groupsense

DATA SHEET

Ransomware Response Readiness Assessment (R3A)

Ransomware attacks are sudden and devastating. Most companies aren't prepared for a ransomware attack outside of technical and incident response. Companies need to be prepared for the fallout, both internal and external, that occurs post-ransomware.

Why GroupSense

GroupSense is the world's leading firm for ransomware negotiation. We understand the ransomware threat groups and how they work better than most firms because we've negotiated with them numerous times. Many firms can do incident response inside your firewall; while that's important, dealing with the external threat is much more critical due to the media attention ransomware attacks bring.

GroupSense is the best at preparing you for the worst-case scenario. Having GroupSense's experience on your side can turn a high-profile public relations disaster into a mere blip on the radar.

Overview

You need to assume a ransomware attack will happen to your organization. Ransomware readiness isn't incident response. When a ransomware attack happens, you may only have hours to respond to the attackers.

Ransomware attacks have surged since the increase in employees working from home. It is one of the most destructive cyber attacks, as

GroupSense provides clients with specialized intelligence and cryptocurrency services should there be a ransomware attack and/or data extortion incident. Preventative monitoring, post-breach monitoring and breach notification services are also available.

AS SEEN IN:

The Washington Post · SC Media · WSJ Pro Cybersecurity · POLITICO · Dark Reading · Business Insider · TechRepublic

Cyber Reconnaissance uses highly trained analysts, empowered by technology, to deliver threat intelligence specific to your digital risk.

GO RECON

it affects its victims financially in both the short and long terms. Preparing a ransomware playbook in the event your organization is hit with malware is vital to successfully dealing with the cyber attack, because it enables the organization to continue its day-to-day business activities. GroupSense is the world's foremost expert in dealing with ransomware attacks.

We will help you prepare or deal with a ransomware attack in the likely event your organization is hit.

We're one of the few acknowledged experts in ransomware negotiations, which gives us insights into how the attackers get in, their actions and all the different ransomware groups behave.

Our Model

Organizations all are unique in maturity, size, goals and threat profile. The Ransomware Response Readiness Assessment (R3A) fits your exact needs; typical checklists fail to give critical context around the complications that ransomware attacks bring.

Table 1. Ransomware Response Readiness Assessment (R3A)

Tiers and Options	TIER 1 ASSESSMENT	TIER 2 PLAYBOOK	TIER 3 EXERCISE
Typical Duration (weeks)	4	5	6
Ransomware Readiness Assessment	X	X	X
Financial review	X	X	X
Legal Review	X	X	X
Document Review	X	X	X
Operational Review	X	X	X
Incident Response Review	X	X	X
Virtual Workshop	X	X	X
R3A Report	X	X	X
Ransomware Response Playbook		X	X
Existing Collateral Review		X	X
Disaster Recovery Plan Review		X	X
Ransomware Playbook Briefing		X	X
Ransomware Playbook Report		X	X
Dark Web Assessment			X
Ransomware Tabletop exercise			X
Critical Business Component Review			X
Regulatory requirement Review			X
Disaster Recovery/Business Continuity Plan review			X
Reputation Impact Analysis			X
Audit and Compliance Review			X

Our Approach

GroupSense performs a deep dive into your organization's documents, digital assets and procedures to provide mitigation measures and guidelines for preventing or responding to a ransomware attack. Specifically, GroupSense will evaluate six main areas to assess your organization's ransomware readiness:

Cyber Threat Intelligence

Intelligence on threat actor tools, tactics and relevant dark web chatter on impending cyber attacks to better inform decision making during incident response.

Threat Detection

The various components an organization has to detect threats across it's infrastructure. Specifically what technology, people and processes it has in place.

Communication Processes

The flow of communication between different stakeholders in the organization, either external or internal.

Incident Response

How an organization validates, prioritizes and takes action on threats to their people or infrastructure.

Cyber Gap Metrics

Any financial obligations or other metrics to improve cyber defense strategy, technology and processes or deal with a cyber incident's impact on business activities.

Operational Tasks

How an organization handles and distributes all roles and responsibilities in responding to a cyber incident.

After reviewing all relevant items, GroupSense will hold a virtual workshop to run through the R3A report and above assessed items as well as answer any questions or concerns.

OTHER OPTIONS

Ransomware Incident Support

GroupSense will be on-call 24x7 to provide cyber intelligence specific to the threat actor, type of ransomware, typical behaviors of the cyber crime group, technical indicators of concern, and strategy. When requested, GroupSense will engage anonymously on your behalf with the threat actors to gather more intelligence, potentially degrade the attack, and potentially negotiate a settlement.

Settlement Support

If a threat actor is not on the OFAC sanctions list, GroupSense can at your direction take the lead on negotiating with the threat actor with the objective of de-escalating the matter, de-valuing the demands and achieving an agreeable settlement. While every case is different, GroupSense has been successful in securing significant reductions in ransom and extortion demands. GroupSense operates in a fully transparent manner with clients throughout the process, keeping clients informed, and providing clients the ultimate decision making authority. GroupSense will guide you on the most appropriate funding strategy to complete the settlement. GroupSense does not charge for settlement support services.

Post-Incident Monitoring

While threat actors typically honor settlement agreements, at least with regards to producing decryption keys and ceasing the immediate release of data, there are no guarantees they will destroy the data they have taken, or later distribute or sell it, leading to later exposure and threats. GroupSense highly recommends that clients activate post-incident monitoring for client-specific threats and risks on the dark web, deep web, hacker channels, social media and open sources. Please request a separate quote.