CYBER THREATS TO PUBLIC SAFETY

2019 INSIGHTS FROM THE MOTOROLA SOLUTIONS CYBERSECURITY TEAM

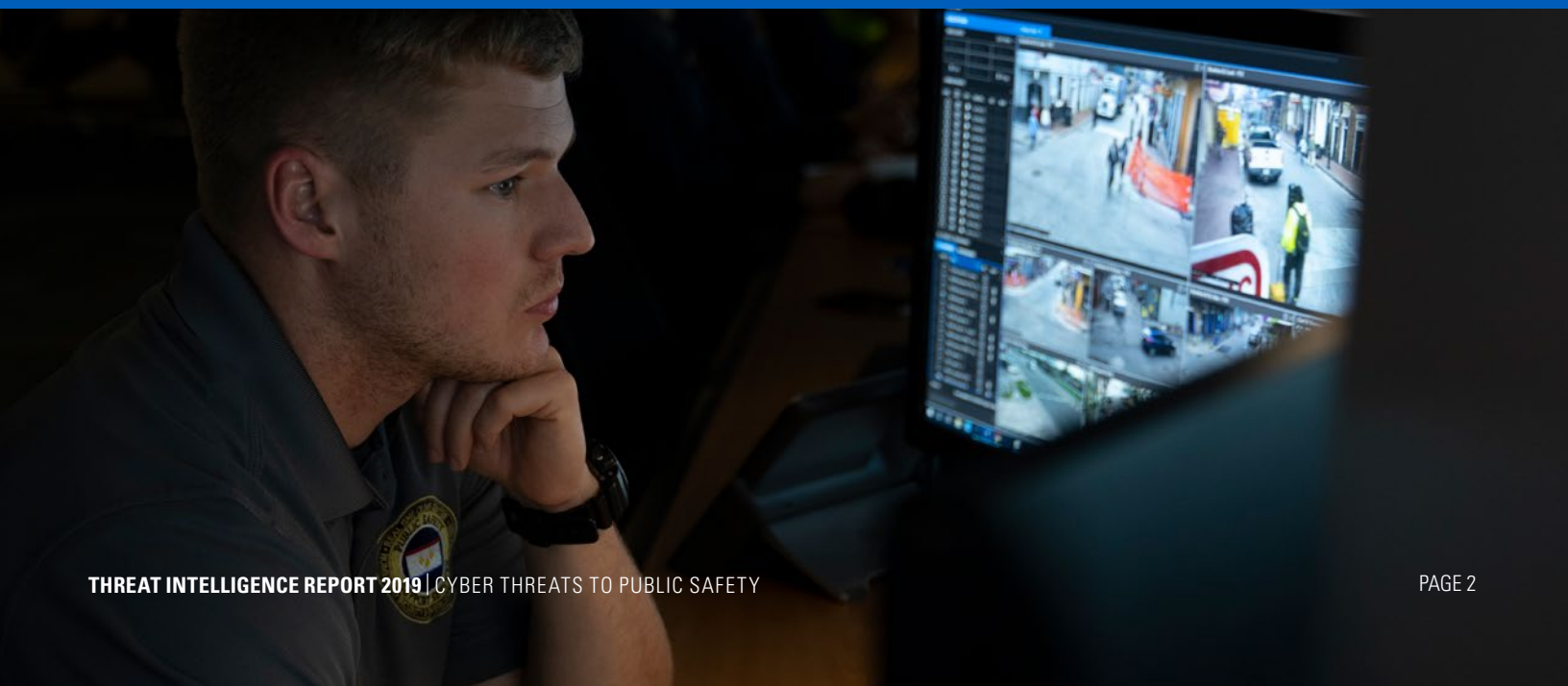
MOTOROLA SOLUTIONS

Motorola Solutions is uniquely placed in the public safety sector. As both a leading cyber security practitioner and public safety solutions provider, we regularly engage a broad swath of emergency services customers including public safety (police, fire, EMS, 9-1-1) and federal agencies. Our public safety cybersecurity services approach follows the National Institute of Standards and Technology (NIST) Cybersecurity Framework, to help you manage your cyber risk surrounding Identification, Protection, Detection, Response, and Recovery. We closely follow leading governance and oversight strategies throughout the Product Development, Implementation and Operational Support Lifecycle.

We have comprehensively aggregated and analyzed our 2019 cybersecurity data from January 1 to December 31, 2019, along with that of publicly reported cyber attack information, to generate deep insights into the current state of public safety cybersecurity.

The result is the Motorola Solutions 2019 Cyber Threats to Public Safety report. By publishing these findings, we hope to leverage the knowledge we have gained in 2019 to make public safety agencies more secure in 2020 and beyond.

TABLE OF CONTENTS



EXECUTIVE SUMMARY

Despite cybersecurity being a priority for public sector CIOs and CISOs, government agencies at all levels continue to face escalating cyber threats. Cyber intrusions and attacks increased dramatically over the last decade, exposing sensitive personal and organizational information, disrupting critical operations and causing substantial economic losses to individuals, corporations and governments. Hostile actors such as hackers, organized criminals and foreign countries are rapidly improving their technical cyber capabilities. They continue to target federal, state and local governments in attempts to steal or manipulate sensitive data and disrupt operations.

Today, ransomware attacks pose an especially urgent threat. In 2019, there was a notable increase in ransomware attacks against cities and municipal authorities. Agencies are now increasingly targeted with more sophisticated ransomware as hostile actors refine and shift their tactics to maximize success. While these agencies largely avoided the ransomware scourge in the past, they are now increasingly affected as a result of ransomware's penchant for spreading and infecting beyond its initial target.

Motorola Solutions believes that the sheer criticality of emergency services will likely prompt enterprising actors to launch increasingly targeted and sophisticated ransomware extortion attacks directly against emergency services for potential financial rewards or to cause disruption as a punitive action.

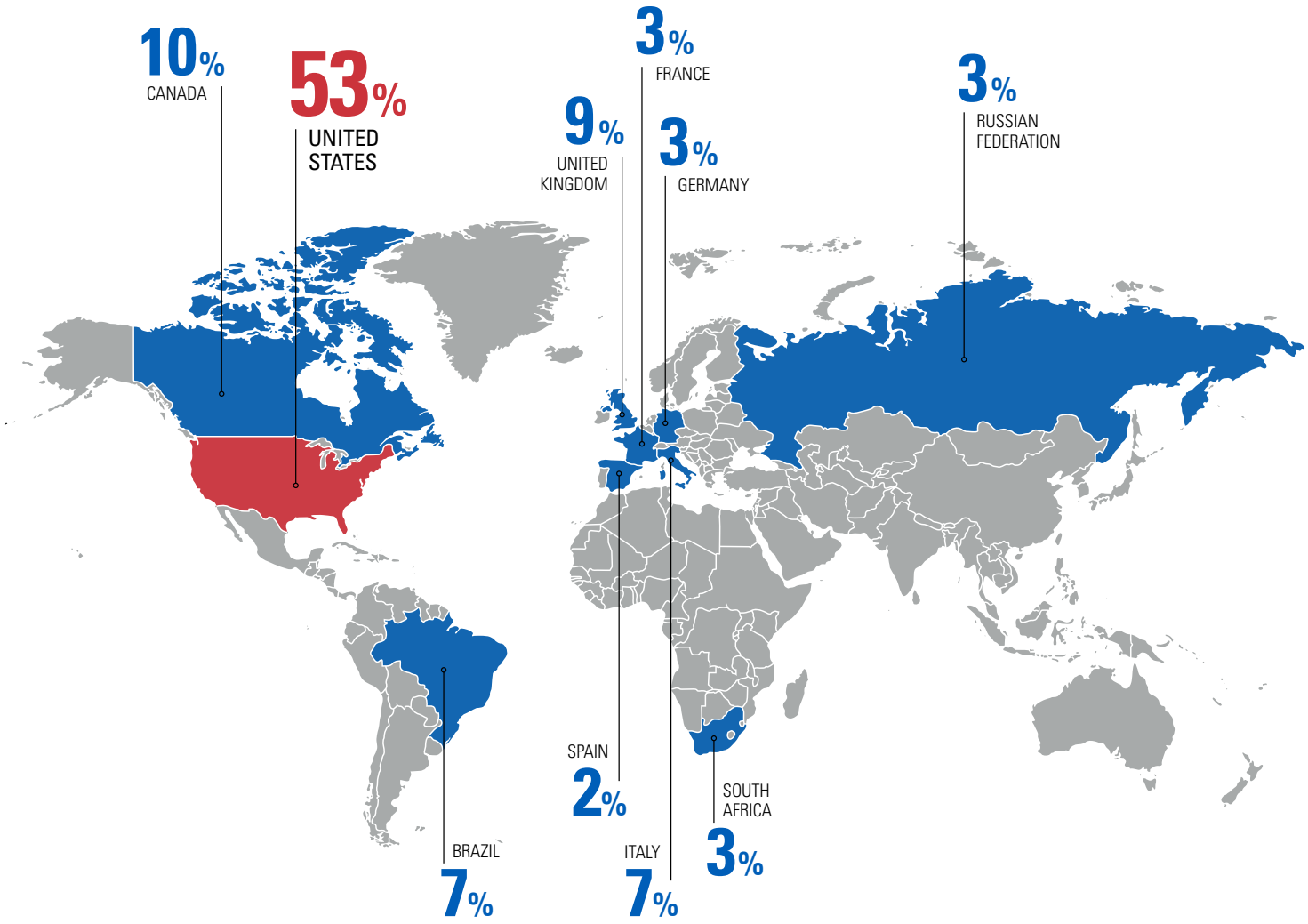
As agencies become more adept at defending against extortion attempts, we believe hostile actors will begin to target more critical systems such as the public safety answering point (PSAP), or managed service providers (MSPs) in order to increase the scale of infection and the likelihood of receiving a payout. Additionally, as demand increases for accessible ransomware options in criminal marketplaces, we predict that the Ransomware-as-a-Service (RaaS) model will grow in popularity to meet that demand.

The stakes are extremely high. Emergency services are a key component of critical infrastructure. Failing to protect the confidentiality, integrity and availability of the information systems that support them, as well as the information resident within them, places lives at risk and endangers public confidence in government itself.

As the cyber attacks highlighted in this report become more sophisticated, organizations of all sizes need to take a proactive, holistic, risk-based approach to cybersecurity, focusing on mitigation options, continuous monitoring, diagnosis and remediation to evolve security practices. This process starts with reviewing existing security strategies to ensure policies and security mechanisms are in line with current best practices.

RANSOMWARE AND PUBLIC SAFETY: THE TOP THREAT OF 2019

Ransomware remains a go-to weapon in hostile actors' toolboxes, driving high demand for effective solutions. In response, the ransomware ecosystem of authors, service providers and distributors continue to demonstrate innovation in creating a product for willing buyers. According to first-quarter 2019 statistics from Malwarebytes, the United States is the most impacted country by ransomware attacks[1], likely due to its high Internet penetration rate.

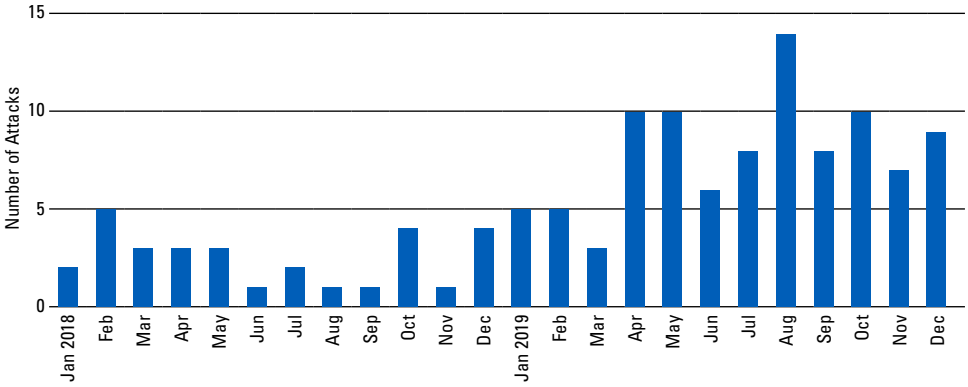


Ransomware has been successfully deployed against a variety of industries, including public safety entities. While healthcare has been a primary focus to date, services such as 9-1-1 and law enforcement are increasingly being targeted. The public's reliance on such services makes them a particularly lucrative ransomware target because governments are more likely to pay than to risk having degraded emergency services available to the public. While there has been some success in arresting ransomware authors, it has not been significant enough to curb the activity. The fact that several compromised targets recently acquiesced and paid ransoms will likely impact the risk vs. benefit analysis and encourage more attacks.

2019: THE TIPPING POINT FOR RANSOMWARE ATTACKS ON US MUNICIPALITIES

By December 31, 2019, Motorola Solutions observed approximately 95 municipalities targeted by ransomware attacks during the year. In comparison, in all of 2018, there were 22 such publically reported incidents impacting state and local governments.

RANSOMWARE ATTACKS TO MUNICIPALITIES



A May 2019 report from the Department of Health and Human Services corroborates this increased targeting of local governments, stating that ransomware incidents have been observed in 48 states and the District of Columbia.[2] Most of the attacks targeted small-town America, because cash-strapped local governments are less likely to update their cyber defenses or back up their data and are more willing to pay the ransom. In general, municipalities tend to be low-hanging fruit for hostile actors, since they often are less prepared than companies because of limited resources and difficulty competing for cybersecurity talent. In 2019, ransomware was observed infecting public safety entities using three predominant methods: brute forcing or exploiting known vulnerabilities in remote desktop protocol, exploiting serialization/ deserialization vulnerabilities in web servers and phishing employees and officers. The majority of these infection methods could have been mitigated through timely, comprehensive patching strategies and multi-factor authentication.

Motorola Solutions believes the intent of targeting cities, municipal agencies and, by extension, emergency services is to extort ransoms from government authorities for financial gain or to erode their reputation. Such a tactic could cause the public to fear that their local governments cannot protect them, thereby reducing public confidence. Ransomware is the type of tool that can benefit all classifications of hostile cyber actors. While cyber criminals are the usual perpetrators of this malware, there is evidence from industry sources suggesting that state actors may have been behind some of the more prominent ransomware campaigns.[3/4] According to intelligence officials, the majority of ransomware attacks, including those that are state-backed and private criminal-led, are sourced from Eastern Europe, Iran and, in some cases, the United States.[5] No matter the original aim of deploying malware, ransomware is a tool that can have a wide range of intended and unintended effects, making it a particularly critical threat while magnifying potential damage.

RANSOMWARE AND THE PSAP: A GROWING THREAT

Any time a public safety answering point (PSAP) is forced offline, the effectiveness of public safety is degraded, placing communities at higher risk. Since the PSAP is one of the most critical municipal functions and must be operational at all times, we believe it is becoming a more enticing target for extortion.

Our reporting shows that ransomware attacks that can successfully compromise the PSAP are relatively rare today. Of the 119 publically reported ransomware attacks against municipalities and emergency service entities in 2019, 12 were reported to have disrupted PSAP operations. Of the 12 attacks, five targeted police departments, six targeted the municipality themselves and one targeted a fire department.

Today, PSAP disruptions are more likely collateral damage from an adjacent attack on a primary municipal target. However, we predict with moderate confidence this will change and in 2020, PSAPs will increasingly become primary targets themselves, as hostile actors prey on a municipality's most critical data and operations.

In
2020
PSAPs will increasingly become primary targets themselves, as hostile actors prey on a municipality's most critical data and operations.

RANSOMWARE COSTS AND RECOVERY

Ransomware attacks are often more damaging than data breaches because they can completely shut down an organization's IT operations. Global damages caused by ransomware attacks are estimated to reach 11.5 billion dollars by the end of 2019. By the end of 2021, ransomware is expected to attack an organization every 11 seconds.[6]

Apart from the cost of the ransom itself, successful ransomware attacks can bring other significant financial consequences, including expenses associated with recovery efforts, such as forensic reviews and assistance in rebuilding servers and workstations. Overall, the longer a ransomware attack endures, the higher the potential loss of life, public trust, revenue loss, reputational damage, loss of productivity through work disruption and the scale of subsequent legal issues.

Unfortunately, many municipalities that have fallen victim to ransomware attacks in 2019 suffered downtime lasting from a few days to numerous weeks in order to completely rebuild their networks and reimage all computers. Those municipalities that were able to recover the fastest were only able to do so with updated and offline backups and a well rehearsed incident response recovery plan.

Protect your PSAP

When configured correctly, the PSAP operates on a protected and isolated network to ensure it cannot be impacted by an attack to the greater organization. The 2016 Task Force on Optimal Public Safety Access Point Architecture (TFOPA) report,[7] sponsored as part of a United States Federal Communications Commission (FCC) initiative, outlines specific cybersecurity protections that have proven effective in defending against ransomware attacks. The protections include developing and practicing an incident response plan; establishing a vulnerability management program with patch remediations, data backups and testing of the protections on a regular basis; developing network security monitoring and response capabilities; and aligning solutions with the NIST Cybersecurity Risk Framework. Additionally, the Cybersecurity and Infrastructure Security Agency (CISA) has unveiled a 9-1-1 self assessment tool that can assist 9-1-1 agency leadership, improve the cybersecurity posture of their system through enhanced planning and the implementation of cyber hygiene best practices.[8]

NOTABLE 2019 PUBLIC SAFETY CYBERATTACKS

Augusta, Maine

In April, a ransomware attack successfully impacted public safety computers, rendering the public safety dispatching network unusable and forcing dispatchers to manually track the movements of police, firefighters, and ambulance crews.[12]

Albany, New York

In March, a ransomware attack negatively affected some police department systems, including scheduling and email. In addition, the attack impacted computers in police patrol cars, hindering their ability to process incident and accident reports, thereby increasing response time to service calls.[9]

Vigo County, Indiana

In August, the Sheriff's office was attacked by an unknown ransomware variant. The ransomware was able to shut down police email systems and the 9-1-1 CAD system. Dispatchers were forced to handle calls manually and work with neighboring dispatch centers to ensure no calls were missed. The county was prepared for such an event and were able to maintain public safety services with minor delays.[14]

Baltimore, Maryland

In March, a ransomware attack on Baltimore successfully impacted the city's computer-aided dispatch system for approximately 20 hours. This impacted the 9-1-1 system, requiring manual dispatch for public safety calls. Additionally, dispatch calls were not recorded during this period.[10]

Jackson County, Georgia

In March, a ransomware attack was successfully deployed against Jackson County government systems. The ransomware locked out many government systems, including the sheriff's office's ability to book criminals.[11]

Stuart City, Florida

In April, a ransomware attack successfully struck police and fire department computers forcing personnel to resort to pen and paper as a work-around. Communications via email were severely impacted.[13]

DATA LOSS AND BREACHES

A data breach or data leak is the release of sensitive, confidential or protected data to an untrusted environment that can occur as a result of a malicious attack, current or previous employees or the unintentional loss or exposure of data through negligence or vulnerabilities.

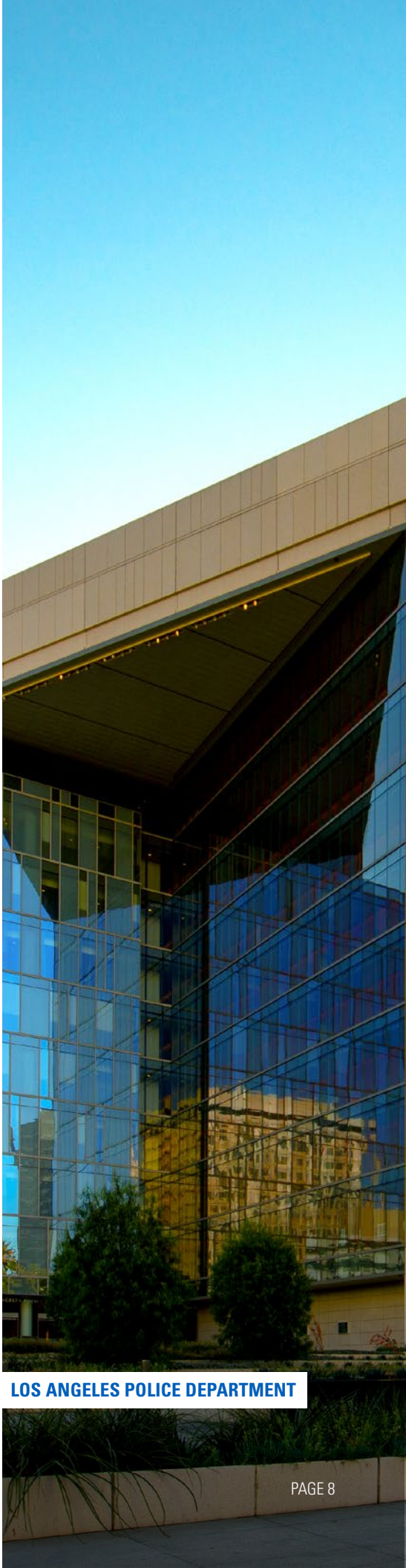
Since 2018, data breaches have gotten bigger, hackers have become more savvy and the amount of compromised data is on the rise. As breaches become more routine, it is apparent that public safety organizations are still underprepared. In July 2019, an unknown hacker stole personally identifiable information on 2,500 serving Los Angeles police department officers, trainees and recruits, along with records belonging to roughly 17,500 would-be officers enrolled in the Candidate Applicant program.[15] The data breach exposed names, dates of birth, email addresses and passwords, as well as the last four digits of Social Security numbers. Despite the constant barrage of cyber attacks against the city of Los Angeles, this was the first successful breach and highlighted the vulnerabilities within government systems. The city has secured the database and is conducting an internal investigation.

Generally, employee negligence and poor security practices are among the major causes of data breaches. The 2018 Insider Threat Report asserted that 90% of organizations are likely to be attacked or exposed to attacks through an insider, and more than 50% have experienced an insider attack.[16] Many organizations have training and policies in place to teach their employees good cyber practices and protect data. However, often these efforts are not frequent or prevalent enough to truly protect an organization.

Phishing is one of the most prevalent ways an employee can expose sensitive information. On July 10, 2019, Arlington County, Virginia, suffered a data breach compromising the personal data of all county employees after an unauthorized party gained access to the county's payroll system.[17] The initial compromise occurred when a county employee was tricked by a well-crafted phishing email, which then allowed access to sensitive county data. Phishing messages used by hackers are cleverly and carefully crafted to appear legitimate to staff members and are often excellent in masking their exact origin and purpose. They will often pass many standard email filters and appear to be from a trusted source to the average eye.

In many cases, data leaks and exposure take place as a result of an employee's negligence. For instance, in August 2019, the New York Fire Department warned 10,000 individuals about a potential data breach stemming from an authorized employee losing an unencrypted external hard drive containing their personal information.[18] The loss took place as a result of the employee's failure to follow the department's data security policies. The hard drive contained confidential information provided by 9-1-1 callers, such as name, address, telephone number, date of birth, insurance number, health condition and, in some cases, Social Security number. The fire department has since offered free credit monitoring to all people whose Social Security numbers were compromised.

Negligence and lax security policies can also add risk to an organizations' reliance on third parties. Third-party risk is now a common and dangerous issue, costing organizations around the globe an estimated $10 billion. Public safety organizations face increasing risk from third parties, whose networks and cybersecurity practices are outside of organizations' visibility and control. For instance, in August 2019, the fingerprints of over one million people, as well as facial recognition information, unencrypted usernames and passwords and personal information of employees, was discovered on a publicly-accessible database of a security company used by the UK Metropolitan Police.[19]



LOS ANGELES POLICE DEPARTMENT

The Rise of Phishing Attacks on Municipal Governments

In 2019, we saw sharp quarter-over-quarter increases in email-based ransomware attacks on municipal governments. Email phishing continues to grow as a means to precipitate a ransomware attack, especially in larger enterprises and the public sector. Phishing campaigns typically range from highly generic, to highly targeted and bespoke.

For example, in June 2019, the City Council of Riviera Beach, Florida, agreed to pay nearly $600,000 in ransom to hackers who paralyzed the city's computer systems.[20] The Riviera Beach attack reportedly began May 29, 2019 after a city police department employee opened an infected email attachment. All online city systems went down, including but not limited to, email, some phones, online billing and payment systems and water utility pump stations. The only way the city could collect utility payments was by check or cash delivered either in-person or by mail.

Email-based threats are not something to be ignored. According to the 2019 Verizon Data Breach Investigations Report, the average company receives 94% of all detected malware through email.[21] Additionally, 45% of email-based malware is delivered via email attachments such as Microsoft Office documents.

Based on our observations and guidance from the FCC's Task Force for Optimal PSAP Architecture,[22] we recommend that agencies segregate mission-critical systems from portions of the network that provide email services or have internet browsing access.

HACKTIVISM

In 2019, instances of hacktivism against the public sector remained a problem, although these numbers have yet not reached the tempo of hacktivist attacks seen in 2015 and 2016.[23]

For instance, in late 2018, the Anonymous collective announced it hacked into the website of the Italian Trade Union of State Police Officers, resulting in the release of personal information on 200 Italian police officers.[24] As observed in previous years, common hacktivist tactics like denial-of-service attacks and website defacements have continued into 2019. For instance, a slew of massive cyber attacks against the government of Sudan took place in early 2019 as part of an international #OpSudan campaign aimed at the military regime in the country. While researchers typically do not attribute high technical capabilities to hacktivists, for all of their limitations, the collectives do have a large platform to push their ideas. Researchers note that in today's online climate, hacktivists could potentially use their platforms to further criminal or nation-state-backed hacking campaigns.

TELEPHONE DENIAL-OF-SERVICE

The critical nature of PSAPs makes them a lucrative target for attackers seeking to extort, or to further a political or personal agenda through a denial of service attack.

A telephone denial-of-service (TDoS) attack is a unique attack type that is simple, yet can be effective against 9-1-1 centers given their reliance on voice communications. A TDoS attack is comprised of hundreds, thousands, or tens of thousands of calls which serve to deplete emergency system resources, saturating dispatch centers with bogus calls while potentially denying calls from legitimate persons in need due to either operator or technical capacity saturation. Typical TDoS attacks attempt to extort dispatch centers by degrading critical functions until payment is received, or as a disruptive prank for an attacker to prove their capability.

The TDoS threat remains in both legacy and Next Generation 9-1-1 (NG9-1-1) systems, and this threat is especially viewed as a NG9-1-1 related threat given the fundamental shift to IP based technologies involved in that transition. This shift will increase the scope of attacks able to target the PSAP, as IP-based technologies could allow an attacker to conduct a remote attack, which were difficult to attack in legacy circuit based telephony systems. Practically however, NG9-1-1 systems are significantly less vulnerable than E9-1-1 systems if the calls are delivered natively as IP because of the built-in flexibility and capacity of those IP-based systems.

TDoS attacks are not typically reported in the media, but remain a concern to public safety organizations. According to Jay English from the Association of Public-Safety Communications Officials-International (APCO), there have been "hundreds of TDoS attacks targeting public safety in the past three years and these are just the attacks that have been reported. We suspect the actual number is higher." While TDoS attacks do not cause a compromise event (with the recovery requirements implied such a situation) they do cause meaningful effects to emergency service operations.

To better combat TDoS attacks targeting the PSAP, operators can assign levels of confidence and direct suspect call traffic to lower priority queues, or in some cases, enable automated call back features or automated answer and proof of life features. This action can ensure dispatchers are able to service critical emergency calls, while managing the influx of malicious call traffic.

CYBERSECURITY BEST PRACTICES FOR PUBLIC SAFETY

In light of the growing cybersecurity threat to public safety, it is critical that organizations invest in proactive and holistic cybersecurity. We highly recommend the following approach.

HAVE AN INCIDENT RESPONSE PLAN AND PRACTICE IT

There is more to ransomware response than restoring data from known good backups. It may take time for the organization's IT professionals to isolate and remove the ransomware threat and restore normal operations and data. In the meantime, organizations should take steps to maintain their essential functions according to their business continuity plan.

Organizations should implement and regularly test backup plans, disaster recovery plans and business continuity to ensure that they are able to get the systems back online in the expected timeframe. The practice will also provide IT teams with confidence to perform flawlessly under pressure when the need arises.

PROACTIVE DEFENSES

One of the first steps in establishing a holistic cyber protection plan is to establish proactive defenses. These defenses start with the presumption that you will be breached, then consider how you will detect, contain and recover from the attack. A comprehensive patching plan is a basic, but vital, starting point in an organization's defense. A large portion of ransomware attacks exploit known vulnerabilities, which have patches available, and are highly successful because organizations are unable to identify or update unpatched systems. Additionally, public safety organizations can limit their cyber attack surface by disabling unused ports, especially those highly targeted by ransomware actors such as remote desktop protocol, port 3389.

One of the most effective proactive strategies is to enact user awareness training that focuses on real world cyber threats. The end user is frequently the most targeted aspect of an organization's cyber defense and a workforce trained in identifying suspicious emails with strong computing hygiene and security can act as a front line defense, blocking and flagging intruders who have thwarted the network defenses.

External assessments are a valuable resource when deciding on the best way to spend limited budgets. A knowledgeable and experienced third-party, who understands the unique operations and risks around public safety, can provide valuable insight and advice on where to make investments in cyber protection and monitoring.

MAINTAIN ROBUST BACKUP AND RECOVERY

One of the most important defenses against ransomware is having a robust backup strategy in place that includes off-site storage and regular testing of images and other saved data to ensure its integrity.[25] If ransomware manages to install and execute on a machine, a recent, comprehensive backup is an essential remedy. Rather than attempting to remove the malware and decrypt affected files, the infected machine can be wiped and restored from the clean backup with minimal impact on operations. Backups should be performed regularly and stored on media that is not connected to the machine, as new ransomware variants like WannaCryptor and CryptoLocker are known to destroy all shadow copies and restore point data. A software agent-based backup solution that does not leave backup media exposed as mounted drives on network segments is highly recommended. Frequent backups minimize the impact of a ransomware attack as only hours or days of data is lost as opposed to weeks, months or even years, as evidenced by the examples in this report.

DEVELOP ADEQUATE POLICIES

It is important for organizations to develop policies that are focused on the various email, web, collaboration, social media and other tools that their IT departments are using or that will likely be used in the foreseeable future. These policies should focus on legal, regulatory and other obligations to encrypt emails and other content if they contain sensitive or confidential data; monitor all communication for malware

that is sent to blogs, social media and other venues; and control the use of personal devices that access corporate systems. Organizations should align their cybersecurity policies to the National Institute of Standards and Technology (NIST) Cybersecurity Framework to fully understand their current cybersecurity posture and assess their progress of securing identified areas of risk.[26] Additionally, the FCC's Task Force on Optimal PSAP Architecture has released policy guidance to ensure PSAPs and 9-1-1 authorities have guidance on an optimal approach to secure architecture, complying with regulatory obligations and developing cyber protections to identify and mitigate cyber risk. Establishing robust policies will be useful in limiting the number of tools that employees use when accessing organizational resources. In turn, these limitations decrease the attack surface and the number of ingress points for ransomware, other forms of malware, phishing attempts and other content that could pose a security risk.[27]

INVEST IN SECURITY MONITORING

In order to further mature an organization's cyber protections, public safety organizations should invest in a meaningful security monitoring service. A provider who understands your operational and network requirements will be able to augment your current security team in identifying and remediating malicious activity. As attackers frequently evolve their tactics and increase their pace, it is also advisable to integrate security monitoring with threat intelligence in order to stay ahead of existing and emerging threats. Understanding techniques, tactics and procedures employed in various attacks will help organizations prioritize investment allocation and fine tune security controls. This layer of protection can further an organization's cybersecurity strategy and ensure they remain compliant with state and federal regulations to protect their citizens' data. As the cybersecurity workforce shortage continues, a managed security monitoring service can be leveraged to address that shortfall with centralized and qualified security operations personnel.

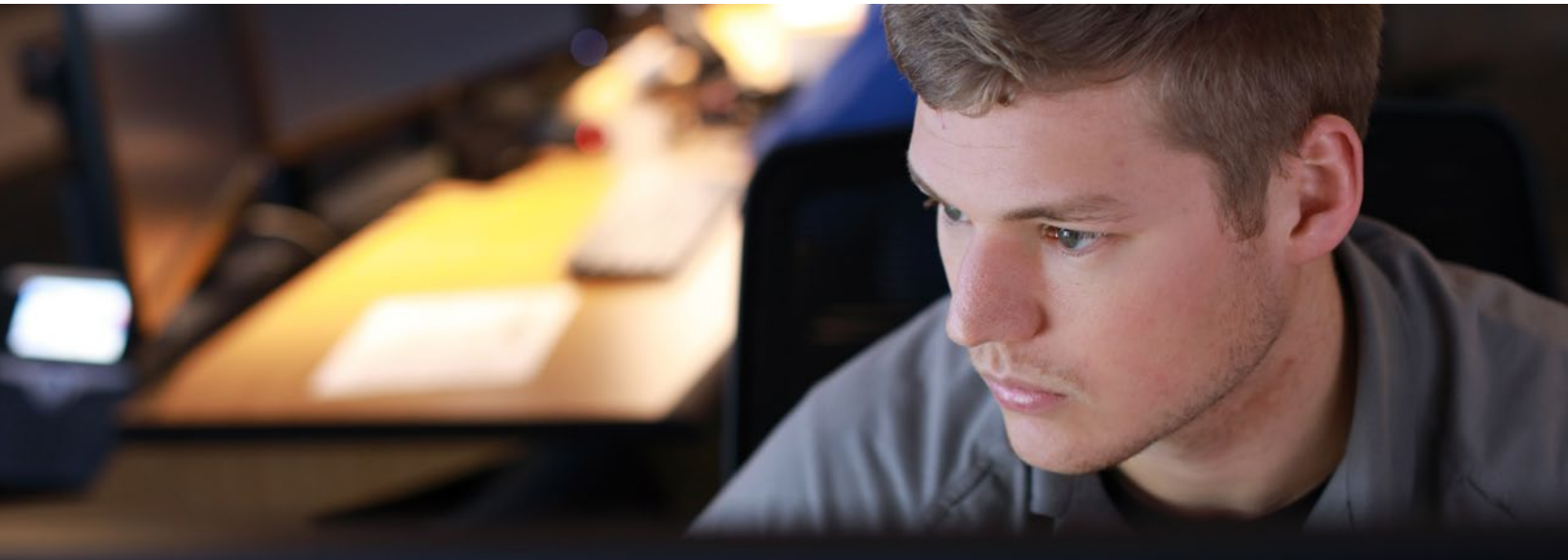
Since PSAP networks are relatively static in nature, honeypots are a highly effective tool in a defender's toolkit to detect or deflect attacks from the legitimate PSAP network. A honeypot works by mimicking a PSAP network to lure in attackers. Defenders are able to gain vital early warning about attacker operations targeting the PSAP by observing their tactics, techniques and procedures on the honeypot, which is not tied to the legitimate network.

A comprehensive solution should also include proactive threat hunting tools that incorporate automated and manual hunting with customized queries. These tools should support behavioral detection such as those defined in the MITRE ATT&CK Matrix, which is a knowledge base of cyberattack tactics and techniques used as a foundation for the development of specific threat models and methodologies in the private sector, government and cybersecurity community.[28] This hunting framework adopts an "assume the breach" mentality to proactively pursue an adversary within the environment that traditional security solutions cannot detect. In other words, solutions need to be deployed that address all the steps an attacker takes from their initial reconnaissance to the execution of malware or data exfiltration, also referred to as the cyber kill chain.

LEARNING THE CYBERSECURITY LESSONS OF 2019

The complexity of public safety, along with its mission to protect citizens and infrastructure, creates unique challenges in developing and implementing a risk management approach. Public safety organizations must understand that they face threats from a wide range of cyber attacks across all of their communication and collaboration systems, the personal devices that their users employ and even their users themselves.

Cybercrime is an industry with significant technical expertise, extensive funding and a target-rich environment. We hope that this report provides a baseline of knowledge, helping public safety organizations fight back with a proactive, holistic cybersecurity approach steeped in real world insights. By heeding the lessons from this year's report, we are confident public safety agencies can emerge more secure in 2020 and beyond.



For more information about our Cybersecurity Services, contact your Motorola Solutions representative or visit **motorolasolutions.com/cybersecurity**

SOURCES

1 https://go.malwarebytes.com/q1-2019-ctnt-report-lp.html
2 https://content.govdelivery.com/attachments/USDHSCIKR/2019/06/04/file_attachments/1224512/TLPWHITE_UNCLASSIFIED_20190530_State%20Local%20Gov%20Ransomware.pdf
3 https://www.vircom.com/blog/biggest-cyber-attacks-of-2017/
4 https://www.csoonline.com/article/3227906/ransomware/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html
5 https://www.nytimes.com/2019/08/22/us/ransomware-attacks-hacking.html
6 https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/
7 https://www.fcc.gov/document/fcc-releases-tfopa-final-report
8 https://www.cisa.gov/news/2019/12/06/new-self-assessment-tool-helps-identify-next-generation-911-readiness
9 https://www.timesunion.com/news/article/Albany-police-can-t-access-scheduling-system-13730578.php
10 https://chypernews.com/robbinhood-ransomware-attack-brings-down-parts-of-the-city-of-baltimore-computer-network/167/
11 https://www.natlawreview.com/article/jackson-county-georgia-pays-hackers-400000-after-ransomware-attack
12 https://www.centralmaine.com/2019/04/18/city-of-augusta-hit-by-computer-virus-city-center-closed/
13 https://www.tcpalm.com/story/news/local/martin-county/2019/04/22/city-halls-ransomware-attack-may-linked-phishing-email-scam-ryuk/3540067002/
14 https://www.wthitv.com/content/news/Vigo-County-911-operators-remain-calm-during-a-malware-attack-524933591.html
15 https://www.zdnet.com/article/thousands-of-los-angeles-police-caught-up-in-data-breach-personal-records-stolen
16 https://www.enzoic.com/employee-cybersecurity-weak-link
17 https://www.arlnow.com/2019/07/10/arlington-investigating-cyber-attack-on-county-payroll-system/
18 https://www1.nyc.gov/site/fdny/news/fa5719/fdny-sends-notices-10-000-individuals-concerning-possible-data-breach#/0
19 https://www.theverge.com/2019/8/14/20805194/suprema-biostar-2-security-system-hack-breach-biometric-info-personal-data
20 https://www.nytimes.com/2019/06/19/us/florida-riviera-beach-hacking-ransom.html
21 https://enterprise.verizon.com/resources/reports/dbir/
22 https://www.fcc.gov/document/fcc-releases-tfopa-final-report
23 https://securityintelligence.com/posts/the-decline-of-hacktivism-attacks-drop-95-percent-since-2015
24 https://www.databreaches.net/italian-trade-union-of-state-police-officers-hacked-defaced-by-the-anonymous-anarchist-agency
25 https://digitalguardian.com/blog/ransomware-protection-attacks
26 https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf
27 https://www.knowbe4.com/phishing
28 https://attack.mitre.org/

MOTOROLA SOLUTIONS

Motorola Solutions, Inc. 500 West Monroe Street, Chicago, Il 60661 U.S.A. **motorolasolutions.com**