Doron Levy

Security Consultant & Criminologist

PQCT Department · ICTS Europe

Criminologist and internationally recognised security expert with over 25 years of experience in aviation security, crisis management, and high-risk threat assessment. Accredited by the DGAC (French Civil Aviation Authority), holding the INHESJ title of Expert in Corporate Security & Economic Intelligence (Master Level I), and AVSEC-qualified by ENAC. A trusted advisor to governments, law enforcement agencies, and Fortune-500 organisations across Europe and internationally — combining strategic intelligence, operational depth, and academic rigour. Doron Levy is based in France, working within ICTS Europe's PQCT (Professional Quality, Compliance & Training) department. Doron brings a rare combination of operational depth and academic rigour to the organisation. He is also a published author — his latest book, on human error in data centres, is due out this September.

EXPERIENCE	FOCUS	NEXT BOOK
25+ years	**Quality, Compliance & Training**	**September 2026**

Q1 You've been with ICTS Europe for several years now — what drew you to the company, and how has your role evolved since you joined?

What drew me to ICTS was the breadth of what the company actually does. Very few organisations in our sector operate simultaneously across aviation security, corporate consulting, training, and compliance at a genuinely pan-European scale. For someone with my background — which straddles criminology, security operations, and training — that breadth matters. I didn't want to end up siloed.

My role has evolved considerably. I came in with a strong consulting and audit focus, but over time the training dimension has become increasingly central. Today, within the PQCT department, I'm involved in everything from quality audit programmes for major contracts to designing and delivering Train the Trainer programmes. The AWS engagement is a good example — we built an entire TTT framework from scratch, covering ethics, operational reporting, communication skills, and cyber-physical convergence. That's a long way from a single-site security review.

Q2 Your career spans corporate security consulting, university lecturing, and published authorship — how does someone end up doing all three at once?

Honestly, one thing leads to another, and then one day you look up and realise you've built something you couldn't have planned from the start. I trained as a criminologist — that gives you a particular way of reading situations, understanding behaviour, and constructing analytical frameworks. When you apply that lens to security operations, you start seeing things that pure technical training sometimes misses: the human dynamics, the organisational culture, the gap between written procedure and lived practice.

The lecturing came naturally from that — universities in France were interested in the practitioner-academic profile, someone who could bring real cases into the classroom. And the books came from the conviction that certain knowledge was being generated in the field and not being written down in a form that professionals could actually use. Co-authoring with Xavier Raufer and Christophe Naudin on subjects like robbery, hostage crises, and now data centre security has been one of the most intellectually demanding things I've done — and one of the most satisfying.

Q3 Not many security professionals write books on the side. What made you want to commit expertise to print, and what is the main challenge you face when doing this?

The impulse is simple: books force rigour. A conversation, a training session, even a well-structured report — you can hedge, qualify, update. A book is a commitment. You're saying: this is what I understand to be true, to the best of my knowledge, as of today. That discipline is uncomfortable, but it sharpens everything.

The main challenge is time — specifically, the absence of it. Security consulting doesn't have quiet seasons. Writing a serious work of this kind means research, structured drafting, peer review, revision — often done in early mornings, weekends, and the margins of client travel. The second challenge is translation: converting operational knowledge into something a reader who wasn't in the room can fully understand. Jargon is the enemy of that. Every time I write something I wouldn't say to a non-specialist, I delete it.

Q4 Your upcoming book focuses on human error in data centres. Without giving too much away — what's the central argument, and what surprised you most in your research?

The central argument is that data centres are among the most critical and least humanly understood infrastructures in the modern economy — and that their vulnerability is primarily not technical, it's behavioural. We have invested massively in redundancy, in physical hardening, in cybersecurity architecture. But we have dramatically underinvested in understanding what happens when a fatigued technician makes a wrong call at 3am, or when a team normalises a deviation because it has never yet caused a problem. The Swiss Cheese Model is a useful framework here — single failures rarely bring systems down; it's the alignment of multiple human and organisational gaps that creates catastrophe.

What surprised me most? The degree to which major, well-documented incidents — OVH Strasbourg, AWS US-EAST-1, SK C&C in Korea — could be traced back not to equipment failure but to compounded human decisions, some of them entirely rational in isolation. There was no stupidity involved. There was cognitive bias, organisational pressure, and the absence of a safety culture that would have caught the trajectory before it became irreversible.

Q5 Where does human error sit in the threat landscape right now? Is the industry taking it seriously enough?

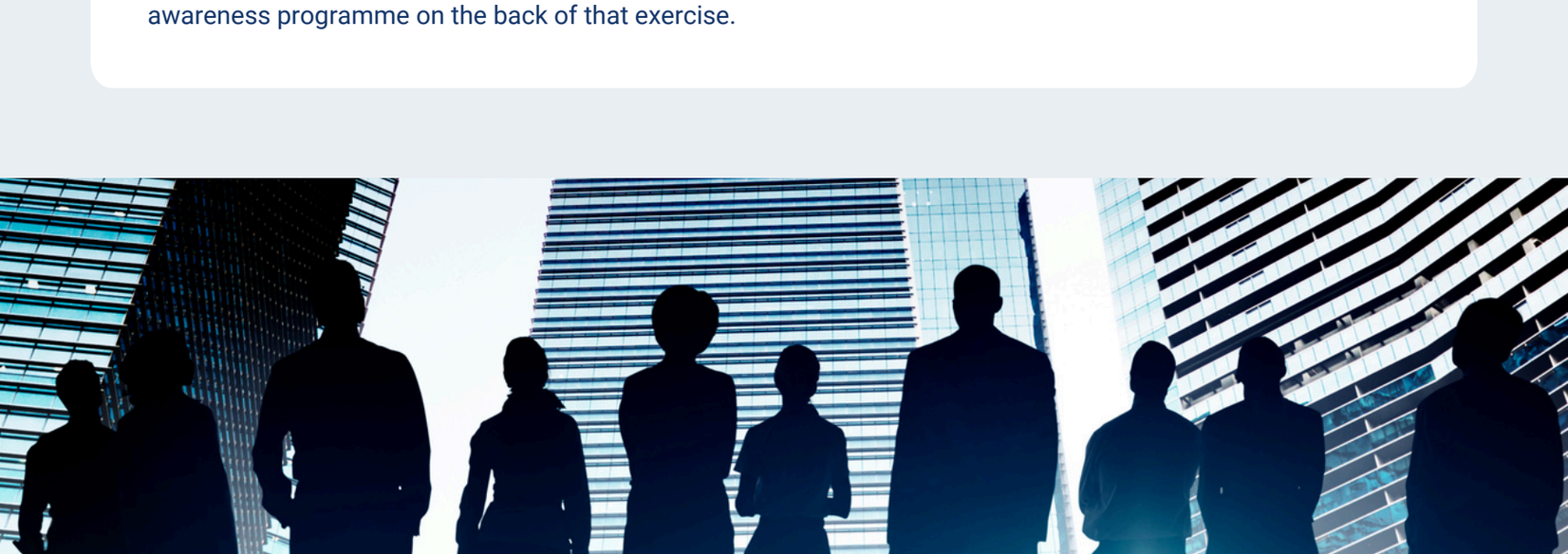
It sits at the centre of it, and no — the industry is not taking it seriously enough. The data is not ambiguous: somewhere between 70 and 80 percent of significant data centre outages have a human error component as a primary or contributing cause. And yet the investment in human factors — in ergonomics, cognitive load management, crew resource management-style training, safety culture — remains a fraction of what goes into hardware redundancy.

Part of the problem is that human error is harder to sell as a budget line. You can show an executive a Tier III redundancy diagram and explain what it costs and what it prevents. It is much harder to quantify the value of a shift-handover culture that eliminates ambiguity. That doesn't mean we should stop trying — it means we need to get better at making the business case.

Q6 You've conducted penetration tests with striking findings. Can you share an example — without naming names — that changed how a client thought about their own security posture?

There's one that stays with me. A client — a large, well-resourced European organisation — was confident in their perimeter. CCTV, access control, visitor management on paper. We ran a physical intrusion assessment. Within the first hour, a member of my team had accessed a restricted floor by simply following a member of staff through a secured door while carrying a box of supplies. No one challenged them. No one asked for a badge. The psychological principle is well known — people holding objects are perceived as having a reason to be there, and challenging them feels socially awkward.

The striking part was not the breach itself. It was the debrief. The client's security manager looked at the footage and said, "I would have done the same thing." That moment — when the person responsible for security recognises themselves in the vulnerability — is when real change begins. We redesigned their challenge culture and staff awareness programme on the back of that exercise.



Q7 What's the most common thing organisations think they've secured but haven't — and what's the mistake that keeps creating that blind spot?

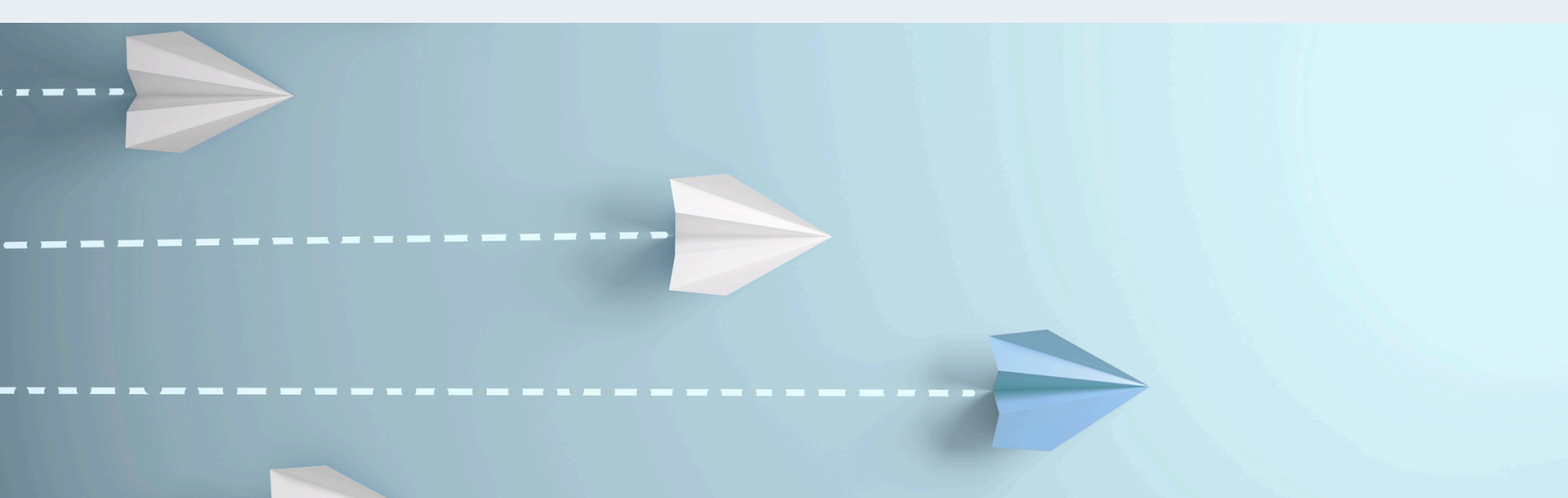
The insider threat, without question. Organisations invest in keeping the outside out. They are far less comfortable with the idea that risk also lives inside — in the form of disgruntled employees, compromised contractors, or simply staff who have far more access than their role requires. The ICTS Insider Triad framework captures this well: the convergence of motive, means, and opportunity. Remove any one of those three, and the threat collapses. But most organisations don't systematically audit all three.

The mistake that creates the blind spot is cultural. Raising the insider threat internally is uncomfortable — it can feel like accusing your own people. So it doesn't get raised with the same rigour as external threats. Leadership teams prefer not to sit with that discomfort. The result is a systematic gap in the threat picture.

Q8 As someone focused on quality and compliance, what does "good" look like in security operations — and how far are most organisations from it?

"Good" looks like alignment — between written policy and actual practice, between what management believes is happening and what is actually happening on the ground, between the training people received and the decisions they are capable of making under stress. ISO 9001 gives you a framework. What it cannot give you is the culture that makes the framework live.

Most organisations are further from that than they think, because the indicators they use to measure themselves — audit scores, incident counts, certification status — are lagging and often self-referential. An organisation can pass every audit and still have a deeply fragile operation, because the audits measure documentation rather than behaviour. Closing that gap requires a different kind of assessment: observational, ethnographic almost, looking at what people actually do rather than what they say they do.



Q9 What's the one process or habit that separates a mature security programme from a mediocre one?

After-action review, genuinely practised. Not the checkbox version — a form completed and filed. I mean the organisational habit of sitting down after every significant incident, near-miss, or exercise and asking: what happened, why did it happen, what did we learn, and what will we do differently? And then actually doing it differently.

Mature programmes have institutional memory. Mediocre ones repeat the same failures because nothing was ever captured and fed back into the system. Kirkpatrick's model for training evaluation is relevant here — most organisations only measure Levels 1 and 2 (satisfaction and knowledge). Very few measure Level 4: whether the behaviour change actually improved results. That measurement discipline, applied broadly, is what separates the good from the rest.

Q10 Your next book is out in September — what do you hope organisations take away and act on?

One concrete shift: treat human reliability with the same seriousness as technical reliability. When a UPS fails, there is a root cause analysis, a maintenance review, a supplier conversation. When a technician makes an error, there is often a reprimand and nothing more. That asymmetry is a strategic mistake. I want readers — particularly operations directors and security managers — to walk away with both the conceptual framework and the practical tools to build human error prevention into their operating model, not bolt it on after the fact.

If the book contributes to even a handful of organisations genuinely rethinking their approach to training, shift management, and safety culture in the data centre environment, it will have done its job.

Q11 What's the conversation you wish the security industry was having more openly right now?

The one about failure. We are extraordinarily good, as an industry, at projecting confidence — to clients, to boards, to regulators. We are far less good at openly discussing where our models have failed, where our assumptions were wrong, and what the near-misses looked like before they were contained. That culture of silence around failure is itself a security risk: it prevents learning, it creates overconfidence, and it means the same errors propagate across organisations that never speak to each other honestly.

Aviation learned this. After decades of catastrophic accidents, the sector built a culture where near-misses are reported, analysed, and shared — even when they are embarrassing. Security, particularly physical security, has not made that transition. We should.

Q12 What advice would you give to someone just entering the security profession today?

Three things. First, cultivate intellectual curiosity beyond the technical. Read criminology, read behavioural psychology, read history. Security is fundamentally about human beings — why they behave the way they do, what makes organisations fragile, what creates the conditions for failure. The tools change; the underlying dynamics don't.

Second, find the people in the room who ask uncomfortable questions and stay close to them. The most important security failures I have studied were preceded by someone who saw the problem and didn't feel empowered to say so clearly enough. Your value to any organisation is partly your expertise, but mostly your willingness to say what is true even when it's unwelcome.

Third, write things down. Your observations, your assessments, your hypotheses. The discipline of writing clarifies thinking in a way nothing else does — and over a career, it becomes an irreplaceable record of how you've grown.

PUBLISHED WORKS

His latest work, **"Data Centers — Les Gardiens Fragiles du Monde Numérique"** , is due for publication in **September 2026**.