Energy Theft Forum

28 June 2023

Housekeeping

Videos and microphones: please keep turned off unless speaking

Opportunities for Q&A: we'll be running two Q&A sessions where you can raise your questions

Recording: this meeting will be recorded. Please note that by joining you are consenting to being recorded.

Welcome

Aiyesha Andrade

Agenda

01 RECCo Theft Strategy Update

02 Crimestoppers Marketing Campaign and Annual Performance Update

03 Smart Meter Data in Theft Detection

04 Q&A Session

05 Police Engagement

06 Improving Data Collection and Reporting

07 Engagement with Water Companies

08 Third Party Theft and Demand Side Response

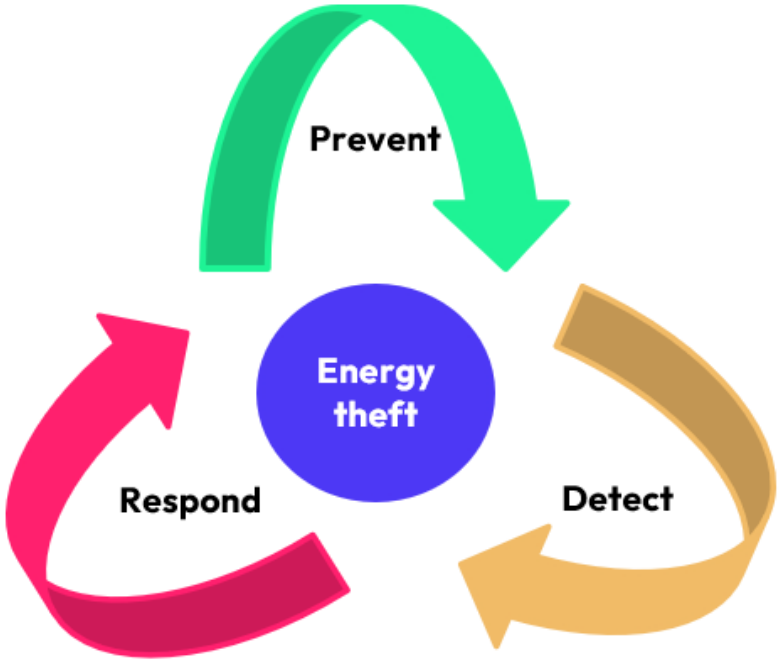
09 Q&A Session

10 Close

RECCo Theft Strategy Update

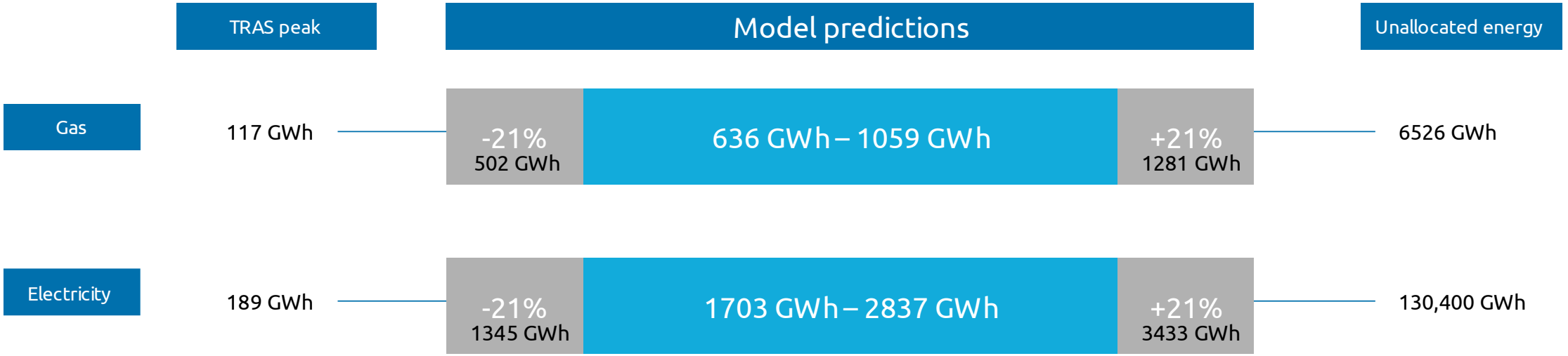
Jon Dixon & Tracy Hardy

Theft Reduction Strategy



1. Better understand the problem;
2. Prevent theft – raise awareness of risk to safety and of prosecution;
3. Improve industry ability to detect theft that does occur;
4. Improve industry ability to act upon confirmed theft –share lessons, gather evidence

Understanding the problem: Theft Estimation Methodology



Theft losses in monetary terms will obviously vary with prices, but at Dec 2022 when report published, that equated to:

- £737m - £1233m for electricity; and
- £93m - £155m for gas.

Adding £29 to £48 per year to the average household energy bill.

Future work will seek to narrow range within TEM estimate, and make better use of smart data and network data on non-technical losses, etc.

How we will deliver the strategy

Five priorities identified from November 2022 industry workshop and carried into 2023/24 Forward Work Plan:

1. Re-establish theft expert group and stakeholder forum

2. Raise awareness of scale and impacts of energy theft

3. Develop theft data hub and analytics

4. Improve whole-of-system incentives to prevent, detect and investigate theft

5. Explore feasibility of improving police focus on energy theft

We are adopting an agile delivery method for the delivery of these objectives, with all associated actions and initiatives captured as a series of ‘Epics’.

23/24 Theft Programme: Prioritised Epic's Report

Ref	Epic Title	Status
TE001	Raising Awareness of Energy Theft for Consumers	In Progress
TE002	Raising General Awareness of Energy Theft Across Industry	In Progress
TE003	ETTOS Service	In Progress
TE006	Review End to End Theft processes	In Progress
TE004	Identification of Non-Industry Agencies to Collaborate with for Energy Theft	Not started
TE005	Engage with Non-Industry Agencies for Energy Theft	Not Started
TE007	Pilot Data Driven Detection Service	Not Started
TE008	Integration of Tampering Alert Alarms Data into Theft Estimation Methodology Model	Not Started
TE009	Integration of Low Voltage Network Data into Theft Estimation Methodology Model	Not Started
TE010	Implementation of Energy Theft Detection System	Not Started
TE011	Obtain Smart Meter Data, relevant to Energy Theft	In Progress

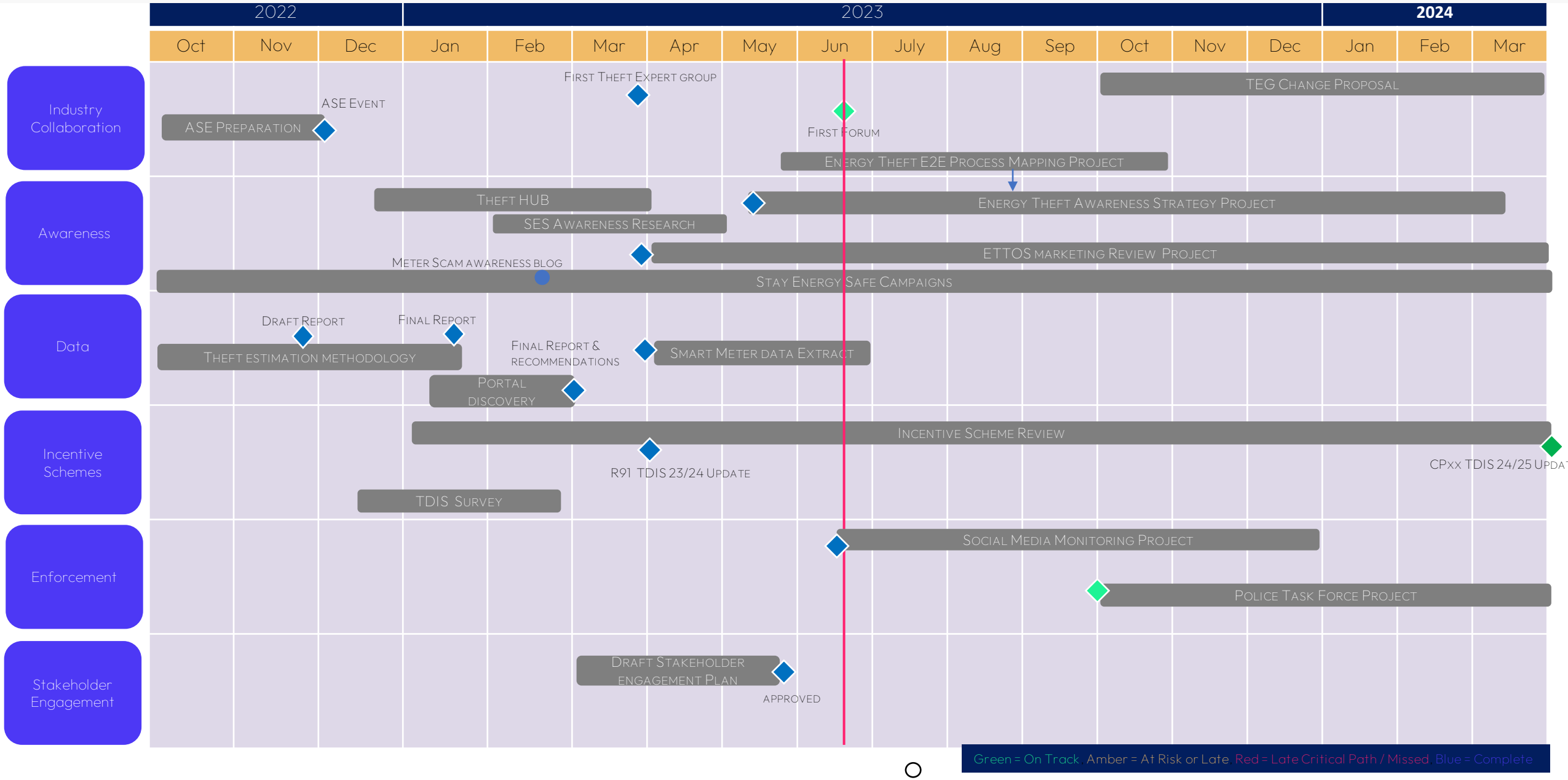
Green = On Track Amber = At Risk or Late, Red = Late Critical Path / Missed Blue = Co

23/24 Theft Programme: Prioritised Epic's Report

Ref	Epic Title	Status
TE013	Review data sources and create business case / approach for Theft Detection System	Not Started
TE014	Engagement with Industry for Data Driven Services for Energy Theft	Not Started
TE016	Back testing of theft detection	Not Started
TE018	Solution Development for Energy Theft Data Portal	In progress
TE020	Empowerment for Parties to Take Action on Energy Theft	Not Started
TE021	Police Engagement and Partnership Feasibility	Not Started
TE022	Improvement To Energy Theft Detection Incentive Scheme	In Progress
TE023	Re-establish Dedicated Theft Expert Group	Complete
TE024	Implement Energy Theft Stakeholder Forum	Complete
TE025	Threat Intelligence/Social Media Monitoring Service	Not Started
TE026	Wider incentives	Not Started
TE027	Amnesty	Not Started

Green = On Track Amber = At Risk or Late, Red = Late Critical Path / Missed Blue = Co

Energy Theft Reduction Programme



The Energy Theft Forum
28 June 2023

The Energy Theft Tip-off Service (ETTOS) and Stay Energy Safe

STAY ENERGY SAFE

CrimeStoppers.
Speak up. Stay safe.

Today's update includes:

- Crimestoppers – our proposition
- The Energy Theft Tip-Off Service (ETTOS)
- Keep In Touch
- Stay Energy Safe – the Comms and Marketing
- The Partner Section
- Success To Date
- Feedback
- Information is Vital

STAY ENERGY SAFE

CrimeStoppers.
Speak up. Stay safe.

CrimeStoppers.

Crimestoppers is an independent charity that gives people the power to speak up, to stop crime. **100% anonymously. Always.**

CrimeStoppers.
Speak up. Stay safe.

Crimestoppers - About Us

Detect

Reduce

Deter

- We take information 24/7, 365 days a year as a charity and for commercial partners
- Over 600,000 contacts are received each year
- We haven't broken our guarantee of anonymity in over 35 years

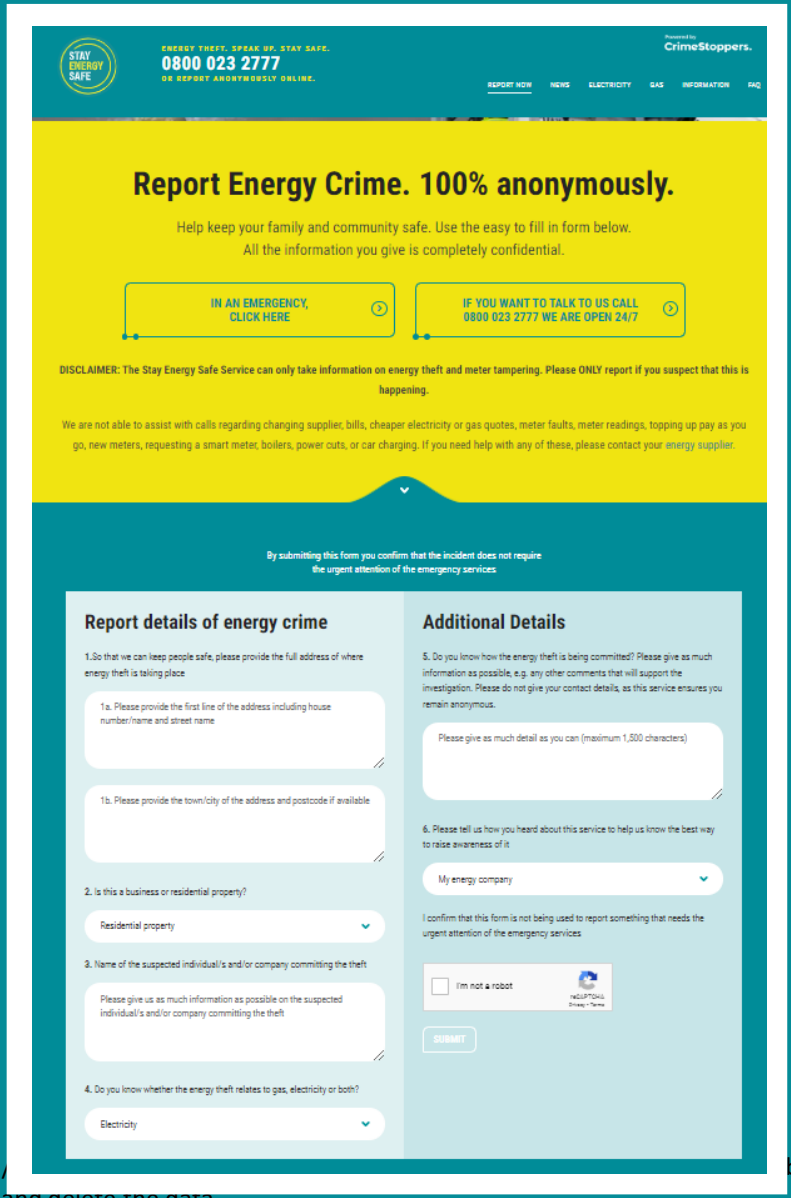
25% of information by phone

vs.

75% from online forms

CrimeStoppers.
Speak up. Stay safe.

The Energy Theft Tip-Off Service – Empowering People



The Energy Theft Tip-Off Service consists of:

- Crimestoppers information sharing
- Dedicated phone number:
  0800 023 2777
- Unique online reporting form:
  stayenergysafe.co.uk/report-energy-crime/
- A specific website:
  stayenergysafe.co.uk

The Energy Theft Tip-Off Service – The Process

Crimestoppers manages the delivery of this service:

- Those with information contact us via the Crimestoppers or Stay Energy Safe forms or by phone
- Upon receipt of the information the Crimestoppers Contact Centre team will
  - Check and sanitise the details – so it can't identify the person giving the information
  - Assess the information – is it actionable?
  - Follow a match process to identify the supplier who should receive it to investigate
  - Disseminate the actionable reports to industry partners securely

STAY ENERGY SAFE

Keep in Touch

When you receive a report that has been generated by a Crimestoppers online form it offers you a keep-in-touch option.

This shows that the contact has opted in to keep in touch with Crimestoppers, 100% anonymously, should our partner/s wish to ask further questions.

When you see this option on the report you can:

- Email CSI@treblefive.org.uk
- Putting the ISR number in the subject line
- Pose questions you wish to ask in the body of the email

You have 14 days in which to do this, and the quicker you ask the questions, the more likely you are to receive a reply. Please note - every time you ask a question, the 14-day response time renews.

STAY ENERGY SAFE

Stay Energy Safe – the Comms and Marketing

- Stay Energy Safe is the public facing brand of the Energy Theft Tip-Off Service.
- Developed to engage with energy customers across the country
- To alert them to the dangers and encourage them to tell the sector when they suspect energy theft is happening.
- The safety of themselves and their loved ones is an important motivation for them to tell us what they know.

Stay Energy Safe – the Comms and Marketing

To support the Energy Theft Tip-Off Service we run ongoing, year-round comms and marketing. The aim of which is:

- To drive reports about suspicions of energy theft .
- To raise awareness of the crime and the severe dangers it poses.
- To deter people from tampering with their meters or energy supply.
- To help people know what to look out for if energy theft is taking place.

Awareness

Education

Deterrent

Identification

STAY ENERGY SAFE

Stay Energy Safe – the Comms and Marketing

We have produced a whole range of assets which are promoted on social media, Google, in media publications, as well as via radio and out of home:

Film:

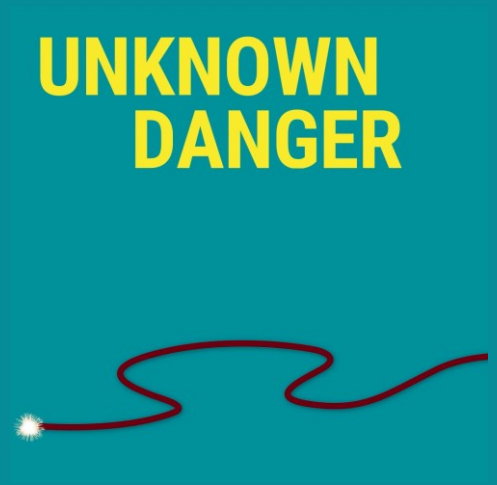
Tick Tock

Unknown Danger

Radio:

Stay Energy Safe – the Comms and Marketing

Social Media:



Stay Energy Safe – Partner Section

We are soon to launch our updated partner section on www.stayenergysafe.co.uk.

The new look partner section aims to provide you with:

- A range of Stay Energy Safe assets.
- The social media schedules.

The new lay out aims to be:

- Easier to use, so you can find what you want more easily.

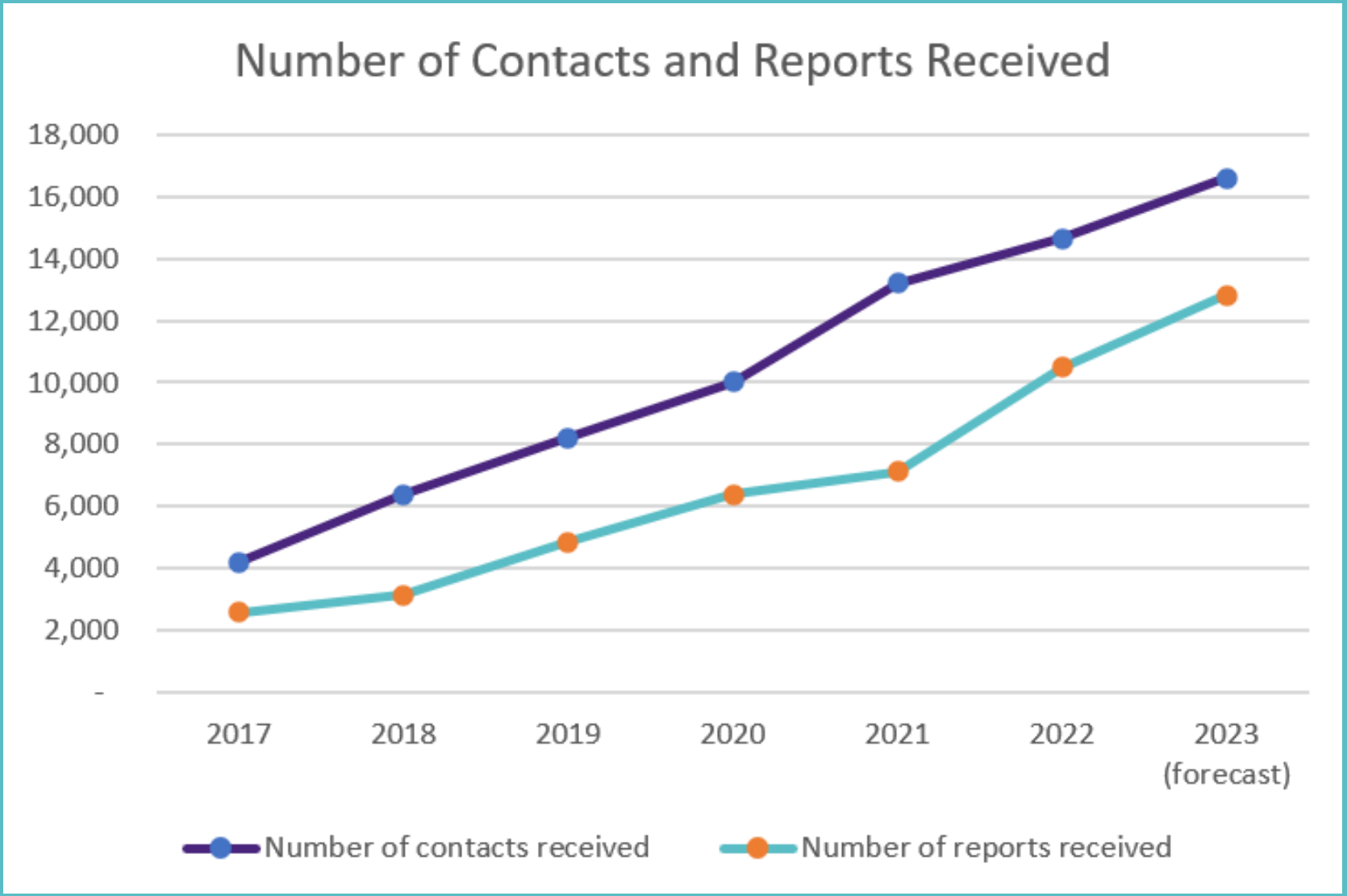
ETTOS Success To Date

Since the launch of the ETTOS in 2016, we have seen a year-on-year growth in reports

Year	Number of contacts received	Number of reports received
2017	4,190	2,566
2018	6,398	3,131
2019	8,212	4,840
2020	10,024	6,376
2021	13,202	7,122
2022	14,639	10,497
2023 (forecast)	16,595	12,806
2023 actual YTD	6,914	5,337

CrimeStoppers.
Speak up. Stay safe.

ETTOS Success To Date



This graph plots the figures shown on the previous slide.

CrimeStoppers.
Speak up. Stay safe.

Feedback

Sharing your stories and successes with us can be really positive. It can help us:

- Educate the public on the dangers of tampering with energy supply.
- Demonstrate how important speaking up is.
- Encourage people who may have doubts about contacting us to get in touch.

You can share positive outcomes by emailing me at annette.booysen@crimestoppers-uk.org

CrimeStoppers.
Speak up. Stay safe.

Information is Vital

By working together to:

- Raise awareness of the issues of energy theft and meter tampering and the dangers they pose.
- Advise individuals what to look out for to identify the crime of energy theft.
- Let people know what information will help in the fight against energy theft.
- Promote the channels through which information can be given (Crimestoppers and Stay Energy Safe)
- Reassure individuals that they will remain 100% anonymous, however they contact us

We can empower people to speak up and stay safe.

CrimeStoppers.
Speak up. Stay safe.

Using Smart Meter Data in Theft Detection

Rosalind Timperley

Overview

Purpose

Work is underway to explore the feasibility of using smart meter data to improve the assumptions and data contained within the Theft Estimation Model (TEM). The intention is to complete back testing on already reported thefts to determine which, if any, smart meter alerts are correlated to instances of energy theft and could be used to better predict and detect energy theft in the future.

Activities completed

- Identified which smart alerts could be relevant to energy theft and have a potential use in analysis
- Engaged with DCC and other market participants to understand data is available and how it might be obtained
- Consultation issued to industry participants to understand the data they are currently using, any issues experienced and any additional datasets that may be of use
- Review of governance documentation to understand the path for RECCo gaining smart meter data on an enduring basis (subject to the findings of the back test)

Summary Findings

Data Availability

- Historic data from the DCC is available at MPxN level however DCC are not able to share it with RECCo without additional authorisation. This needs to be provided either by individual organisations (suppliers / DNOs) or by Ofgem for market wide information
- Discussions were held with three REC Parties and it was confirmed that historic data is available and could potentially be shared at the required granularity. Data Privacy Impact Assessments (DPIAs) need to be completed with relevant sharing agreements in place before any data is shared

Understanding of Smart Meter Alerts

- The full list of smart alerts was reviewed with a number highlighted as potentially useful for analysis

Event / Alert Code	Alert Name
0x81A1	Battery Cover Closed
0x81B8	Incorrect Polarity
0x8F36	Supply Outage Restored - Outage >= 3 minutes
0x8F74	Unauthorised Physical Access - Meter Cover Removed
0x8F76	Unauthorised Physical Access - Terminal Cover Removed
0x81AC	Error Measurement Fault
0x81A3	CH Disconnected from ESME

Summary Findings

Consultation summary

- A total of 13 responses received – 8 suppliers, 5 DNOs / Gas Transporters
- Suppliers and DNOs/Gas Transporters do not have access to all of the same alert types leading to approaches to theft management which can differ.
- DNOs would benefit from the ability to view consumption on an MPAN-by-MPAN basis and would be able to make improvements in their theft management activities if this was to be made available.
- Using smart alerts is a manual, time consuming process due to the "false positives" needing to be filtered out
- There is a lack of clarity across the industry regarding the trigger for many alert types which is hampering theft management activities, and, in some cases, these alert types are not used.
- Using smart alerts on their own does not provide a reliable indicator of energy theft due to the large volume and spurious nature of why some alerts are generated. Additional dataflow and other property and consumption information is required.

Summary Findings

Examples of spurious alerts

- *Strong Magnetic Field Removed – One meter generated more than 3,000 of this type of alert over approximately one week. A site visit was conducted which determined the alert was being caused by the magnets holding the meter box cupboard closed.*
- *Tamper alert – One meter that generated a large number of this alert which, after investigation were determined to be triggered when a nearby light was turned on*
- *Meters from one manufacturer generating a significant volume of tamper alerts. Of the 13m of this type received in 2022, by one respondent 90% (c.11.5m) were from the meters made by a single manufacturer*

Local Catalogue Reference	Market Message Name
D0001	Request Metering System Investigation
D0002	Fault Resolution Report or Request for Decision on Further Action
D0136	Report to Supplier of Possible Irregularity
D0139	Confirmation or Rejection of Energisation Status Change
MIO	Meter Inspection Response
ONJOB	Notification of Metering Job (ONJOB)
SFN	Site Visit and Fault Notification

Next steps

Based on the findings of the work, RECCo intend to proceed with data requests to obtain historic smart meter alert data to conduct back testing and analysis. Three REC Parties and Smart DCC have been engaged with.

The following additional actions have also been noted as part of the work:

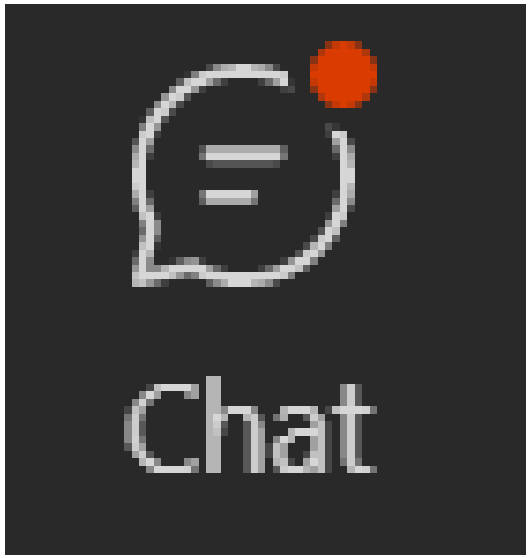
- Engage with organisations to discuss the approach for gaining access to dataflow information to complement the smart meter alert data
- Engage with SECAS regarding the feasibility to develop additional educational material related to smart meter alerts including the scenarios when alerts will be generated and clarification on the meaning of alerts

Action points for attendees: if your organisation could potentially share Smart Meter Data with RECCo for its back test (subject to the appropriate GDPR controls) please let us know via TechnicalEnquiries@recmanager.co.uk

Q&A Session 1

Q&A Session

Please use Teams to raise your hand, or type your questions in the meeting chat



Break: 5 Minutes

Police Engagement

Rebecca Lowe

Engaging with Police

In previous discussion forums such as the Nov 22 Energy Theft ASE workshop and UKRPA sessions the issue of police engagement and support has often been raised.

RECCo want to work collaboratively to empower parties to take action and understand gaps and obstacles in processes with an aim to improve areas which may not currently be working as well as they could, for REC Parties and Police Forces.

Superintendent Patrick Holdaway from the City of London Police and leader of the National Business Crime Centre (NBCC) is also on the call with us today.

Focus on 4 areas today:

- Information Exchange
- Warrant Execution Support
- Prosecutions
- Processes & Guidance

Engaging with Police

Information Exchange

- What do REC Parties share with the Police
  - Is information shared when the police request it?
  - Is information that may be useful to the police shared proactively?
- What do the Police share with REC Parties
  - Do REC Parties get the information they would like?
  - Can they get the information when they need it?
- What mechanisms are used for sharing
  - Is it the same nationwide or different for each police force?
  - Is it the same for each Supplier/Network Party?
  - Could there be a better and more consistent way to share information?

Share your views….

Poll: Are you able to get the information you need from the police to facilitate your Energy Theft Investigations?

1. Yes, I'm normally able to get the info I need.
2. Yes, but it takes a long time, or I only get partial info.
3. Yes, but I'm being asked to pay a fee.
4. Sometimes, depends on which police force or the individual.
5. No, in most instances I'm unable to get the info I need.

Engaging with Police

Warrant Execution Support

- What is the process to request police support
  - Is it the same nationwide or different for each area force?
  - Does the process work?
- Is police support on warrants available fit for purpose when necessary
  - What will the police do to support warrant execution?
  - What can't the police do – are expectations realistic?
  - How often is support unavailable when needed?
  - What are the consequences of support being unavailable?
  - If support is not given is this due to resourcing issues or lack of knowledge and awareness?
  - Is enough guidance available - to police and REC Parties?

Share your views….

Poll: Are you able to get police support when needed for Energy Theft Warrant Executions?

1. Yes, normally not an issue.
2. Sometimes, depends on when and where.
3. Partly, can get police attendance but not supportive when onsite.
4. No, struggle to get support.

Engaging with Police

Prosecutions

- REC Parties completing witness statements
  - Are they provided to the required standard?
  - Are they only requested when needed or too frequently?
- REC Parties collecting and retaining evidence
  - Do investigations carried out by REC Parties obtain the right information and data?
  - Is adequate physical and photographic evidence being collected to support charges/prosecutions?
  - Is it being logged and stored adequately?
  - Is it available if requested by the police/CPS?
- Are enough cases of Energy Theft proceeding to prosecution
  - Are enough cases suitable for prosecution being reported to the police?
  - Are the CPS willing to proceed?
  - Are cases that do proceed successful?
  - Is there adequate reporting of successful prosecutions of Energy Theft?

Share your views....

Poll: What is your view on prosecutions for Energy Theft?

1. We do not actively seek prosecution – up to the Police and CPS/COPFS
2. We seek prosecution but cases are often not progressed by CPS/COPFS
3. We seek prosecution and cases normally progress but are unsuccessful
4. We seek prosecution and cases are normally successful

Engaging with Police

Processes & Guidance

- Are there any defined processes for different touchpoints with the police during the life of an Energy Theft investigation.
- Do the Police have guidance documents
  - Are they regional or nationwide?
  - Are they up to date?
  - Are they widely used?
- Does the industry have the guidance documents they need.
  - Who owns any guidance documents?
  - Are they complete and up to date?
  - Are they used?

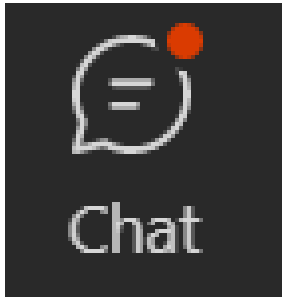
Share your views….

Poll: Are there clear processes and guidance for engagement between REC Parties and the police?

1. Yes, no additional process info and guidance is needed.
2. Some process info and guidance available but more is needed.
3. No, process info and guidance is insufficient or does not exist.

Share your views....

Ideas and Solutions What ideas and solutions do people have to address the areas discussed, please raise your hand or add to chat, add a like reaction to anything you agree with.



Information Exchange

Warrant Execution Support

Prosecutions

Processes &Guidance

Improving Data Collection and Reporting

Lynne Fallon

Current Theft Data submissions

The purpose of current submissions is limited to:

- A Supplier Party's inclusion in the Energy Theft Detection Incentive Scheme
- Compliance with REC Theft Reduction Schedule (Sch 7, Annex 3)
- Consideration when developing the Theft Estimation Methodology

Submissions should be all suspected tampering & theft investigations:

- Desktop exercises where the need for further investigation is ruled out
- Open investigations
- Completed investigations with an unconfirmed or no theft outcome
- Completed investigations with a confirmed theft and/or tampering outcome

Combination of mandatory, conditional and optional items based on investigation status:

Lack of clarity or purpose with some of the data items required:-

- Account holder – they are the beneficiary but no confirmation they are the perpetrator
- Meter serial number – which one if the meter has been illegally replaced?
- Does anyone fit security devices anymore?

Current TDIS data items

Residential and Commercial data items		Additional Commercial data items	
Supply MPxN Supply address incl Postcode Record Type **Meter** Meter serial number **Supplier Account** Account Number Account holder's name Account holder's DoB Billing Address	**Investigation Outcome** Supplier Investigation ID Theft Lead Source Date investigation closed Current Investigation code Type of Theft Crime Reference No Assessed start date for Theft Assessed end date for Theft Assessed losses Tampering code Tampering report date Tampering report source Security devices fitted	**Additional Supplier Information** Supplier's Customer Number Customer Name Customer Company Registration Number "Trading As" Company Name Customer Address Customer Postcode Customer email address Customer Telephone Number Supplier's Account Number	Account holder's name Account holders Date of birth Billing Company Name Billing Company Registration Number "Trading As" Account Company Name Billing Address Billing Postcode

Additional theft data requirements

Funded Prosecutions Unit

-Details of the perpetrator or enabler

-Development of a risk scoring mechanism for prioritisation,

    -eg. impact or potential impact on others

-Comprehensive details where there is an abuse of a position of trust

Lead Generation

-Public domain data, eg. Indices of Multiple Deprivation;

-Business Types & food hygiene ratings

-Smart data – tamper alerts combined with consumption data

-Network data – eg. requests for service upgrades not progressed

Health & Safety

-Information to safeguard Industry operatives eg. Threats; assaults; injuries dealing with tampered installations etc.

-Incidences of fires, explosions or personal injury to consumers or other members of the public as a result of tampering

Additional theft data requirements

Theft Estimation Methodology

- Network data (Individual Secondary Substation or Local Area throughput); technical losses
- Supplier smart data (tamper alerts and consumption)
- Business types and food hygiene ratings
- Theft in conveyance data

Theft Trend Analysis

- Repeat offender indicators
- Consumer Switching activity following 'suspected but not confirmed' or 'confirmed theft' outcome
- Home/business mover information following 'suspected bit not confirmed' or 'confirmed theft' outcomes

Share your views….

Poll – What are your priorities for potential additional data requirements?

Rank in order of priority:

1. Funded Energy Theft Prosecutions Unit
2. Lead Generation
3. Reporting of Health & Safety information for RP Operative Safety
4. Reporting of Health & Safety information for Public Safety
5. Revision of the Theft Estimation Methodology
6. Theft trend analysis
7. All equally important

Engagement with Water Companies

Shamil Udayar

In the News

New Power

Expert information for all those invested in the UK's energy future

In one incident, an energy supplier was called in by police to help investigate a restaurant that was still trading, despite having had its electricity cut off since 2013. It was found that five other properties owned by the same person had recently been raided, revealing a number of dangerous activities:

- An illegal fuse carrier had been attached to an electricity meter with crocodile clips – resulting in a burnt meter box.
- A gas meter had been illegally removed, which resulted in the restaurant being evacuated and secured.
- A water valve had been installed in the ground to illegally divert the supply; and
- A gas flue had been redirected to the inside of the building – which meant that everyone inside had been in serious danger of carbon monoxide poisoning.

The restaurant was shut down, and the police arrested the restaurant owner for energy theft and other offences, including possession of stolen goods and growing cannabis.

jetcool

How Water Cooling is Driving Sustainability in Mining Farms

Liquid cooling is increasingly seen as the way of the future for bitcoin mining. The benefits of liquid cooling are clear: it helps extend device lifetime, improves performance, and offers a much higher energy-efficiency to power ratio than air cooling. Moreover, it can allow miners to pack more rigs into a smaller space, which is crucial as mining farms grow.

Today's most prevalent liquid cooling solution in the mining community is immersion cooling. This method works by submerging the entire mining rig in dielectric oil. The oil dissipates heat away from the sensitive components, and the rig is cooled without any external fans. Immersion cooling has its drawbacks; it's more expensive than most other efficient cooling alternatives, can be challenging to deploy at scale, and when miners inevitably require maintenance, it takes time to clean off the oil.

Another form of liquid cooling that has gained traction in the bitcoin mining community is water cooling. Water cooling enables miners to adopt liquid cooling in an air-cooled form factor, creating high-density deployments and scaling better than immersion cooling.

Technology

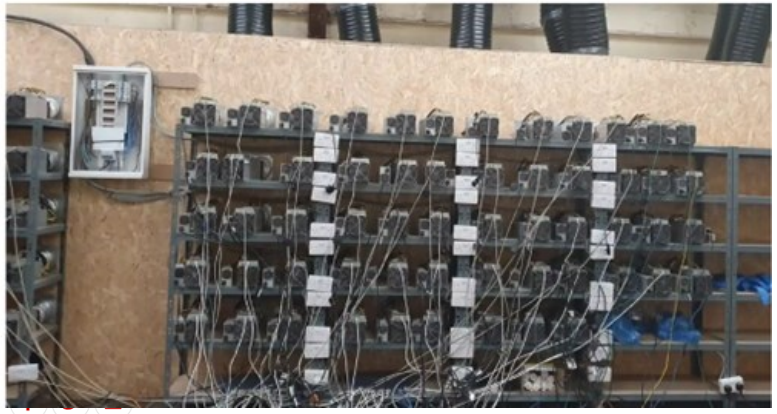
Bitmain Says New Liquid Cooling Miner Is its Most Power-Efficient Model to Date

The world's biggest manufacturer of crypto mining rigs, Bitmain, released a new liquid cooling mining rig which boasts the best power efficiency among all of the firm's models.

- The new Antminer S19 XP Hyd. boasts 255 terahash/second (TH/s) of computing power at 20.8 joules per terahash (J/T) of power efficiency, running on 5,304 watts, according to Bitmain's website. They cost just under $20,000 per unit and will ship in the first quarter of 2023, according to the site.
- Its energy efficiency narrowly beats Bitmain's previous best, the Antminer S19 XP, which brings up to 140 TH/s at 21.5 J/T at $11,620, and competitor MicroBT's Whatsminer M30S++, which delivers 112 TH/s at an efficiency of 31 J/TH.
- The hydro cooling rigs are designed to be used in Bitmain's own containers. Liquid cooling is a method of using a liquid, such as coolant going through pipes, to release heat from the machine.
- The firm also announced a new container, dubbed the ANTSPACE HK3, which fits 210 mining machines and consumes 1 megawatt of power.

Police find bitcoin mine using stolen electricity in West Midlands

Officers expected to discover a cannabis farm when they raided building on industrial estate



Police have discovered a cryptocurrency operation that used stolen electricity to mine bitcoin in the West Midlands.

Officers from West Midlands police raided a building in an industrial estate on 18 May expecting to find a cannabis farm, but instead stumbled upon the cryptocurrency scheme. No arrests have been made.

Users gain bitcoin and some other cryptocurrencies through "mining", a process in which computers solve complex mathematical puzzles. Those puzzles have by design become more difficult as more bitcoin has been awarded to users, meaning more powerful computers and significantly more energy are needed to make mining worthwhile.

However, it can be lucrative. A single bitcoin was worth $36,392 (£25,732) on Friday afternoon. That was below its all-time high above $64,800 but about five times its value at the start of 2020.

Water, Energy Theft and Cryptocurrency

- Is there potential opportunity to work together with water companies to understand the site profiles based on their usage of water – sites with high water usage are likely to have high energy usage?

- There have been several cases reported via Crimestoppers that sites where there's been energy theft, the water was also on bypass.

- The identification of energy theft in the commercial segment has been difficult and from the very little data available on Water meter tampering, we can say that water meter tampering/bypass exists in the commercial segment.

Water, Energy Theft and Cryptocurrency

- Cryptocurrency Mining is known for it's high energy consumption, the cases identified by police forces have found mines using stolen electricity. The latest cryptocurrency mines are set up with water cooling systems
- Can water companies identify abnormal water usage in sites or areas? Can the data of these sites be used by energy suppliers and networks to investigate energy theft?
- Could a framework be established to facilitate energy suppliers and networks sharing data of confirmed cases of energy theft, so water companies can investigate for water meter tampering and vice versa?

Share your views….

Poll: Do you feel that there would be value in RECCo exploring opportunities to work with water companies as part of its Theft Reduction Strategy?

1. Yes
2. No
3. Unsure

Poll: What areas should RECCo focus on?

1. Sharing data on investigations between water and energy companies
2. Identification of properties with higher than expected water usage
3. Other (add to meeting chat)

Does your organisation already work with water companies on theft reduction initiatives? Please put your hand up to share what you have been doing?

Or you can email us after the event via TechnicalEnquiries@recmanager.co.uk

Third Party (after the meter) Theft and Demand Side Response

Rosalind Timperley

Third Party Theft

Industry arrangements focus on tackling theft in conveyance (upstream of the meter) or interference with the register of consumption on meter.

We are aware of instances of theft that are not clearly captured by current arrangements, i.e., theft by a neighbour or other third-party downstream of the meter.

Whilst the scale of this problem is not currently known, we consider that this could appropriately be within scope of the Theft Reduction Strategy as:

- Crimestoppers receive reports of third-party theft and these should be dealt with and forwarded appropriately;
- Cases are occasionally referred to the energy ombudsman, whose decisions can impact upon suppliers despite there being a lack of clear responsibilities;
- Greater clarity will be of benefit to industry parties and the consumers who are impacted; and,
- We consider that market developments may provide greater opportunities for theft and fraud that could be mitigated early.

Third Party Theft and Demand Side Response

Demand Side Response

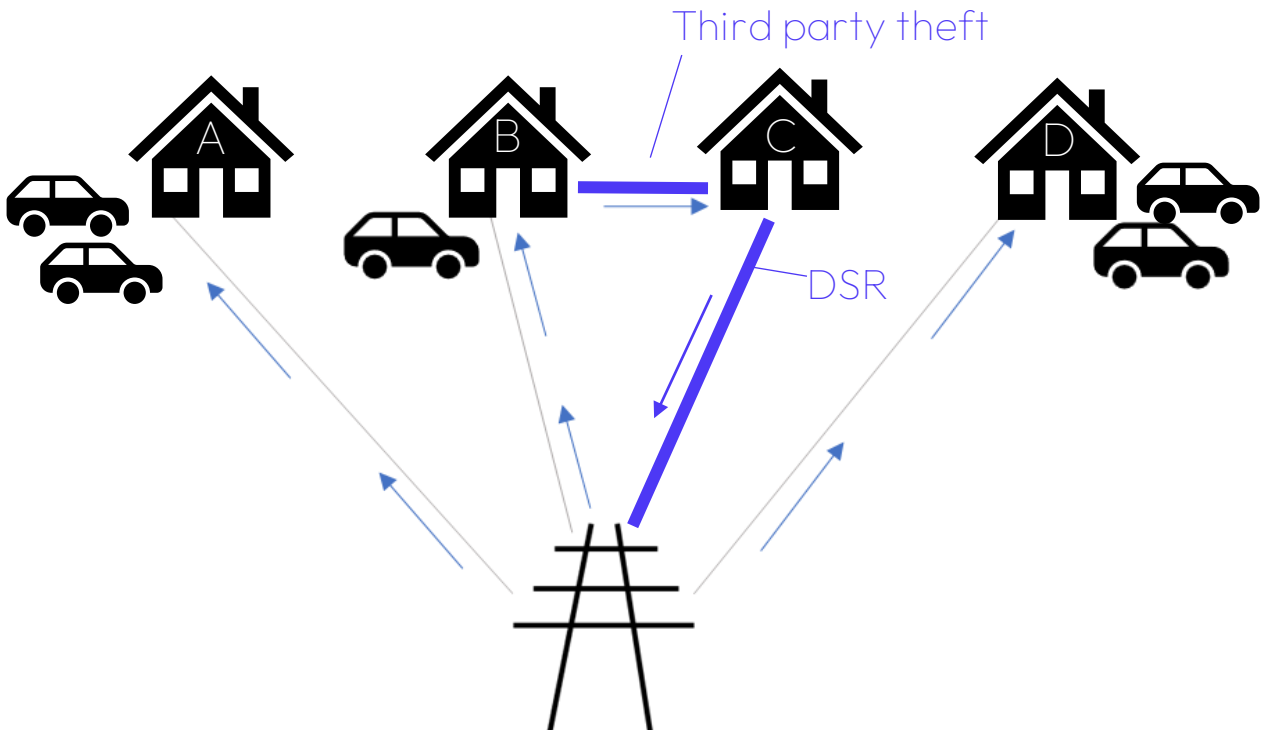
Demand side response (DSR) involves using financial incentives to encourage system users to change their energy usage to help balance the system.

Advances in technology are opening up new potential opportunities for households and businesses to get involved in Demand Side Response, including:

- Smart appliances
- Electric Vehicle charging and also discharging to the grid
- Home battery storage

Energy Theft Risks

As demand side response schemes evolve, there is a risk that new opportunities and greater financial incentives for theft/fraud may also evolve



As the energy is coming via third party theft, there are no current REC provisions which address this type of scenario.

How Can the Risks be Mitigated?

There are various options that could be explored, including:

- Could new guidance and/or obligations for REC Parties and/or non-REC Parties mitigate the risks? (For example, guidance to suppliers on best practice where third-party theft is suspected)

- What future data sets would be required to monitor these type of energy theft? (For example, could instances of third-party theft be reported via the Theft Detection Incentive Scheme data submissions?)

- What regulation and/or system changes would reduce the risk of these types of theft occurring? (For example, for DSR related theft meter and asset level mapping that ensures that DSR energy fed on to the system cannot exceed the stated capacity of the EVs/batteries/micro-generation registered to the property)?

Share your views....

Poll: Have you ever encountered third party or DSR related Theft?

1. Yes, third party theft
2. Yes, DSR related theft
3. Yes, both
4. No, I have not encountered either
5. Unsure/Not applicable

Poll: Do you feel third party theft should be within scope of the Theft Reduction Strategy?

1. Yes
2. No
3. Unsure

Poll: Do you feel DSR related theft is an emerging risk that should be within scope of the Theft Reduction Strategy?

1. Yes
2. No
3. Unsure

Open question: Do you believe there are any other future theft risks that should be considered under RECCo's Theft Strategy?

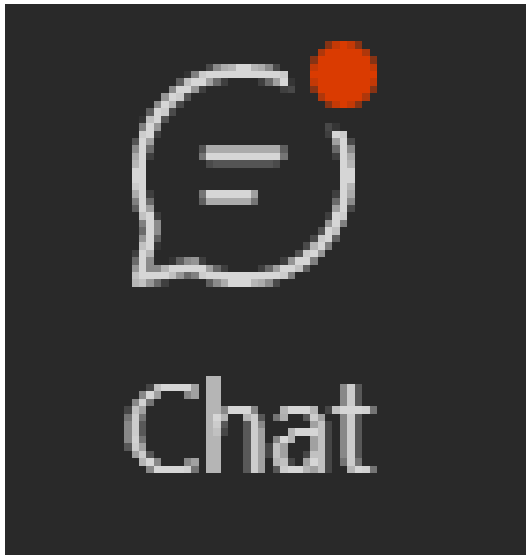
Please raise your hand or add to chat.

Add a like reaction to anything you agree with.

Q&A Session 2

Q&A Session

Please use Teams to raise your hand, or type your questions in the meeting chat



Thank you for Attending

If you have a discussion topic for the next forum, email us at TechnicalEnquiries@recmanager.co.uk