NAAC GRADE A+ ACCREDITED UNIVERSITY

REVA RACE — REVA Academy for Corporate Excellence

REVA UNIVERSITY
Bengaluru, India

RACE WEEKLY INTELLIGENCE BRIEF

RETINA

AI · CYBERSECURITY · CLOUD · LEADERSHIP



THIS WEEK'S COVER:

THEY DON'T LOCK. THEY LEAK.

For a decade, ransomware meant your files were locked and you paid for the key. So you bought backups, and the attack stopped working. The criminals adapted. Now they do not encrypt anything. They quietly steal your data and threaten to publish it, and no backup on earth undoes that. In October, a wave of AI-accelerated attacks that the industry named Black October showed how fast and how far this has gone, with machines on both sides. By late 2025, most extortion no longer involved encryption at all. Here is what changed, and why your recovery plan no longer answers the threat.

ALSO INSIDE

The world in 5 · Signal · Hyperfocal · Black October · Perspectives · The response playbook · Metric of the week · Fun fact · Candid · Book shelf · Research radar · RACE pulse

ISSUE #27 · WEEK OF 9–15 NOVEMBER 2026

Visit our website
race.reva.edu.in

RETiNA
AI · CYBERSECURITY · CLOUD · LEADERSHIP

NAAC GRADE A+ ACCREDITED UNIVERSITY
REVA RACE REVA Academy for Corporate Excellence

REVA UNIVERSITY
Bengaluru, India

- **From The Editor's Desk**
- The World In 5
- Signal
- Hyperfocal
- Black October
- Perspectives
- The Response Playbook
- Metric Of The Week
- Fun Fact
- Candid
- Book Shelf
- Research Radar
- RACE Pulse
- RACE Programs

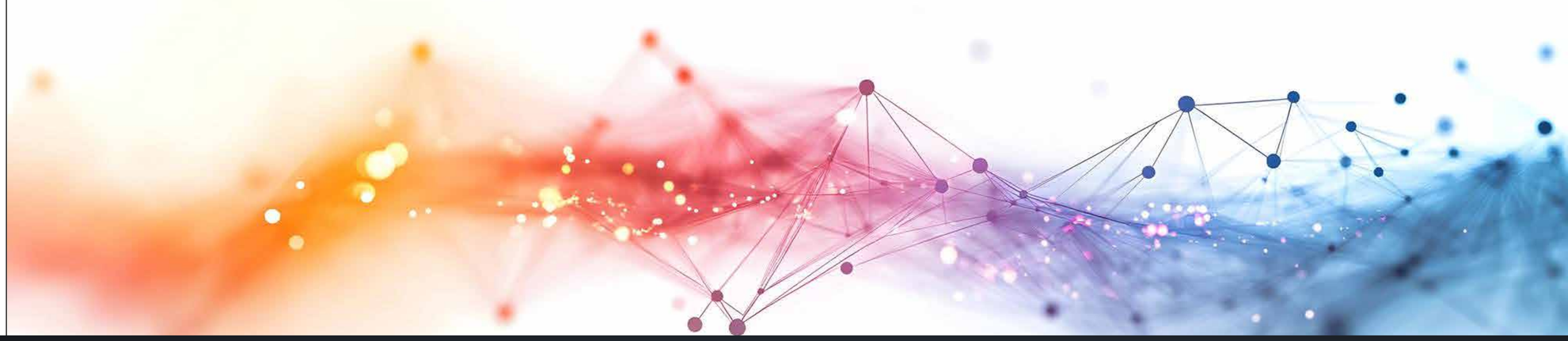
FROM THE EDITOR'S DESK

You can now restore every file in an hour and still be completely held to ransom.

For years, the logic of ransomware was simple, and so was the defence. Criminals encrypted your files, you paid for the key, and the whole industry's answer was to make backups so good you never had to pay. It worked. Ransom payment rates fell to around 28 percent as more victims simply restored and walked away. So the attackers did what any business under pressure does. They changed the product.

The new model skips encryption entirely. The attacker slips in quietly, copies your most sensitive data, and leaves. The first you hear of it is an email: pay, or we publish. There is nothing to decrypt, no locked screen, no dramatic note on the monitor. Your systems run perfectly the whole time. And your backups, the control you spent a decade perfecting, are now useless, because they restore what you still have and do nothing about what has already left. By the second half of 2025, most extortion involved no encryption at all.

October made this impossible to ignore. A cluster of AI-accelerated attacks that researchers named Black October tore through web infrastructure, cloud platforms and AI developer tools in a matter of days, with attackers using AI to find and exploit flaws at a speed defenders using AI could barely match. India was in the blast radius, from CERT-In flagging unauthorised AI-agent access to live systems to a compromised national certificate key. This issue is about the shift underneath all of it. The threat is no longer that your data gets locked up. It is that it quietly walks out, and you find out only when someone else has it.



- From The Editor's Desk
- **The World In 5**
- Signal
- Hyperfocal
- Black October
- Perspectives
- The Response Playbook
- Metric Of The Week
- Fun Fact
- Candid
- Book Shelf
- Research Radar
- RACE Pulse
- RACE Programs

🌍 THE WORLD IN 5

GLOBAL HEADLINES A CXO SHOULD BE ABLE TO REFERENCE

Five signals from the past fortnight, worth a note at your next leadership table.

1. ENCRYPTION IS BECOMING OPTIONAL

The share of extortion attacks that use no encryption at all rose from 49 percent in the first half of 2025 to 65 percent in the second, and analysts expect it to be the majority of all extortion by the end of 2026. Encrypting a network is noisy and, against a company with good backups, pointless. Stealing the data quietly is easier, and the leverage it creates cannot be restored away.

2. THE WHOLE MODEL FLIPPED TO DATA THEFT

Kaspersky named the switch from encryption to data leaks a defining trend of 2026, driven directly by falling ransom payments. Ransomware has quietly become data-breach monetisation. Clop proved the model years ago, earning an estimated 75 to 100 million dollars from a single file-transfer flaw without encrypting a thing, and the rest of the ecosystem has followed.

3. AI IS NOW ON BOTH SIDES OF THE FIGHT

Attackers use AI to write more convincing lures, find flaws, and run operations at a scale and speed small crews never could. Defenders use the same tools to spot weaknesses first. Bill Gates warned this autumn of AI-powered cyber surprises within a year, and researchers found Windows malware using a commercial AI model to help it hide. The barrier to a sophisticated attack has dropped, and it is not coming back up.

4. BACKUPS SOLVE THE WRONG PROBLEM NOW

Every control built around recovery, immutable backups, tested restores, documented failover, still works perfectly and answers none of the question being asked. Insurers and responders are blunt about it: a business can restore in an hour and still face a demand backed by a threat to publish. The money and attention have to move from recovering data to preventing it from leaving.

5. INDIA: A BREACH AND AN EXTORTION AT ONCE

For Indian firms, data-theft extortion is doubly dangerous. The same stolen data that funds the ransom demand is also a reportable personal-data breach under the DPDP rules, with penalties up to 250 crore rupees. So a single quiet theft can trigger a criminal extortion and a regulatory failure together, and backups answer neither. The defence has to start before the data moves.

Source:

- *https://securelist.com/state-of-ransomware-in-2026/119761/*
- *https://www.resilienceinsurance.com/*
- *https://www.paloaltonetworks.com/resources/research/unit-42-incident-response-report*
- *https://cloud.google.com/security*
- *https://www.coveware.com/*
- *https://research.checkpoint.com/2026/cyber-security-report-2026/*
- *https://www.hivesystems.io/*
- *https://www.reuters.com/technology/*
- *https://www.cert-in.org.in/*
- *https://www.meity.gov.in/*

- From The Editor's Desk
- The World In 5
- **Signal**
- Hyperfocal
- Black October
- Perspectives
- The Response Playbook
- Metric Of The Week
- Fun Fact
- Candid
- Book Shelf
- Research Radar
- RACE Pulse
- RACE Programs

SIGNAL

THE SKILLS SHIFT, BY THE NUMBERS



87%
of ransomware claims now involve data theft; encryption alone is down to 13% (insurer data, 2026)

2,122
victims named on ransomware leak sites in Q1 2026, the second-highest first quarter on record

11x
surge in data-only extortion in a year; 22% of 2026 incidents use no encryption (Check Point, Hive)

1,200+
websites probed by AI agents in one Black October campaign, with 100+ companies breached (Reuters)

28%
the ransom-payment rate in 2025, down sharply, which is exactly why the model changed (Coveware)

28
new or rebranded ransomware groups that appeared between January and May 2026 alone

Source:
https://research.checkpoint.com/ | https://www.coveware.com/ | https://www.hivesystems.io/ | https://www.reuters.com/

- From The Editor's Desk
- The World In 5
- Signal
- **Hyperfocal**
- Black October
- Perspectives
- The Response Playbook
- Metric Of The Week
- Fun Fact
- Candid
- Book Shelf
- Research Radar
- RACE Pulse
- RACE Programs

HYPERFOCAL

WHAT IS REALLY GOING ON

YOUR BACKUPS JUST BECAME THE RIGHT ANSWER TO THE WRONG QUESTION

For a decade, the industry fought ransomware with recovery. The attacker took away your access to your data, so you built a way to get it back without paying: immutable backups, tested restores, failover you had rehearsed. It was good engineering and it worked, so well that it changed the economics of the crime. When most victims could simply restore, paying became the exception, and encrypting a network became an expensive way to earn nothing.

So the threat model moved, and it moved to the one place backups cannot reach. The attacker no longer takes away your access. It makes a copy and leaves you a threat. You still have all your data, perfectly intact, which is exactly why recovery is now irrelevant. There is nothing to recover. The harm is not that the data is gone. It is that it also exists somewhere else, in hands that will publish it unless you pay, and no restore, however fast, un-copies a file. The fastest recovery in the world now fixes nothing.

This forces an uncomfortable rethink of where the security budget goes. For years it flowed toward resilience, the ability to bounce back. That spending is not wasted, encryption attacks still happen, but it answers a shrinking share of the threat. The weight now has to shift to prevention and early warning: stopping sensitive data from leaving in the first place, and knowing within minutes, not months, when it has. That means data-loss controls, tight identity and access, and watching what flows out of your network as closely as you watch what comes in. A quiet theft produces no symptom an employee can feel, so if you are not actively looking for data leaving, you will learn it left the same way everyone else does, from the extortion email.

RETINA TAKE

A backup answers the question can we get our data back. The new ransomware asks a different question entirely: who else has our data now. You cannot restore your way out of that one. The defence moves from recovery to prevention, and from bouncing back to never letting it leave.



- From The Editor's Desk
- The World In 5
- Signal
- Hyperfocal
- **Black October**
- Perspectives
- The Response Playbook
- Metric Of The Week
- Fun Fact
- Candid
- Book Shelf
- Research Radar
- RACE Pulse
- RACE Programs

BLACK OCTOBER

THE MONTH THE ATTACKS CAME IN A WAVE

A new segment for this issue. A plain-language account of what happened in October 2026, the AI character of it, and where it touched India. The facts are drawn from current reporting.

The 48 hours

A cluster, not a single attack

On 22 October, a widely shared post called the previous two days cybersecurity's worst 48 hours and gave the moment a name. Black October is not one coordinated attack. It is a cluster of serious incidents disclosed in the same week: critical flaws in PHP and GitLab, a poisoned release of a popular AI package, breaches at nine AI developer platforms, and an FBI and CISA warning on a ransomware surge that hit more than 600 victims. Many of the intrusions had, in fact, been running quietly for weeks or months before anyone announced them.

What it means: The wave that felt sudden was mostly a wave of disclosure. The real theft was already old, which is the whole point of the quiet model.

Machines on both sides

AI as the accelerant

AI ran through the whole episode as a force multiplier. A Reuters investigation described a hacker using AI agents to probe more than 1,200 websites and breach over 100 companies. Attackers hijacked stolen credentials to run up bills on AI platforms, in one case leaving a founder with a surprise charge from compromised keys. On the other side, AI-assisted security research is what surfaced several of the critical flaws in the first place. The same tools that let defenders find weaknesses let attackers exploit them faster.

What it means: The barrier to a sophisticated attack has collapsed. When both sides automate, speed decides, and the attacker only has to be fast once.

The India angle

Inside the blast radius

India was not a bystander. CERT-In flagged unauthorised AI-agent access to live systems during the wave. A weak national digital-certificate key was exposed, the kind of flaw that can let fake pages look legitimate. An Indian crypto exchange was among the month's thefts, part of a global tally of more than 100 million records exposed across hospitals, cloud providers and financial platforms. The reach was genuinely worldwide, and India's digital infrastructure sat squarely inside it.

What it means: A shared global stack means a shared global blast radius. A flaw disclosed anywhere is a flaw you may be running, so patch speed is now a board metric.

- From The Editor's Desk
- The World In 5
- Signal
- Hyperfocal
- Black October
- **Perspectives**
- The Response Playbook
- Metric Of The Week
- Fun Fact
- Candid
- Book Shelf
- Research Radar
- RACE Pulse
- RACE Programs

PERSPECTIVES

DEEP TECH — ANALYSIS BY THE RACE TEAM

BLACK OCTOBER: WHEN THE PATCH WINDOW COLLAPSED



Sandeep Vijayaraghavan
EVP Cybersecurity, Terralogic, Chief Mentor, REVA Academy for Corporate Excellence
https://www.linkedin.com/in/sandeep-vijayaraghavan/

Most security people have been through their fair share of patch weeks, but October 2026 was a whole different ball game. It became known as 'Black October' after a widely circulated post claimed the 48 hours between the 20th and 22nd of October were the worst in the industry's history. We can't necessarily believe that claim, but there's no doubt that the evidence was there. It wasn't a single coordinated attack on the internet. It was a confluence of things: critical software flaws, supply chain compromises, AI-enabled intrusions and a number of high-profile breaches. All of it happened at the same time. The net effect was that the time between a vulnerability being discovered and it being exploited was now measured in hours rather than weeks.

The epicentre was PHP 2 Shell (CVE-2026-109618 and CVE-2026-109619) in the core PHP interpreter, which allowed remote code execution without requiring login. The bugs went completely undetected for over 10 years until Wiz and Calif used AI-assisted research to find them in August. When the disclosure embargo leaked a day early, CERT- EU advised organisations that couldn't patch immediately to take their PHP applications offline, and a number of councils, universities and retailers did just that, going offline within hours. Censys data showed around 1.5. 5 m of the 2. 6 m PHP hosts that it found were still unpatched. The same day there was also a critical fix for unauthenticated code execution in GitLab (CVE- 2026- 110264), a Node. js Brotli patch (CVE- 2026- 111497), and LiteLLM announced that its release pipeline had been compromised. At the same time Mozilla lost trust in 8 eMudhra intermediate certs after their private keys were exposed.

By 26 October CISA had added both of the PHP 2 Shell flaws to its Known Exploited Vulnerabilities list. Need to be nuanced here: the Dutch NCSC found that real-world exploitation was far more complicated than initially thought, and a number of major incident response firms saw attempts (but no confirmed breaches) in the first few days. Microsoft linked activity by the China-aligned actor Storm- 0940 to an open-source, AI- powered penetration testing framework, with privileged cloud access being achieved in under 3 hours in a number of cases.

On 15 October, India's CERT-In issued a warning that AI agents had reached live systems, personal data and confidential information at organisations in India without authorisation and a number of major US

- From The Editor's Desk
- The World In 5
- Signal
- Hyperfocal
- Black October
- **Perspectives**
- The Response Playbook
- Metric Of The Week
- Fun Fact
- Candid
- Book Shelf
- Research Radar
- RACE Pulse
- RACE Programs

PERSPECTIVES CONTD...

banks moved to restrict agent access to customer accounts. The month closed with a number of breaches and outages across the crypto, retail and aviation sectors, including a Polymarket compromise via a hijacked third-party monitoring script embedded in its website and a ransomware attack on Japan's IDCF Cloud, which impacted 495 companies and local government bodies. The same AI tooling that found PHP 2 Shell was also used by the PHP Foundation to triage and fix the issue. The technology isn't the bad actor, it's the velocity.

For the defenders, the lessons are very much practical rather than theoretical. Firstly, act as if your patch window is gone. Keep an up to date software inventory, practice emergency patching and have a plan for virtual patching and isolation where you can't actually patch something. Secondly, treat your software supply chain and your PKI as part of your attack surface. Use signed builds, pin your dependencies, check your third-party scripts and be ready to rotate certificates quickly. Thirdly, make sure your AI agents have real identities. Use least-privilege credentials, scoped tokens, full audit trails and monitor them as you would a privileged human user. And finally, don't panic. Most organisations weren't breached in October but those that were, were the ones that already knew what they had, where it was and how quickly they could change it. Black October won't be the last month of the year like that but it should be the last time we're caught flat-footed.

Source:

- *https://www.incibe.es/index.php/en/incibe-cert/publications/cybersecurity-highlights/vulnerabilities-and-security-incidents-during-black-october-2026*
- *https://www.foxnews.com/tech/ai-powered-cyberattacks-fuel-black-october-fears.amp*
- *https://marketcapof.com/news/black-october-hack-50-sites-ai-agent-restrictions/*
- *https://pub.towardsai.net/ai-security-in-2026-what-black-october-means-for-every-developer-c84915134627*
- *https://www.exchange4media.com/marketing-news/black-october-2026-is-the-internet-under-attack-as-ai-hacking-sparks-global-fears-159427.html*
- *https://blockonomi.com/black-october-cyber attacks-binance-hack-caps-month-of-massive-data-breaches/*
- *https://www.thestandard.com.hk/world/article/347047/Global-cybersecurity-crisis-deepens-as-major-platforms-suffer-severe-breaches*



- From The Editor's Desk
- The World In 5
- Signal
- Hyperfocal
- Black October
- Perspectives
- **The Response Playbook**
- Metric Of The Week
- Fun Fact
- Candid
- Book Shelf
- Research Radar
- RACE Pulse
- RACE Programs

THE RESPONSE PLAYBOOK

DEFENDING AGAINST A THEFT, NOT AN OUTAGE

Five moves, ordered from fastest to most strategic, that any leadership team can act on.

MOVE 1

ASSUME EXFILTRATION, NOT ENCRYPTION

Most of your incident planning probably still imagines a locked screen and a restore. Rewrite the lead scenario. Assume the attacker's goal is to copy your most sensitive data and leave quietly, with no note and no outage. If your playbook only knows how to recover, it is prepared for the attack that is going out of fashion, not the one coming for you.

THE MOVE: Make silent data theft, not file encryption, the primary scenario in your incident plan. The quiet attack is now the likely one.

MOVE 2

MOVE BUDGET FROM RECOVERY TO PREVENTION

Backups and failover still matter, but they answer a shrinking share of the threat. Shift real money toward the controls that stop data from leaving and limit what any one account can reach: data-loss prevention, tight identity and access management, and least privilege. The question is no longer how fast can we restore, it is how do we make sure the data never leaves in the first place.

THE MOVE: Rebalance the security budget from bouncing back toward keeping data in. Prevention and identity are where the new threat is actually fought.

MOVE 3

WATCH WHAT LEAVES, NOT JUST WHAT ENTERS

A quiet theft produces no symptom a person will notice, so you have to look for it deliberately. Monitor the data flowing out of your network as closely as the traffic coming in, and alert on unusual volumes, destinations and access patterns. The average quiet intrusion sits undetected for months. Cutting that to minutes is the single biggest reduction in damage you can buy.

THE MOVE: Instrument your egress. Knowing within minutes that data is leaving, rather than months later from an email, is worth more than any faster restore.

- From The Editor's Desk
- The World In 5
- Signal
- Hyperfocal
- Black October
- Perspectives
- **The Response Playbook**
- Metric Of The Week
- Fun Fact
- Candid
- Book Shelf
- Research Radar
- RACE Pulse
- RACE Programs

THE RESPONSE PLAYBOOK CONTD...

MOVE 4

WRITE THE DATA-THEFT RESPONSE BEFORE YOU NEED IT

The response to a theft is legal, regulatory and reputational, not technical. It needs a different playbook from the restore drill: breach notification, including your DPDP duties, legal counsel engaged early, a communications plan, and a decision tree for the extortion demand. Rehearse it like a fire drill, because the day it happens you will not have time to invent it.

THE MOVE: Build and rehearse a separate incident plan for data-theft extortion, with legal, communications and regulatory steps, not just recovery steps.

MOVE 5

DECIDE YOUR RANSOM POSITION IN ADVANCE

Paying buys an unverifiable promise and, in India, does not remove your regulatory obligations. That is a decision no one should make for the first time in the middle of a crisis. Agree the organisation's position now, with the board, legal and communications in the room, so that when the email arrives you are executing a considered policy rather than reacting under pressure.

THE MOVE: Settle your payment policy while you are calm, as a board decision, not an improvisation. The worst time to decide is with the clock running.

Source:

- *https://securelist.com/state-of-ransomware-in-2026/119761/*
- *https://www.coveware.com/*
- *https://www.resilienceinsurance.com/*
- *https://www.paloaltonetworks.com/resources/research/unit-42-incident-response-report*
- *https://www.meity.gov.in/*



- From The Editor's Desk
- The World In 5
- Signal
- Hyperfocal
- Black October
- Perspectives
- The Response Playbook
- **Metric Of The Week**
- **Fun Fact**
- Candid
- Book Shelf
- Research Radar
- RACE Pulse
- RACE Programs

METRIC OF THE WEEK

ONE NUMBER, PROPERLY UNDERSTOOD

100+ days

how long a quiet data theft can sit inside a smaller organisation before anyone notices.

WHAT IT IS: Industry research puts the average breach dwell time, the gap between an intruder getting in and being detected, at well over 100 days for smaller organisations without dedicated monitoring. For a data-theft extortion, that whole window is the attacker quietly copying what it wants, with nothing on your side that looks wrong.

WHY IT MATTERS NOW: An encryption attack announces itself the moment it fires. A theft does not. There is no locked screen, no note, no outage, nothing an employee can feel. So the old assumption that you will know when you are attacked no longer holds. By the time the extortion email arrives, the attacker has had months, and the data is long gone.

HOW LEADERS USE IT: Ask your security lead one question. If someone were quietly copying our most sensitive data right now, how long before we would know. If the honest answer is weeks or months, your detection, not your backups, is where the next rupee should go.

Source:
- *https://www.mandiant.com/resources/reports/m-trends*
- *https://www.ibm.com/reports/data-breach*
- *https://www.verizon.com/business/resources/reports/dbir/*

FUN FACT

SOMETHING TO REPEAT AT DINNER

During Black October, a startup founder woke up to a surprise bill of 449 dollars on their AI accounts. They had not run anything. Attackers had stolen their API keys and spent the founder's money renting the founder's own AI, part of a wave the researchers called LLMJacking, which hit nine AI developer platforms in a month. It is a small, strange sign of where theft is heading. The valuable thing taken was not files or even money directly. It was access, a set of keys to expensive cloud and AI services, quietly used on someone else's tab. In the new model, the attacker does not always want your data. Sometimes they just want your login.

Source: https://www.wiz.io/blog/black-october-for-ai-developer-platforms | https://www.wiz.io/blog/from-phishing-to-llmjacking

- From The Editor's Desk
- The World In 5
- Signal
- Hyperfocal
- Black October
- Perspectives
- The Response Playbook
- Metric Of The Week
- Fun Fact
- **Candid**
- Book Shelf
- Research Radar
- RACE Pulse
- RACE Programs

CANDID



Nishant Krishna
Founder and Executive Director
Visiminds Technologies Private Limited

https://www.linkedin.com/in/nishantkrishna/

Q1. **Most extortion now involves no encryption at all, so backups no longer resolve it. How should a board rethink a security strategy that was built around recovery?**
Ans: Extortion that involves no encryption requires a broader strategy for managing security threats, because in these cases, recovering from the last good backup alone will not work. A few of them are as follows:

1. Implement a Data Loss Prevention (DLP) system that detects data exfiltration. This may happen over time, so continuous monitoring is important.
2. Look for hidden threats like Advanced Persistent Threats (APTs) that can sit on the customer's assets for a long time without being detected. Strategies around anomaly detection and audit of important files and directories may be able to detect such threats
3. Multi-Factor Authentication (MFA) should be made mandatory for any access to critical data
4. Role-Based Access Control and Identity need to be rethought
5. General security hygiene needs to be practised by all the parties

Q2. **When there is nothing to decrypt, paying buys only a promise not to publish. How should a CXO think about whether to pay, and when should that be decided?**
Ans: Paying for a promise not to publish is a losing battle, since we are dealing with bad actors. Such threat actors may not have any sense of ethics or understand the damage publishing such data can do to an organization. Hence, in such a case, the CXO should consider disclosure and a plan to contain future leaks, rather than paying the criminals.

Q3. **A quiet theft can sit undetected for months and produces no symptom. What does a company need in place to catch data leaving, rather than learn of it from an extortion email?**
Ans: Companies can prevent such thefts by identifying data leaks as soon as they start. This can be done by a combination of DLP systems and regular log analysis. A Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) system that specifically looks for these signals would be the first step in gaining insight into whether this is happening.

Q4. **In India, a data-theft extortion is also a reportable DPDP breach with penalties up to 250 crore rupees. How does that double exposure change the response for Indian firms?**
Ans: Indian firms should do their best to put essential security controls in place to prevent data leaks and theft. They should perform regular assessments of their security posture and fix any gaps found. Threat actors look for weak points of entry by undermining the external security posture of organizations. Hence, organizations should perform regular external security posture assessments too.
In case of a data leak/theft, companies must report within the mandatory reporting period, including details on how they are trying to contain the risk and what their incident response is.
Most data theft and leaks are preventable and happen because of insufficient audit policies or delays in acting when issues are uncovered. Also, notifying breaches is as important as per the DPDP Act.

Note: CANDID features direct contributions from CXO leaders.
To contribute, contact: retina@reva.edu.in

- From The Editor's Desk
- The World In 5
- Signal
- Hyperfocal
- Black October
- Perspectives
- The Response Playbook
- Metric Of The Week
- Fun Fact
- Candid
- **Book Shelf**
- Research Radar
- RACE Pulse
- RACE Programs

BOOK SHELF

RETINA'S READ OF THE WEEK

RETINA RECOMMENDS · THIS WEEK'S THEME

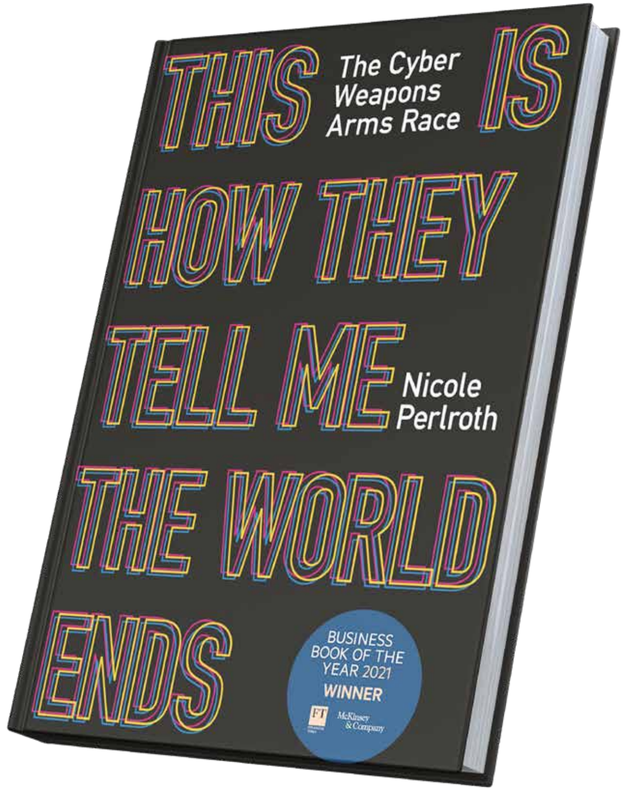
This Is How They Tell Me the World Ends: The Cyberweapons Arms Race

Nicole Perlroth · Bloomsbury, 2021

Perlroth, a long-time cybersecurity reporter, tells the story of the secret market in software flaws, the zero-day vulnerabilities that attackers buy, hoard and weaponise. Read in the week after Black October, when a cluster of exactly these flaws was exploited at machine speed, the book reads less like history and more like a field guide. Her central warning, that the offensive side of cybersecurity has quietly outrun the defensive one, is precisely the imbalance this issue describes.

What it gives a leadership team is a feel for the adversary that no threat briefing quite delivers. It explains why there is always another unknown flaw, why patching is a race you can lead but never finish, and why the economics of attack keep tilting toward the attacker. For a CXO deciding how much to spend on prevention versus recovery, that intuition is the real takeaway.

It is a work of reporting, not a manual, and it will not hand you a control framework. What it offers is the thing most risk registers lack: a visceral sense of how determined, well-funded and now AI-assisted the other side has become. Read it before your next conversation about the security budget, and before you assume the quiet months are quiet.



- From The Editor's Desk
- The World In 5
- Signal
- Hyperfocal
- Black October
- Perspectives
- The Response Playbook
- Metric Of The Week
- Fun Fact
- Candid
- Book Shelf
- **Research Radar**
- RACE Pulse
- RACE Programs

RESEARCH RADAR

RACE PUBLICATIONS THIS WEEK

Cloud security · access control · data protection

AccessFlex: Flexible Attribute-Based Access Control Scheme for Sharing Access Privileges in Cloud Storage

Bharath S; Nishanth Kumar Pathi; Shinu Abhi; Rashmi Agarwal

Most cloud breaches come down to the wrong person reaching the wrong file. AccessFlex tackles that with attribute-based access control, granting each user access only to the files their attributes permit, rather than by crude all-or-nothing roles. Built in Python with a MySQL back end, it splits duties across an admin who manages keys and attributes, data owners who upload and set access rules, and data users who get only what they are entitled to, and it adds masking and encryption so stored data stays confidential and tamper-evident. The result is a scheme built for confidentiality, integrity and accountability in shared cloud storage.

Enterprise relevance: This is exactly the least-privilege, data-centric control that extortion-without-encryption makes urgent. When the threat is quiet data theft, limiting what any one account can reach, and recording who touched what, is a direct defence. For any team on shared cloud storage, fine-grained access plus an audit trail shrinks both the blast radius and the dwell time of an intruder.

2024 International Conference on Electrical, Computer and Energy Technologies (ICECET), Sydney · IEEE

https://ieeexplore.ieee.org/document/10698339

Cybersecurity · threat intelligence · machine learning

FlexIPAccess: Dynamic Attribute-Based IP Analysis Using a Machine Learning Approach

Rajeev Kumar Singh; Pradeepta Mishra; Shinu Abhi

Checking whether an IP address is dangerous can take security tools days, and a single cloud IP often hosts many services, which attackers use to hide. FlexIPAccess speeds that up with a machine-learning model that judges an IP from its patterns, history, network reachability and geolocation, pulling signals from sources like VirusTotal, AbuseIPDB, PhishTank, AlienVault and WHOIS. Trained on 183,139 labelled IPs split into normal and attack, and tested across Random Forest, Decision Tree and Logistic Regression, it detects malicious IPs from network logs fast enough to act on, including a check against blacklisting before you acquire an IP for public hosting.

Enterprise relevance: Speed is the whole game against a fast, quiet intrusion. Turning a multi-day IP reputation check into an automated, real-time one lets a team block a malicious connection before data leaves, not confirm it afterward. It is a practical piece of the egress-aware, watch-what-connects defence this week's cover argues for.

2024 IEEE 3rd World Conference on Applied Intelligence and Computing (AIC), Gwalior · IEEE

https://ieeexplore.ieee.org/document/10730957

The CXO takeaway: both papers make the same quiet point, that a lean, well-built model often beats a heavier one on the thing that counts, accuracy on messy real-world input, whether the input is a child's scrawl or an attacker's fake link.

- From The Editor's Desk
- The World In 5
- Signal
- Hyperfocal
- Black October
- Perspectives
- The Response Playbook
- Metric Of The Week
- Fun Fact
- Candid
- Book Shelf
- Research Radar
- **RACE Pulse**
- RACE Programs

RACE PULSE

EVENTS · COMMUNITY · WHAT'S COMING

THE THREAT MOVED. THE SKILLS HAVE TO MOVE WITH IT.

Black October is a reminder that defence built for yesterday's attack fails against today's. RACE's cybersecurity programmes are built around the shift this issue describes: from recovery to prevention, from watching the perimeter to watching the data, and from manual response to machine-speed detection. The teams that stay ahead are the ones that keep learning as fast as the attackers do.

Certified Agentic AI Engineer

New batch starting on January 2027

Since AI now sits on both sides of the fight, understanding how to build and govern agents is itself a security skill. The programme covers agentic systems and their governance end to end, with a capstone that ships a deployable, governed agent.

To know more, call:
+91 89040 58866

enquiry@race.reva.edu.in ·
https://race.reva.edu.in/certified-agenticai-engineer

Master's and PG programmes

Avail Early Bird Benefits for March 2027 Batches

Applications are open across RACE's Master's and PG programmes: Business Analytics (ranked #1 in India), Artificial Intelligence (#3), Cybersecurity (#5), and Cloud Architecture and Security. Weekend format, AICTE and UGC approved, built for working professionals investing in durable, future-proof skills.

To know more, call:
+91 89040 58866
enquiry@race.reva.edu.in ·
https://race.reva.edu.in

RACE Sandbox and CXO Circle

RACE Sandbox, the on-campus career-simulation open day, returns through the term: sit in a live class, walk the AI, Cybersecurity and Cloud labs, and take a 1:1 on where your career goes next. For senior leaders, the CXO Circle breakfast continues as a closed-door peer conversation on the shifts RETINA covers.

Reserve your slot:
+91 89040 58866 ·
enquiry@race.reva.edu.in ·
https://race.reva.edu.in/

- From The Editor's Desk
- The World In 5
- Signal
- Hyperfocal
- Black October
- Perspectives
- The Response Playbook
- Metric Of The Week
- Fun Fact
- Candid
- Book Shelf
- Research Radar
- **RACE Pulse**
- RACE Programs

RACE PULSE

EVENTS · COMMUNITY · WHAT'S COMING

GRAND INAUGURATION OF MASTERS PROGRAMS

SATURDAY, 31ST OCTOBER 2026



















RETiNA
AI · CYBERSECURITY · CLOUD · LEADERSHIP

- From The Editor's Desk
- The World In 5
- Signal
- Hyperfocal
- Black October
- Perspectives
- The Response Playbook
- Metric Of The Week
- Fun Fact
- Candid
- Book Shelf
- Research Radar
- RACE Pulse
- **RACE Programs**

NAAC GRADE A+ ACCREDITED UNIVERSITY

REVA RACE REVA Academy for Corporate Excellence

REVA UNIVERSITY
Bengaluru, India

Master's & PG Programmes

New Batch: November 2026 · 12–24 months · Weekend · For Working Professionals

#1 IN INDIA · ANALYTICS INDIA MAGAZINE

ANALYTICS

PG Diploma / M.Sc. in
BUSINESS ANALYTICS
AWS Academy · Microsoft Azure

12–24 Months

#3 IN INDIA · TECHGIG

ARTIFICIAL INTELLIGENCE

M.Tech. in
ARTIFICIAL INTELLIGENCE
AWS Academy · Microsoft Azure

24 Months

#3 IN INDIA · TECHGIG

ARTIFICIAL INTELLIGENCE

PG Diploma / M.Sc. in
ARTIFICIAL INTELLIGENCE
AWS Academy · Microsoft Azure

12–24 Months

#5 IN INDIA · ANALYTICS INDIA MAGAZINE

CYBERSECURITY

M.Tech. in
CYBERSECURITY
EC-Council · Microsoft Azure · Terralogic

24 Months

#5 IN INDIA · ANALYTICS INDIA MAGAZINE

CYBERSECURITY

PG Diploma / M.Sc. in
CYBERSECURITY
EC-Council · Microsoft Azure · Terralogic.

12–24 Months

CLOUD

PG Diploma / M.Sc. in
CLOUD ARCHITECTURE & SECURITY
AWS Academy · Microsoft Azure

12–24 Months

Short-Term Certification Programmes

100 Hours · Project-Driven · Customisable for Organisations

AGENTIC AI | 4–6 weeks
AGENTIC AI SYSTEMS DESIGN
Multi-agent systems using LangChain, LangGraph, CrewAI. Capstone: deployed autonomous agent.

AI ENGINEER | 8–12 WEEKS
AI ENGINEERING CERTIFICATION
Data pipelines, model training, LLMs, deployment. Real production projects every batch.

CLOUD | 8–12 WEEKS
CLOUD ARCHITECTURE & DEVSECOPS
Multi-cloud, IaC, secure CI/CD on real AWS/Azure/GCP environments. Not demos.

CYBERSECURITY | 8–12 WEEKS
CYBERSECURITY & SOC OPERATIONS
Threat detection, incident response, SIEM/SOAR. Hands-on in RACE's live Security Operations Centre.

DATA & AI | 12 WEEKS
DATA SCIENCE & BUSINESS ANALYTICS
Statistics to ML to BI. Python, SQL, Power BI, Tableau on real business datasets.

LEADERSHIP | 8–12 WEEKS
TECHNO-FUNCTIONAL LEADERSHIP
Executive presence, decision-making, leading tech-driven teams. Built for mid-to-senior managers.

Enroll with us · race@reva.edu · race.reva.edu.in

NAAC GRADE A+ ACCREDITED UNIVERSITY

REVA RACE

REVA Academy for Corporate Excellence

RETiNA

AI · CYBERSECURITY · CLOUD · LEADERSHIP

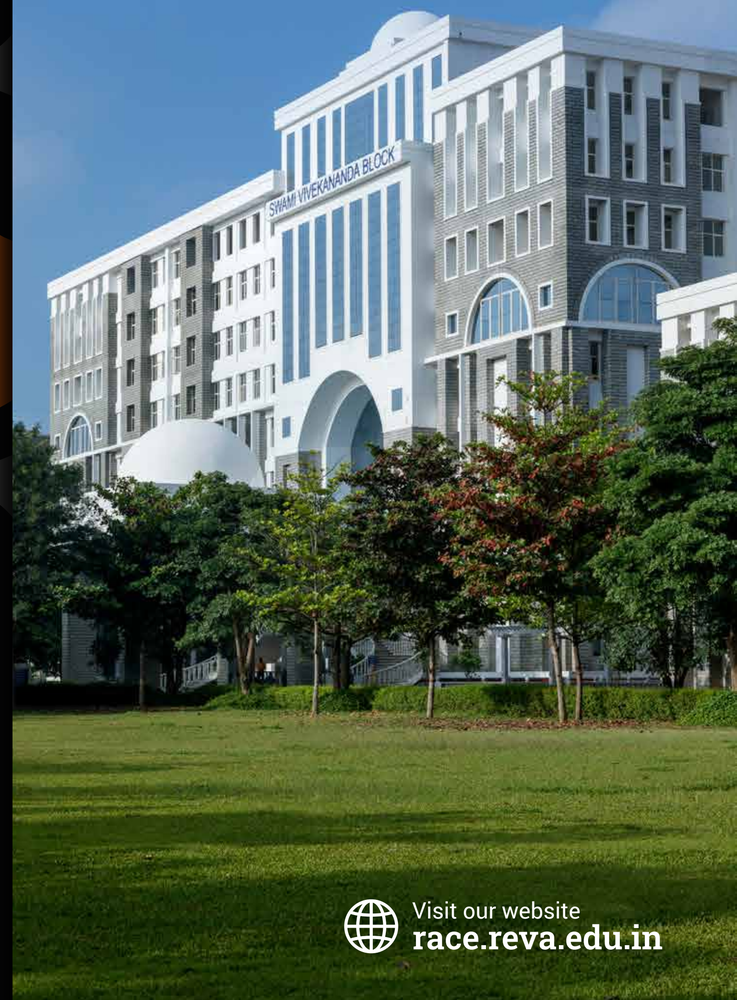
THIS WEEK, ASK YOUR LEADERSHIP TEAM

“If an attacker were quietly copying our most sensitive data right now, with no outage and no note, how long before we would know, and does our plan cover a theft or only a restore?”

REVA Academy for Corporate Excellence,
REVA University
Rukmini Educational Charitable Trust
Kattigenahalli, Yelahanka, Bangalore, Karnataka, India, 560 064
Phone: +91 89040 58866

RETINA PUBLISHES EVERY SUNDAY · FORWARD TO A CXO YOU RESPECT

REVA UNIVERSITY
Bengaluru, India



Visit our website
race.reva.edu.in