GRA QUANTUM

CASE STUDY

Expelling the source of malicious virtual attacks on leading pharmaceutical firm

Industry:

Pharmaceuticals

Goals:

- Identify the source of disruptive security incidents

Service:

Digital Forensics

Results:

- Identified source to be an executive
- Spared the client millions in severance and litigation fees, a further dip in stock value, and brand tarnishing public embarassment

About GRA Quantum:

GRA Quantum is a pioneering information security firm with a mission to build close partnerships with our clients, serving them as trusted advisors in building effective, proactive plans. We believe in comprehensive strategies designed to harden networks, deflect attackers, and rapidly recover from any incidents.

One of the nation's leading publicly-traded pharmaceutical companies was disrupted by a series of damaging cybersecurity attacks that were harming both their internal and external operations.

The Challenge

The disruptive offenses included email spoofing, anonymously written emails threatening certain employees, and a number of anonymously posted blog entries detailing company trade secrets. The firm needed a way to stop these attacks before the financial and reputational damage became irreparable.

The Solution

The firm reached out to GRA Quantum to identify the source of the disruptive security incidents, assess their full scope, and advise the company on steps to resolve the problem.

Our engineers began immediately with a careful, detailed review of evidence provided by the client and systematic examinations of leads ascertained via dark web resources.

This analysis soon revealed the malicious attacks as coming from an internal source. The engineers established the personal identity and location of the anonymous email account used by the perpetrator and decided to conduct a site visit to the client's headquarters for further investigation.

The Outcome

Pulling from the compelling evidence accumulated in the analysis, GRA Quantum examiners conducted a rigorous interview with the suspect that ultimately resulted in a full confession. The suspect, a senior executive, admitted his role as the sole source of all the malicious activity and agreed to resign his positions in the company leadership and on the board of directors.

This clean break spared the client millions in severance and litigation fees, a further dip in stock value, and brand tarnishing public embarrassment.

A complete network security architectural review was subsequently implemented to strengthen the company's cybersecurity protocols to prevent similar incidents from occurring again.