e-REAL®
by LOGOSNET

Cybersecurity



Confidentiality and decisions under attack

Prevention and on-site support for law firms, legal departments and compliance teams

www.e-real.net

e-REAL by LOGOSNET

Confidentiality and decisions under attack

Prevention and on-site support for law firms, legal departments and compliance teams

We support law firms, in-house legal departments and compliance teams facing cyberattacks, theft of client information, extortion and pressure on the people who hold confidential data and decide what to disclose. We help them stay clear-headed, protect clients, privilege and reputation, and coordinate the response with technical specialists, insurers and authorities as events unfold.

Prevent

Practical support to verify suspicious instructions, protect client files and payment details, use the right channels and prepare a response.

Manage the crisis

On-site support and real-time advice for immediate decisions: what to tell clients, courts and authorities, and when. We also provide rapid and emergency interventions, activating as needed without prior notice.

Learn by doing

Realistic simulations and work on real cases to practice decisions on disclosure, notification and communication under pressure.

Making safeguards work through people

We understand how security systems work and the constraints they impose on a practice: document management, e-discovery platforms, client portals, payment procedures. We do not design them: we help lawyers, paralegals and compliance officers understand them, interpret alerts and turn procedures into effective behaviors, even under pressure. We work alongside the firm's or the company's technical specialists to connect tools, people and responsibilities.

The expertise we bring to your side

Our team includes experts in psychology and organizational behavior, civilian and military PSYOPS specialists, including retired Italian Armed Forces officers, criminal lawyers, criminologists and ICT experts.

Training and practical intervention before and during a crisis.

e-REAL by LOGOSNET

CASE EXAMPLES

When an attack disrupts the practice

Ransomware, stolen client files, payment fraud and threats of disclosure.



01 Ransomware and locked case files

Document management, email and billing become unavailable before a filing deadline or a closing. Clients, courts and counterparties expect answers and timelines that the team does not yet have.

Our work: define priorities, communicate uncertainty to clients and courts, distribute responsibilities and contain conflict and overload.

02 Stolen client data and extortion

A demand for money comes with the threat to publish privileged documents and client information. Fear, urgency and the duty of confidentiality pull in different directions.

Our work: recognize psychological pressure, verify messages and support a structured discussion between partners, general counsel, compliance and ICT specialists, including what to tell clients and when.

In simulations and real cases, we follow events as they unfold and adapt our support to the decisions required.

CASE EXAMPLES

When the target is a person

Impersonation, payment diversion, intimidation and disinformation.



03 A fake instruction from a partner or a client

An email, a phone call or a cloned voice asks to change the bank details of a settlement or escrow payment, or to release confidential documents before a deadline.

Our work: recognize the use of authority and urgency, verify through reliable channels and manage the fear of challenging a partner or an important client.

04 Threats and reputational attacks

A partner, a general counsel or a compliance officer receives threats while manipulated documents and accusations circulate. A client or a journalist asks questions. The team is divided over how to respond.

Our work: assess available information, manage fear and anger, agree on messages and responsibilities, and sustain team cohesion.

PSYOPS expertise helps explain influence and manipulation and supports informed responses.

DURING A CRISIS

Support as events unfold

Practical support for people who need to decide and act.



05 Notification and disclosure under pressure

A breach touches personal data and client secrets. Deadlines run under GDPR, sector rules, client contracts and insurance policies, while the facts are still incomplete and legal, compliance and management disagree on what to say.

Our work: make priorities and roles explicit, order the facts, support decisions on notifications and communications to clients, authorities and insurers, and manage communications and handovers.

Practical intervention and prevention

During a crisis, we help organize information, clarify roles and manage difficult interactions. Before a crisis, we work on everyday activities: verifying instructions, protecting client files, reporting channels, shared decisions and behaviors to practice. Action learning connects development with practical work on the actual case.

After the critical phase, we reconstruct what happened and turn experience into useful practices for future crises.

e-REAL by LOGOSNET

OUR CONTRIBUTION

Understanding the threat and supporting those facing it

Different areas of expertise working on the same case.

The team

Experts in psychology and organizational behavior

Stress, emotions, group dynamics, conflict and decisions under uncertainty: we work on the factors that can help or hinder the response of partners, lawyers and compliance staff.

Civilian and military PSYOPS specialists

Our team includes retired Italian Armed Forces officers. Expertise in psychological operations helps explain influence, intimidation, deception and pressure, and recognize their effects.

Criminal lawyers and criminologists

They help interpret conduct, responsibilities and professional duties, inform communication decisions, and understand relationships between victims, those behind the threats and other parties.

ICT experts

They understand tools, systems and operational constraints. They connect the cyber incident with people's decisions and collaborate with the firm's or the company's technical specialists.

From understanding systems to using them effectively

We help people understand alerts, use the right channels, apply procedures and report anomalies. Technical knowledge becomes behavior and strengthens safeguards.

e-REAL by LOGOSNET

OBSERVING TO IMPROVE

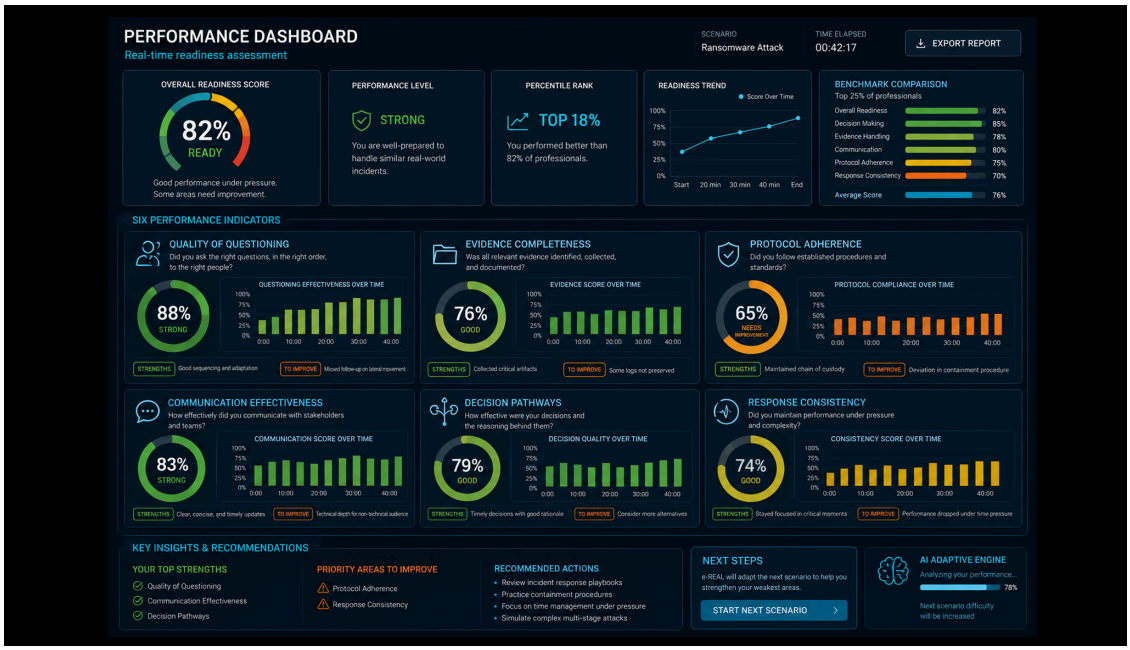
Making capabilities and development priorities visible

Feedback connects behaviors with specific simulation events.

Simulate. Reflect. Try again.

Participants tackle individual or group scenarios, interact with conversational AI avatars playing clients, counterparties, authorities and colleagues, and encounter new events during the exercise. Feedback and debriefing help them recognize observed behaviors, understand choices and test more effective responses.

Example of feedback after a simulation



Questions, decisions and communication

The dashboard connects simulation events with performance areas: quality of questions, information verification, use of procedures, communication with clients and authorities, and consistency of the response under pressure.

Feedback that helps identify the next step

We compare dialogue, checks and decisions with the exercise objectives. Debriefing reveals strengths and practical priorities for everyday work and future simulations.