

SAFETY GAP

REPORT

Insights on the Safety Gaps Impacting
Enterprise Businesses — and How To Close Them



Contents

Introduction	4
Safety Is Now Digital — Even 911	8
The Value of Safety	12
Understanding the Response Process	14
The Stages of Intelligent Safety	16
Closing the Safety Gap	18

USE CASES	6
Active Shooter	7
Transportation	11
Medical Emergency	15

● **LOCATION & TIME**
UNKNOWN TO
SECURITY OPERATIONS

● **POWER GRID**
UNKNOWN TO 911

● **NUMBER OF STORES**
UNKNOWN TO 911

● **EMERGENCY EXITS**
UNKNOWN TO 911

● **VIDEO SURVEILLANCE**
UNKNOWN TO 911

● **FLOOR PLANS**
UNKNOWN TO 911

● **UTILITY CONTROLS**
UNKNOWN TO 911

● **NUMBER OF SHOPPERS**
UNKNOWN TO 911

● **TRAFFIC PLAN**
UNKNOWN TO 911

THE SAFETY GAP CREATES TOO MANY UNKNOWNNS

When critical information isn't connected to those who need it during an emergency, there's an over-response or dangerous under-response. Closing the gap and connecting that information means first responders don't just arrive — they arrive ready.

Introduction

In 2023 alone, the U.S. faced 250 million emergencies.

As this number continues to grow, enterprises are ramping up investments in new monitoring equipment and other digital safety tools. Yet, despite nearly \$200 billion in collective spend annually, many businesses still struggle to adequately secure their people, customers and physical infrastructure.

Businesses are failing to reap the benefits these new digital solutions provide. Why? Inundated with signals from sources like Internet-enabled cameras, sensors and other devices, safety professionals are unable to quickly surface the necessary intelligence from the abundance of raw information, leading to inefficient operations, slower response times, wasted resources and, ultimately, a false sense of security.

And this is just for the events corporate security teams know about. There are many situations they are not aware of. Sometimes, it may even take first responders arriving on the scene for internal safety professionals to figure out what is happening.

In an emergency, the natural instinct is to contact 911. And the majority of the time, that is on a mobile device. Last year, 80% of 911 calls came from cell phones, which are outside the reach of corporate security centers. But thousands of Emergency Communication Centers, or ECCs, across the country are able to extract important information from mobile calls. It is why 911 regularly finds out about potentially life-threatening situations before security teams.



SAFETY GAP

80%

OF 911 CALLS CAME FROM CELL PHONES, WHICH ARE OUTSIDE THE REACH OF CORPORATE SECURITY TEAMS.

We call this the safety gap, when critical intelligence isn't seamlessly shared between 911 centers, field responders and internal security professionals. And it's leaving many enterprises vulnerable to disaster.

Instead of information silos, companies need to harness the power of their own digital safety tools, as well as tap into investments other security organizations are also making in new technology. With access to a unified emergency response ecosystem, corporate security operations and external safety professionals can tap the real-time intelligence they need to work together to mitigate disaster — and protect themselves and others in the process.

Safety isn't top of mind until it's too late. And too many internal decision-makers still view security as simply a cost-center. Safety can't be an afterthought. In fact, with the right approach, it can become a value-driver for the business, one that helps instill deeper brand loyalty from customers and employees.

To do this, companies must close the safety gap.



USE CASES

There are several real-world examples of the safety gap.

The common theme in each of these examples?

The lack of critical safety intelligence.

Whether responding to an active shooter, massive train derailment or health emergency, first responders spring into action without vital context that could help save their lives — and the lives of others. And security operation centers are forced to operate from a disadvantaged position — which is uncomfortable for a team tasked with ensuring safety in an organization.

Instead, Telecommunicators in 911 centers need to be able to quickly get information — like feed from security cameras, summaries of cargo by train car, or past medical conditions — to emergency professionals before they show up on the scene. And security operations need to be connected to 911 centers so they know what's going on in real-time and can work collaboratively with first responders.

USE CASE

Active Shooter

It's the call no first responder wants to get: an active shooter situation. Unfortunately, these now happen far too frequently. Each incident — whether at a movie theater, mall or school campus — presents its own set of challenges. However, there are unique hurdles when responding to a situation at a retail location, like a large grocery store, that make it particularly dangerous.

Immediately after the first shot, chaos ensues. 911 is likely inundated with calls. Operators are overwhelmed, and unable to piece together all the rushed information that frantic individuals fleeing from the scene attempt to provide. Field responders show up, often unaware how many people are still in the store, or where anyone is located — including the shooter (or shooters).

Carefully making their way through the store, they rush by rows of shelving and other objects someone could hide behind. It's an incredibly risky situation. And while these heroes risk their lives, dozens of security cameras overhead capture it all. But none of this footage is available to public safety for hours, even days after the accident.

Every single one of these "eyes in the sky" should be helping first responders. It is a situation where collaboration between security operations centers, which often have control over internal security technology, and 911 is necessary.

Collaboration
between security
operations centers,
which often have
control over internal
security technology,
and 911 is necessary
to improve safety
outcomes.



Safety Is Now Digital — Even 911

In the past, safety was actually a game of telephone. Panicked callers on the scene, or coming from it, would instantly call 911 and give usually scatter-shot, and potentially inaccurate, details about the situation. Operators would then have to use this unreliable information to inform the dispatch.

Once off the phone, the caller might alert the corporate security team, which then must rush to coordinate the response across both emergency professionals and internal stakeholders, like onsite employees. But in some cases, security operations centers are left entirely out of the loop, meaning at no point are 911 and the business coordinating in advance.

This process is a breeding ground for chaos and uncertainty, ultimately prolonging a resolution. It also makes it much harder to optimize the response. Imagine a world where every time you used the Uber app, the system didn't know if you were riding by yourself, or with twenty other people. Absent key information, Uber sends three cars for two people. This scenario plays out on 911 calls everyday. First responders show up, [either overstaffed or under-resourced](#), to security teams that are still scrambling to get a grasp on the evolving situation.

There's a smarter way.

Safety is now digital, spanning text messages, video feeds from intelligent monitoring devices and other sources.

There's a smarter way. Safety is now digital, spanning text messages, video feeds from intelligent monitoring devices and other sources. By 2030, there will be an estimated 32 billion so-called 'Internet of Things' devices worldwide — double the current amount. These solutions, including internet-enabled cameras, sensors and wearable devices — assist companies in monitoring key operations for potential safety issues.

All of these devices are constantly sending signals that can help both internal and external stakeholders better detect, respond to, and even prevent emergencies. Retailers can identify weapons in their stores before shots are even fired. Manufacturers can more quickly detect and remediate problems like a fire or gas leak. Railway operators can closely track the movement of their fleet.

However, in many cases these transformations are far too superficial. They give the appearance of better safety, but in reality enterprises could be at the same level of risk as before they bought these shiny new tools. It's not enough to just buy and deploy digital technology. Businesses need to figure out how to now manage the constant stream of data flowing from these devices to actually enhance their safety operations.

And ultimately, identifying known safety issues is only part of the challenge. Corporate security teams must also make sure they're connected into the public safety centers, which are often the first to know of emergencies. Then, once enterprises and 911 centers build the connection between their digital environments, information can be more seamlessly shared. It's the only way to close the safety gap.



USE CASE

Transportation

In 2023, on a cool, February evening in Northern Ohio, volunteer firefighters around the East Palestine area were settling down after dinner, maybe even already in bed, when the alert came in with a brief message: “Train on fire.”

Like modern day superheroes, these first responders dropped everything they were doing, and rushed to the site. As they turn a corner on a dark road, a wall of flames, towering several stories high, ravages before them. In these situations, firefighters don’t have time to think. Fear is replaced by adrenaline. But as they carefully charge their way to the source of the disaster, the first responders suddenly find themselves wading through a pool of toxic chemicals.

Frantically, they coordinate with headquarters. Operators scurry to find information they need in an over 30-page safety document. They must then cross-reference that against other files, then triage those insights back to the first responders. And while this convoluted process is going on, the fire continues to rage, and the chemicals continue to flow.

Meanwhile, the train owner is trying to figure out what’s happening. They struggle to get reliable information from the chaotic scene. They have no idea what intelligence first responders need — or even where they are. And ultimately, the company’s security team, which is tasked with keeping employees and operations safe, is playing catch-up with 911, which at this point has far more knowledge about the unfolding situation.

Instead of responding in silos, the company’s security operations center should have been notified the second the 911 alert went out. Then, internal security professionals could have quickly gathered information on the hazardous materials that were being shipped, and which cars they were located in, to help minimize the time that first responders were wading through the toxic sludge.

The Value of Safety

Every company's top priority is protecting their employees and customers.

But few actually use safety to drive better financial outcomes. While 94% of enterprises view safety as a core value, according to a *Harvard Business Review* survey, just 17% made safety an actual part of their overall business strategy.

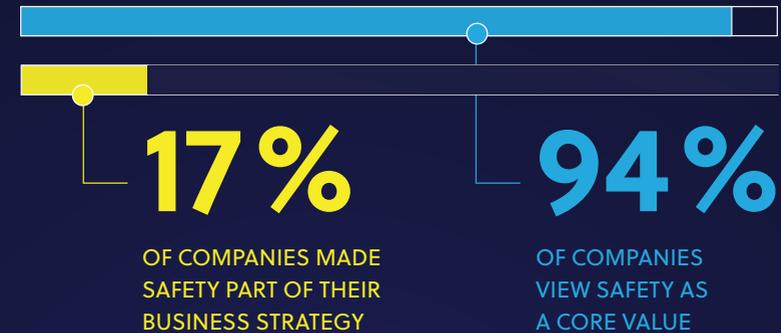
Making sure the workforce and physical property are secure is more than just a line-item in the budget. In fact, safety can be a significant competitive advantage. The Boeing fiasco proved consumers are willing to avoid brands they deem "unsafe." Meanwhile, the blowback to self-driving cars showed that the public has no appetite for businesses or industries that appear to flaunt safety standards. Conversely, they reward those enterprises that do take safety seriously.

According to a 2021 study, better safety drives as much as a 9% boost in customer satisfaction, a metric that's increasingly important to sales and shareholder returns. As pressure from regulators and other factors force companies to ramp up funding for new protective measures, they should look to corporate security teams to take charge in reframing the organization's mindset around safety.

Often under-resourced, these nerve-centers oversee security across hundreds to thousands of retail locations, manufacturing plants or miles of railways. Armed with the right technology, safety teams can unify the abundance of information flowing from new digital tools to improve how they coordinate with first responders and internal stakeholders during emergency situations. This leads to a more efficient operation, with fewer wasted resources. And the reputational improvements can help companies secure greater market share.

Corporate security operations can spearhead preventative efforts that also create real business benefits. For example, mandatory safety training reduces injury rates by as much as 18%, while monthly training can curb hazards by as much as 10%, saving companies millions of dollars. Awareness is not just about creating a safe environment; it is also key to running an efficient business.

Too few companies use safety to drive better financial outcomes.



Customers reward companies that take safety seriously.

Customer satisfaction is a metric that is increasingly important to sales and shareholder returns.

BETTER SAFETY BOOSTS CUSTOMER SATISFACTION BY AS MUCH AS

+9%

Preventative efforts protect employees and can save companies millions of dollars.

MANDATORY SAFETY TRAINING REDUCES INJURY RATES BY

-18%

MONTHLY TRAINING CAN CURB HAZARDS BY AS MUCH AS

-10%

Source: Vikas Mittal, Alessandro Piazza and Sonam Singh, "Safety Should Be a Performance Driver," *Harvard Business Review*, September-October 2024, <https://hbr.org/2024/09/safety-should-be-a-performance-driver>.

Understanding the Response Process

Despite all this new digital tooling, many safety professionals struggle to get accurate and timely insights. Instead, they're stuck trying to navigate a litany of new information silos.

Because these systems can't naturally "talk" to one another, it becomes challenging to pool the data from the various sources — whether it's on-site security cameras, or sensors that detect gas leaks or fire hazards. As a result, there are often huge gaps in key data sets, forcing operators to base decisions on incomplete or inaccurate intelligence.

Safety is now a data problem.

Critical data is often unknown to 911 and field responders, so they are forced to find the necessary information, slowing down response timelines and leaving first responders guessing about what might lay ahead. Emergency professionals need the protection of intelligence. They must be armed with as much information about the situation as possible. Then, they can map out a strategy that ensures the highest-level of protection for themselves and others.

But because of data silos, they often must act without critical context. Despite all the new digital tooling, safety teams are still running like they did in the analog era. Fire alarms cannot tell access control systems how many people are inside. First responders cannot access vital system data to assess the situation. And critical systems like security cameras or door controls remain inaccessible to emergency services.

USE CASE

Medical Emergency

At a large manufacturing plant, a worker suddenly starts to feel chest pains. Growing increasingly nervous, he looks around and realizes all other nearby employees are gone.

While standard protocol might be to call for help on a company-provided device, instinct kicks in. The worker calls 911, which dispatches an ambulance. Shortly after, first responders arrive, see an unconscious worker, and immediately begin treating him. Meanwhile, after hearing the ambulance sirens, on-site security starts scrambling to figure out what's going on.

Ultimately, the employee is fine. This is, of course, extremely welcomed news for the business. But it also leaves the security operations team feeling frustrated. Tasked with keeping employees safe, they were not able to help in this situation. In fact, they didn't even realize something was wrong until the ambulance showed up.

If the security operations center was connected to 911, however, they would have also known right away what was going on — and potentially provided care in the interim, in the form of an AED. In fact, with every minute that passes during a heart episode, a victim's chances of survival decrease by as much as 10%. Having visibility enables corporate security to activate those response protocols faster to improve outcomes.

However, with the right underlying technology, companies can establish the connections they need between different endpoints, creating the safety ecosystem that can lead to better, more complete intelligence, as well as more seamlessly share those insights with both internal and external stakeholders.

The Stages of Intelligent Safety

While each business will ultimately face their own unique safety challenges, there are stages that every enterprise must progress through to start to close the safety gap.

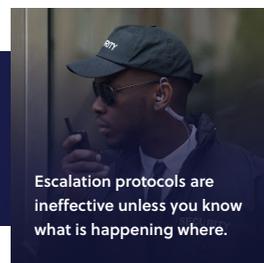
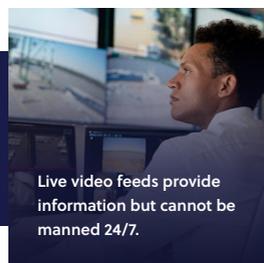
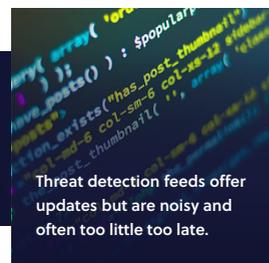
STAGE ONE

Overcoming Ignorance

The first step for leaders is realizing the business and its employees are not as protected as they think. And often, it is a hard reality to come to terms with. Companies have spent potentially billions of dollars on new digital security tools. Naturally, it is frustrating that, independently, these measures ultimately might fail to enhance their overall response capabilities. And even with all this new tooling, most employees still turn to 911 in an emergency. They don't follow established protocols, use their own devices, and ultimately are a barrier to security operations staying in the loop. This behavior is tough to change.

Instead, organizations need to connect to existing digital public safety ecosystems to break-down the communication barriers between internal security teams and 911. Then, they can strive to unify siloed technology landscapes to share deeper safety intelligence across both internal and external emergency professionals to improve the response process. Ultimately, by acknowledging their own unique points of vulnerability, businesses can begin the harder job of actually fixing them.

Acknowledging these points of vulnerability is the first step to fixing them.



STAGE TWO

Establishing the Necessary Connections

While data is fundamental to better intelligence, that information has to reach the individuals that need it. To make sure they're plugged into events as they unfold in real-time, enterprises need to connect their own safety operations to ECCs across the country. Once integrated, security operations centers can start to receive alerts when 911 does. Enterprises are also able to gain access to all the rich information that public safety centers are now able to extract from mobile calls, including name, location and other vital data. This gives corporate security teams the important background they need to immediately start to coordinate the response. And when first responders arrive, it's a collaborative process, built on a foundation of common knowledge about the situation.

STAGE THREE

Unifying Data Silos

Once the external connections are established, companies can start to think about closing their own internal safety gap by combining the various data feeds together. But there are key challenges to building these connections. The number of digital devices is only growing. And many new pieces of equipment are likely running on their own proprietary technology. These are the data silos that prevent real-time information from reaching corporate security teams and 911 operators – and they're popping up constantly. With the right, independent platform solution, businesses can more easily build connections between these different ecosystems. This centralized stream of data becomes the driver of enhanced intelligence.

Closing the Safety Gap

Closing the safety gap isn't about ditching the existing strategy. It's about taking common-sense approaches, like connecting into already operational 911 digital ecosystems, to make immediate improvements. Then it's about taking on the bigger challenge of integrating the many different pieces of safety technology together to maximize the investments enterprises are already making.

This will be an ongoing effort, especially as new applications come to market that help security operations centers with their primary goal of keeping employees, customers and operations safe. It's why efforts to close the safety gap have to be embedded into the culture, not just a one-time exercise. It's about future-proofing the foundation so security operations can seamlessly integrate future innovations.

When safety professionals have the benefit of better intelligence, responses become more streamlined, ultimately lowering the risks enterprises face. And taking the steps now to lay the right emergency response foundation will also enable organizations to more quickly take advantage of automation and new AI-powered solutions to make even more transformative improvements to safety. This isn't just how companies close the safety gap. It is how they drive real-world value from their safety investments.

At RapidSOS, our goal goes beyond simply closing the safety gap—we're committed to revolutionizing emergency response through intelligent safety. By integrating advanced technology, data, and real-time communication, we're empowering 911 and first responders with the critical information they need to save lives.

Without RapidSOS

31 MINUTES

- 10:04 AM** An employee, John, experiences a medical emergency and calls 911 from his mobile phone in Building B.
- 10:05 AM** John struggles to describe his exact location within the large corporate campus to the 911 operator.
- 10:10 AM** The 911 operator dispatches an ambulance to the campus location.
- 10:15 AM** The ambulance arrives at the main entrance, and campus security staff remain unaware of the emergency.
- 10:20 AM** Security staff notify the security team that an ambulance is there and they begin checking camera feeds to locate the emergency.
- 10:35 AM** Security personnel locate John on the cameras and direct responders to Building B, but the delay impacts his condition.

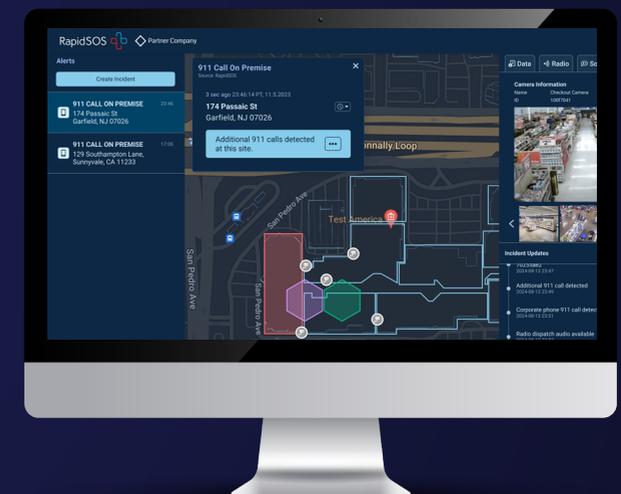
With RapidSOS

REAL-TIME

- 10:04 AM** Real-time alerts for 911 calls made onsite, with contextual data to enhance response and coordination with emergency services and first responders.

Detect onsite emergencies as they happen.

With RapidSOS, receive real-time alerts for emergency escalations within your facilities, enabling faster, focused responses and strengthening your duty of care.



[Learn More](#)

RapidSOS 