CRA | Business Intelligence

CyberRisk ALLIANCE

For Immediate Release

Contact: Matt Alderman
Phone: 720-244-9652
Email: Matt.Alderman@CyberRiskAlliance.com

CRA/InfraGard Study: Critical Infrastructure Organizations Struggle to Fight Ransomware

New York, NY, December 20, 2021 -- Critical infrastructure companies continue to struggle when it comes to identifying, responding to and recovering from ransomware attacks, according to a new survey from CRA Business Intelligence, the research and content arm of cybersecurity information services company CyberRisk Alliance.

The survey assessed malware and ransomware readiness among 380 security practitioner members of InfraGard, a nonprofit public-private partnership between U.S. businesses and the FBI. Respondents represented the manufacturing, chemical, healthcare, and financial services sectors.

Sponsored by technology solution providers eSentire and Palo Alto Networks, the survey questions mapped to the industry's benchmark five NIST areas -- Identify, Protect, Detect, Respond, and Recover -- and results aggregated into readiness/resilience scores for each of the measures, as well as an overall composite score.

Among the findings:

When it comes to identifying and protecting systems, assets, data, and capabilities against ransomware and other destructive incidents:

- Only 28% of organizations said they had established integrity baselines of files and systems to monitor for potentially suspicious changes.
- By comparison, only 24% of respondents can enforce configuration baseline/policies on target systems throughout their environment with yet-to-be-mitigated vulnerabilities.

Regarding financial services and insurance firms' progress in their capabilities to detect and respond to ransomware and other destructive events:

- 43% said they have implemented a formal crises management program that details internal stakeholders, legal teams, and enforcement agencies.
- Interestingly, 10% have no plans to create such a capability.

The best way to recover from a ransomware attack for many organizations is to have a trusted backup. To that end:

- Only 40% of healthcare organizations have the full ability to back up their data and recover their backups based on priority, while 45% can protect their backup files and ensure those backup files remain unaltered.

“Detection of lateral movement is difficult without proper staff or tools,” said a respondent from the financial services/insurance industry.

Top Gaps

Following is a summary of the top security gaps cited by companies in financial services and insurance, healthcare, chemical and critical manufacturing:

Identify & Protect:

- Enforcing configuration baselines/policies on target machines across the enterprise with unresolved vulnerabilities
- Establishing integrity baselines of files and systems to monitor change activity

Detect & Respond:

- Implementing forensics and analytics capabilities to discover the source and effects of any destructive event on data and enable security teams to make necessary changes
- Implementing mitigation and containment capabilities to limit a destructive event’s effect on the enterprise

Recovery:

- Implementing a corruption testing capability to verify the last known good state and oversee restoration of data to that state
- Implementing methods for reviewing and auditing security and crisis management programs for effectiveness and improvement

The full research report is available for download here.

About CyberRisk Alliance

CyberRisk Alliance (CRA) is a business intelligence company serving the high growth, rapidly evolving cybersecurity community with a diversified portfolio of services that inform, educate, build community, and inspire an efficient marketplace. Our trusted information leverages a unique network of journalists, analysts and influencers, policymakers, and practitioners. CRA's brands include SC Media, Security Weekly, InfoSec World, Cybersecurity Collaboration Forum, our research unit CRA Business Intelligence, the peer-to-peer CISO membership network, Cybersecurity Collaborative, ChannelE2E and MSSP Alert. More information is available at http://cyberriskalliance.com/.

About InfraGard

InfraGard is a partnership between the Federal Bureau of Investigation (FBI) and members of the private sector for the protection of U.S. Critical Infrastructure. Through seamless collaboration, InfraGard connects owners and operators within critical infrastructure to the FBI, to provide education, information sharing, networking, and workshops on emerging technologies and threats. InfraGard's vetted membership includes business executives, entrepreneurs, lawyers, security personnel, military, and government officials, IT professionals, academia, and state and local law enforcement—all dedicated to contributing industry-specific insight and advancing national security. The InfraGard National Members Alliance, a nonprofit 501(c)3 organization, is comprised of 77 chapters across the country.

About eSentire

eSentire, Inc. is the Authority in Managed Detection and Response, protecting the critical data and applications of 1000+ organizations in 70+ countries from known and unknown cyber threats. Founded in 2001, the company's mission is to hunt, investigate and stop cyber threats before they become business disrupting events. Combining cutting-edge machine learning XDR technology, 24/7 Threat Hunting, and proven security operations leadership, eSentire mitigates business risk, and enables security at scale. The Team eSentire difference means enterprises are protected by the best in the business with a named Cyber Risk Advisor, 24/7 access to SOC Cyber Analysts & Elite Threat Hunters, and industry-leading threat intelligence research from eSentire's Threat Response Unit (TRU). eSentire provides Managed Risk, Managed Detection and Response and Incident Response services. For more information, visit www.esentire.com and follow @eSentire.

About Cortex XDR

Cortex XDR is the industry's first extended detection and response platform that stops modern attacks by integrating data from any source. With Cortex XDR, you can harness the power of AI, analytics and rich data to detect stealthy threats. Your SOC team can cut through the noise and focus on what matters most with intelligent alert grouping and incident scoring. Cross-data insights accelerate investigations, so you can streamline incident response and recovery. Cortex XDR delivers peace of mind with best-in- class endpoint protection that achieved the highest combined protection and detection scores in the MITRE ATT&CK® round 3 evaluation. The Cortex XDR platform collects and analyzes all data, so you can gain complete visibility and holistic protection to secure what's next.