5 Readiness Tips for a Ransomware Attack

DON'T PANIC!

Try to remain calm and rely on your preparations and team to proceed.

REFER TO YOUR INCIDENT RESPONSE PLAN

The plan holds valuable information you and your IT team need if you are experiencing a security incident. Be sure the IR plan is updated frequently and printed out on paper.

Don't have an incident response plan?

Contact our team of security experts to get started.

REACH OUT TO YOUR TRUSTED ADVISORS

Insurance brokers, insurance claims team, legal counsel, etc.

ISOLATE YOUR BACKUPS

Backups should be stored off-domain and ideally network-segmented from everyday users and systems to prevent threat actors from impeding restoration by finding and destroying your backups.

DISCONNECT SERVERS AND CRITICAL DEVICES FROM THE INTERNET AND EACH OTHER

If an attacker is taking data from your network in real-time, cutting off the internet will kill this action.

To proactively prepare for an incident, learn more about our Incident Response JumpStart Retainer (IRJS). IRJS combines an industry-leading 1-hour response time with IR planning and preferred rates to our insurance-approved, experienced IR team.

© 2024 Arctic Wolf Networks, Inc. All Rights Reserved. | Public

ARCTIC WOLF

Are you experiencing a ransomware attack?

Scan the QR to submit the case

ABOUT

Arctic Wolf Incident Response

Arctic Wolf Incident Response is a trusted leader in incident response that enables rapid remediation to any cyber emergency at scale. Valued for breadth of IR capabilities, technical depth of incident investigators, and exceptional service provided throughout IR engagements, Arctic Wolf Incident Response is a preferred partner of cyber insurance carriers.