groupsense

DATASHEET

RANSOMWARE NEGOTIATION TRAINING

Prepare your negotiators for threat actor engagement.

Approaching threat actor engagement with tested negotiation experience.

With FBI ransomware complaints increasing 62% from 2020 to 2021, your clients' organizations are most likely feeling pressure to harden their security processes and implement ransomware plans before attackers get to their systems. If your client is hit with ransomware, negotiation with threat actors is a crucial part of getting the business back up and running and reducing permanent data loss.

While you have probably negotiated on your client's behalf on numerous occasions, you may not have experience communicating directly with threat actors under such high pressure. Arming your negotiators with the proper strategy is critical to combatting the myriad consequences of a ransomware attack on your client's organization.

WHY GROUPSENSE?

Throughout the last few years, GroupSense ransomware experts have participated in some of the world's largest ransomware and extortion negotiations. Through these interactions with threat actors, our negotiators have gained practical knowledge and developed a negotiation method that's been proven to garner the best-case outcome for clients again and again.

We teamed up with Max Negotiating, a negotiation training firm, to pair our field expertise with lawyers who understand the art and science of negotiation. With GroupSense and Max Negotiating's Ransomware Negotiation Training, your negotiators will be well-prepared for engaging with threat actors.

HOW IT WORKS

Before an immersive three-day, in-person training with GroupSense experts and Max Negotiating, our team will develop a case simulation that is tailored to your client organization's goals and needs, suggest reading materials, and direct your team to complete testing to determine participants' Thomas-Kilmann negotiation styles.

BUSINESS IMPACT

- Revenue Loss
- Brand and Reputation Damage
- Operational/Business Disruption
- Increased Cyber Insurance Premiums
- Legal Consequences

BENEFITS

- Save Time and Resources
- Reduce Risk
- Stay ahead of emerging threats
- Protect your reputation on social media
- Avoid brand damage
- Avoid business loss
- Identify scammers

GROUPSENSE PROVIDES

- Assigned Threat Intelligence Analyst
- TraceLight™ portal access for client support
- Assigned client engagement representative
- Custom threat actor investigation and reconnaissance
- Knowledge Base articles and reports for general information

The agenda for the training is as follows:

DAY 1
Participants begin by learning the anatomy of a ransomware attack: how they are conducted, the roles involved, and the ransomware ecosystem. Next, our team provides a framework for conducting negotiations and delves into core negotiation principles as they apply to cybercrime and developing a ransomware negotiation strategy.

DAY 2
We put our framework to the test in a complex, dynamic, multi-party simulation of a ransomware attack. We record the simulation for future review and coaching on Day 3.

DAY 3
Our team provides feedback as participants review recordings of the previous day's negotiation simulation. Facilitators lead participants in exercises to strengthen the vulnerabilities identified in the simulation. We conclude by building out a team response plan.

BENEFITS

Ransomware negotiation training reduces panic and decision fatigue in the event of a ransomware attack. With emotions and stakes running high after an attack, arming your response team with negotiation skills is critical to remaining in control of the situation. After the training, your team will:

- Know the in-and-outs of a ransomware attack
- Discern their role in a ransomware negotiation
- Master a tailored ransomware negotiation strategy
- Understand the science of negotiation
- And more…

ABOUT GROUPSENSE

GroupSense is a digital risk protection services company that delivers customer-specific intelligence that dramatically improves enterprise cybersecurity and fraud-management operations. Unlike generic cyber-intelligence vendors, GroupSense uses a combination of automated and human reconnaissance to create finished intelligence that maps to each customer's specific digital business footprint and risk profile. This enables customers to immediately use GroupSense's intelligence to reduce enterprise risk, without requiring any additional processing or management by overstretched security and fraud-prevention teams.

GroupSense is based in Arlington, Va., with a growing customer base that includes large enterprises, state and municipal governments, law enforcement agencies and more.

Find out how GroupSense can help your organization at www.groupsense.io

ABOUT MAX NEGOTIATING

At Max Negotiating, we help lawyers negotiate better outcomes with actionable, research-based toolkits, customized simulations, and personalized video review. Learn more about our services at www.maxnegotiating.com