Welcome to this week's edition of Defuse News

A weekly briefing for people whose profile attracts attention.

Threats, and the money that follows them

A threat arrives by email, through a social media account, or in an envelope posted to the office. Or nothing arrives at all and the threat is identified for you, by a monitoring provider, a contact in the police, or a member of staff repeating something they overheard.

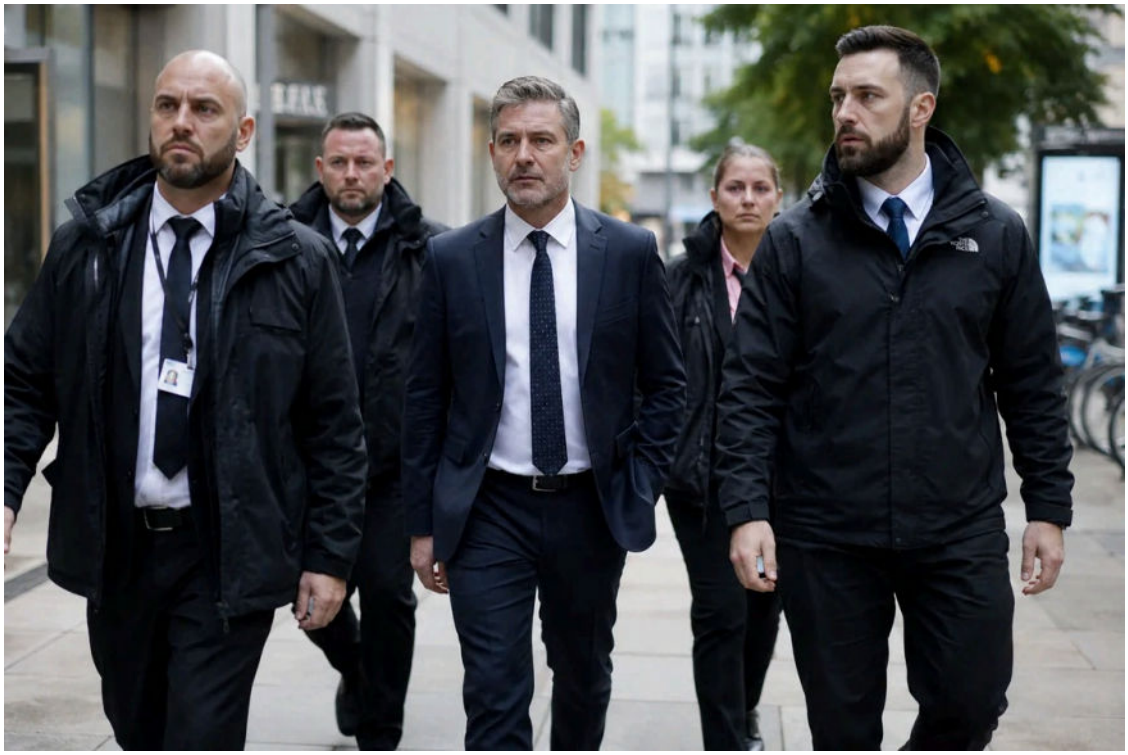
Identified is not the same as assessed.

What usually follows is a fast response to the warning itself:

- a close protection team within a day or two
- residential guarding at the home
- a curtailed diary

Costs that would need a board paper anywhere else get approved on a phone call, because nobody argues about money on the day a threat lands. The assessment, if it happens, comes later.

A good deal of wasted spend starts with three terms being used interchangeably, so it is worth taking them in order.



📐 Threat, vulnerability and risk

THREAT = INTENT + CAPABILITY

You need both, and neither is ever assumed. Somebody in another hemisphere sending messages at three in the morning may have intent, though that still has to be established, but has no realistic means of reaching anybody. Reverse it, and a neighbour with a shotgun certificate and a boundary grievance already has all the capability they need. Whether they have the intent is the whole question, and it is answered by what they do rather than what they say.

VULNERABILITY

The gaps somebody could use, which shift with circumstance. A family is more exposed in the week a magazine features the house, or when the school run follows the same route every day of term. It is the only one of the three that can be reduced directly.

RISK = LIKELIHOOD + IMPACT

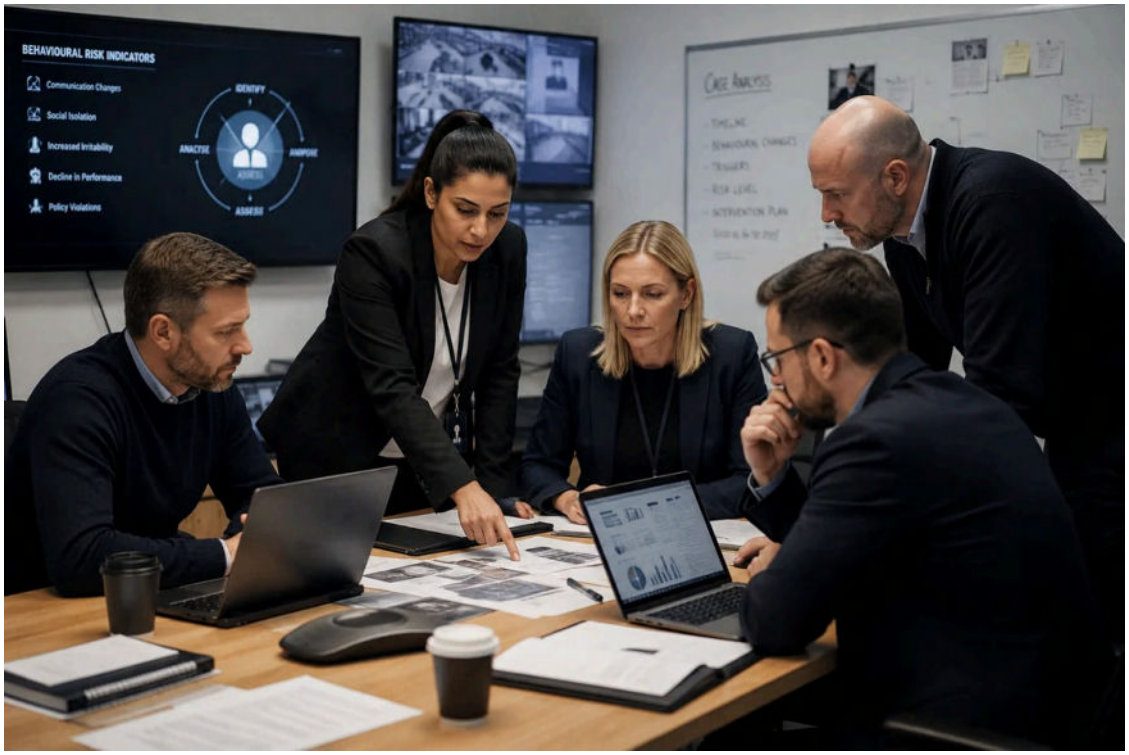
Likelihood is the probability that the harmful event happens. Impact is how severe it would be. Together they tell you how much to worry and where to spend.

Likelihood is not one figure lifted from one place. It draws on:

- how far along the pathway the person appears to be
- what they are capable of
- what they could reach, and how easily

- what is already in place to stop them
- what is coming up that might act as a trigger

A risk assessment is only ever as sound as the threat assessment feeding it.



🔍 Assessing the threat

The research into people who have attacked public figures, including the work that shaped US Secret Service practice, runs against instinct. Those who send direct threats very rarely attack, and those who do attack rarely announce it first. They leak their intentions, though usually to somebody else. The warning exists; it just does not arrive in the letterbox with a signature on it.

Calhoun and Weston gave us the shorthand:

- **Howlers** write, post and telephone, sometimes for years, and seldom attack
- **Hunters** plan, and go quiet while they do it

A communicated threat is a weak indicator on its own, whatever its wording.
That is also the limit of the phrase 'credible threat'. It describes a statement showing intent to cause harm and the apparent means to do it, specific enough about time, method or place to frighten a reasonable person. It is a judgement about the statement, not about the person, and it says nothing about whether the sender is moving toward violence.

Behavioural threat assessment and management, or BTAM, is the science-based method built for that question, and the one I was trained in by the architect of the US Secret Service methodology for assessing targeted attacks.

People who attack a chosen target rarely snap. They move along a pathway that leaves traces: a grievance hardens into a fixation, the fixation narrows until the target seems to explain everything wrong in that person's life, and then come the research, the approach and the means.

So the assessment looks for change, and for what drives it. Behaviour that has shifted since last month, and the events that tend to shift it: a job lost, a hearing date, a refusal, an anniversary.

- Have they gone looking for an address?
- Have they turned up somewhere they had no reason to be?
- Have they acquired something they did not have before?

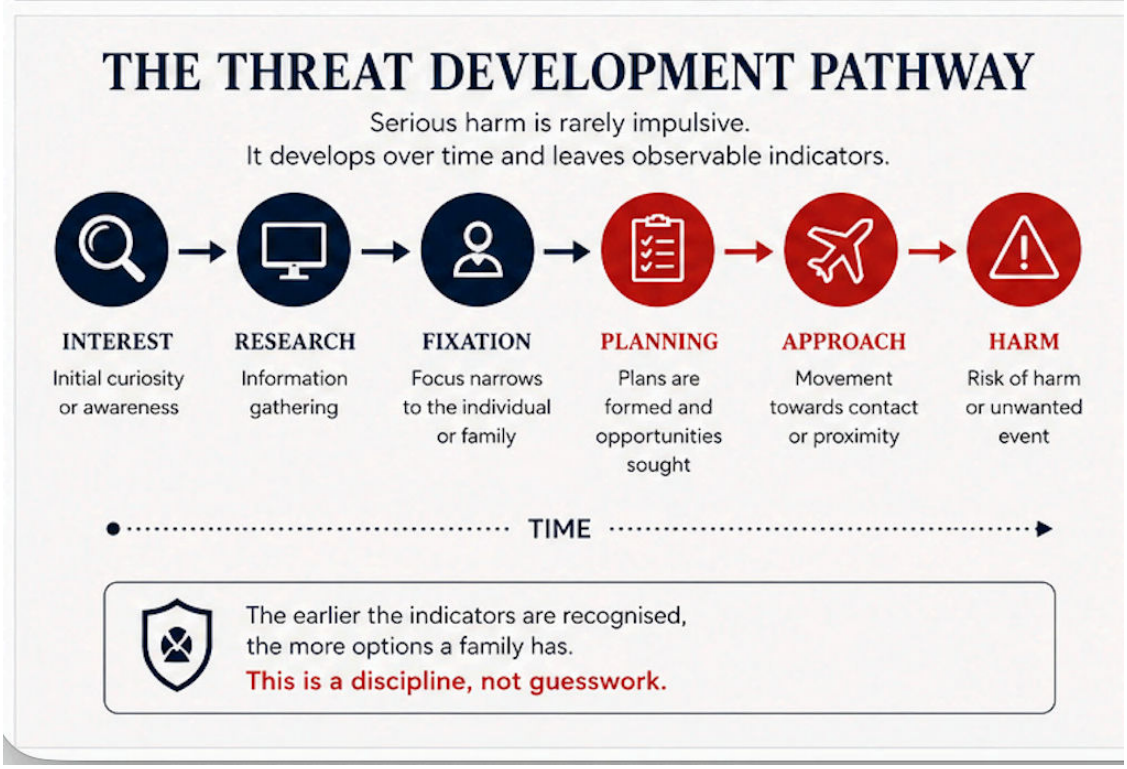
None of this needs a name attached to be useful. An anonymous message is still evidence, and usually the only evidence available on day one. The same applies to intelligence: that somebody has been making remarks about the principal is a starting point, not a finding. Identifying the sender matters and should run alongside, but it takes time the family does not have.

🛡️ Reducing the vulnerability

Start with a digital exposure assessment, because that is where most openings now sit and nothing can be closed until it is found. Protective security then works in layers, and not all of them are physical.

- **Physical**: fences and cameras deter, detect and delay
- **Procedural**: who holds access, and how callers are verified
- **Information**: what is discoverable about the family online

A vulnerability assessment is a photograph rather than a film. It is accurate on the day and out of date by the next house move, company filing or magazine feature. Monitoring is what keeps pace with the exposure, and what picks up pre-attack indicators while there is still time to act on them.



💷 Where the money goes

Security is one of the few lines of spend in a family office that is rarely tested for value, and three patterns recur.

Spend goes to the innermost layer. A protection team is the last line rather than the first, and by the time it engages, everything further out has already failed. There is no shortage of examples of public figures attacked with a detail alongside them, and in this country those officers are unarmed as well.

Spend never stops. A team goes on during a difficult month and is still there years later, because the situation was never reassessed.

Spend is withheld on a misreading. The family is told there is no credible threat, hears that everything is fine, and a fixated individual who has never written a word carries on unexamined.

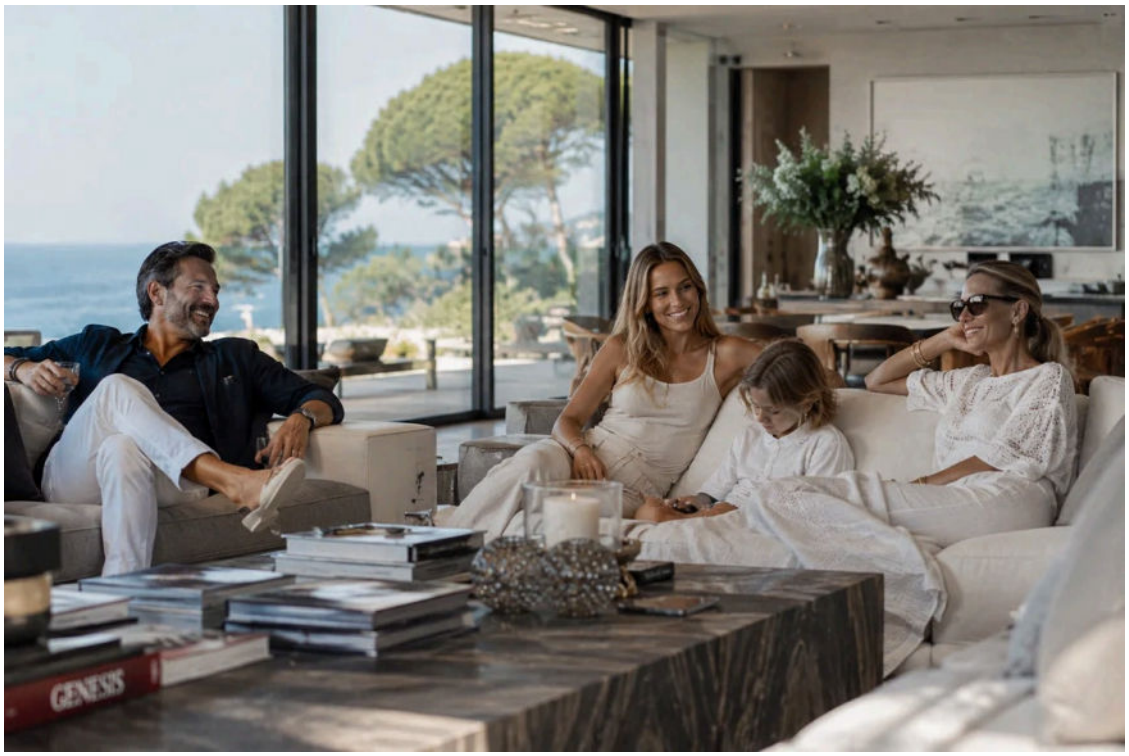
Independence guards against all three. Where the same provider assesses the threat and supplies the response, confirmation bias tends to shape the recommendation, and a team already in place will rarely conclude it should stand itself down. An assessment from somebody with no stake in what gets bought costs a fraction of the response, and it is the part of the process that establishes whether the rest is needed.

✅ The order of work

- **Assess the threat**
- **Map the gaps** that could realistically be used against it
- **Spend** against whatever harm is left

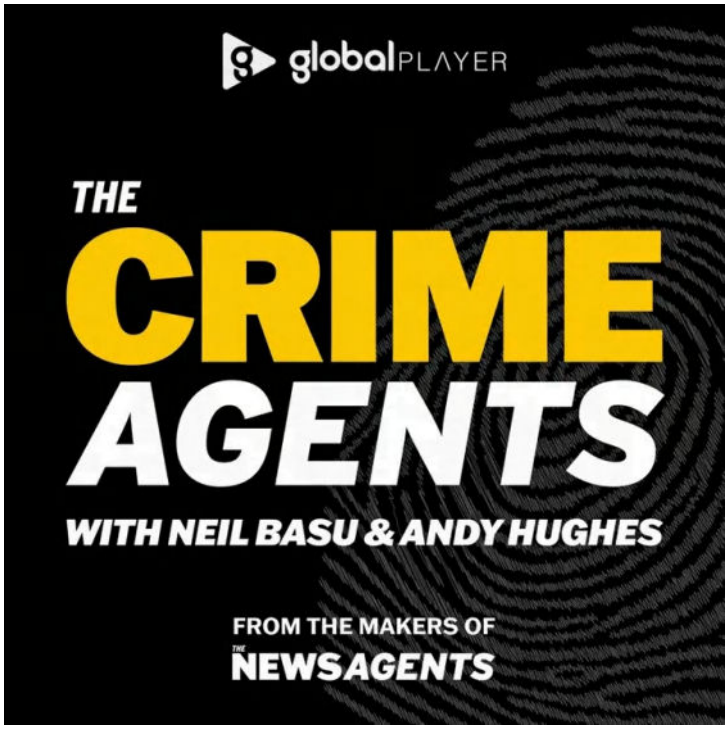
Clients do not want to feel guarded. They want to feel safer, and those two pull in opposite directions unless the assessment comes first.

If a threat has landed and you are unsure whether the response on the table is proportionate, speak to a specialist.



Being wealthy does not make you vulnerable. Being easy to find does.

Be hard to find. Even harder to target.



🎙️ New episode: The Crime Agents, with Neil Basu, Andy Hughes and me on threats to public figures.

Neil was my boss at Scotland Yard. After Jo Cox was murdered, he asked me to go into Parliament and set up and run The Parliamentary Liaison and Investigation Team.

We covered a lot of ground.

🔷 What separates the people who make threats from the people who carry them out.

🔷 Why most of the abuse aimed at public figures never becomes anything, and why that makes the rest harder to spot rather than easier.

🔷 What happens to someone when the protection ends and the profile does not.

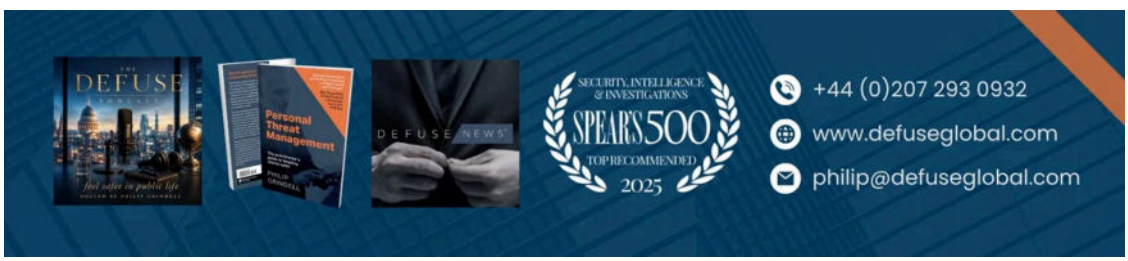
🎧 The episode is out on Monday.

The Crime Agents comes from Global, the team behind The News Agents, and it is on Apple, Spotify, YouTube and the usual platforms.

🛡️ If you look after someone with a public profile, a principal, a client or a family member, it is worth an hour of your time.

📈 The wealth arrived before the security awareness did.

Click here to download



If anything in this newsletter has caused you to think, you may benefit from our help.

Contact us at info@defuseglobal.com

Defuse Ltd, 124 City Road, Old Street, London EC1V 2NX, United Kingdom, +44 02072930932