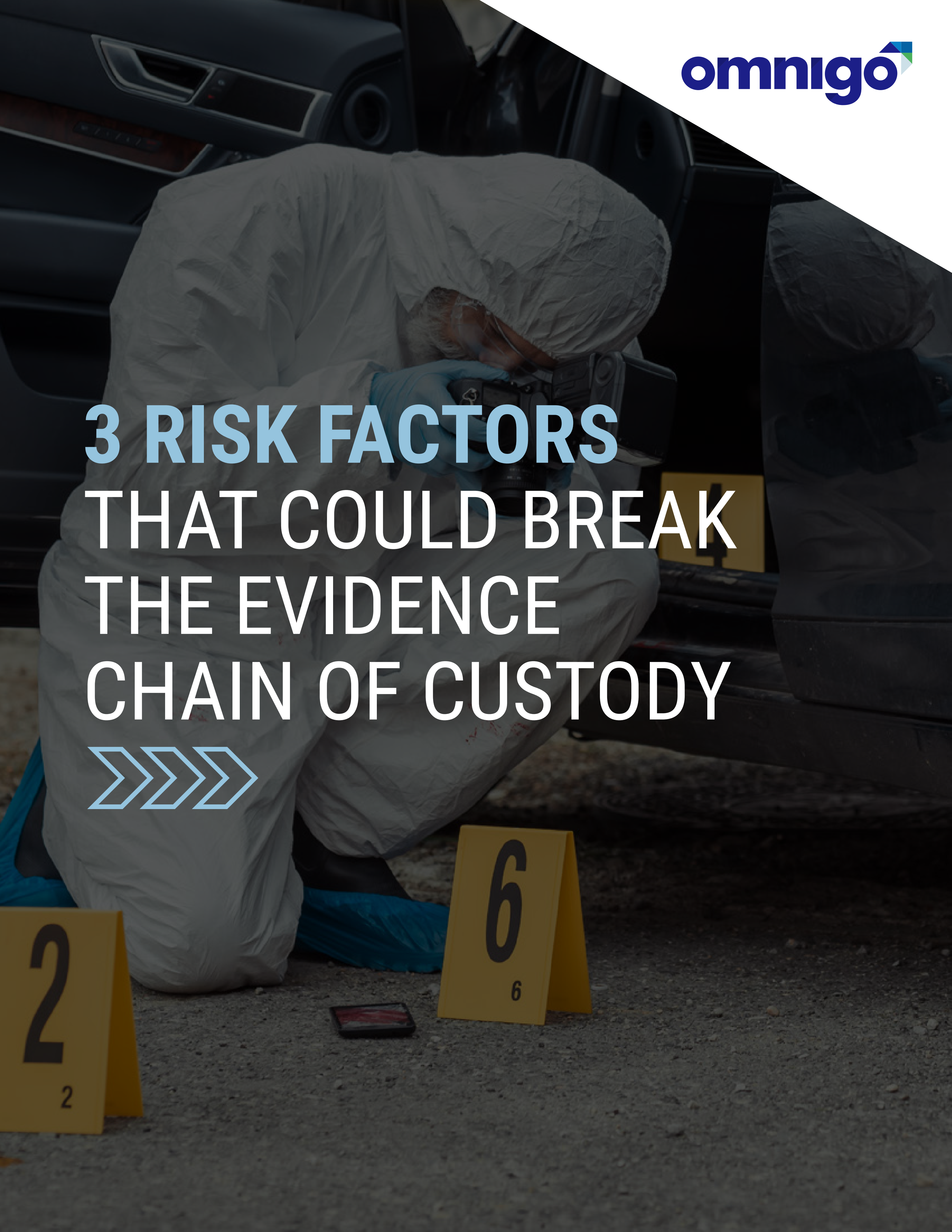
omnigo

3 RISK FACTORS THAT COULD BREAK THE EVIDENCE CHAIN OF CUSTODY



In early 2021, news broke of massive evidence deletion within a Texas-based police department.

A total of 8.26 million individual case files – roughly 21 terabytes of data – were erroneously and irretrievably removed from the department's network drive. Archived evidence ranging from video and audio files to case notes and administrative documents simply vanished.

Well over a year after the fact, investigations remain ongoing as to the cause and impact of the data loss. Police department personnel and other city officials cannot cite with certainty the number or types of cases affected, nor how the missing evidence could influence outcomes.

This event illustrates the power and vulnerability of data.

> **Within the legal system, public agencies and courts work together to rigorously protect the evidence chain of custody. The process is typically logical and ordered, but digital evidence handling isn't infallible.**
>
> **Improper evidence collection and preservation affect evidence admissibility, the trying of cases, and ultimately the application of justice.**

To guard against the serious consequences of breaking the chain of custody, it's imperative to understand 3 key risk factors that could jeopardize digital and physical evidence.

RISK FACTOR 1:

Inadequate Storage

The amount of digital and physical evidence gathered for a legal case is profound. A single file may require up to 1.5 terabytes of storage space.

Technologies are catching up to the need, but common storage solutions are proving insufficient and potentially detrimental:

- Average cloud-based storage lacks the security measures necessary to protect evidence from unauthorized viewing or hacking
- On-premise hard drives lack needed space and upload attempts could corrupt files or cause outright failure
- External storage such as discs or jump drives can be physically damaged, go missing, or fall into the wrong hands

RISK FACTOR 2:

Digital Evidence Collection Disparity

There are many viable forms of digital evidence such as 911 call recordings, body cam and dash cam footage, mobile device and computer data, and evidence uploads from stakeholders. The information is often compelling and central to building or defending a legal case.

Given the different types of media, file formats could differ widely and may not be compatible with all digital evidence management systems. The chances of data corruption increase, as does the probability of a broken chain of custody.

RISK FACTOR 3:

The Human Element

As demonstrated by the Texas police department situation, human error can dramatically impact the chain of custody.

It's common for many agencies and stakeholders to be involved in a single case. This means many people will contribute and/or handle evidence. An overabundance of evidence, along with too many touchpoints, can potentially cause confusion, procedural delays, and harm to evidence integrity.

Likewise, court clerks already juggling heavy dockets and time constraints may overlook communication back to the interested parties or otherwise inadvertently mismanage evidence. Even a small error can have big repercussions.

A break in the chain of custody could have one or several causes, but the potential outcome is the same: inadmissible evidence that – by its absence – could lead to misinformed judges, juries, and verdicts.

Bridging the Gaps

Gaps in technologies, storage, and cross-agency efficiencies raise some of the greatest chain-of-custody concerns.

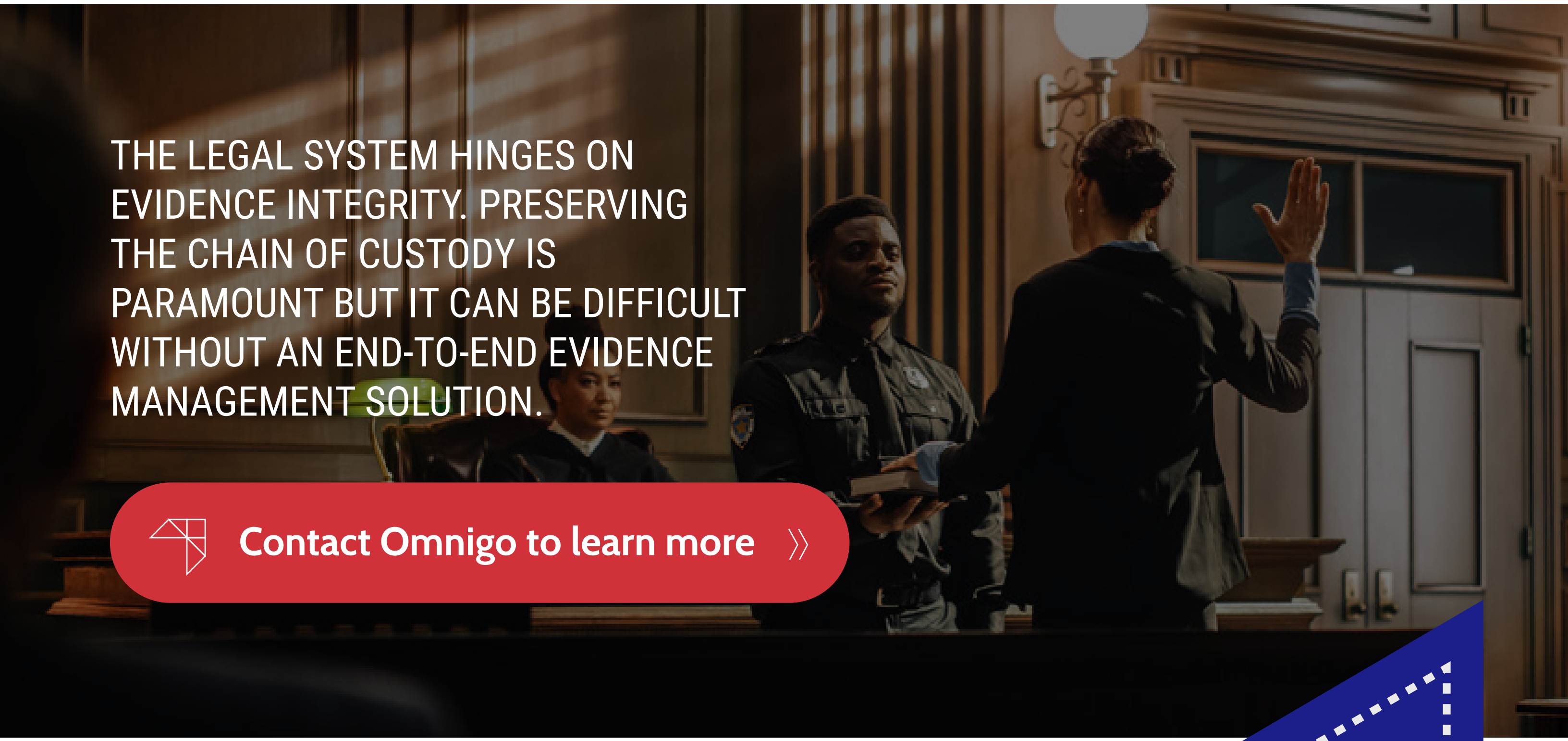
Finding work-arounds may provide temporary fixes, but ultimately the gaps – and evidence vulnerabilities – still exist. Scrambling to react to issues as they arise isn't practical or effective.

> **Instead, implementing an integrated end-to-end evidence management system such as Omnigo Investigation and Case Management with Digital Evidence is the safest, most effective way to eliminate process inconsistencies and maintain a complete, secure evidence chain of custody.**
>
> **The centralized digital ecosystem hosted on a CJIS-certified cloud-based server allows for the uninterrupted capture, storage, sharing, and protection of evidence gathered from multiple sources. Having one repository provides seamless evidence management, simplifies case data organization, and streamlines communication.**

ABOUT OMNIGO INVESTIGATION AND CASE MANAGEMENT WITH DIGITAL EVIDENCE

Case management involving large amounts of data can be especially demanding. But Omnigo's powerful end-to-end solution simplifies and safeguards digital evidence at every step in the process:

- Access an easy-to-understand view of mobile data in minutes
- Multiple search options make it easy to find data in phone logs, contacts, text messages, and browser history
- All captured GPS data is plotted on a Google map; see where a person was, and when using specific time frames or map data points
- Store traditional, structured records data and all multimedia data in one centralized location
- Create a full audit train to ensure evidence is handled correctly with a complete chain of custody
- Filter files by folder name, uploaded by, uploaded between selected dates, category, and file type



THE LEGAL SYSTEM HINGES ON EVIDENCE INTEGRITY. PRESERVING THE CHAIN OF CUSTODY IS PARAMOUNT BUT IT CAN BE DIFFICULT WITHOUT AN END-TO-END EVIDENCE MANAGEMENT SOLUTION.

Contact Omnigo to learn more »

OMNIGO SOFTWARE HEADQUARTERS

10430 Baur Boulevard
St. Louis, MO 63132

Tel. 1.866.421.2374
sales@omnigo.com