DATA ON THE FRONTLINE



Picture credit: Ted Eytan/Flickr

Chris Jacob *explores how geopolitical tensions can affect cybersecurity*

There is a particular kind of unease that comes with geopolitical tension. It rarely arrives for security teams as one clean, obvious event. More often, it shows up as a change in tempo across the environment. Scanning increases and phishing attempts feel sharper. Then you start having leadership asking harder questions about exposure, suppliers, regions and sensitive data. The SOC feels the pressure before the rest of the business fully understands that anything has changed.

Then there is the complexity of interpretation. A suspicious login could be routine, but a new phishing campaign could be opportunistic. A vulnerability alert could be noise, but a third-party issue could become material faster than expected. Security teams are now having to make sense of all of it while the business keeps moving. Data is the true separation between concern and evidence, but during times of geopolitical tension, evidence becomes one of the most valuable things security operations can produce.

Organisations need to understand where critical data lives, who can reach it, how it moves and whether behaviour around it has changed. That sounds straightforward until you look at the shape of a modern enterprise. Data is spread across cloud platforms, SaaS applications, endpoints, identity systems, collaboration tools, legacy infrastructure and third-party ecosystems. Some of it is governed well while some is governed in theory. And then some of it is sitting in places no one has revisited in months.

Attackers understand the value of that data. Altered data undermines trust in decisions and exposed data can create regulatory, reputational and operational consequences long after an incident has been contained. During global turmoil, data becomes the measure of control. The organisations that know where it is, how it is protected and what activity around it means are in a stronger position than those trying to piece together the answer during an incident.

A crisis rarely creates a security weakness from nothing. It tends to expose what was already fragile. An overprivileged account, storage bucket with the wrong setting or service account no one owns are normal enterprise problems, and normal enterprise problems become more serious as threat activity increases.

Geopolitical tensions create both conscious and subconscious uncertainty for organisations that may never see themselves as direct targets

Defenders often organise around systems, ownership boundaries and ticket queues. Attackers organise around paths and they only need a usable one. That path to sensitive data rarely stays inside one clean category and it may begin with identity, move through cloud access, touch an endpoint, and end in a storage location that was never part of the original alert.

Recent breach reporting shows how much security still comes down to fundamentals. Verizon's 2026 Data Breach Investigations Report found that vulnerability exploitation accounted for 31 percent of confirmed breaches, while only 26 percent of critical vulnerabilities were fully remediated throughout 2025. The reported median patch time was 43 days. And that 43 days is time an attacker can use, especially during a period where attention is divided and threat activity is higher.

A few years ago, defenders could often rely on a larger window of time to identify breakouts. A suspicious event could be investigated, escalated, correlated and reviewed through a familiar process. That margin is shrinking quickly. CrowdStrike reported that average breakout time dropped to 29 minutes in 2025, with the fastest observed breakout taking just 27 seconds. In one intrusion, data exfiltration began within four minutes of initial access. Four minutes is barely enough time for an alert to land, route and get noticed.

There is now a value for visibility. Logs cannot just exist somewhere. Analysts need to search them quickly and connect the dots. Identity data cannot sit in one workflow while endpoint, cloud, network, and application signals sit in others. Analysts need enough context to understand whether a behaviour is isolated, part of a broader pattern or tied to sensitive data exposure.

Many organisations are skilled enough to investigate, but their environments are not built for the kind of pressure we are experiencing today. Data is increasing in volume, but volume by itself does not make an organisation safer. Data becomes useful when it is applied to the company's security posture, when it helps explain what matters, what is exposed, who has access and whether behaviour has changed. That is when data turns into intelligence. At the same time, telemetry is being filtered to control cost and investigation workflows are depending on people piecing together context from tools that were never designed to work together. In a slower environment, this combination is frustrating. In a high-pressure environment, it's a constraint on response.

A clear path to sensitive data starts with legitimate access. A stolen password, a successful phishing attempt, a compromised session token or a contractor account with too much reach can all give attackers a quiet way in. They may not look too dramatic at first, and that's a problem.

Valid credentials mean moving with less friction. Those credentials can search, test access, pull files, create persistence and blend into ordinary workflows. Everything seems business as usual. But that changes once those actions are viewed together, against the user's role, location, device, history, and access pattern.

Additionally, Verizon's 2026 Data Breach Investigations Report found that the human element was involved in 62 percent of breaches. It is a reminder that attackers continue to target the habits, urgency, trust,and routine that keep organisations moving. During geopolitical tensions, those pressures increase with people moving faster, executives asking for updates, vendors sending urgent messages, and teams coordinating across regions and time zones. Attackers know how to hide inside that pace.

Most organisations are not waiting for perfect governance before adopting AI. Executives or employees found useful tools and started using them to summarise documents, draft communications, analyse spreadsheets, write code and speed up work that used to take hours. But don't get me wrong, the productivity increase and tangible results are real. Security teams should not dismiss it. However, the risk comes from unmanaged use, especially when sensitive data moves into tools that security, legal and compliance teams have not approved.

AI-POWERED ACTIONS SHOULD BE SUPERVISED, EXPLAINABLE, AUDITABLE AND REVERSIBLE

Shadow AI creates a quieter form of data exposure. A user can paste confidential information into an AI tool with good intentions and teams may rely on AI-generated output without knowing how the underlying data was handled. Workflows can connect to systems in ways that are useful but invisible to the SOC. Organisations benefit in the moment, while the teams who mitigate risk loses clarity over where sensitive information went and how it may be retained.

IBM's 2025 Cost of a Data Breach report found that 20 percent of surveyed organisations experienced breaches involving shadow AI and high levels of shadow AI added an average of $670,000 to breach costs. That same reporting indicated that only 3 percent of affected organisations had adequate AI access controls. The data governance issue is starting to become an AI issue.

And Geopolitical tensions place a premium on control. Organisations need to know which systems are using AI, what data those systems can access, who is allowed to prompt them, how outputs are reviewed and which actions require human oversight. AI can help security teams move faster, but unmanaged AI can also move sensitive data into areas the organisation cannot see.

Threat intelligence tends to arrive quickly during tense periods. The volume can overwhelm analysts who are already managing more alerts than they can reasonably investigate by hand.

A threat report, a feed, a briefing or a spreadsheet of indicators do not reduce risk by themselves. The same is true of internal data. Intelligence is useful when it helps a team answer practical questions about its own environment. Have we seen this behaviour? Did these indicators appear in historical telemetry? Are any users, systems, cloud workloads or third parties exposed? Does this matter to our sector, region, suppliers, customers or critical operations?

Stronger security programmes can take external context and connect it to internal evidence without forcing analysts through hours of manual research. They preserve investigation context, support clear escalation and help leadership understand what is known, what remains uncertain and what action is already underway.

Security leadership needs a defensible view of exposure and response to present to executives. The SOC has to translate intelligence into decisions

that are clear enough to act on and strong enough to explain later.

Every signal that appears during a period of elevated activity can become a scale issue and not a staffing issue. AI and automation helps analysts move faster by enriching alerts, linking related activity, summarising case details, correlating indicators and surfacing the events that are critical. Used well, automation reduces repetitive work and gives analysts more time for judgment. Used wrong, automation becomes hard to explain.

VERIZON'S 2026 REPORT FOUND THAT THE HUMAN ELEMENT WAS INVOLVED IN 62% OF BREACHES

Analysts and leaders need to know why something was prioritised and why action was taken. Auditors and regulators may later ask how a decision was made. During geopolitical tensions, those questions are pivotal because the organisation may be operating under more scrutiny, more urgency, and more public attention.

AI-powered actions should be supervised, explainable, auditable and reversible. However, this isn't a catch-all. Not every action needs manual approval. It means the organisation has to clearly define where automation can assist, where human judgment is required and how decisions are documented. Speed is valuable, but speed without accountability creates exposure.

Security leaders should begin with the data that would cause the most harm if it were stolen, altered or made available. That includes customer information, employee records, financial data, intellectual property, privileged identity data, incident response records and operational systems tied to continuity. The review should cover where the data is stored, who can access it, which third parties interact with it and how quickly the SOC can determine whether it has been touched.

Access deserves particular scrutiny. Privileged users, contractors, service accounts, non-human identities, API tokens, cloud roles and third-party connections all need review against current business needs. Excess access becomes more dangerous when attackers are actively looking for ways to move from one system to another.

The same applies to telemetry and retention. Teams need enough searchable history to validate exposure as new threat intelligence emerges. Short retention windows and disconnected logs can make it difficult to determine whether suspicious behaviour is new, isolated or part of a longer pattern.

Escalation paths should be stress tested before they are needed. Legal, compliance, communications, IT, security and executive leadership need a shared understanding of who approves containment actions, who briefs the business, who handles customer or regulatory questions and how outside partners will be engaged. Many response delays come from uncertainty about ownership rather than uncertainty about the threat.

Geopolitical tensions create both conscious and subconscious uncertainty for organisations that may never see themselves as direct targets. It is an uncertainty which is difficult to remove, but a good time to determine if blind spots can be reduced. Data resilience is the ability to understand what data matters, how it is protected, who can reach it and how activity changes around it. It is the ability to explain decisions clearly while the business is under pressure.

The strongest security programmes connect data protection, identity monitoring, threat intelligence, automation and human judgement into a practical operating discipline. Not a perfect model, but a usable one. One that helps teams move quickly without losing accountability. Attackers look to data for leverage. Defenders need to use it for clarity, confidence and control ●

Chris Jacob is Field CISO at Securonix.

During times of geopolitical tension, evidence becomes one of the most valuable things security operations can produce

