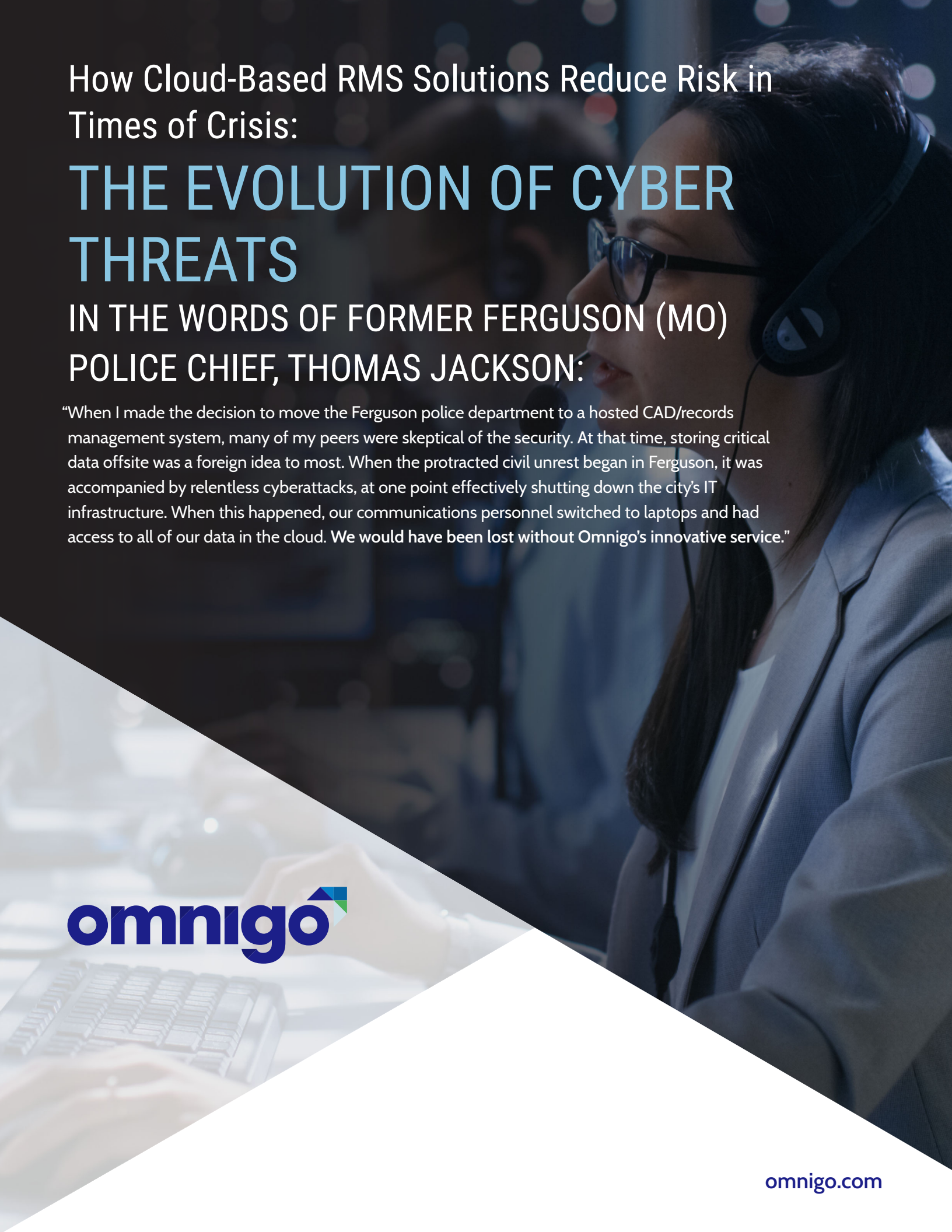

How Cloud-Based RMS Solutions Reduce Risk in Times of Crisis:

THE EVOLUTION OF CYBER THREATS

IN THE WORDS OF FORMER FERGUSON (MO) POLICE CHIEF, THOMAS JACKSON:

"When I made the decision to move the Ferguson police department to a hosted CAD/records management system, many of my peers were skeptical of the security. At that time, storing critical data offsite was a foreign idea to most. When the protracted civil unrest began in Ferguson, it was accompanied by relentless cyberattacks, at one point effectively shutting down the city's IT infrastructure. When this happened, our communications personnel switched to laptops and had access to all of our data in the cloud. **We would have been lost without Omnigo's innovative service.**"

omnigo

Over the last five years, cyberattacks against law enforcement agencies have skyrocketed to epic levels. In 2019, hackers gained access to LAPD's databases and secured the names, email addresses, and social security numbers of more than 2,500 officers and 17,500 prospective employees. One year prior, in July of 2018, cyber extortionists launched a ransomware attack on the City of Atlanta, Georgia. The perpetrators managed to knock several municipal services offline—including the police department and judicial systems—and threatened to delete scores of critical data unless city officials forked over $51,000 in Bitcoin. Moreover, in that same month, the Baltimore Police Department fell victim to a denial-of-service attack that locked up their dispatching systems for 17 hours. Even more startling: Baltimore is only one of 12 public safety agencies nationwide to suffer an attack on their 911 systems.

These incidents only scratch the surface, serving as a precursor for what's to come. Aside from experiencing the destructive and trying effects of cyberattacks, these agencies also share a common link—they are all massive departments with access to cutting-edge cybersecurity technology. If cybercriminals were able to penetrate these IT fortresses, what might happen if they decided to target a smaller department? As we shift to a culture of hacktivism, ransomware, and denial of service attacks, law enforcement agencies are becoming prime targets for cybercriminals looking for notoriety and seeking retribution for perceived wrongs.

According to a recent survey of government agencies nationwide, 44% of participating agencies admit cyber threats are a daily occurrence.

More staggering—this finding only represents the frequency of attacks during everyday operations. But what happens if your agency is the subject of national controversy? What if your officers find themselves on the nightly news, and your department becomes the object of online scandal? While all instances are different, and all cases are subject to broad interpretation, one fact remains the same: In the wake of a crisis, your agency will face an influx of cyber threats not only stemming from your own backyard but from threat actors across the globe.

Make no mistake, within minutes of the story breaking, your systems will be attacked, your records will be compromised, and a tidal wave of traffic will flood your servers in attempt to hurl your agency in the dark.

Will you be ready? Or, will your staff be left scrambling to plug the dam before critical information leaks out and exposes the names, addresses, and phone numbers of your officers, leaders, investigators, and informants?

– How will you manage an elevated call volume without access to your CAD, internal records, asset location services, or shared criminal databases?

– What about citizen services like 911?

– What happens to your community and your officers when a breach in security compromises their safety?

– Will your interrogation and surveillance footage become the next viral video, or will confidential evidence be sold to the highest bidder?

If you're not confident in your department's abilities to handle a full-scale cyberattack, it's time to bolster your resources. While it's true budget and funding present barriers, they are far from impenetrable roadblocks.

You can protect your agency and your community without breaking the bank or compromising on service.

In this paper, we'll examine the security risks facing law enforcement data, analyze best practices for managing sensitive information, and shed light on how agencies can leverage off-site records management systems and cloud security to increase resiliency during a crisis—safeguarding their data and keeping their personnel informed and aware.

GAUGING READINESS

Protecting sensitive data from falling into the wrong hands is not a new task for law enforcement. For decades, departments have kept systems in place to prevent unauthorized access and misuse of information.

Traditionally, law enforcement agencies have relied on on-site data centers to house and store data in controlled settings. Aside from the costs of infrastructure and equipment, this method comes with the added burden and responsibility of paying personnel to manage and maintain the system. The task of securing the latest technology and employing those with the clearance and expertise to operate these systems has left smaller agencies struggling to keep pace with changing industry standards.

While the largest law enforcement agencies employ dedicated IT staff, smaller departments are at a distinct disadvantage when it comes to service and support. Often, technology services are supplied by the municipality or county IT department, or in some cases, tech-savvy police officers. Though these solutions might make sense on the surface, neither option is ideal. Grouping critical policing service with community programs results in a lack of prioritization and round-the-clock support. Taking an officer out of the field or a supervisor off the street is neither beneficial to the agency nor cost-effective. There is also a question of readiness and skill. Without the knowledge and expertise to tackle advanced cybercriminal activities, a full-scale attack could devastate a law enforcement agency's ability to keep their officers safe while responding to life-threatening emergencies.

In 2016, the ICMA, in partnership with the University of Maryland, conducted a study to gauge cybersecurity plans among state and local governments. Of the 411 agencies that responded, 70% of participants identified the lack of trained cybersecurity personnel as having a noticeable impact on their agency's resiliency. Even more surprising, an overwhelming 60% of agencies rely solely on their IT managers to handle the task of safeguarding their data, along with various other job duties.

ADDRESSING STOPGAPS

For agencies that outsource their IT, data protection can present an even larger challenge. Full-scale information security is often cost-prohibitive and impractical for agencies operating on limited budgets. Deferring maintenance and software updates for the sake of saving money or reducing interruption can leave systems vulnerable to attack, while unplanned outages often result in unacceptable downtime waiting for third parties to resolve the issue. Furthering the problem, quick-fix solutions are costly and nothing more than temporary band-aids. Yet full-scale resolutions may take years to configure and deploy.

While risky in any setting, in law enforcement, this practice of catch-all information security has the potential to foil investigations, compromise sensitive documents, and impact millions of lives—especially during a crisis. Policing cannot take a backseat to IT operations. An agency in crisis has neither the time nor the luxury of shutting its doors while data systems are repaired and brought back online. Siloed communication is no longer practical, as more and more officers rely on departmental data and cross-agency intelligence to help them maintain situational awareness, respond to emergencies, combat crime, and protect lives and property.

Unfortunately, cybercriminals are notoriously strategic. They will capitalize on crises and strike while your officers and dispatchers are busy protecting lives and maintaining order.

CYBERSECURITY IN THE CLOUD

Police agencies need a better way to manage their data and safeguard their operations. In turn, cloud solutions are becoming the go-to for agencies looking for a one-step solution to data management and top-tier security. While cloud solutions alone cannot stop cyberattacks, they can ensure your department remains agile and resilient before, during, and after a crisis or accidental security breach.

Cloud solutions enable your agency to maintain stricter data controls and allow you to manage what comes in and what goes out. Whether your information is in transmit or receive mode, it's fully encrypted and secure. Responsibility to maintain CJIS compliance for data storage is shifted from your organization to your cloud provider. This cuts down on liability and allows you to operate without worrying if software updates and security patches are current. Data back-ups are automatic, which results in higher uptime, fewer hassles, and fewer expenditures for infrastructure, equipment, storage, and personnel.

Another benefit to cloud-based records storage: It requires no space-wasting storage areas or expensive equipment to purchase, manage, update, and maintain. Programs are subscription-based and can be built into the yearly cost of operation. You pay for what you need when you need it. Your system remains flexible and scalable, so you can add or subtract services according to your agency's needs. Not only does this ensure future proofing, but it allows you to determine the exact cost of ownership from the beginning, without fear of unwelcomed surprises or unexpected hits to your budget.

What's more—even if cybercriminals attack your network, you can still access your data, maintain control of your information systems, and continue to function by moving operations to any windows-based device. Regardless of the type of attack, your personnel will have instant access to the systems they rely on, such as CAD functions, mobile data terminals, internal records, shared databases, asset location and tracking tools, incident reports, and arrest platforms.

In effect, hosting your data off-site enables you to put a barrier of protection between your agency and your information. So, while system hacks may cause temporary nuisances, your department's situational awareness and mission-critical functions will remain fully functional and resilient throughout an attack.

ASSESSING PITFALLS

Unfortunately, most of these platforms are built for large agencies with exorbitant IT budgets. While these programs can work well for departments that can afford the cost of yearly upgrade fees, licensing restrictions, and regional data sharing—they don't address the looming problem.

All police agencies need data security. Classified information, investigative data, and officer safety is an industry-wide issue that has nothing to do with how many names appear on duty charts or how many citizens live in your community. The only difference is the fact that smaller agencies make better targets and are more vulnerable to breaches because of the massive gap in the services small departments can afford.

However, more expensive doesn't necessarily mean better control. While excessive functions may seem like must-haves, most often they equate to cumbersome features that are too complicated and time consuming to use.

When searching for a software solution, department leaders must balance which services are mission critical as opposed to options that are merely nice to have. A secure records management system that integrates with your department's other essential platforms can supply you with a streamlined, reliable, and cost-effective way to keep your officers and your community connected, protected, productive, and informed.

SECURE, RESILIENT, AND RESPONSE READY

Now, migrating to a cloud-based solution has never been simpler or more affordable. With Omnigo's suite of public safety software, fast and effective information management, and ironclad security are within reach of all law-enforcement agencies, regardless of size or budget.

Designed for small to medium policing organizations and built using feedback from law enforcement agencies across America, Omnigo's ITI platform provides the security you demand, the flexibility you want, and the information your agency needs to keep your officers safe and your community protected, regardless of the threat.

Whether you're powering through a crisis or just another day, Omnigo's clean design and user-friendly interface increases productivity and streamlines information transfer from the communication center to your officers in the field. Backed by a robust 256-bit encryption standard, the innovative platform integrates and supports a host of vital services, such as records management, CAD, GIS data, incident reporting, jail management, and regional information sharing.

Better yet, Omnigo's ITI software is easy to learn and even easier to use. Envisioned and perfected by a team of law enforcement professionals, the platform performs like a true workhorse, putting productivity front and center while ensuring minimum frustration.

Pre-populated data fields, in-platform editing, and simple screen navigation eliminates errors and reduces data-entry requirements, enabling your officers to generate professional reports on the go. While predictive technology and any-field event queries enable investigators to conduct effective and transparent post-incident analysis. In addition, the system comes preloaded with features like one-touch report submission to help facilitate a painless transition from the Uniform Crime Reporting program to the National Incident-Based Reporting System.

Unlike most systems on the market, Omnigo software doesn't restrict functionality for mobile terminals or back-up workstations. Even in a crisis, you can be sure your team has access to a full-line of secure, reliable, response, and recovery tools via any Windows-supported device.

In fact, Omnigo Software played a vital role in helping the Ferguson Police Department remain resilient during a recent crisis in Ferguson, Missouri.

LEVERAGING KEY TAKEAWAYS

During a crisis, your agency will face elevated call volumes, extreme fatigue, and mounting performance pressure. IT and communications outages will only add to the stress by hindering response times and reducing situational awareness. While it's impossible to predict every variable or eradicate cyber threats, you can gauge your readiness and bolster your resources well in advance.

Much like any facet of law enforcement, when it comes to cybersecurity, there is no such thing as over-prepared. As the threat landscape evolves and the number of cyberattacks against law enforcement increase—now more than ever—it's imperative to identify, analyze, and assess your agency's response and mitigation strategies.

While it's true most law enforcement agencies lack the bandwidth and in-house expertise to deal with the ever-changing complexity of cybercrimes, cloud-based data solutions offer your department the security and protection to remain running and stay safe from onset to recovery.

Not all solutions come with astronomical price tags. You can afford to protect your officers, your agency, and your community without sacrificing security or functionality. It's never too early to start planning for the next crisis. Developing a formal strategy backed by a proven and effective cloud-solution is a critical first step.

ABOUT OMNIGO

For more than 20 years, Omnigo software solutions have been the preferred choice for law enforcement, education, healthcare, gaming, hospitality, and corporate enterprises. Currently, Omnigo's solutions are used by over 2,000 customers in 20 different countries. At Omnigo, we're committed to helping customers secure their organizations' property, control operational costs, and ensure the safety of the general public.

We believe our customers deserve the best support available to protect their people, assets, and brand. We also understand how challenging it can be to protect the community without the proper resources. We're here to arm users with the best tools in the industry. With a team that includes former law enforcement, first responders, and other public safety professionals, we're uniquely qualified to understand exactly what our customers need to protect their community.

LEARN MORE OR REQUEST A LIVE DEMO

call: 866.421.2374
email: sales@omnigo.com

omnigo