EVOLVING THREATS, ADAPTING TECHNOLOGY:

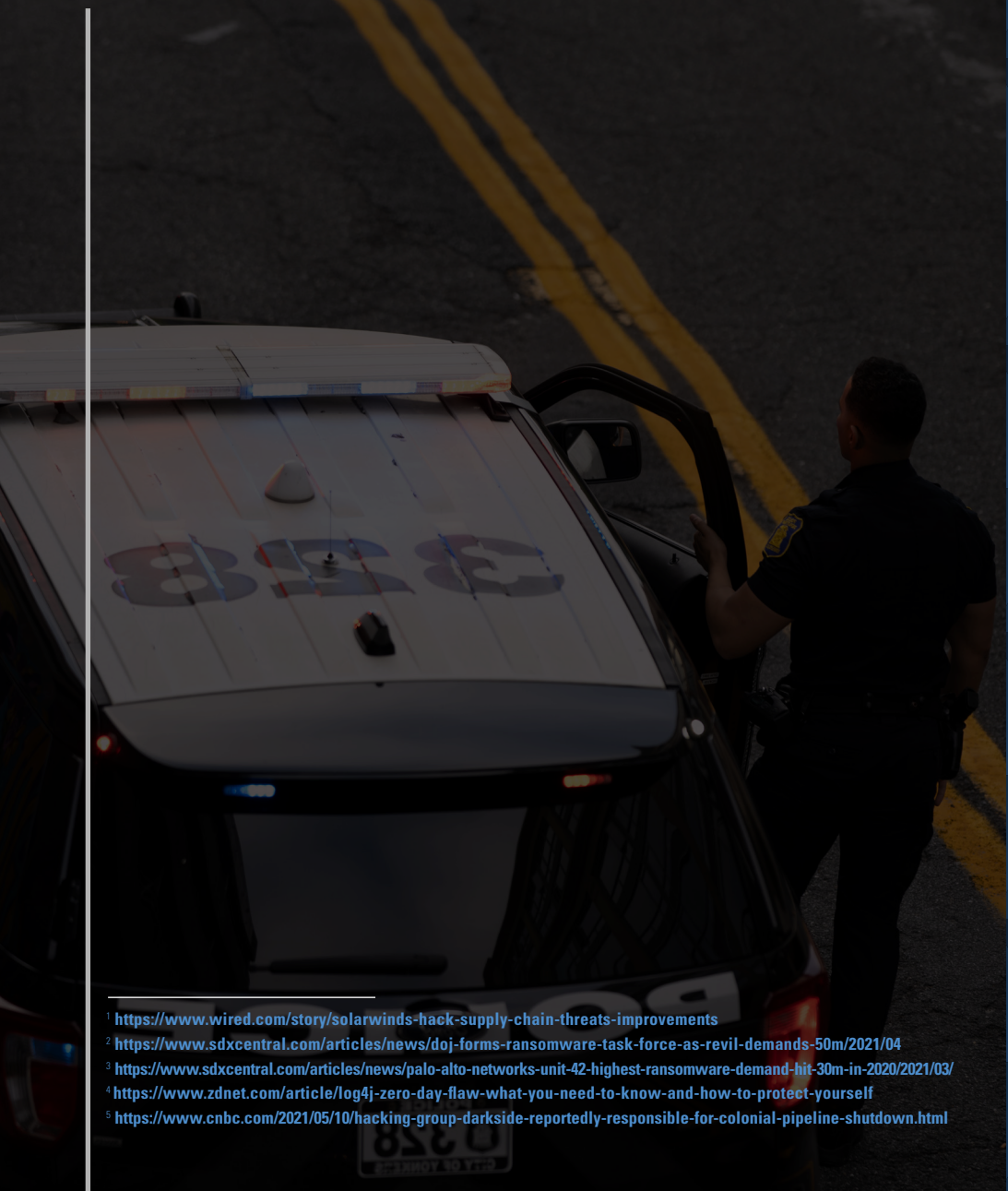
DEFENDING LAW ENFORCEMENT IN THE DIGITAL ERA

2022 MOTOROLA SOLUTIONS LAW ENFORCEMENT SURVEY

MOTOROLA SOLUTIONS

It's clear the pandemic has not sidelined cyber criminals. Just consider the last few years. The trend of increasing cyber breaches and their increasingly devastating impact is easy to spot. Consider:

- The continued fallout from the late 2020 SolarWinds hack;[1]
- The Russian ransomware-as-a-service gang REvil hitting a major electronics supplier in a $50 million ransomware attack;[2]
- Then the same gang demanding $70 million, the largest ransom demand to date, through an exploit to Kaseya VSA software;[3]
- The infamous zero-day vulnerability in the popular Apache Log4j open-source logging library that's used in nearly every enterprise application, which the U.S. Cybersecurity and Infrastructure Security Agency gave a perfect 10 out of 10 severity score; and[4]
- The criminal group DarkSide breaching Colonial Pipeline's systems and shutting down a major fuel supply for the East Coast, which created gas shortages across the East Coast and woke the average American up to the danger of cybercrime impacting industrial and critical infrastructure targets.[5]



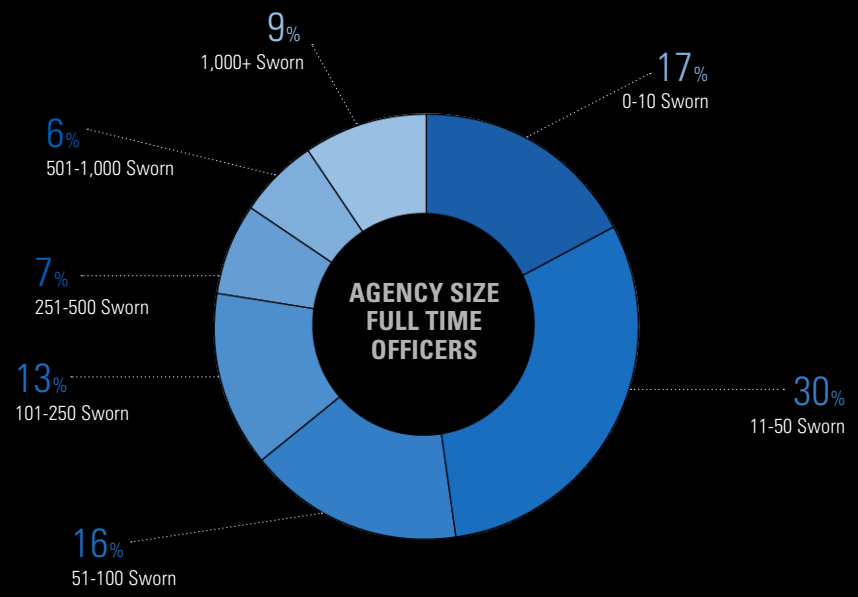
These weren't the only types of systems under attack. Reported attacks on public safety answering points (PSAPs) increased almost 40 % from just August 2020 to the beginning of 2021, according to the Motorola Solutions 2021 Threat Intelligence Report, **2021 Threats to Public Safety: Criminal Operations Focus**. That percentage is very likely higher if you consider that many Telephony Denial of Service (TDoS) attacks go undisclosed.

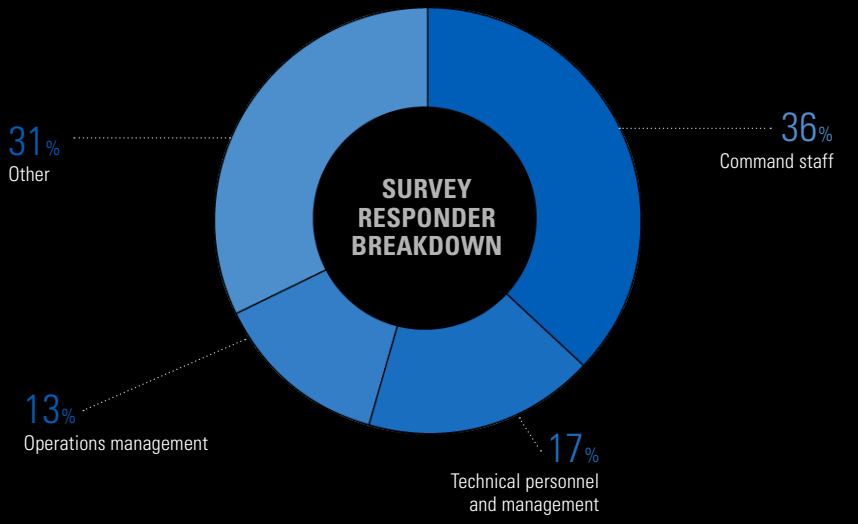
As we rang in the New Year in 2022, Motorola Solutions sought to understand the views and expectations of public safety professionals' around this new reality of cyberthreats. To do so, we queried just under 1,000 public safety personnel, including chiefs, sheriffs, district attorneys, CIOs, CTOs and other agency IT professionals.

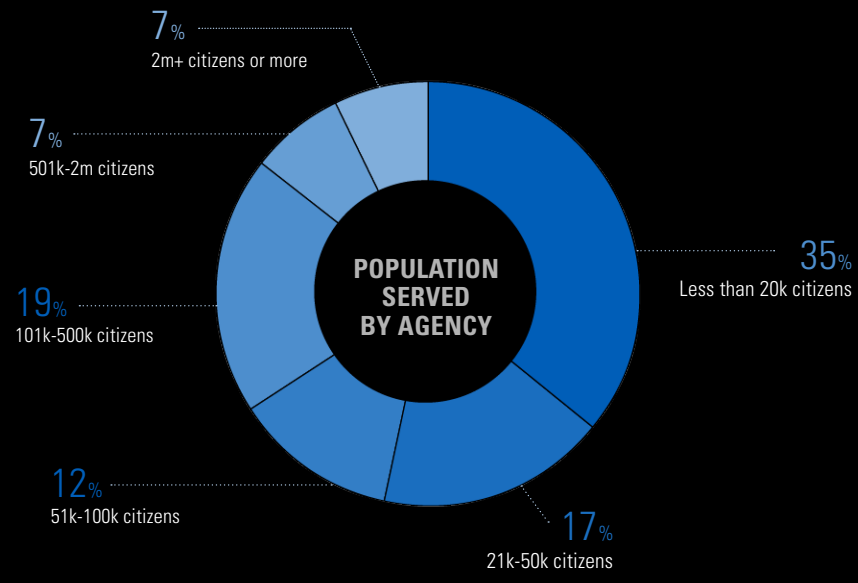
The result is the 2022 Motorola Solutions Law Enforcement Survey.

Survey respondents represent law enforcement agencies ranging in size from less than 10 to more than 1,000 full-time officers, serving from 20,000 to more than 2 million citizens. Each survey participant self-identified in one of four categories: Command Staff, IT, Operations Management or First Responders.

[1] https://www.wired.com/story/solarwinds-hack-supply-chain-threats-improvements
[2] https://www.sdxcentral.com/articles/news/doj-forms-ransomware-task-force-as-revil-demands-50m/2021/04
[3] https://www.sdxcentral.com/articles/news/palo-alto-networks-unit-42-highest-ransomware-demand-hit-30m-in-2020/2021/03/
[4] https://www.zdnet.com/article/log4j-zero-day-flaw-what-you-need-to-know-and-how-to-protect-yourself
[5] https://www.cnbc.com/2021/05/10/hacking-group-darkside-reportedly-responsible-for-colonial-pipeline-shutdown.html







The 2022 Motorola Solutions Law Enforcement Survey uncovers widely applicable insights, highlighting current cybersecurity understandings, implementations and opportunities for public safety professionals.

Our survey demonstrates the impact modern, end-to-end integrated public safety technology can have on securing operations across agencies while increasing officer efficiency and effectiveness. It also highlights the opportunity for law enforcement to further improve their cyber knowledge and strategies against all types of current and potential cyber threats.

TABLE OF CONTENTS

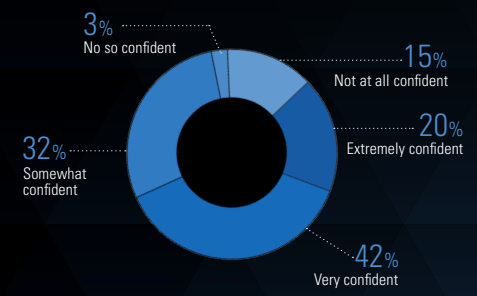
UNDERSTANDING THE UNKNOWN: CURRENT VIEWS ON CYBER THREATS

In the rapidly evolving world of cybersecurity, the challenge is always staying a step ahead of malicious actors and their constantly shifting tactics. It can seem as if the moment a new cybersecurity initiative is launched, cybercriminals have already adapted. This cat and mouse game, albeit one with deadly and costly consequences, creates uncertainty. And uncertainty saps confidence. So, it's no surprise that when we asked law enforcement professionals how confident they felt in their department's current cybersecurity program, only 20% responded that they were extremely confident. Just over 40% cited feeling very confident.

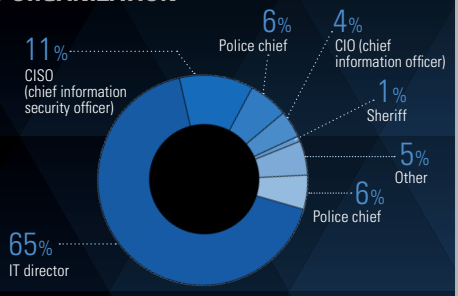
Of course, confidence in cybersecurity rests on a number of factors. One is the cybersecurity technology, products and services an agency deploys. Another is the leadership overseeing it. Yet, as technology evolves and cyber criminals adapt their tactics, there's an increasing need for more dedicated resources responsible for cybersecurity best practices across a department. Over 60% of respondents, an overwhelming majority, said that an IT director is currently responsible for overseeing the cybersecurity program at their agency. Many smaller agencies reported that this responsibility has fallen to the police chief or sheriff.

Perhaps in response to the many news reports of attacks on private companies, agency resources and public infrastructure, when asked which concerns were top of mind, an overwhelming majority of respondents identified ransomware as their agency's top concern. While only 6% cited telephony denial-of-service/distributed denial-of-service (TDoS/DDoS) attacks as their top concern, more public safety personnel should be wary, since according to the Motorola Solutions 2021 Threat Intelligence Report, along with ransomware, these are among the most common attacks facing public safety agencies today, especially PSAPs. When taken together with 27% of respondents who are simply unsure about the top cyber threats facing their agency, it's clear that more cybersecurity education is needed among a broader mix of agency personnel.

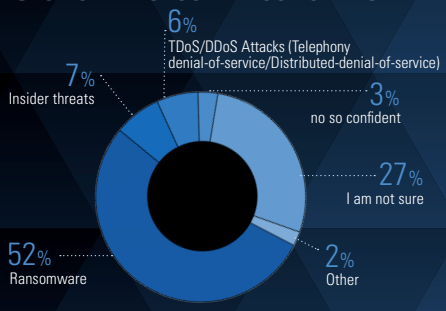
CONFIDENCE IN CURRENT CYBERSECURITY PROGRAM



RESPONSIBLE FOR CYBERSECURITY AT ORGANIZATION



LARGEST CYBERSECURITY CONCERNS



IMPLEMENTATIONS AND 2022 CYBERSECURITY BEST PRACTICES

With so many ongoing threats to public safety networks and systems, it's critical that agencies commit to implementing a holistic cybersecurity approach. It should be centered around a risk mindset that focuses on patching; regular incident response; readiness exercises and assessments; deploying modern EDR solutions; continuous monitoring to enable rapid threat detection; and remediation. This "gold standard" approach helps better detect zero-day exploits, discover adversaries escalating privileges within a network or system and prevent data exfiltration or compromise.

Yet, this approach requires experienced professionals to monitor systems, investigate alerts and determine how to implement and update policies and technology specific to agency environments and needs. That can be difficult, since finding, hiring and retaining staff with cybersecurity expertise is a constant challenge facing agencies of all sizes that can slow implementation of the critical tools and processes required for effective protection.

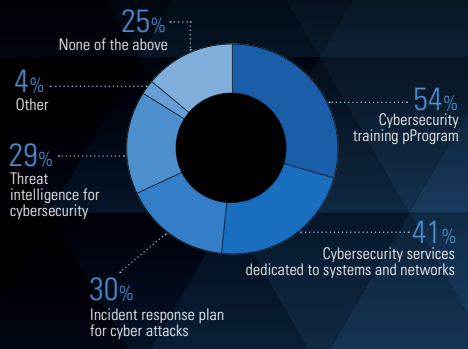
That difficulty is reflected in our survey results, as respondents cited low deployment across a range of critical cybersecurity solutions. For instance, less than half of respondents' agencies deploy cybersecurity services dedicated to systems and networks such as security monitoring and patching (41%). Only 30% of respondents have a cyber incident response plan or utilize threat intelligence and only 54% conduct cybersecurity training programs (respondents could choose more than one response).

Even more alarming, one quarter of respondents indicated their agency doesn't deploy any of those at all.

Of those who indicated their agency already implements cybersecurity services, the most widely cited examples were security monitoring, encryption and managed detection and response. Security patching and risk assessment were implemented much less often.

That level of vigilance is simply not sufficient to protect against or combat today's cyber threats. From CAD and call taking systems to networks and radios, it's critical that agencies think holistically about their technology, mindful of the cybersecurity risks associated with each and how they affect their larger technology ecosystem.

CYBERSECURITY SOLUTIONS DEPLOYED



TOP CYBERSECURITY SERVICES IMPLEMENTED

1. Security Monitoring
2. Encryption
3. Managed Detection And Response
4. Security Patching
5. Risk Assessment And Penetration Test

MOTOROLA SOLUTIONS: ONE SERVICE PARTNER FOR ALL YOUR CYBERSECURITY NEEDS

With more than 90 years of experience managing mission-critical technologies and more than 20 years of developing cybersecurity solutions, Motorola Solutions is well-positioned to be the 'one service provider' for your cybersecurity needs.

With best-in-class people, processes and technology, we bring scalable operations that can help agencies manage cyber risk awareness, detection, response and recovery. Our cutting-edge security automation and orchestration (SOAR) platform delivers deep insights for security management, system performance and service delivery, enabling a co-managed approach to security management.

Motorola Solutions' Managed Detection and Response (MDR) service provides a complete managed security solution to surface risks, identify imminent threats and provide a quick response to mitigate cybersecurity attacks around the clock. The service includes a technology platform enriched with public safety threat intelligence and third-party threat intelligence sources, along with 24/7 support from our Security Operations Center (SOC) staffed with cybersecurity experts to investigate threats and initiate a response.

ActiveEye Platform: The core of our ActiveEye security management platform is an analytics and automation engine that learns which cyber events require action and surfaces these to security analysts. Using advanced analytics machine learning and automation, our security systems can pinpoint substantiated threats and alleviate false positives and omissions. Both our customers and our SOC team use ActiveEye to get complete visibility into what's happening in their environment.

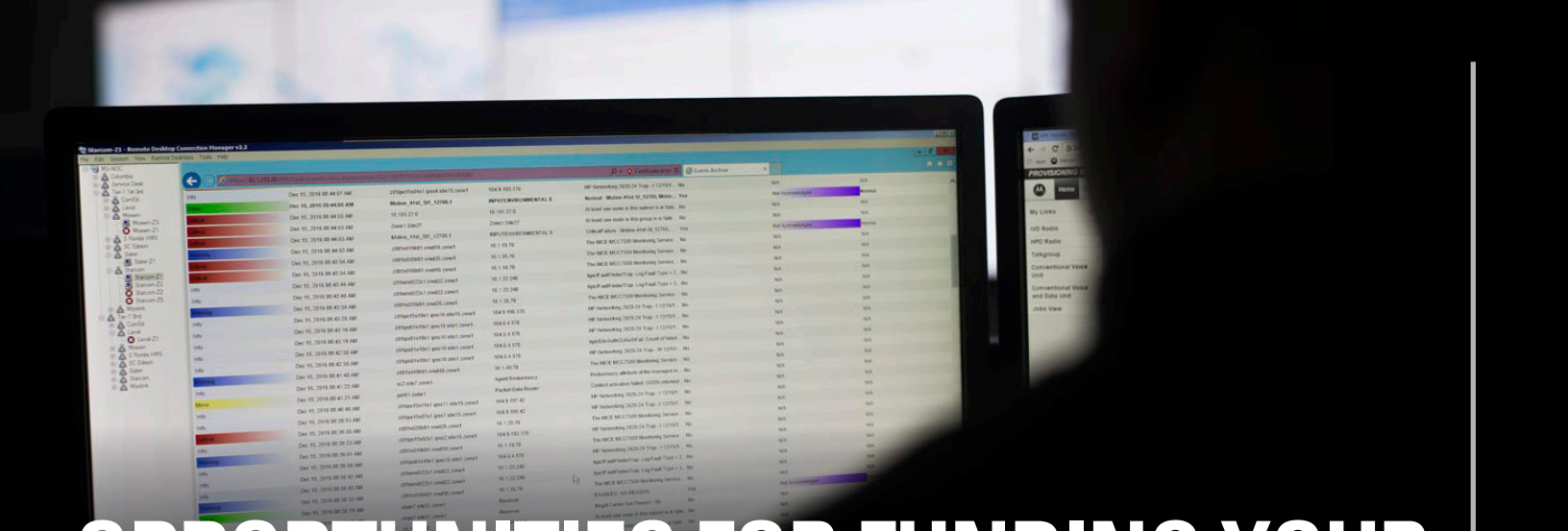
24/7 SOC: Our U.S.-based SOCs are staffed 24/7 with cybersecurity experts who have a broad set of skills and platform knowledge. These experienced, highly trained and certified security professionals are dedicated to monitoring the secure state of your mission-critical system. They are well-versed in incident response scenarios and will investigate and initiate a response when necessary. The team is continuously responding to attacks on public safety such as ransomware and has the skills to begin remediation immediately.

Endpoint Detection and Response: Our endpoint security services provide protection against known and unknown threats, quickly identify anomalies and enable investigation if there's a suspected incident. We deploy endpoint security agents to monitor for attacks on all types of PSAP workstations and servers required to access critical applications, including CAD, records management systems and evidence access stations, both on-premises and hosted in the cloud. If your agency has already deployed a next-generation EDR solution to protect workstations and mobile devices, but are struggling to manage them, we can provide 24/7 managed security services to support you via our deep API integrations.

Public Safety Threat Alliance (PSTA): Motorola Solutions has established a cyber threat Information Sharing and Analysis Organization (ISAO) to provide public safety agencies the capabilities they need to defend against attacks. The Public Safety Threat Alliance (PSTA) serves as a cyber threat intelligence sharing, collaboration and information hub for the evolving cyber security challenges faced by the global public safety community.

Managed Detection and Response is just one component of Motorola Solutions Cybersecurity Services. Our portfolio also includes advisory services such as cyber exercises, risk assessments and penetration testing, as well as services such as Incident Response readiness planning and System Recovery.

To learn more, visit: www.motorolasolutions.com/cybersecurity



OPPORTUNITIES FOR FUNDING YOUR NEXT CYBERSECURITY INITIATIVES

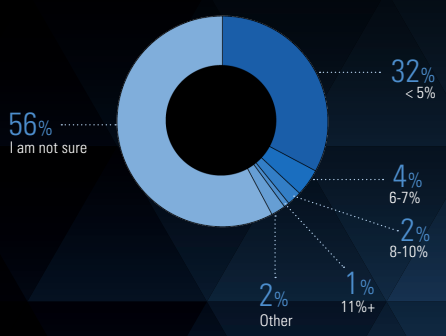
It's no secret that state and local governments are challenged with cybersecurity expenses. From hiring experienced IT personnel, to vetting software and systems, to patching and monitoring, agencies of all sizes struggle with funding.

We asked respondents to estimate how much their agency plans to spend on cybersecurity specific initiatives within its annual budget. Of those that answered, the top response was the lowest figure provided as a choice: less than 5%. Just as concerning, over 50% of respondents weren't even able to estimate a general budget percentage.

While cybersecurity expenses can be steep, the cost of not adequately protecting mission-critical systems and networks is much higher, both in dollar amounts and, even worse, in potential losses. For many agencies, the combination of competing priorities and the fact that they don't believe they've ever been breached may make cybersecurity less urgent. Yet, the moment these agencies are hacked, it's already too late and many avenues to remediate the situation and keep systems operational will be closed.

Put simply, our survey highlights that the amount of cybersecurity spending and mindshare among public safety agencies does not align with the sophisticated cyber threats facing them today.

ESTIMATED PERCENTAGE OF ANNUAL BUDGET SPENT ON CYBERSECURITY



The good news is that many different forms of funding assistance are available. These include federal programs, such as the Infrastructure Investment and Jobs Act which includes about one billion dollars towards the State, Local, Tribal and Territorial (SLTT) Cyber Grant Program. The program is expected to be operational by Summer 2022.[6]

In addition, funding is available through the American Rescue Plan, with a final rule loosening restrictions on the $350 billion that states and localities can receive under the act, making it easier to spend funds on cybersecurity.[7]

In partnership with the grant experts at Lexipol, Motorola Solutions also offers free grant assistance for public safety cybersecurity along with assistance for mission-critical communications, video security and access control, command center software and dispatch consoles.

---

[6] **https://statescoop.com/state-local-cyber-grant-program-summer-cisa**
[7] **https://home.treasury.gov/news/press-releases/jy0550**

SECURING THE ECOSYSTEM: THE POWER OF INTEGRATED PUBLIC SAFETY TECHNOLOGY

Today, keeping the public safe requires modern, effective operations, and effective operations require maximum connectivity. For instance, a dispatcher interfaces with an officer and the officer may collaborate with other first responders. Video and data may be shared for increased situational awareness, even before a responder arrives at the scene. Suspects may need to be tracked and apprehended. Evidence must be securely collected and shared. Communities need to be informed and public/private partnerships strengthened through transparent sharing of information.

That's why modern public safety requires a unified technology ecosystem that integrates people, assets and operations, simplifying tasks and creating new workflow efficiencies so responders can focus on their core mission, not their technology.

When asked what they'd like to have seamlessly integrated, respondents selected a range of technologies and services, from body-worn cameras and two-radios to evidence software and cybersecurity services. This large collection of solutions highlights how complex public safety technology can become, especially when systems, devices and networks are added at different times across years of deployments. That's why seamlessly integrating them into one ecosystem that can grow over time is so important.

PUBLIC SAFETY TECHNOLOGIES THAT RESPONDENTS WANT INTEGRATED

- ✓ Two-Way Radios
- ✓ Dispatch Software
- ✓ Smartphones
- ✓ Body-Worn Cameras
- ✓ In-Car Cameras
- ✓ License Plate Recognition
- ✓ Fixed Cameras
- ✓ Call Taking Software
- ✓ Evidence Software
- ✓ Cybersecurity Services

IMPORTANCE OF INTEGRATING TWO OR MORE PIECES OF PUBLIC SAFETY TECHNOLOGY

- 78/100

TOP CITED BENEFITS OF INTEGRATING YOUR PUBLIC SAFETY TECHNOLOGIES

- Increased Efficiency
- Streamlined, Collaborative Workflows
- Centralized Data
- Enhanced Cybersecurity Protection
- Cost Effectiveness
- Improved Response Times
- Scalability

That type of integration is clearly significant to law enforcement. When asked how important it is to integrate two or more pieces of public safety technology, respondents averaged a score of almost 80 out of 100, with one not important at all and 100 being the most important.

Unifying public safety technology in one ecosystem also enhances cybersecurity by streamlining the people, processes and tools needed to keep systems and networks safe. Rather than attempting to secure multiple siloed technologies, agencies can centralize and streamline data and systems enhancing overall security for the entire ecosystem. Survey respondents agreed, including cybersecurity among the top benefits of integrating public safety technology, along with increased efficiency and collaboration and more easily accessible data.

BETTER TOGETHER: APX TWO-WAY RADIOS AND V300 BODY-WORN CAMERAS

In an emergency, you need to act fast. Your technology should too, immediately ready to support the safety and wellness of responding officers. Activating body-worn camera video capture is one of the most critical support functions technology can offer in the field. But officer attention should be on the situation in front of them, not on managing that technology. That's why Motorola Solutions APX two-way radios and V300 body-worn cameras now work together seamlessly in the moments that matter most. In an emergency, you know you can always press APX's large orange emergency button for urgent assistance. Now, when you press that button, the V300 will immediately start capturing video evidence that can save lives, ensure accountability, and build cases. The result is unparalleled safety, powerful new capabilities and the peace of mind that your technology always has your back, automatically.

LEARN MORE

DEFENDING LAW ENFORCEMENT IN THE DIGITAL ERA

Today, threats to law enforcement are rapidly evolving. Savvy criminals are altering their tactics while officers are continuously asked to do more with less. At the same time, criminals behind a computer screen can wreak havoc on law enforcement systems that were unimaginable just a few years back. Yet, the answer isn't just more technology.

Modern, effective public safety requires a unified technology ecosystem **that integrates people, assets and operations, increasing efficiency and security for better outcomes.**

When asked about the benefits of this type of integration, respondents were clear that it would help them do their jobs more effectively in a number of different ways: from rapid officer deployment and dispatch, to better control of data and evidence, to faster investigations.

TOP BENEFITS OF INTEGRATING PUBLIC SAFETY TECHNOLOGY

- Deploy Officers To The Front Lines Faster
- Minimized Time To Dispatch
- Effective Data Sharing And Management
- Accelerated Investigation Timelines
- Automated Evidence Capture On Scene

Yet, as the 2022 Law Enforcement Survey highlights, even the best technology ecosystems are only effective if they're available. That's why forward-thinking agencies of all sizes are focusing on building an integrated ecosystem of technology, then investing in securing it.

This type of ecosystem is much greater than the sum of its parts. It helps unify voice, data, video and analytics, breaking down silos that have developed over years of standalone purchases. It simplifies operations, making response times faster and public safety responders more effective. It helps strengthen community trust and transparency. And it's easier to secure against accelerating cyber threats to public safety systems.

That's why technology ecosystems are a critical modern policing tool today, one that's likely to only grow in importance in the years ahead.

Learn more and explore our entire public safety ecosystem of law enforcement solutions at:
www.motorolasolutions.com/lawenforcement

MOTOROLA SOLUTIONS