ADISA Certification
Public Statement

By Steve Mellings – CEO

2nd July 2025

Response for comment on data breach within an ITAD.
I have been asked by Kyle Marks to provide a comment on a news story is the US concerning a court case where an employee was found guilty of theft from an ITAD.

Kyle has raised this petition which contains links to further information on the story.

Petition · Stop Data Breaches: Hold ITAD Certifiers Accountable! - United States · Change.org

---

I have been aware of the court case relating to theft in ITAD, which has been playing out in the US recently, through both industry contacts and media coverage. I don't have any inside information or knowledge about this case beyond what has been made public, which is summarised mainly by the links shared in Kyle's petition.

One thing to note is the lack of commentary from any of the organisations involved in the data breach or those named in the petition. Therefore, my initial observation is that we are not aware of any internal work which may be underway in response to this incident. Without this context, it is unfair to pass comment on a situation where there may or may not be activity which is pertinent to forming an opinion or making a judgement.

Having spoken with Kyle, I have decided to talk more generically about how we (ADISA), as an independent certification body, behave in a situation like this.

Context of ADISA

ADISA is an independent certification body, so it may differ slightly from those within the situation, as they are more aligned with either trade bodies or industry figureheads. Our role as a certification body is to act impartially and consistently in our conformity assessments to ensure that all awards (certifications) issued are achieved through the same means, against the same published set of requirements, and all companies are held equally accountable for maintaining their compliance with those certifications.

As a certification body, we have a liability to ensure that our statement of conformity regarding a product or service accurately reflects the truth, and if not, we may be held liable for any public statements that are not accurate.

For this reason, our audit process is rigorous, and our approach to auditing is based on evidence and affirmative confirmation of compliance. We have a reputation for being exacting, and I have been criticised in some quarters for explaining that certification will be tough; I make no bones

about that. Certification should be earned, not given, and all companies that hold a certification issued by ADISA have earned it, making our certifications meaningful and valuable.

Dealing with Data Breaches

Despite my confidence in the previous part of this statement, the reality of certification is that no system is infallible. The responsibility ultimately lies with those applying for certification to implement and maintain repeatable processes, ensuring the outcome is achieved consistently. It would be naive to claim that "it would never happen", as even in the most well-drilled businesses, mistakes happen, and bad actors influence the outcome to be less desirable for all.

Therefore, we cannot claim that incidents "never" occur in a company holding an ADISA Certification. Instead, our ITAD Standards and audit process have been designed to assess how risk is being mitigated, and as such, the likelihood of incidents is reduced, but it can never be zero.

- Setting the bar.

We begin with the rigorous auditing previously mentioned, as this lays the foundation for our certification process. When we audit, we not only assess existing processes and procedures but also see how they could be undermined. If an organisation "dresses" for an audit, we may not accept their processes as being reflective of business as usual.

- Working together.

Once certified, we maintain a full and open relationship between the certified company and ourselves, and trust between both parties is critical in building a mutual approach to certification. Our relationship is governed by our Code of Conduct, which documents the expectations for all parties (ADISA included). This is a mandatory part of certification, and non-compliance with it can result in the withdrawal of certification.

Should a data breach occur within Standard 8.0 (all regions), criterion 2.4.1 addresses security incidents and mandates the ITAD behaviour, which includes a disclosure plan to customers and a root cause analysis to be carried out.

These requirements are critical to ensure transparency not only among themselves but also for customers who may be involved.

Incident Management

Of course, bad things which are outside of anyone's control do happen. In these situations, our approach is not to immediately assign blame or distance ourselves. Instead, we work with the organisation and follow our **Incident Investigation Process.** This ensures we follow a consistent and fair process to investigate the incident, protect our brand and reputation, and treat the company in question with respect.

This process is started when we find out that there has been an incident, either directly from the company holding an ADISA Certification or via other sources including the press or whistleblowers. NB: Certified Companies are mandated to inform ADISA of any such incidents as per our Certification Agreements.

We initially capture as much information as we can, as our first decision is to decide whether there is actually an incident to investigate. Vexatious claims or complaints about organisations happen more than one might expect so we must ensure we don't jump to conclusions.

We then establish timeline and participants as well as the scale of the incident. We also identify whether this is an ongoing incident or whether the risk mitigation has been applied to contain it.

These steps are completed remotely within 48 hours of notification.

Depending on the nature of the incident, our response is to put boots on the ground and send in one of our auditors to review matters. Where a softer approach is required, one of our management team members may attend the site, with the decision being based on the incident itself.

An example of incident management occurred in 2014 when four ADISA-certified sites were broken into over four days, each attack using techniques more aligned with 'Mission Impossible' than opportunistic burglaries. That was not a time to pile even more pressure on businesses going through the grieving process of a break-in. Our role in those situations was to act as a stabilising force, guide them through incident management, provide peer group resources, and ensure they identified and then liaised with impacted parties. I firmly believe that the calibre of a business is how they respond to something terrible, and I can assure everyone that all four businesses concerned behaved impeccably.

We, of course, conducted a root cause analysis of these break-ins, and in these instances, no non-conformance could be identified – that attacks were so well organised by motivated gangs that we viewed them as a zero-day exploit. We did, however, immediately issue an addendum to the certification to factor in new controls needed to reduce the effectiveness of these levels of attack, and we scheduled physical security audits for everyone. This addendum was then formally adopted at the next standard review.

Consequences

Following our incident management process, which typically is concluded within five working days from notification, or in some instances, if the ITAD hasn't complied at all, organisations can have their certification suspended and then withdrawn. Those who have it withdrawn do go on a public register, which is our very last resort.

We operate with a carrot in one hand and a stick in the other at times. But the most important thing is that certified companies and the certifying body must share the same goals. Without that alignment, it really is a game of cat and mouse, and no one truly benefits.

Data Security isn't a popularity contest. It's about building trust and assurance, rewarding achievement, encouraging improvements, and, sadly, in some cases, identifying bad actors.

This statement is given on behalf of ADISA to Kyle Marks is response to his petition and can only be produced in its full original format.

Steve Mellings
CEO
ADISA Certification
2nd July 2025