July 26 Read Time - 15 min

TECH mahindra

Whitepaper

Triple Extortion Tactics and Why Cyber Insurance is No Longer a Substitute for a Mature Incident Response Architecture

Author **Ashish Kumar Mishra**
Group Manager
Service Delivery, CSRM, Tech Mahindra

Content

Executive Summary

Ransomware has officially crossed its Rubicon. Cybercriminals no longer just encrypt files and hope for a payout; they have evolved into a mass-industrialized extortion cartel. Today's ransomware landscape operates like a dark-web Fortune 500 company complete with specialized corporate roles, calculated multi-tiered psychological pressure, and a clinical, data-driven understanding of exactly which financial levers will force an organization to pay.

The most significant characteristic of this era is triple extortion: encrypting data, exfiltrating it, and making demands that, if ignored, allow criminal organizations to communicate directly with your customers, regulators, and partners. There's a pressure level applied for each type of resistant victim. Cyber insurance, which most organizations rely on as their backstop to recovery, has slowly but surely begun to fail. Its sub-limits, nation-state exclusions, control warranties, and waiting periods have begun to undermine the basic recovery models that were established over the last five years.

The organizations that weathered the storm with the minimum damage from their major ransomware attacks were not those with the most extensive insurance policies; rather, those with the most developed incident response infrastructure, validated controls for identity, proven capability in detecting and analyzing, immutable backups, and teams who rehearsed response procedures before an attack occurred. The rationale for this investment is outlined in this white paper.

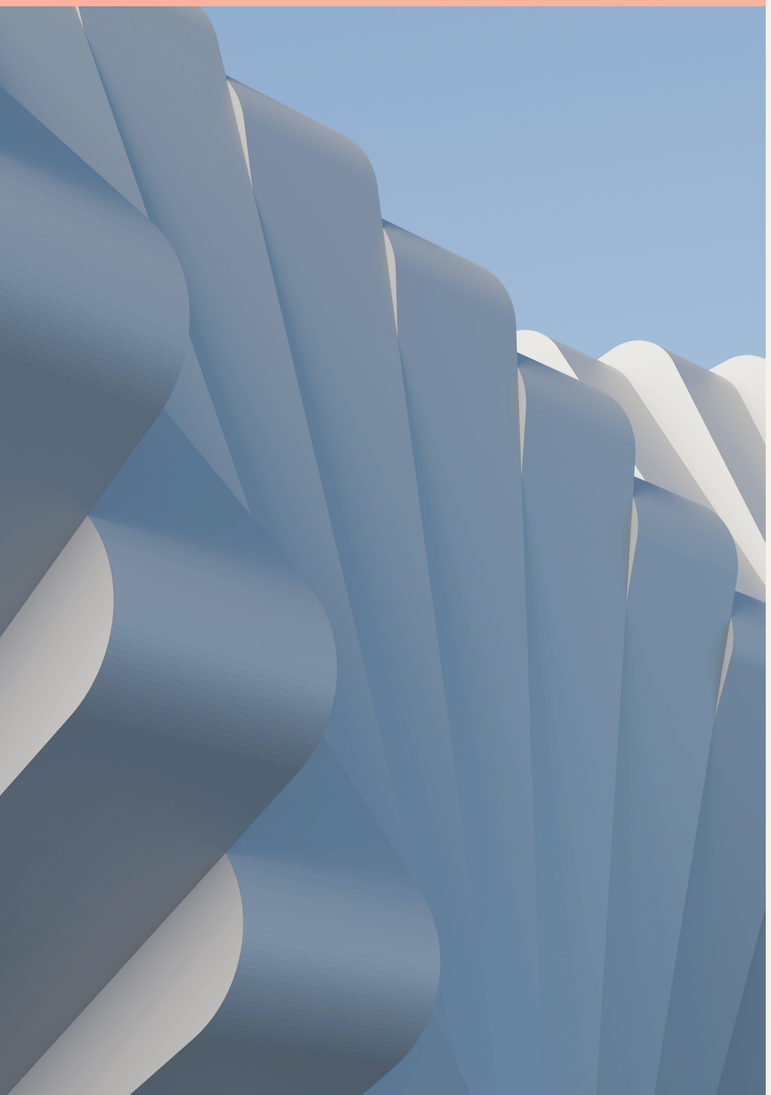
Introduction

For the most part, most security teams are fighting an enemy that has long since moved on. Perimeter solutions, signature detection, and insurance-backed recovery are based on a ransomware model that relied on speed and volume. This current model relies on leverage, and accordingly, the underlying infrastructure has professionalized.

Ransomware-as-a-Service has divorced development from execution. The affiliate who injects your systems with the encryptor may not have written a line of code. They are operating a licensed criminal franchise, buying access brokers with confirmed footholds in the network, and offloading ransom negotiations to professionals. The remainder is outsourced.

Why is this important to defenders? This model can't be dissuaded by friction; it will simply bypass it methodically and with considerable operational support. Ransom demands are also no longer made at random. Previous payment amounts, calculable limits for insurance policies, and sector-specific regulatory exposure all factor into the size of your bill.

The Ransomware 3.0 Economic Model



- **From Opportunistic to Industrialized**

  Initial ransomware was volume-based. Attack enough people, encrypt enough systems, and extract payment from whoever complies. Low per-attack cost with high failure rate wasn't a problem. It was groups like REvil and Conti who changed the game when they discovered that a single, carefully vetted enterprise target compromised through patience, not velocity, was worth more than ten thousand scattershot attacks. Ransom demands jumped from tens of thousands to tens of millions. It was an investment. And the return justified it.

  Ransomware 3.0 pushes this to its logical extreme. The significant shift is not technological, but rather the deliberate application of every available point of leverage to the pre-attack, attack, and post-attack phases.

- **The Triple Extortion Mechanism**

  Encryption hits first. All systems are locked down, business is down, and revenue has stopped instantly before anyone has time to truly process what has happened.

  The most glaring omission is that the attacker took data from your organization before encrypting anything. The attacker was probing customer lists, internal communications from the board, and sensitive M&A materials; data was copied from the environment while the attacker mapped its resources. Your clean backup only restores your systems; it doesn't remove any data that has already fallen into another's possession.

  This is the third stage, the least anticipated. Customers, partners, regulators, and even shareholders are contacted directly. Not by an anonymous ransom note. Certain groups, such as ALPHV/BlackCat, sent an email directly to patients of a breached healthcare organization, which would have caused them the most harm. At this stage, one is not negotiating with a threat actor. One is handling the immediate fallout of the crisis.

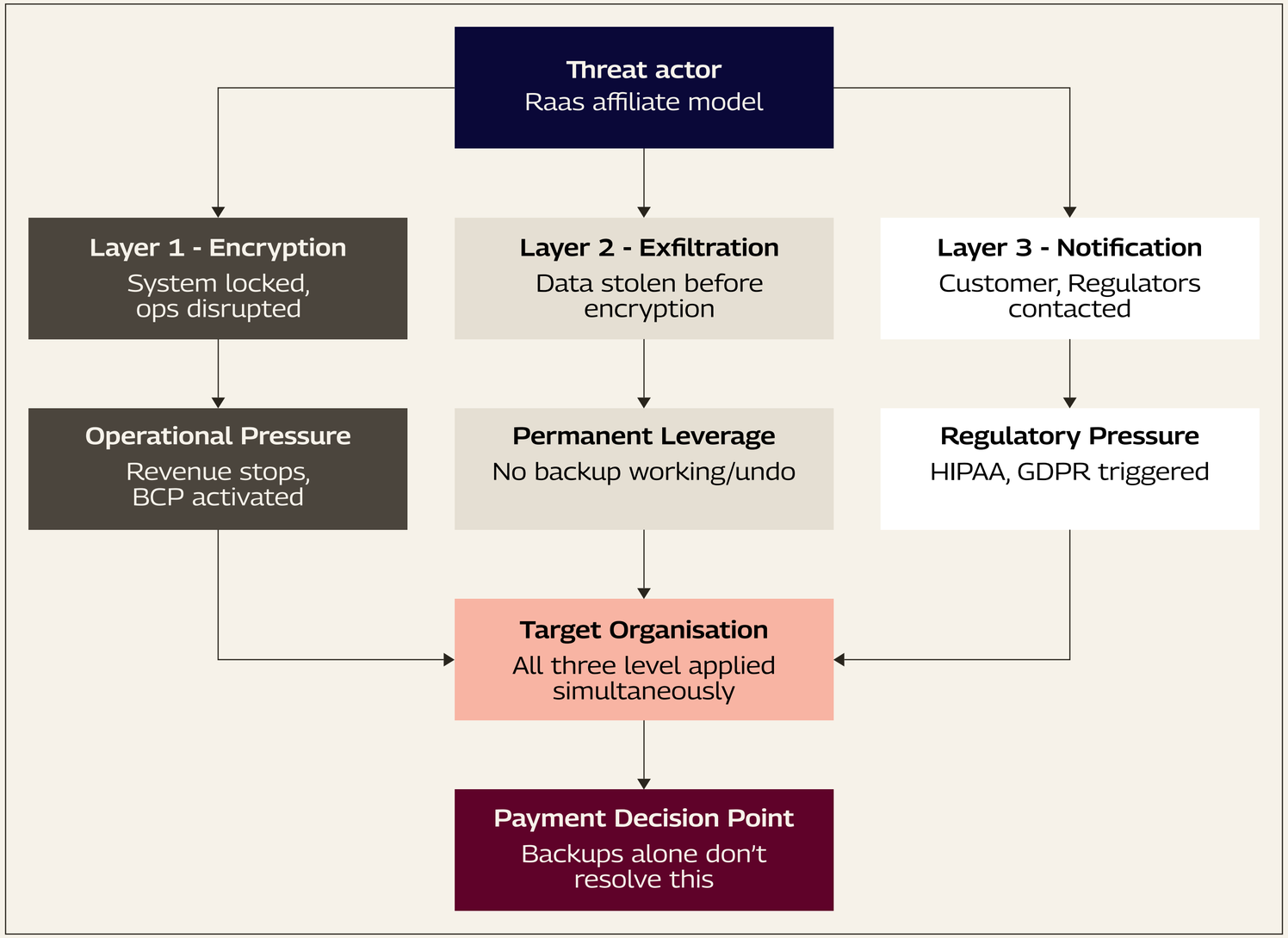


Figure 1: Triple Extortion Mechanism

- **The RaaS Supply Chain**

  This is how ransomware 3.0 scales: it relies on an affiliate model. Core developers design and host the encryptor, negotiation portal, and data leak site, then license the whole platform to affiliates who conduct actual campaigns and take 70 to 80 cents of each dollar of ransom. Initial access brokers supply network foothold access as a commodity; negotiation specialists offer ransom negotiations as a service.

  The result is a business that can quantify and value its victims. Past payment data, available SEC filings that reveal your insurance coverage limits, and the unique regulatory exposure of your sector all contribute to the rationale for your ransom demand. Discoverable insurance limits may become your minimum demanded payment.

Real-World Incidents—Lessons from the Front Line

- **Change Healthcare (2024): The Cost of a Missing Control**

  ALPHV/BlackCat didn't pull off a high-tech zero-day attack; instead, they were handed a Citrix remote access portal that lacked multi-factor authentication. They simply used a set of stolen credentials and strolled right in. What followed was weeks of unnoticed snooping, moving laterally through the network, and siphoning off 6 TB of data before the encryptor kicked in back in February 2024. At that point, the organization had no clue how deep the breach was, leaving it unable to act.

  The massive scale of Change Healthcare meant that the fallout was significant; about a third of all U.S. patient data flows through its systems.[9] Pharmacy claims processing stopped, forcing thousands of organizations to revert to manual operations and leaving some patients without access to their prescriptions for weeks. UnitedHealth Group ended up paying the $22 million ransom[10]. ALPHV received the money but didn't provide a decryptor and stopped communication. RansomHub, armed with the stolen data, reappeared and reiterated the demand with a fresh set of terms. The total cost for 2024? A staggering $3.09 billion.[11]

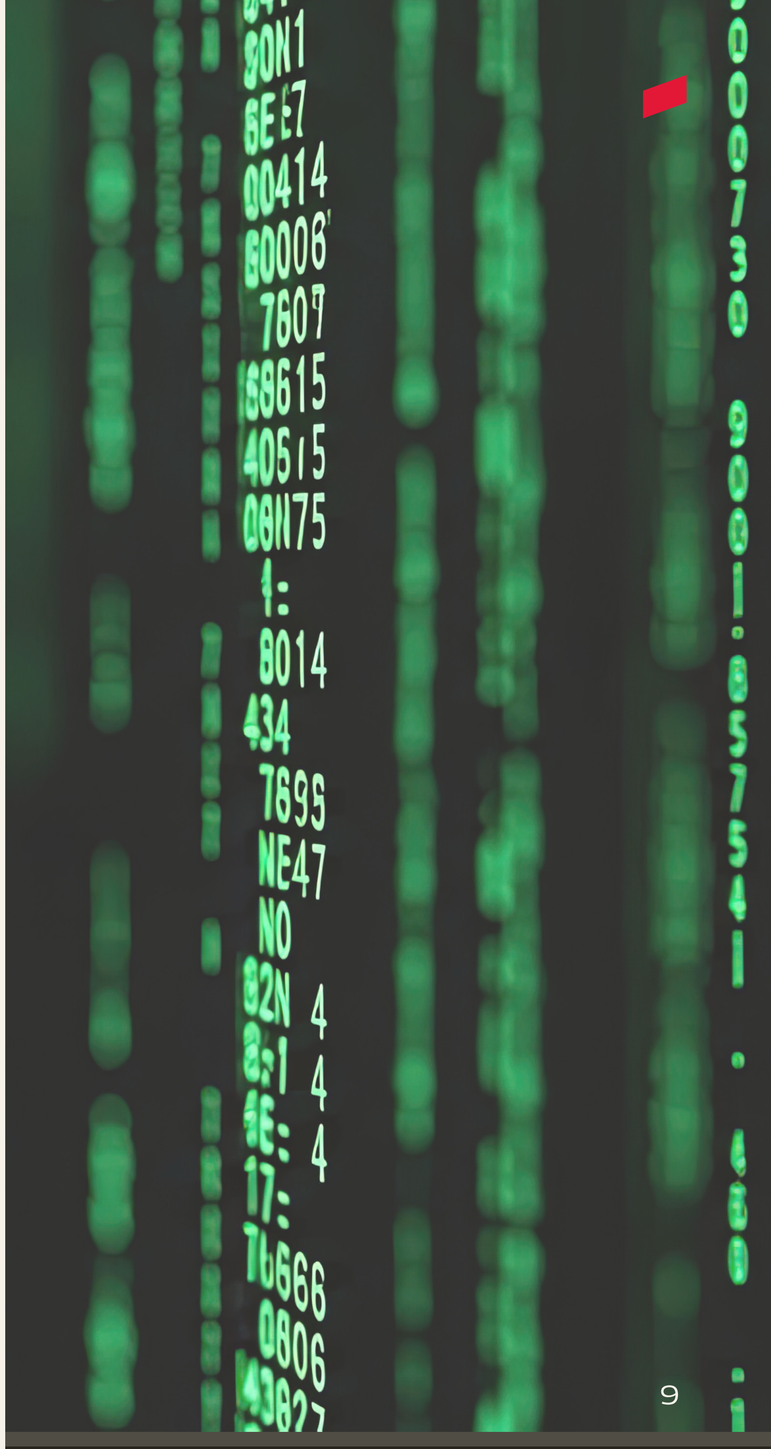
  For the professionals involved, the real issue lies in the narrative; it wasn't about the sophistication of the attack because there was none. A portal that claimed to be secure in its documentation was anything but. Weeks of internal movement didn't trigger any alerts, and this combination of factors points to an organization whose security measures existed mostly on paper. It's the actual verification of deployment, not just the documentation of plans, that truly defines your risk.

- **MGM Resorts (2023): When the Human Layer Fails**

It turns out there were no technology vulnerabilities at play. Scattered Spider managed to find an employee on LinkedIn, call MGM's help desk, and cleverly social-engineer a credential reset. Within just 10 minutes of establishing the connection, they allegedly accessed the Active Directory. Shortly after, BlackCat Ransomware struck, compromising check-in, slot, key, and reservation systems across various Las Vegas properties in a single, coordinated attack.

In just one month, their bill skyrocketed to around $100 million for one-time expenses, with remediation efforts likely pushing future SEC filings even higher.8

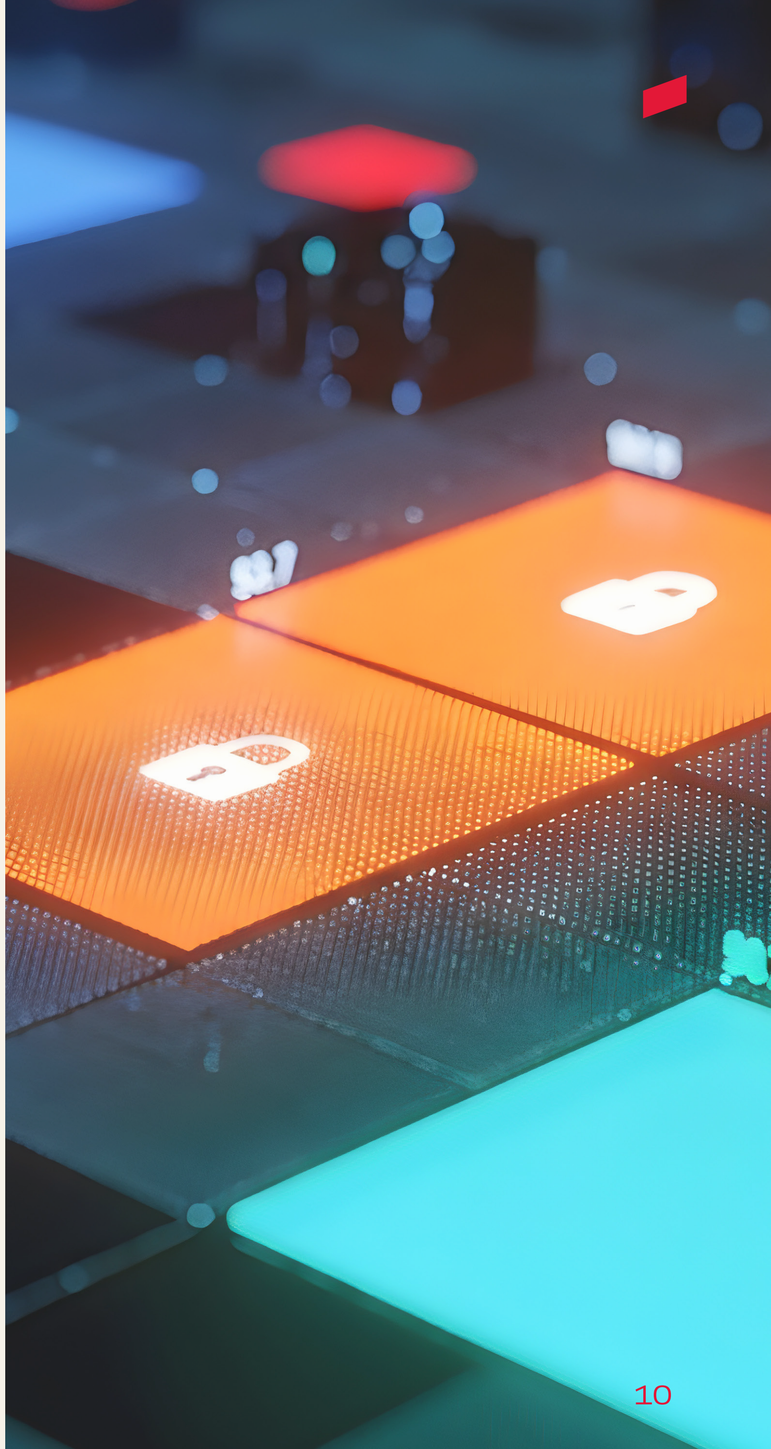
The crucial takeaway here is to know where your perimeter lies. Technical controls can’t protect you when someone is literally walking through the front door of your Active Directory instance, armed with a legitimate credential obtained in just a three-minute phone call. Out-of-band credential resets, privileged identity management, and social-engineering testing at the help desk aren’t just awareness-training items; they’re essential architectural controls that need to be integrated into your baseline security setup.



- **The ClOp MOVEit Campaign (2023): Encryption Is Optional**

  ClOp's use of CVE-2023-34362 in Progress Software's MOVEit Transfer has highlighted a crucial lesson for defenders: you don't need to encrypt anything to pull off a successful extortion scheme.[1] Just days after discovering the zero-day SQL injection vulnerability, ClOp managed to breach file transfer systems at more than 2,700 organizations worldwide, including big names like British Airways, the BBC, and Shell, as well as several U.S. federal agencies, often without even using an encryptor.[2] Simply having access to the data was enough leverage for them.

  If your ransomware defense strategy relies mainly on backup and recovery, the MOVEit campaign poses a serious threat to that approach. Exfiltration-based extortion doesn't care about how robust your backup systems are. Now, data classification, minimization, and egress monitoring have shifted from being secondary measures to essential ones. The speed of patch management for internet-facing systems, the actual time it takes from public disclosure to deployment, has become a critical, measurable risk factor with real consequences.[3]



- **Merck / NotPetya (2017–2024): The Insurance Precedent**

NotPetya ended up costing Merck around $1.4 billion.[4] When they filed a claim, the insurers denied it, citing a hostile or warlike action exclusion. Merck took the matter to court in New Jersey and came out on top at both the trial and appellate levels. The court determined that using 'hostile' to encompass a cyberattack on a civilian company not involved in any armed conflict was a stretch that the policy language simply didn't support. In January 2024, the remaining insurers decided to settle just days before the New Jersey Supreme Court was set to hear oral arguments.

Lloyds, however, didn't want to wait for that decision. In August 2022, they issued Market Bulletin Y5381, which required clear state-backed cyberattack exclusions in all standalone cyber policies starting March 2023.[5] The legal loophole that Merck's team managed to close over seven years of litigation has now been incorporated into standard policy language. Future policyholders won't have the same options available to them.

Insurance markets base their coverage pricing on past loss data rather than anticipating future threats. Exclusions that weren't present during your last renewal can suddenly pop up at the next one without any warning. Your cyber policy should be scrutinized just like any other significant contract. Sublimits, control warranties, attribution exclusions, and business interruption triggers should all be reviewed annually with legal counsel, not just handed off to procurement and forgotten.

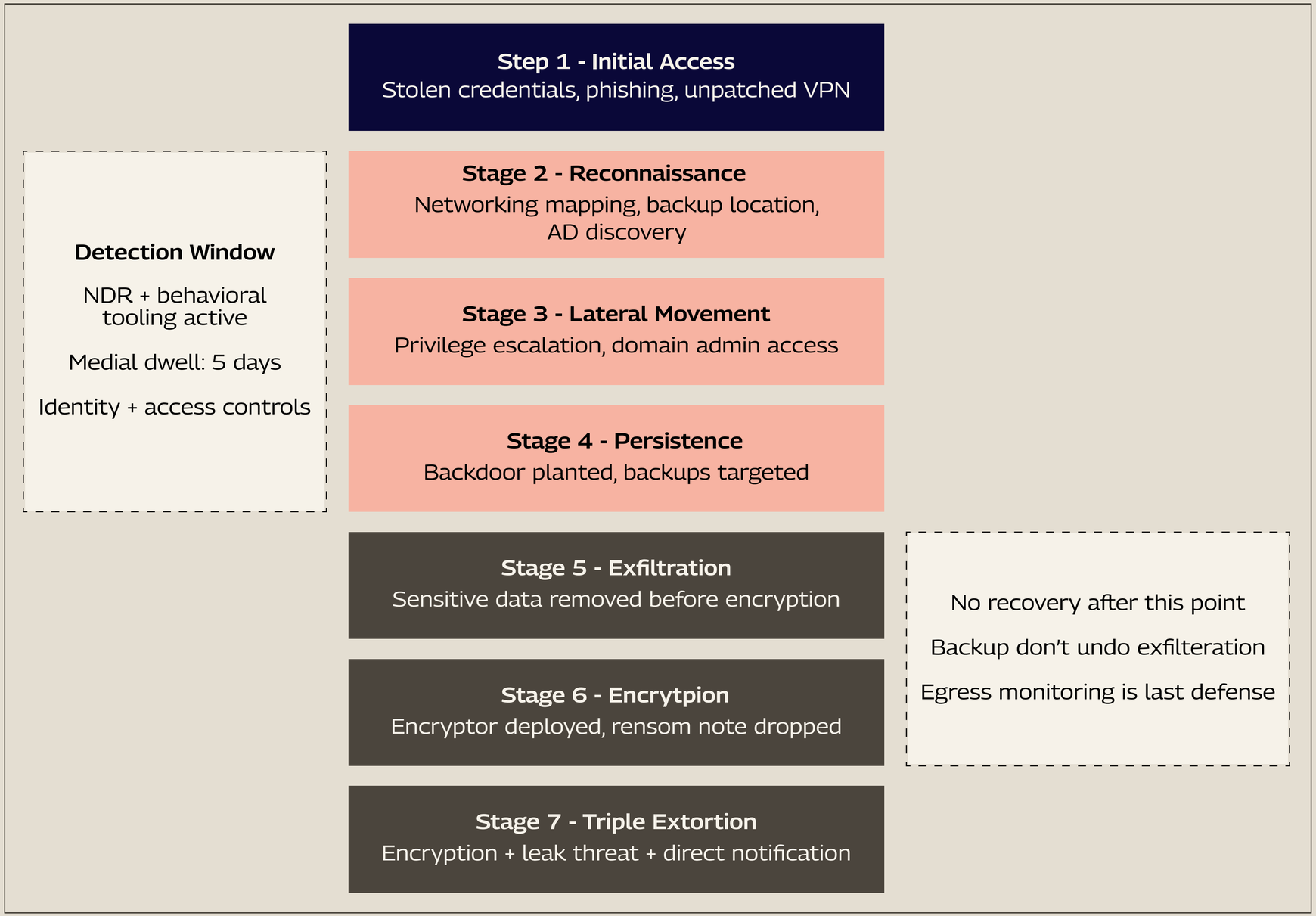


Figure 2: Ransomware 3.0 Kill Chain

The Cyber Insurance Erosion

- **How the Market Has Shifted**

  Cyber insurance gained traction in the late 2010s, but it was based on loss experiences that hadn't quite caught up with the actual threats out there. That all changed dramatically starting in 2020. Insurance carriers began to reprice, impose restrictions, and restructure their offerings, leading to a significant yet subtle shift in what you can expect from a policy when you really need it.

  Now, it's common to see ransomware sublimits. For instance, a $10 million policy might only cover $2 to $3 million for ransomware incidents specifically. Plus, co-insurance clauses can mean you have to take on a certain percentage of the losses yourself, and don't forget about those business interruption waiting periods, which usually last between 8 and 24 hours. This means the most damaging part of an attack might not even be covered.

- **The Control Warranty Problem**

  Security control warranties, which are often set as conditions for coverage, are where policies tend to fall short just when they're most needed. Sure, having multi-factor authentication (MFA) for remote access, endpoint detection and response (EDR) on devices, and offline backups all sound like sensible requirements on paper. But the real issue arises during a forensic review after an incident. If there's just one outdated portal without MFA or a gap in EDR on a single system, it can completely void your coverage. Not just reduce it but void it entirely. Organizations that thought they had solid policies in place have found out this harsh reality under the worst possible circumstances.

- **The Attribution Exclusion Risk**

  Attribution in ransomware cases is rarely straightforward, and insurers are well aware of this. When an insurer seeks to deny a significant claim, it has considerable leeway under Lloyd's Y5381, which has required state-backed cyberattack exclusions for all standalone cyber policies since March 2023.4 This allows them to invoke nation-state attribution and shift the burden of proof onto you. This isn't just a rare occurrence anymore; it's become standard practice.

  Cyber insurance should be part of your risk management strategy, serving as a backup for gaps your controls might miss. It was never intended to be the sole focus of a program.

Building a Mature Incident Response Architecture

- **The NIST CSF 2.0 is the Reference Framework**

The NIST Cybersecurity Framework 2.0, released in February 2024,6 remains the most practical guide for aligning incident response capabilities with the triple-extortion threat model. Its six key functions, Govern, Identify, Protect, Detect, Respond, and Recover, correspond directly to the phases of a ransomware attack. Your position on the maturity curve plays a crucial role in determining how quickly you can detect threats and how effectively you can bounce back if detection fails.

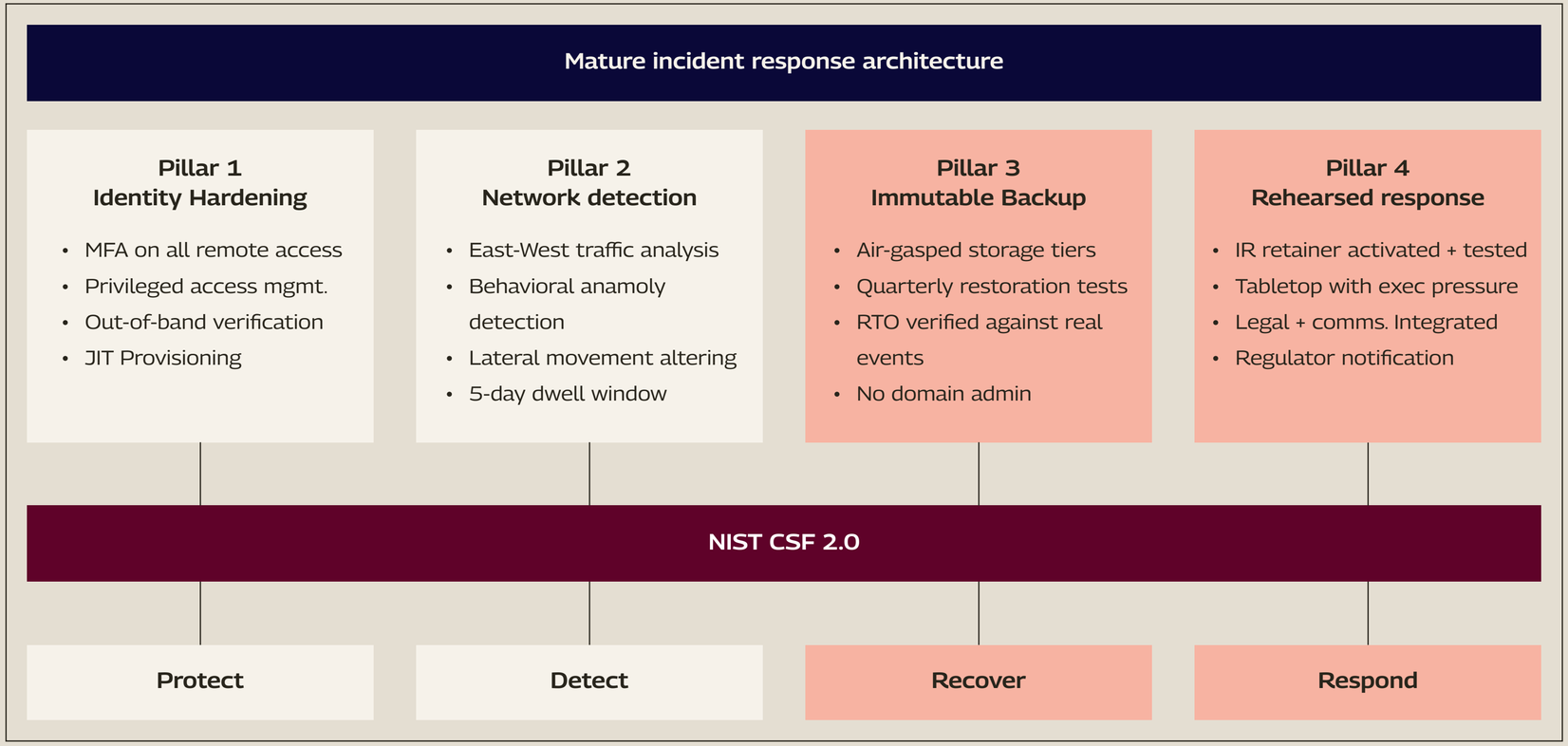


Figure 3: IR Architecture Stack

- **Identity and Access Hardening**

  Change Healthcare and MGM both faced the same fundamental issue with their identity controls, which failed before any technical defenses could kick in. One of them didn't have multi-factor authentication (MFA) set up on a Citrix portal, while the other lacked out-of-band verification for help desk credential resets. Fixing these gaps wouldn't have cost much at all.

  Implementing MFA for all remote access, ensuring privileged-access workstations are secure, using just-in-time provisioning, and requiring strict verification for credential resets aren't cutting-edge measures. They're the basics. The real problem in many environments isn't about having the right tools; it's the disconnect between what the policy documents state and what's in place.

- **Network Detection and Response**

  Imagine an attacker lurking in your environment for three weeks, already having infiltrated your domain controllers, prepped data for exfiltration, and mapped out your backup infrastructure, all before the encryptor kicks in. Each of these actions sends out network signals. The real question is whether there's anything in place to catch them.

  NDR tools monitor east-west traffic that perimeter tools often miss, creating a behavioral baseline and highlighting oddities, such as a workstation pinging Active Directory at 2 AM or unusual data volumes being funneled to an internal staging area. According to Sophos's 2024 Active Adversary Report, the median dwell time for ransomware is just five days. 7 That window of opportunity only exists if your tools are ready to act.

- **Immutable Backup Architecture**

  Sophisticated attackers are quick to locate your backups before they unleash the encryptor. They pinpoint the management console, grab the service account credentials, and take out the backup infrastructure right off the bat. If an attacker with domain admin credentials can access your backup environment, and in most organizations, they can, then you really don't have a solid recovery option.

  Immutability means that once data is written, it can't be changed or deleted for a set retention period, and this is enforced at the storage level. Think air-gapped or object-locked tiers, service accounts separate from your main active directory setup, and those quarterly restoration tests that measure recovery time against your recovery time objective (RTO). That last point is where many organizations hit a hidden snag: they often discover during an incident that recovery can take weeks rather than hours, making ransom payments seem like a reasonable choice, even if backups are technically available.

- **Rehearsed Response Capability**

  A response plan that just sits in a document isn't really a capability. Your incident response retainer needs to be activated and tested before you need it. Tabletop exercises should mimic scenarios that can truly stress organizations, such as communication breakdowns, legal hold requirements, regulatory notification deadlines, and the need for executive escalation all at once. The organizations that managed to contain major ransomware incidents the quickest weren't necessarily the ones with the fanciest tools. They were the teams that had faced similar challenges before, even if only in a simulation.

Recommendations for Organizations

- **Immediate Actions**

  Let's begin with verification rather than diving straight into documentation. Make sure to audit your MFA coverage across all remote access points—not just what your policy states, but what's in place and enforced. After that, grab your cyber insurance policy and have a sit-down with your legal counsel to closely review sublimits, control warranties, attribution exclusions, and the conditions that trigger business interruptions. Don't wait until renewal time to uncover any gaps; by then, it might be too late to negotiate.

  There are two controls that can significantly reduce your exposure without breaking the bank: implement out-of-band verification for credential resets as part of your process, not just as a training exercise, and conduct a tested backup restoration that aligns with your actual recovery time objective (RTO). If you haven't recently measured your real recovery time from a clean backup, you might be in the dark about your true negotiating power when an attacker comes knocking.

- **Strategic Initiatives**

  NDR tooling for east-west visibility addresses the dwell-time window more effectively than nearly any other investment. While perimeter detection might miss lateral movements, behavioral detection within the network picks up on those shifts. Plus, your incident response retainer should be operational before you need to activate it. It's crucial to practice against a triple extortion scenario and have escalation procedures in place that link your security, legal, and communications teams, not just IT.

  When it comes to data classification and egress monitoring, these should be part of your main control set, not just a box to check for compliance. Regulatory notification obligations like HIPAA, GDPR, and SEC disclosure rules require pre-drafted templates and legal processes that are already approved and integrated into your runbook. Making improvised notification decisions under the pressure of an active incident is where organizations often incur their most costly mistakes.

- **Cultural Shifts**

  A triple extortion event is a serious business crisis that kicks off with a security breach. From the moment an incident is declared, various teams like legal, communications, finance, and executive leadership each have specific roles to play, and it's crucial that they practice these roles ahead of time. Interestingly, the organizations that managed major ransomware incidents the best didn't necessarily have the largest security budgets. Instead, they had cross-functional teams that had trained together, backed by executive support, and engaged in exercises designed to create real pressure rather than just comfortable rehearsals.

Conclusion

Ransomware 3.0 isn't just a fancier version of an old problem; it's a whole new beast. This threat operates on economic principles, exploiting weaknesses in identity, leveraging regulatory pressures on engineers, and using your insurance coverage as a bargaining chip. The defenses we built for the last generation simply weren't made for this new model, and it's becoming painfully clear where the vulnerabilities lie.

Moving forward isn't rocket science, but it does call for some honest reflection. We need to focus on strengthening identities, detecting unusual behaviors, creating unchangeable backup systems, and developing well-practiced responses across teams—not because these measures will make us invulnerable, but because they're the only strategies that can effectively counter the way Ransomware 3.0 operates.

Insurance should be part of the strategy, but it can't be the entire strategy.

About the Author

Ashish Kumar Mishra

Group Manager
Service Delivery, CSRM
Tech Mahindra

Ashish Mishra is a seasoned IT professional and author with over 20 years of experience in the industry. He has a strong grasp and command of the IT (Information Technology), IS (Information Security), and Cyber Security domains. Ashish is also experienced in managing large IT and IS operations, strategy building, transformation journeys, project and program management, and service delivery. His expertise includes Public Cloud, Private Cloud, Cloud Security, Network Security, SASE, and Zero Trust.

With the thought process of 'continuous learning is the key to success,' he has obtained more than 150 professional certifications across various technologies and platforms related to public and private cloud, cloud security, information security, cybersecurity, compliance, infrastructure management, leadership, project management, and many more.

References

1) Cybersecurity and Infrastructure Security Agency. (2023). #StopRansomware: CL0P ransomware gang exploiting MOVEit Transfer vulnerability (Cybersecurity Advisory AA23-158A). U.S. Department of Homeland Security. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a

2) Emsisoft. (2024). MOVEit hack victim list. Emsisoft Blog. https://www.emsisoft.com/blog/

3) Verizon. (2024). 2024 data breach investigations report. https://www.verizon.com/business/resources/reports/dbir/

4) Insurance Journal. (2023, May 4). Merck wins appeal in $1.4B NotPetya cyber insurance lawsuit. https://www.insurancejournal.com/news/national/2024/01/05/754582.html

5) Lloyd's. (2022). Cyber-attack exclusions: Market bulletin Y5381. https://assets.lloyds.com/media/35926dc8-c885-497b-aed8-6d2f87c1415d/Y5381%20Market%20Bulletin%20-%20Cyber-attack%20exclusions.pdf

6) National Institute of Standards and Technology. (2024). The NIST cybersecurity framework (CSF) 2.0 (NIST Risk Management Framework 1). U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.29

7) Sophos. (2024). The 2024 active adversary report. https://www.sophos.com/en-us/content/active-adversary-report

8) MGM Resorts International. (2023). Form 8-K: Current report (SEC Filing). U.S. Securities and Exchange Commission. https://www.sec.gov/Archives/edgar/data/789570/000119312523251667/d461062d8k.htm

9) UnitedHealth Group. (2025). Fourth quarter 2024 results (SEC Earnings Release).
https://www.unitedhealthgroup.com/content/dam/UHG/PDF/investors/2024/2025-16-01-uhg-reports-fourth-quarter-results.pdf

10) U.S. Department of Health and Human Services, Office for Civil Rights. (2024). Change Healthcare investigation.
Change Healthcare Data Breach: 192.7 Million Affected - The HIPAA Guide

11) Mishra, A. (2026, May 15). The economics of ransomware 3.0. CSO Online.
https://www.csoonline.com/article/4171407/the-economics-of-ransomware-3-0.html

About Tech Mahindra

Tech Mahindra (NSE: TECHM) offers technology consulting and digital solutions to global enterprises across industries, enabling transformative scale at unparalleled speed. With 152,000+ professionals across 90+ countries helping 1100+ clients, Tech Mahindra provides a full spectrum of services including consult-ing, information technology, enterprise applications, business process services, engineering services, network services, customer experience & design, Al & analytics, and cloud & infrastructure services. It is the first Indian company in the world to have been awarded the Sustainable Markets Initiative's Terra Carta Seal, which recognises global companies that are actively leading the charge to create a climate and nature-positive future. Tech Mahindra is part of the Mahindra Group, founded in 1945, one of the largest and most admired multinational federation of companies. For more information on how TechM can partner with you to meet your Scale at Speed™ imperatives, please visit https://www.techmahindra.com/.

TECH mahindra

www.techmahindra.com
www.linkedin.com/company/tech-mahindra
www.twitter.com/tech_mahindra