CYBERSECURITY READINESS PODCAST SERIES

Episode 114

The New Playbook for Ransomware Preparedness

with Mark Lance, Senior Vice President of Digital Forensics, Incident Response, and Threat Intelligence, GuidePoint Security

Host	Dr. Dave Chatterjee, Duke University
Guest	Mark Lance, Senior Vice President of Digital Forensics, Incident Response, and Threat Intelligence, GuidePoint Security
Topic Focus	The Professionalized Ransomware Economy — Double Extortion, Ransomware-as-a-Service, Planned Containment, and Governance-Driven Preparedness
Podcast Portal	https://www.cybersecurityreadinesspodcast.com/

Summary

In Episode 114 of the Cybersecurity Readiness Podcast Series, Dr. Dave Chatterjee is joined by Mark Lance, Senior Vice President of Digital Forensics, Incident Response, and Threat Intelligence at GuidePoint Security, to examine what a more organized, better-resourced ransomware adversary means for organizational preparedness. Dr. Chatterjee opens with a striking data point: roughly 69 ransomware groups were active in a given quarter in early 2025, but by the second quarter of 2026 that number had grown to 91 distinct groups, with new groups emerging about five times faster than existing ones disappear. Ransomware, he observes, has become a fluid, professionalized market with its own supply chains and support desks.

Lance, who brings 26 years of cybersecurity experience and 16 years in incident response, traces how ransomware evolved from opportunistic attacks on individual consumers into targeted, persistent campaigns against organizations — progressing from encryption to attacks on backups, then to double extortion through data theft, and in some cases triple extortion through DDoS threats. He explains how ransomware-as-a-service platforms, often more sophisticated than the environments they target, have turned cybercrime into a highly profitable enterprise. The conversation then turns to a real incident in which GuidePoint found not one but two threat actors inside a client's network, and Lance walks through how his team used a carefully planned containment and eradication strategy — including corrupting data an attacker was exfiltrating from the CFO's mailbox — rather than a knee-jerk response that could have tipped off the adversary.

Analyzed through Dr. Chatterjee's Commitment–Preparedness–Discipline (CPD) Framework, the discussion frames the incident as a governance failure rather than simply a tools failure: the victim organization had 24x7 managed detection and response, centralized logging, and endpoint solutions, yet was treating them as compliance checkmarks. The episode closes with practical guidance on threat modeling, foundational controls, rehearsed incident response plans, “destroy your business” scenarios to earn leadership commitment, and the value of sharing hard-won lessons across the defender community.

Discussion Highlights

From 69 to 91: A Fluid, Professionalized Ransomware Market

Dr. Chatterjee opens the episode by grounding listeners in the scale of the problem. Roughly 69 ransomware groups were active in a given quarter in early 2025; by the second quarter of 2026, research identifies 91 distinct groups, with new groups arriving at roughly five times the rate that existing ones go defunct. For listeners newer to the topic, he explains that a ransomware attack typically begins when a threat actor steals access credentials — often through phishing or other social engineering — then encrypts files, steals data, and demands payment to restore access or to prevent the stolen data from being published. What began as single-operator extortion has matured into a highly organized, well-resourced criminal network.

> *The ransomware adversary has evolved into a fluid, professionalized market with its own supply chains and support desks.*
>
> **— Dr. Dave Chatterjee**

From Opportunistic Attacks to Double and Triple Extortion

Lance traces the evolution of ransomware step by step. Early attacks were scattershot efforts against individual consumers, betting that a few victims would pay. Attackers soon realized that organizations, colleges, and universities had far deeper pockets, and shifted first to automated, self-propagating attacks and then to targeted techniques borrowed from advanced persistent threats — lateral movement, persistence, and entrenchment. When organizations responded with backups, attackers targeted the backups; when organizations moved to offline backups, attackers began exfiltrating sensitive data to extort victims even after operational recovery. Double extortion is now the model almost all ransomware groups follow, some add a third lever by threatening DDoS attacks, and some groups skip encryption altogether and rely solely on data theft and extortion.

> *It's not just about operational impacts and encryption; it's also about data theft and extortion and the threat to release that data.*
>
> **— Mark Lance**

Ransomware-as-a-Service: Criminal Platforms More Sophisticated Than Their Victims

Lance describes two dominant operating models: insular groups that handle everything themselves, from initial access to encryption, negotiation, and collection, and — more commonly today — ransomware-as-a-service, in which operators have invested heavily in building platforms used by affiliates and initial access brokers. Dr. Chatterjee reflects that his earliest podcast episodes, in 2021 and 2022, centered on ransomware, and that five years later the threat has not gone away. He also cautions that paying a ransom offers no guarantee the attackers will keep their promises, and may even mark an organization as a repeat target.

> *They've invested tons of money and effort into building platforms that are more sophisticated than the victim environments that they're targeting... and it's making them a heck of a lot of money. So they're not going anywhere.*
>
> **— Mark Lance**

Know Your Adversary: Cybercrime, Nation-State, and Hacktivist Motivations

Turning to a real case, Lance explains that it is not uncommon to find more than one threat actor in the same environment. Understanding what motivates each is essential to anticipating their next move. He groups threat actors into three categories: cybercriminals such as ransomware and business email compromise operators, who are monetarily motivated; advanced persistent threat and nation-state actors, who pursue low-and-slow access to intellectual property and other information; and hacktivists, who are driven by ideology and may resort to defacement or operational disruption to spread a message.

Lance also recounts a recent ransomware-as-a-service incident in which the affiliate and the platform operator issued separate, conflicting ransom demands to the same victim — an internal rift his team was able to exploit during negotiations by questioning how the attackers could be trusted at all.

Anatomy of an Intrusion: When Successful Logins Look Suspicious

Asked by Dr. Chatterjee how the case began, Lance explains that the client had noticed anomalous inbound authentication. Their remote access relied on on-demand tokens — a user requests access, receives a token, and then connects — yet the client was seeing successful authentications without the initial request ever occurring. GuidePoint's investigation revealed that the attacker had exfiltrated backup servers containing the organization's authentication infrastructure and was issuing its own tokens. One threat actor appeared to be running a ransomware campaign, while a second, more sophisticated actor had been present even longer.

Don't Tip Your Hand: Planned Containment over Knee-Jerk Reactions

Lance explains that responding to an advanced threat still in its staging phase differs sharply from responding to ransomware after encryption. Premature containment — such as immediately disabling accounts — may be ineffective because the full breadth of access is not yet known, and it can alert the attacker, prompting them to entrench further. Instead, his team

designed a coordinated eradication event scheduled for 1 a.m. on a Saturday, with a progressive list of actions for the first one to two hours, the following two days, and the next two weeks, 30, 60, and 90 days.

> *If you lock the two doors and only get four of the windows and leave one open, then [they're] right back in.*
> **— Mark Lance**

Corrupting the CFO's Mailbox: Buying Time for Eradication

One week into the two-week preparation window, the threat actor returned and began exfiltrating multiple gigabytes of the CFO's email and calendar data. Faced with a dilemma — contain and risk making things worse, or let sensitive data walk out the door — the team made the download session appear to time out and corrupted the file being exfiltrated. When the attacker returned the next day, it downloaded a corrupted version of no value. That bought the client enough time to expedite its preparatory activities and successfully remove the attacker from the environment. Dr. Chatterjee describes the approach as both interesting and innovative.

A Governance Failure, Not Just a Tools Failure: The CPD Framework

Dr. Chatterjee reframes the incident as a lesson in governance and introduces his Commitment–Preparedness–Discipline (CPD) Framework, a holistic model for cybersecurity and AI governance focused on sustaining a robust security posture over time. Commitment is leadership's sustained resolve to treat cybersecurity as a strategic priority; Preparedness is the operational readiness to detect, respond to, and recover from incidents; and Discipline is the governance rigor — real-time audits, continuous training, and continuous monitoring — that keeps security strong over time. He offers two initial takeaways: recalibrate the threat model to match the sophistication of a coordinated, multi-dimensional adversary, backed by leadership resources; and proactively and continuously assess and remediate vulnerabilities rather than waiting for disaster to strike.

Lance confirms the governance diagnosis: the organization in his story had 24x7 managed detection and response, centralized logging, and endpoint solutions, yet no one was verifying whether the policies behind those tools were effective or looking for indicators beyond the tools' output.

> *They were using it almost as a check mark, as a compliance piece, like, oh, we're doing this — but is anybody actually making sure that the policies that are being implemented there are effective?*
> **— Mark Lance**

Foundations Plus Enablement: Threat Modeling, Controls, Playbooks, and Tabletops

Lance urges organizations to model the threats most relevant to their own environment — whether ransomware, targeted attacks on personal information, third-party and supply chain risk, or remote workforce exposure. Foundational controls matter: multi-factor authentication for remote access and for critical servers and infrastructure, along with network segmentation that limits access between networks, can be enough to push opportunistic attackers on to an easier target. But technology is only the start. Every organization needs an incident response plan that defines who is involved and informed, how severity is determined, and which third parties will be engaged, supported by threat-specific playbooks — and plans are only as good as people's ability to execute them, which is why crisis simulations and tabletop exercises for both senior leaders and technical teams are essential.

Rehearsed Plans and “Destroy Your Business” Scenarios

Dr. Chatterjee observes that many organizations have well-documented incident response and disaster recovery plans, but when asked how often they rehearse them, he frequently meets “a deafening silence” — and some plans are five years out of date. To earn genuine leadership commitment, he advises clients to assemble a team to develop six or seven “destroy your business” scenarios that graphically connect potential incidents to the top line, the bottom line, reputation, and the future of the company. A reactive mindset is costly, he warns, since the cost of recovery is often significantly higher than the cost of proactive preparation. He also stresses the importance of real-time audits and of acting on findings, noting that valuable threat intelligence too often sits unread in someone's inbox.

> *Just like we have fire drills, we need to have security drills.*
> **— Dr. Dave Chatterjee**

Closing Reflections: Plan Like the Adversary, Share Like a Community

Dr. Chatterjee closes by noting that just as attackers operate with a deliberate plan reflected in their platforms, organizations, and methods of exploitation and collection, defenders need an equally planned and coordinated approach — one that addresses people, process, and technology rather than relying on the latest AI tool. Lance's closing message centers on community: leverage the experience of others who have lived through ransomware and major incidents, and, having gone through one yourself, share those lessons — mindful of legal disclosure and liability considerations — so others can avoid the same fate. Doing so also helps drive board- and senior-leadership awareness that these are organizational problems, not just technical ones.

> *They aren't just IT and security problems; they're organizational problems, they're business problems that have impacts to revenue, the operations, to reputation, and everything else.*
>
> **— Mark Lance**

The CPD Framework Applied to Ransomware Readiness

Dr. Chatterjee maps his Commitment–Preparedness–Discipline (CPD) Framework directly onto the ransomware preparedness themes discussed throughout the episode.

CPD PILLAR	APPLICATION TO RANSOMWARE READINESS
COMMITMENT	Leadership treats ransomware as a strategic business risk rather than an IT problem — approving the resources needed to match a professionalized adversary, and anchoring that commitment in "destroy your business" scenarios that connect potential incidents to revenue, operations, reputation, and the future of the company.
PREPAREDNESS	Organizations recalibrate their threat model to the threats most relevant to them, implement foundational controls such as multi-factor authentication and network segmentation, and build an incident response plan with threat-specific playbooks — including the capacity for planned, coordinated containment and eradication rather than knee-jerk reactions.
DISCIPLINE	Plans are continuously rehearsed through tabletop exercises and security drills, audits happen in real time, threat intelligence is acted on rather than left in an inbox, and security tools are validated for effectiveness instead of being treated as compliance checkmarks.

Actionable Recommendations

RECOMMENDATION	DETAIL
Recalibrate Your Threat Model	Match your threat model to the sophistication of today's coordinated, service-based adversary, and identify the threats most relevant to your environment — ransomware, targeted data theft, third-party and supply chain risk, or remote workforce exposure.
Lock Down the Foundations	Require multi-factor authentication for remote access and for servers and critical infrastructure, and segment networks to limit access — basics that can be enough to push opportunistic attackers toward an easier target.
Treat Tools as Capabilities, Not Checkmarks	Having MDR, centralized logging, and endpoint solutions is not enough; verify that the policies behind them are effective and actively hunt for indicators beyond the tools' default output.
Plan Containment Before You Act	When facing an advanced actor, avoid premature containment that alerts the adversary; design a coordinated, step-by-step eradication event with defined near-term and 30-, 60-, and 90-day follow-up actions.

Build Playbooks and Rehearse Them	Maintain an incident response plan defining roles, severity criteria, and third-party partners, attach threat-specific playbooks, and test them regularly through tabletop exercises and security drills so plans never go stale.
Win Leadership Commitment with "Destroy Your Business" Scenarios	Develop six or seven scenarios that graphically connect potential incidents to the top line, the bottom line, and reputation to secure genuine leadership attention and resources.
Act on Intelligence and Share Lessons Learned	Make sure monitoring findings and third-party threat intelligence lead to action, and — with legal guidance on disclosure and liability — share incident experiences so others can learn from them.
Apply the CPD Framework to Sustain Ransomware Readiness	Use Commitment to secure leadership buy-in and resources, Preparedness to build detection and response capacity, and Discipline to keep plans rehearsed, audits real-time, and controls effective over time.

Time Stamps

TIME	CONTENT
0:02	Introduction — Dr. Chatterjee's background and credentials
0:48	Host framing: ransomware groups grow from 69 to 91; guest introduction
2:58	Mark Lance joins the discussion
3:13	Grounding for new listeners: what a ransomware attack is
5:15	Lance's professional journey and the evolution of ransomware toward double and triple extortion
8:59	Insular groups vs. ransomware-as-a-service platforms
9:49	Ransomware is here to stay — and why paying offers no guarantees
12:14	Multiple threat actors in one environment; cybercrime, APT, and hacktivist motivations
16:14	How multiple actors complicate incident response
16:50	How the incident began: anomalous inbound authentication
17:19	Attacker-issued tokens from exfiltrated authentication backups
18:41	Responding to cybercrime vs. an advanced threat still in staging
20:31	Planned containment, the scheduled eradication event, and corrupting the CFO's exfiltrated data
24:19	A governance failure: the CPD Framework introduced; recalibrating the threat model and proactive assessment
29:43	Tools as checkmarks; threat modeling, foundational controls, IR plans, playbooks, and tabletop exercises
33:46	Rehearsing plans, "destroy your business" scenarios, security drills, and real-time audits
38:22	Defenders need a plan as coordinated as the adversary's
39:01	Closing thoughts from Mark Lance: leverage others and share lessons learned
40:55	Special thanks and episode wrap-up

Memorable Quotes

> *The ransomware adversary has evolved into a fluid, professionalized market with its own supply chains and support desks.*
> **— Dr. Dave Chatterjee**

> *They've invested tons of money and effort into building platforms that are more sophisticated than the victim environments that they're targeting... So they're not going anywhere.*
> **— Mark Lance**

> *If you lock the two doors and only get four of the windows and leave one open, then [they're] right back in.*
> **— Mark Lance**

> *Just like we have fire drills, we need to have security drills.*
> **— Dr. Dave Chatterjee**

Disclaimer

The information contained in this summary is for general guidance only. The discussants assume no responsibility or liability for any errors or omissions in the content of this podcast. The information is provided on an as-is basis with no guarantee of completeness, accuracy, usefulness, or timeliness. The opinions and recommendations expressed are those of the discussants and not of any organization.

Dr. Dave Chatterjee | dchatte.com | dchatte@gmail.com | linkedin.com/in/dchatte