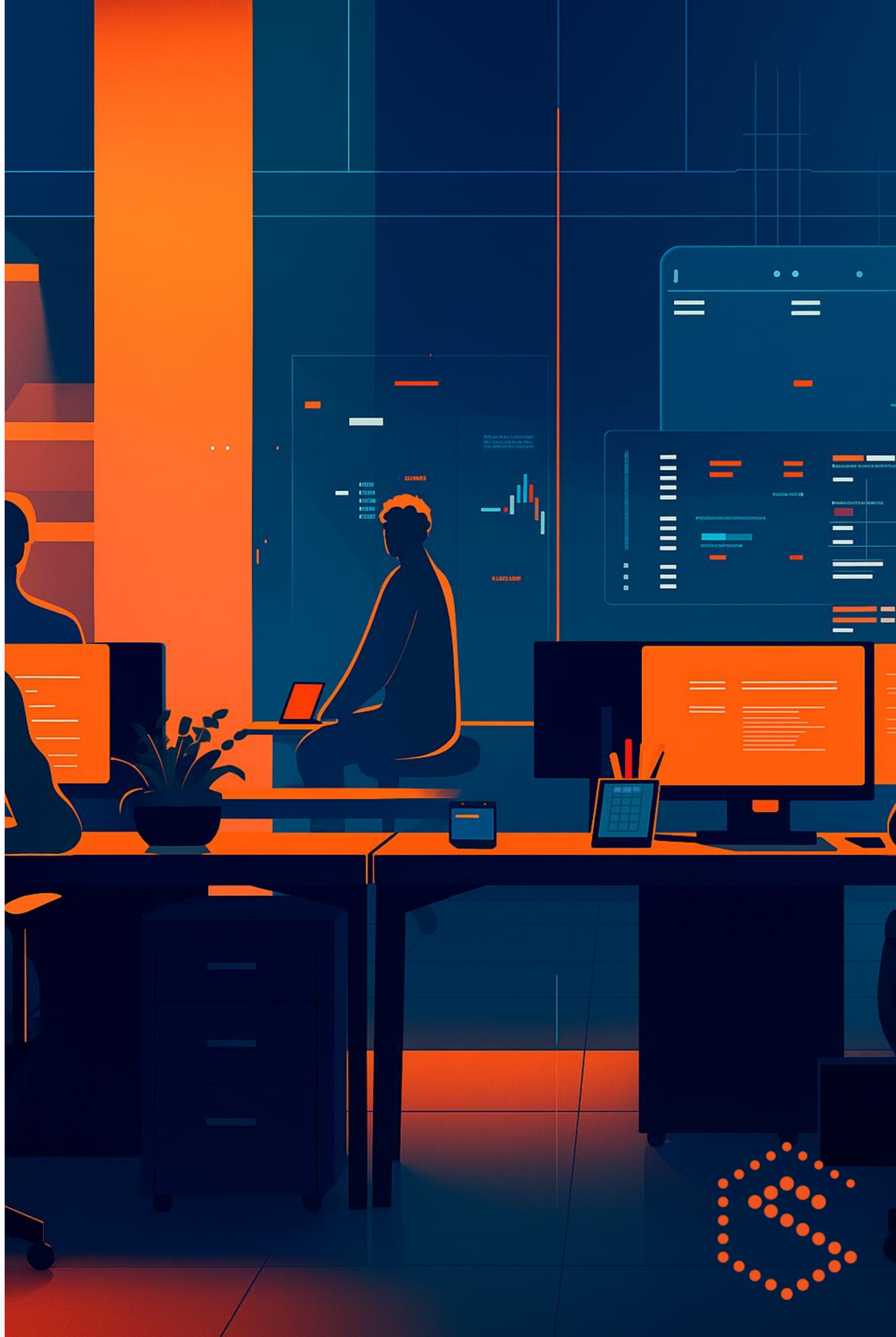
CyberSteward



Privacy + Security Forum

Negotiating with Criminals: A Deep Dive into Ransomware Negotiations

Jason Kotler, Founder & CEO

Washington D.C., US
November 13, 2025

About CyberSteward™ | CEO's Bio

Jason S.T. Kotler
CEO & Founder
CyberSteward Inc.

Jason S.T. Kotler, BA, JD, MBA, CMC – Jason has significant global experience founding, operating and advising to companies and leading strategic corporate cybersecurity and privacy law initiatives.

He has held Founder/CXO/Board, Private Equity, Investor and Management Consultant roles in the Cybersecurity, IOT/IIOT, CleanTech, Renewable Energy, Technology and Medical Devices industries.

Prior to founding CYPFER, was Chief Administrative Officer, Waterton Global Resource Management Private Equity Fund ($2.5B AUM), a Technology Startup Founder / Professional, a Senior Strategy & Transformation Consultant with Capgemini and he practiced Privacy, IP, Technology and Corporate Commercial law with McMillan LLP.

Jason is a former Board Member of The Atmospheric Fund and is a member of its Investment Committee ($100M AUM). Jason is a member of the Law Society of Ontario, holds an MBA (Deans Honours) from the Richard Ivey School of Business, a JD from Osgoode Hall Law School, a Bachelor of Art, Visual Arts (with Distinction) from Western University, and is a Certified Management Consultant (CMC).

About CyberSteward™ | Extensive Cyber-Attack/Extortion Experience

Ransomware-as-a Service (RaaS)

Cyber-Extortion (Data Theft)

Sextortion

Dark Web Sale of Data & Credentials

Cryptocurrency & Digital Assets Theft

North Korean Remote Worker Scams

Domain Hijacking

Cryptojacking

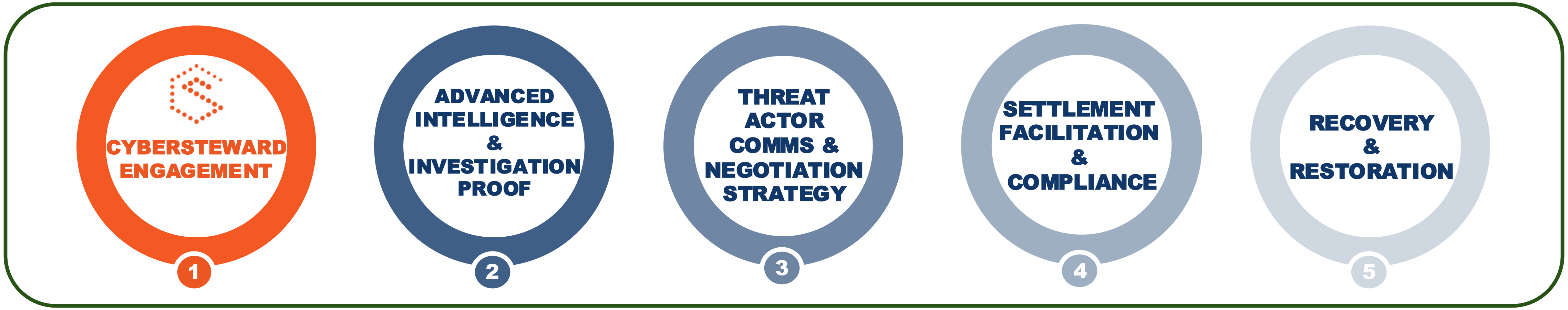
Executive Harassment Doxing / Swatting

“Post-Paid Pentesters” & “‘White Hat’ “Security Researchers”

MSP Breaches – Multi-Client Exploits

Zero-Day Platform Exploits

Collaborative Incident Response | Methodology



1 CYBERSTEWARD ENGAGEMENT

2 ADVANCED INTELLIGENCE & INVESTIGATION PROOF

3 THREAT ACTOR COMMS & NEGOTIATION STRATEGY

4 SETTLEMENT FACILITATION & COMPLIANCE

5 RECOVERY & RESTORATION

Expert Advisory, Investigations, Negotiations and Settlement Facilitation:

1. Engage with Threat Actors to discover their demands and investigate what data was encrypted and/or stolen
2. Develop negotiations objectives and strategy with Breach Counsel, Clients, and Incident Response Team
3. Negotiate with the Threat Actors to try and reduce the ransom demand, stall for recovery, settle (as a last resort)
4. If required, manage the exchange and settlement facilitation process (MSB / KYC / AML / OFAC Compliance)
5. Acquire deliverables: decryption key(s) to recover encrypted data, deletion and suppression of stolen data

Partners: Breach Counsel, Insurance Carriers, Incident Responders, Forensics, Post-Breach Recovery, & PR Firms

Discussion | Cyber-Settlements: To Pay or Not To Pay?

Why Organizations Pay?

- Regain access to data and restore operations, save time over other restoration alternatives
- Suppress publication – (i.e., PII, PHI, IP, contractual breach concerns)
- “Nuisance value” – reduce distractions
- Fear of retaliation for non-compliance
- Personal interests (e.g. protect employees and family members)

Why Organizations Do Not Pay?

- Viable alternate methods to regain access to data, restore systems – e.g. validated backups
- Stolen data is deemed of low value – low publication impact
- Emotional/Ethical reasons; further funding crime
- Fear of subsequent attacks – re-extortion / re-targeting for complying
- Demands far exceed available resources or perception/analysis of value; no cyber-insurance

Considerations:

- **Ransom payments are never the recommended option; they are a LAST RESORT**
- **Consider the current state of Cyber-Extortion Laws, Regulations, OFAC/Sanctions, AML**
- **Regardless of the decision, rapid and appropriate recovery is critical**

Discussion | Non-Payment Considerations

When payment is not received, Threat Actor may **retaliate**, engaging in various coercion and harassment techniques to force a return to negotiation – **or to reinforce their extortion business model.**

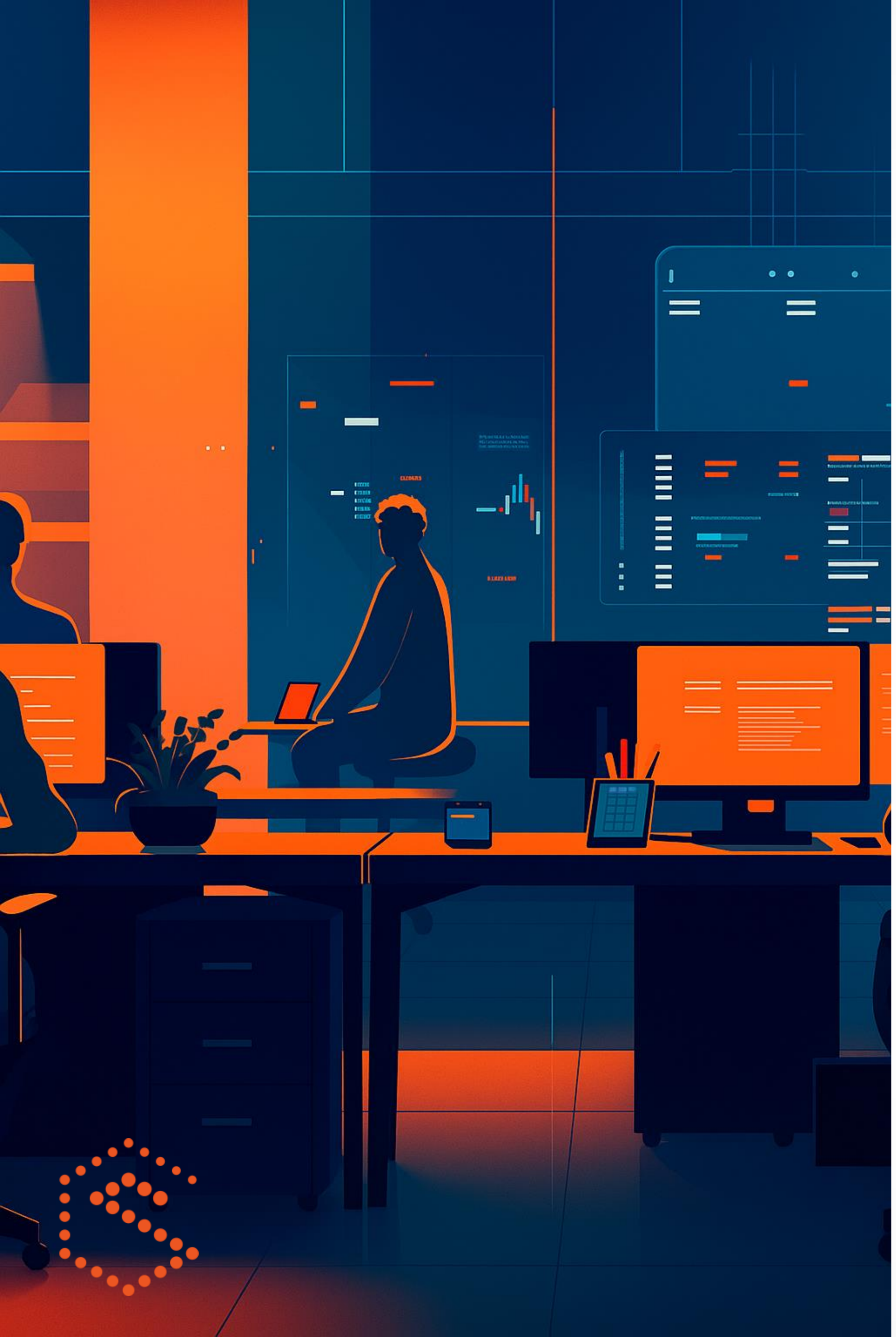
- **Public exposure of stolen data** on Threat Actors' or other dark web leaks sites, or social media platforms
  - **Partial or full data leaks**, released immediately or in staged intervals
  - **Publication of the negotiation chat transcript** to discredit the organization or pressure re-engagement
- **Contact with media outlets** to amplify reputational harm
- **Targeted harassment** of executives, employees, clients, suppliers, and other stakeholders via phone, email, text, doxing, swatting, etc.
- **Distributed Denial of Services (DDoS) attacks** against company websites and/or infrastructure
- **Attempt to re-attack** the environment with the intent to encrypt systems and steal more information
- **Credential sharing** between threat actor groups to facilitate further targeting of supply chain partners
- **Phone spam or scam campaigns** directed at individuals whose data was compromised

KEY INCIDENT RESPONSE READINESS LEARNINGS

- **Prioritize Remediation** – Onsite response is critical for global incidents; having Incident Response Plan and retainers in place ensures rapid action.
- **Agility & Scale Matter** – Optimize resources based on impact; don't overspend on unnecessary solutions.
- **DFIR Must Integrate with Remediation** – Seamless IR collaboration is essential.
- **Reduce Dwell Time** – Faster detection and response to halt attacks before major damage
- **Proactive Programs Are Falling Short** – Many focus too much on external attack surfaces and neglect critical internal assets.
- **Security Controls Must Be Managed** – Firewalls, secure file transfers, VPNs, and more fail if not properly maintained, leading to zero-day exploits.
- **Risk Transfer via Cyber Insurance** – Mitigate financial exposure with a well-structured policy.
- **Breach Coach** – Engage external legal counsel who understands your business and risk profile.
- **Know & Protect Your Assets** – Backup data properly, secure those backups, and test recovery processes regularly.
- **Establish Clear Communication Protocols** – Ensure teams can operate effectively in crisis
- **Never Assume Readiness** – Continuous testing and adaptation are key to staying ahead of evolving threats.

ACTION ITEMS

- Regularly test and validate backups; ensure Immutable
- Continue to be Cyber-Vigilant; conduct System Audits/Pen Tests / User Training
- HIDE Cyber-Insurance Policy + Incident Response Plan – Keep offline with Advisors
- Policy of Least Permissions; Conduct Data Audits & Security; Segregate Data
- Archive / Deletion of "No Man's Land" data on Share Drives
- Cybersecurity Review / Patching of Third-Party Providers (e.g. Cleo / MOVEit)



CyberSteward

Global Cyber-Extortion & Ransomware Recovery Advisory

For more information please contact:

24/7/365 RESPONSE:

(647) 497-7947 ~ ERTeam@CyberSteward.com

www.CyberSteward.com