

Insights from the Cybersecurity Front Lines

NetDiligence® Ransomware Advisory Board: Q2 2025 Meeting - Executive Summary

Each quarter, NetDiligence® brings together their [Ransomware Advisory Board](#), a group of cybersecurity, incident response, and forensics experts, who meet to share their latest insider expertise and strategic insights on ransomware and cyberattacks.

This summary provides an overview of their latest meeting with the goal of informing leaders about current cybersecurity threats and strategic responses—including new trends in attacker tactics, shifting extortion methods, and recommendations for strengthening incident response and resilience.

This brief has been prepared by Sherri Davidoff, CEO of [LMG Security](#) and moderator of the NetDiligence Ransomware Advisory Board.

Executive Summary

At the Q2 2025 meeting, the Ransomware Advisory Board (RAB) explored the evolving cyber threat landscape, revealing notable shifts in adversary behavior and extortion tactics.

Key topics included the implications of the LockBit ransomware leak, the rise of ransomware gang imposters and fake data exfiltration cases, the growing use of remote access scams, and ongoing abuse of personal devices and browser syncing.

Experts emphasized the increasing difficulty of distinguishing sophisticated threat actors from opportunistic impostors and stressed the urgent need for improved coordination and triage during widespread incidents.

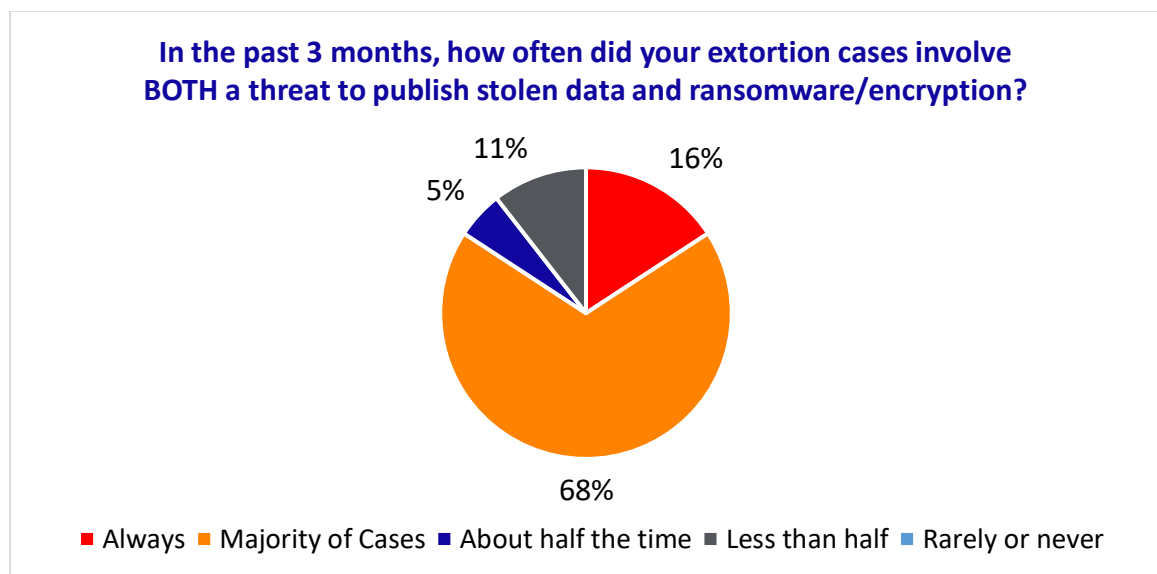
This report summarizes the Board's top observations and provides strategic recommendations for business leaders and insurers alike.

Key Insights & Trends

1. **LockBit Leak Exposes Affiliate Operations:** Experts on the Ransomware Advisory Board shared unpublished insights into the recent LockBit leak, which exposed nearly 60,000 Bitcoin wallet addresses, plaintext passwords, and internal chat logs. The breached affiliate panel featured auto-registration, suggesting low entry barriers. Members noted that more sophisticated affiliates may use the ransomware builder directly, rather than relying on LockBit's hosted entry-level affiliate panel.
2. **Ransomware Impostors on the Rise:** Security leaders reported a surge in threat actors impersonating well-known ransomware groups. These impostors frequently reuse

leaked branding, wallet addresses, and ransom note templates—often lifted directly from exposed playbooks. Members also reported cases where adversaries falsely claimed to have exfiltrated data in an attempt to extort payment, even though investigations found no evidence of data theft.

3. **Data-Only Extortion Becomes Mainstream:** Ransomware groups are increasingly dropping encryption altogether in favor of pure data extortion. Some actors have eliminated public leak sites and instead share stolen data directly on forums or through private channels. Silent malware variants are also becoming more common, complicating detection and delaying response. Board members agreed that the majority of ransomware cases still involve double extortion, but a significant percentage now include only a threat to expose data—no encryption at all.



4. **Callback Scams and Rapid Data Theft Surge:** Attackers are using email bombing and spoofed IT calls to impersonate help desks, quickly gaining remote access via tools like Quick Assist or AnyDesk. Law firms and other professional services firms are top targets—according to the NetDiligence® 2024 Cyber Claims Study, professional services accounted for 20% of all SME claims. In some cases, threat actors exfiltrate sensitive data and issue extortion demands within minutes, bypassing traditional defenses entirely.
5. **Info Stealers Exploit Personal Devices and Syncing:** The Board emphasized the risk of info-stealing malware (e.g., Lumma) targeting personal devices. Chrome browser sync functions often expose internal credentials saved on home computers. These credentials—including VPN, wiki, and Jira logins—are harvested by malware and reused to breach enterprise systems, even bypassing MFA protections.
6. **Widespread Events Reveal Response Gaps:** Members highlighted the lack of standard triage frameworks for large-scale incidents. While insurers often prioritize cases based

on potential financial loss, responders must also account for human safety and critical operations. The Board called for clearer coordination and phase-based models to manage containment, recovery, and investigation efforts across multiple concurrent incidents.

Actionable Takeaways

1. **Prepare for Pure Data Extortion Scenarios:** Develop ransomware response protocols that address non-encryption threats. Ensure teams are trained to handle fast-moving data theft cases that may not trigger traditional ransomware alerts.
2. **Validate Exfiltration Claims Before Paying:** Not all extortion threats are credible. Implement rigorous extortion response processes to confirm data theft and proof-of-life before considering any ransom negotiation.
3. **Harden Defenses Against Callback and Help Desk Scams:** Train employees to detect spoofed IT support calls and enforce strict help desk identity verification. Monitor for abuse of remote access tools like Quick Assist and AnyDesk.
4. **Increase Visibility Into BYOD and Shadow IT:** Expand endpoint visibility to include unmanaged or personal devices, and review conditional access policies. Use telemetry and identity management to detect anomalous login patterns across environments.
5. **Enforce Browser Sync Policies:** Restrict Chrome sync functionality across endpoints and educate staff on the risks of using personal profiles on work devices. Consider enterprise browser controls and session isolation for shared systems.
6. **Clarify Triage Frameworks for Surge Event:** Insurers, incident responders, and legal counsel need to collaborate and create prioritization strategies for widespread incidents. Segment IR capacity across containment, recovery, and analysis phases to optimize resource use.

Conclusion

The Q2 2025 meeting revealed a threat landscape increasingly shaped by impersonation, speed, and unpredictability. Defenders must be equipped to detect fast-moving data theft, rapidly validate extortion claims, and secure personal-device vectors that evade traditional protections. As incidents scale in frequency and complexity, coordinated response strategies—especially in the early containment phase—are more vital than ever. This briefing provides leaders with expert-curated insights to anticipate evolving risks and make proactive, informed risk management decisions.

For any questions regarding this summary or the Ransomware Advisory Board, please contact NetDiligence by submitting [this contact form](#).