ONTIC

GUIDE

From Activism to Geopolitics: Building a Converged Security Operations Model

Table of Contents

From fragmented response to unified action

Ongoing conflicts overseas, rising activism and renewed “days of rage” at home, targeted violence, and high-visibility attacks in public spaces are forcing corporate security leaders to rethink what effective protection looks like. These threats are no longer isolated to a single geography, executive, or facility. They spill across physical locations, digital channels, employee populations, and public perception, often at the same time. The potential for these events to affect share prices and employee trust makes effective management a burning issue.

These situations often result in operating conditions that strain traditional security models, including:

- More threats unfolding simultaneously
- A far greater volume of signals
- Less time between early indicators and escalation
- More teams, systems, and stakeholders involved in response

Coordinated decision-making across the business is a critical element of a successful program. That coordination depends on true convergence across HR, legal, corporate communications, marketing, cyber, and executive leadership. When security operates in isolation, critical information remains fragmented, stakeholder trust suffers, decision-making slows, and the organization is forced to react rather than shape outcomes.

When true convergence is achieved, security plays a key role in protecting reputation, preventing operational disruption, and avoiding financial loss. It enables leadership to make informed decisions under pressure and gives teams clarity when every minute matters. This guide walks through what true convergence looks like, recommends steps to get there, and provides insight into what it looks like when it works during a real, high-pressure situation.

A hypothetical scenario: Activism, visibility, and escalation

The following hypothetical scenario shows how a converged security operating model allows teams to detect risk earlier, align faster, and act with clarity as events unfold.

The scenario

Imagine a large multinational organization operating in several major U.S. cities. A major geopolitical event occurs overseas. Within hours, grassroots activist groups begin organizing protests targeting companies they associate with the issue. Online campaigns call for consumer boycotts. Social media and employee discussion channels light up. External groups publish lists of companies to pressure.

PHASE 1

INTELLIGENCE COLLECTION AND ALIGNMENT

Before this moment, security leadership has an established relationship with executive leadership, corporate communications, marketing, HR, and legal. Security understands:

- What leadership is publicly and privately concerned about
- Which business units, locations, and executives are most visible
- What upcoming campaigns, announcements, or events could draw attention
- Employee sentiment and insider risk concerns
- How cyber threat intelligence and the GSOC monitor digital indicators, and intelligence feeds tied to threats or targeting

Because of these relationships, security intelligence collection is focused. Analysts are not guessing what matters. They are monitoring issues that leadership is already discussing, products and campaigns that are already planned, and locations that have already been assessed as sensitive. Communications lines are established, and playbooks are prepared to guide action.

Signals begin to surface:

- Online chatter calling out the company by name
- Calls for coordinated protests near offices
- Increased hostile messaging directed at senior executives
- Social media accounts linked to staff members are identified, voicing support for activists
- Internal reports from HR of employees expressing concern about safety at work
- Cyber indicators suggesting attempts to gather personal information on executives

All of this information flows into a centralized environment. Physical threat intelligence, digital monitoring, insider signals, and cyber indicators are not siloed by team or tool. They are centralized.

Security leadership has real-time visibility into:

- Who or what is being targeted
- Where activity is increasing
- Which signals are credible versus noise
- How internal concerns align with external pressure

A hypothetical scenario: Activism, visibility, and escalation

The following hypothetical scenario shows how a converged security operating model allows teams to detect risk earlier, align faster, and act with clarity as events unfold.

The scenario

Imagine a large multinational organization operating in several major U.S. cities. A major geopolitical event occurs overseas. Within hours, grassroots activist groups begin organizing protests targeting companies they associate with the issue. Online campaigns call for consumer boycotts. Social media and employee discussion channels light up. External groups publish lists of companies to pressure.

PHASE 2

MITIGATION THROUGH COORDINATED COMMUNICATION

As signals grow clearer, mitigation begins before a single protest occurs.

Lateral communication

Security activates a virtual command post and communicates laterally with HR, corporate communications, senior business leadership, and legal to assess internal risk.

Key information flows easily, such as:

- Are employees directly involved in organizing activity?
- Are there insider access concerns that need to be addressed?
- What guidance should be provided to managers?
- Is additional contract security required?

The right people receive the right information at the right time.

Communication with regional teams

Security also communicates with regional teams and protective staff. They know why certain locations are being prioritized and what indicators to watch for. Because communication channels are established in advance, this does not require ad hoc meetings or informal information sharing.

Communication with executives

Security communicates upward to executive leadership with a clear translation of risk:

- What is happening
- Why it matters to the business
- Which assets and people are most exposed
- What actions are recommended now versus later

A hypothetical scenario: Activism, visibility, and escalation

The following hypothetical scenario shows how a converged security operating model allows teams to detect risk earlier, align faster, and act with clarity as events unfold.

The scenario

Imagine a large multinational organization operating in several major U.S. cities. A major geopolitical event occurs overseas. Within hours, grassroots activist groups begin organizing protests targeting companies they associate with the issue. Online campaigns call for consumer boycotts. Social media and employee discussion channels light up. External groups publish lists of companies to pressure.

PHASE 3

RESPONSE AND ACTIVATION

As events escalate, decisions need to happen quickly. Protests are announced near multiple offices. Media inquiries increase. Online threats toward an executive intensify.

In a converged model:

- Executive protection adjusts travel routes and schedules proactively
- Communications delays or modifies a planned public statement
- Marketing pauses a campaign that could inflame sentiment
- Facilities increase access controls at specific locations
- Guards are augmented as needed
- Law enforcement liaisons are notified
- HR and security issue joint guidance to employees regarding physical safety and reporting of concerns

A connected security system supports this coordination. Intelligence, executive profiles, known threat actors, locations, and response plans live in one environment.

Everyone involved in response sees the same picture. There is no confusion about who is responsible for what or what decision has already been made. Strong process facilitates quick decision making, reduces redundant work, and fosters confidence at the senior leadership level, allowing the ongoing situations to be tracked and mitigated quietly and efficiently.

How to build a converged security operating model

This all sounds compelling in theory, but the real question is how you actually get there. The following steps outline how to build a converged security operating model that works in practice:

STEP 1

BUILD RELATIONSHIPS WITH THE RIGHT TEAMS

Convergence starts by establishing working relationships with:

- Cybersecurity
- Human resources
- Legal
- Communications and marketing
- Executive leadership and key chiefs of staff

The goal is to understand how these teams operate and where risk surfaces in their workflows. Start with simple, face-to-face conversations. Teams need to know who you are and how to reach you before a crisis occurs.

In these conversations, focus on:

- Their priorities and pressures
- The information they rely on to assess risk
- The signals they see that security does not

Equally important, explain how security contributes to their success. Many teams do not understand how security intelligence or threat assessment affects their outcomes. Make the connection explicit.

Creating a detailed RACI (Responsible, Accountable, Consulted, and Informed) chart is highly recommended, as it fosters consensus and alignment.

STEP 2

CREATE SHARED SITUATIONAL AWARENESS

Creating true convergence requires a shared view of situational awareness that centralizes and contextualizes risk signals. Critical signals from across the business must come together in a single operating picture.

For that to happen, security needs visibility into information like:

- Insider risk signals
- HR related data (like performance improvement plans, behavior issues, RIFS, evidence of increased staff frustration or stress)
- Upcoming campaigns and announcements from marketing
- Legal assessments of regulatory or reputational exposure
- Cyber indicators tied to targeting or data exposure

At the same time, those teams will expect access to:

- Threat intelligence relevant to their area of responsibility
- Clear escalation thresholds and response expectations
- Context on why specific actions or mitigations are recommended
- A clear understanding of security capabilities and processes

Security leaders must define what information is shared routinely, what triggers escalation, and how risk is translated for executive leadership so they can act with confidence. Consistency in how risk is communicated builds trust and reduces friction during high-pressure moments.

Centralizing this information in a single system makes convergence operational.

When intelligence, people, assets, and known threat actors are visible in one place with role-based access for each team, signals can be evaluated in context rather than in isolation. If an employee termination, insider concern, or external threat emerges, security can immediately assess how it intersects with broader business risk, ongoing activism, or executive exposure. This shared visibility allows teams to connect signals early and respond before situations escalate.

STEP 3

DEFINE CLEAR ESCALATION AND ACTIVATION PROTOCOLS

Clear escalation and activation protocols are critical to making convergence work in practice. Tabletop exercises, well-defined escalation protocols, and RACIs are a must.

As risk signals increase in volume and complexity, teams need to know exactly when an issue moves from monitoring to action and how that transition happens. This is where many otherwise well-aligned security programs break down.

A converged operating model is truly tested during moments of timely escalation. Decisions stall when roles are unclear or when teams are unsure whether a signal warrants broader attention.

Escalation criteria should be defined in advance, including:

- Which signals require escalation
- Who is notified at each threshold
- Which teams are activated and when
- Where decision authority sits
- Scheduled updates

These protocols should be documented, exercised, and reviewed regularly so they hold up under pressure.

They must also account for overlapping risks, such as insider concerns emerging alongside external activism or public scrutiny.

When escalation paths are clear and consistently applied, teams can move quickly and confidently, even when priorities collide, without losing time to confusion or debate about process.

STEP 4

ESTABLISH AN OPERATING RHYTHM

A strong converged operating model is maintained through a regular operating rhythm that keeps teams aligned before pressure hits. This rhythm ensures that risk discussions stay connected to the business and that coordination does not break down when things are calm.

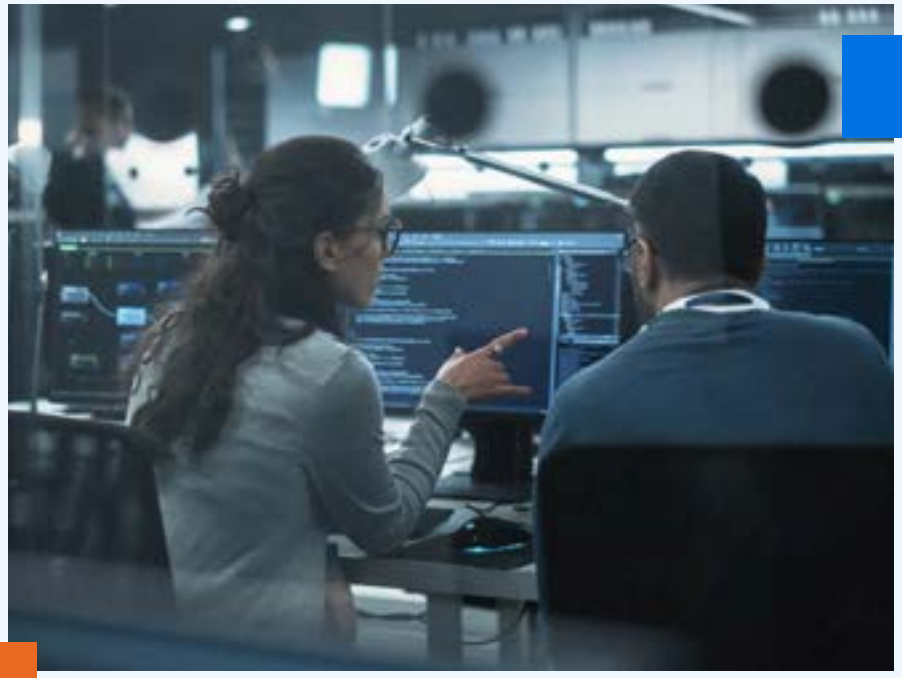
That cadence should include:

- Cross-functional risk reviews where security, HR, legal, communications, and other stakeholders assess emerging issues together and align on priorities
- Regular intelligence briefings tied to business priorities, upcoming moments of visibility, and leadership concerns rather than generic threat updates
- After-action reviews following major events to evaluate decision-making, information flow, and coordination under pressure
- Regular updates to escalation criteria and response plans based on lessons learned and changes in the risk environment
- Bi-annual stakeholder meetings to update security capabilities, realign processes, confirm priorities, and reinforce the RACI

Maintaining this rhythm reinforces relationships, keeps alignment current, and prevents teams from drifting back into siloed ways of working over time.

Checklist: Do you have a truly converged security operating model?

This checklist is intended to help you assess whether convergence is actually operating day to day within your security program, not just existing on paper. As you review it, consider whether these conditions are consistently true across routine operations and high-pressure moments.



- [ ] Security has early visibility into emerging risk across physical, digital, insider, and external domains
- [ ] Risk signals are centralized and assessed in context, not in isolation
- [ ] Leadership receives clear, timely guidance tied to business priorities and decision points
- [ ] Escalation paths are defined, predictable, and exercised before crises occur
- [ ] Teams move in coordination across Security, HR, Legal, Communications, and Operations rather than reacting in silos.
- [ ] Decisions are made with shared situational awareness instead of incomplete information or pressure-driven assumptions. Clearly defined RACI is continually updated.
- [ ] Protective actions account for people, assets, brand, and operational impact at the same time

Security is the connective tissue

The threat landscape facing corporate security leaders will continue to grow more complex, faster-moving, and more interconnected. Activism, geopolitics, insider risk, and public visibility now exist within the same operating environment and routinely intersect in ways that amplify risk.

Addressing this reality requires security to function as the connective tissue across the business, linking people, information, and decision-making at critical moments. A converged operating model takes shape through strong relationships, shared situational awareness, disciplined escalation, and consistent communication that holds up under pressure.

Security leaders investing in this model positions your organization to navigate uncertainty with greater confidence. By connecting signals early and aligning teams before escalation occurs, you can protect people, assets, and reputation before pressure turns into lasting damage.