised groups before they strike again.

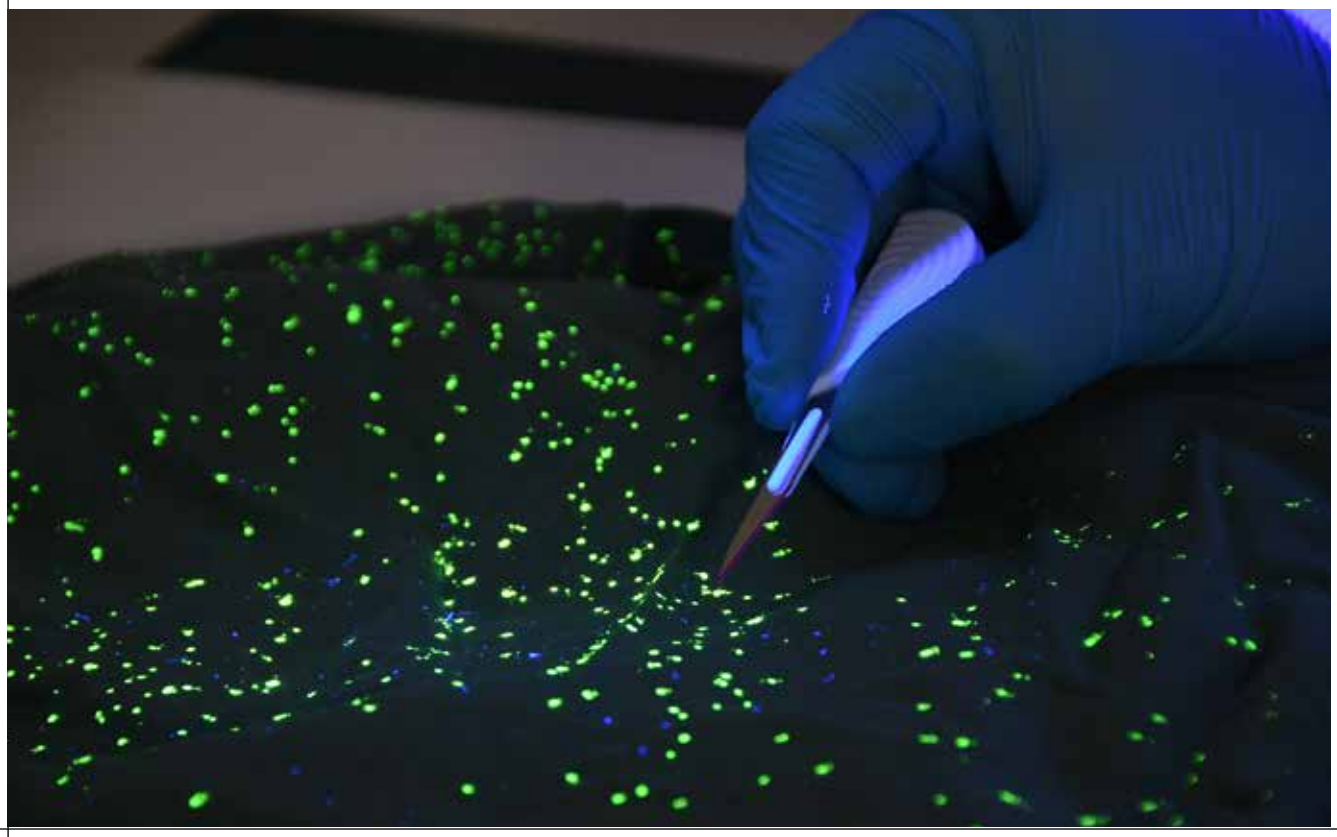
None of these measures will be 100 percent effective when used on their own, but when combined and when site security is treated as an ongoing intelligence-led process instead of something reviewed once and left unattended, sites become a far harder, far less appealing target, and that's what ultimately keeps them off the repeat-victim list.

Copper prices show little sign of reducing in the near future and combined with the increased infrastructure investment across energy, transport, telecoms and other utilities, the pool of potential targets is only going to continue expanding. To ensure all possible preventative actions are taken, site security operators are urged to review their security posture now, rather than after a first incident. The organisations that ensure the risk is too high and the effort is too great are the ones least likely to see multiple attacks.

Ultimately, modern site security isn't a matter of how many cameras are installed. It's about understanding where the real risk is, making the surveillance solution visible enough to deter an offender before they act and being able to respond in minutes rather than hours, if they don't. Sites with effective security measures stop being repeat targets, and those that don't will keep paying the price of chasing evidence after the cable is already gone ●

Mark Kubis Law is Corporate Accounts Director, DeterTech.

SmartWater is extremely useful when it comes to identifying thieves



Picture credit: DeterTech