CYBER THREATS TO PUBLIC SAFETY

MOTOROLA SOLUTIONS 2018 LANDSCAPE OF CYBER THREATS TO PUBLIC SAFETY

This report was commissioned by Motorola Solutions, Inc. and executed by LookingGlass Cyber Solutions.

LOOKINGGLASS

MOTOROLA SOLUTIONS

For 90 years Motorola Solutions has been committed to supporting those who deliver public safety. From the first radios used by police to modern computer-aided dispatch, video collection, analytics and repository solutions to the future capabilities we are working on to help our customers keep their eyes up and hands free, we are committed to helping improve their ability to do their mission and protect them while they do it.

Arguably, the greatest risks to the public safety mission today are those emanating from cyber. However, for one to be able to manage their risks they need to be able to understand them free of fear, uncertainty and doubt. We hope that in this first Motorola Solutions Threat Intelligence report focused on cyber threats to public safety we are able to take a step in that direction, reducing the uncertainty and providing context as to what public safety is facing. In doing this we seek to better partner with the agencies we support, helping them to better manage their risks and protect their mission. Our mission remains to help people be their best in the moments that matter. We know you can't be your best in those moments if malicious actors are denying you the ability to use the technology you need. We seek to ensure that does not happen.

Troy Mattern
VP for Products and Services Cybersecurity at Motorola Solutions

MOTOROLA SOLUTIONS 2018 LANDSCAPE OF CYBER THREATS TO PUBLIC SAFETY

EXECUTIVE SUMMARY

As first responders increasingly rely on computer and communication systems that support all aspects of emergency management, cyber threats to first responders have become a persistent concern.

Failure of these systems, whether accidental or because of malicious action, can have severe implications for emergency management. With such expanding use of internet-connected technologies, first responders are continuously targeted by malicious cyber actors through the deployment of ransomware and proliferation of phishing emails, social engineering and doxing campaigns, launch of denial of service attacks and other techniques and tactics. The best practice to mitigate these types of attacks is investing in a cybersecurity risk posture that enhances physical, technical and administrative controls (commonly referred to as defense in depth). Further, cyber threat awareness and education programs are becoming a critical step in safeguarding public safety.

RANSOMWARE

LAW ENFORCEMENT

Extortion is a cyber crime staple, and no malware does a better job at this than ransomware which perseveres as a go-to weapon in hostile actors' toolboxes. Ransomware has long been a prevalent weapon of choice for enterprising cyber criminals, with damages reaching $5 billion in 2017.

It has become the most prevalent malicious software in all sectors, found in 39% of all malware-related breaches, twice as much as 2017. As such, ransomware has successfully been deployed against a variety of industries, including public safety entities.

Since at least 2015, first responders and law enforcement agencies have been victims to an increasingly complex cyber environment, as cyber criminals who frequently seek to exploit the so-called soft targets make public safety easy prey. While disruptive and damaging in nature on a local scale, ransomware has the potential to lead to larger scale damage. Just as a heating and cooling vendor served as the backdoor to Target's breach, first responders and law enforcement agencies may serve as a backdoor to broader cyber vulnerabilities affecting U.S. national security. For instance, in January 2017, police in Washington, DC discovered multiple disruptions to their surveillance cameras as a result of a ransomware attack that led to the compromise of 70% of the cameras across the city, eight days before the Presidential Inauguration.[i] The attack prevented officials from accessing the command and control center of the surveillance system and crippled the city's ability to monitor public spaces. Furthermore, the hijacked devices then spammed up to 180,000 email addresses with ransomware-laden messages and could have led to a more severe spread of ransomware.[ii] A Romanian woman pleaded guilty to the attack and admitted to conspiring to access 126 outdoor police cameras in a far-reaching extortion scheme. Prosecutors stated that the perpetrator was part of a group of hackers who aimed to take over the DC government computers and use them to email ransomware to 179,600 accounts in order to defraud the owners while hiding their own digital tracks.[iii] The hackers had also stolen banking credentials and account passwords and using police computers, could have committed fraud schemes with anonymity. While the timing of the attack appeared a coincidence, the U.S. prosecutors in the District said the case "was of the highest priority" because of its potential to disrupt security plans for the 2017 Presidential Inauguration.[iv]

Once ransomware enters a police department's system, the damage can be catastrophic if mitigation methods are not in place. Attacks cripple dispatch systems and patrol car computers, slow police response time, expose records and create an unsafe environment for officers in inmate holding areas. For instance, in 2017, the Cockrell Hill Police Department in Texas lost eight years' worth of video evidence and a cache of digital documents after hackers levied a ransomware attack.[v] According to one 2016 source, hackers have compromised departments in at least seven states since 2013. In 2015, five police and sheriff departments in Maine were locked out of their records management systems by hackers demanding ransom.[vi]

Despite having certain resources readily available — like assistance from FBI investigators — police departments are not faring any better than the private sector against ransomware and are frequently forced to pay ransom. In November 2013, officers at the Swansea Police department were forced to pay $750 after a piece of ransomware locked all their files. Investigations and other law enforcement activities were reportedly not impacted, but the department's ability to access files on their computers was limited for three days.[vii]

Some notable statistics regarding law enforcement and their paid ransoms can be seen in Figure 1.

Year	Police Department	Ransom Paid
2013	Swansea	USD 750
2014	City of Dickinson	USD 572
2015	Tewksbury	USD 500
	Lincoln County Sheriff's Office, Houlton, Boothbay Harbor, Damariscotta, Wiscasset and Waldoboro	USD 300-700
	Midlothian	USD 500
2016	Carroll County Sheriff's Office	USD 2,400
2018	Savannah	Number undisclosed

Figure 1. Recent Instances of Law Enforcement Paying Ransom Demands

In addition to the cost of ransom, ransomware attacks against first responders can cost tens of thousands of dollars and can shut down the police department's records management system used to create and store investigative reports, as evidenced by two cyber attacks on the Riverside Police Department in Ohio. In April 2018, Riverside Police Department's access to Ohio's statewide system of law enforcement databases was suspended following multiple ransomware attacks on the city's computers.[viii] The department lost access to the Ohio Law Enforcement Gateway in order to shield the system from damage and protect confidential information from exposure.[ix] The gateway holds police reports and allows officers to quickly search a large variety of databases from police departments and other sources across the state and nation. The second infection took place in May 2018. Due to officials' improved security practices like data backup, the second ransomware attack encrypted data pertinent to the last eight hours of work and the department fully recovered.[x] However, while having backups was instrumental to a shorter downtime, the department's security safeguards were still not adequate to secure against the second attack.

Several months after the last attack, investigators have reported that the two cyber attacks on Riverside's police department servers have crippled law enforcement in ways previously unknown to the public, including the possibility Riverside could permanently lose access to one of the state's police computer networks if attacked again.[xi] As a result of the two attacks, the investigation found police not only lost the ability to access and print past reports but at one point lost the ability to make digital reports altogether. According to the recently surfaced information, the entire digital front of the department went offline after the attack. Losing the gateway forced officers to handwrite reports and type incident narratives into Microsoft Word so that they could be scanned into the system once restored. At the time of this report, access to the gateway, which serves as a backup reporting system and is used for investigations, has not yet been restored hampering the effectiveness of the police department.

More often than not, however, first responders, like private enterprises, do not treat cyber risk as an enterprise-wide threat, but rather attribute it to under-funded and poorly equipped IT departments and vendors. The actual losses suffered by victims of ransomware are much higher due to the disruption of productivity, and when government entities and police departments are increasingly being targeted, public safety becomes an issue. Small-sized law enforcement entities are most at risk of ransomware, as they often have older systems in place and frequently lack budget necessary to implement proper cybersecurity guidelines and improve employee cyber safety awareness. This is especially worrisome given that local law enforcement computer systems can contain plenty of vital — sometimes even deeply personal — information, ranging from rape and other violent crime reports to 9-1-1 call records, case files of ongoing investigations, personnel records and access to law enforcement databases like the National Crime Information Center, which contains criminal case information on federal, state and local investigations.[xii]

PUBLIC SAFETY ANSWERING POINTS / 9-1-1 CALL CENTERS

The potential deployment of ransomware against Public Safety Answering Points (PSAP) and 9-1-1 systems represents a serious threat that can impact the citizens it is intended to serve.

In certain instances, the emergency system may still run on obsolete equipment, some of it dating back to the 1980s. Due to the importance of these systems and their availability, ransomware perpetrators may increasingly target these systems due to the critical role PSAPs play in routing critical communications to first responders.

This is corroborated by the 184 cyber attacks on public safety agencies and local governments in the past 24 months (April 2016 - April 2018). Of the 184 incidents, 9-1-1 centers have been directly or indirectly attacked 42 times.[xiii] While in many instances the origins of the attack and ransomware propagation vector are not reported, frequently it is the human error that enables costly ransomware attacks. Human error is by far the biggest reason why cybercriminals are able to breach corporate data systems and remains a significant vector in ransomware attacks, according to a 2018 IBM report.[xiv] For instance, in March 2018, Baltimore's 9-1-1 systems suffered a ransomware attack that made the city's emergency systems unavailable for approximately 17 hours.[xv] Security researchers state that the attack was made possible after a city IT team troubleshooting a separate communications issue with the server inadvertently changed a firewall and left a port open for approximately 24 hours. Hackers who were likely running automated scans of networks looking for such vulnerabilities found the open port and gained access.[xvi] The attack came at a

particularly bad time, as thousands of protesters from the area gathered Saturday in Baltimore and in nearby Washington, DC as part of the nationwide march against gun violence.

In 2016, similar ransomware attacks impacted 9-1-1 systems in Henry County, Tennessee shutting down the 9-1-1 center's computerized dispatch system for three days.[xxii] Officers were forced to utilize pen and paper to track emergency calls for three days rather than paying more than $2,000 in bitcoin to have the system turned back on. Government employees in Licking County, OH reverted to pen and paper after a ransomware attack impacted the county's government offices, including its 9-1-1 dispatch in February 2017.[xxiii] The county turned off all phones and computers on its government network in order to stop the spread of malware that had been locking down infected PCs and demanding payments. Rather than pay the ransom, Licking County worked to rebuild its system, a move that officials say was possible because of good backups and the quick system shut-off.[xxv] While most county operations were slowed for nearly two weeks, after the initial recovery, most vital systems were back online within a few days.[xxvi] Similarly, in September 2017, a ransomware attack impacted Butler County's first responder 9-1-1 system that included mapping and GPS.[xxvii] Dispatchers were forced to relay info via walkie-talkies and notepads.

MUNICIPALITIES

Ransomware attacks have the ability to disrupt public services to entire cities and municipalities.

Nearly 40% of CIOs and CISOs in charge of protecting public sector IT infrastructure say the frequency of the attacks is increasing, with over a quarter reporting their networks are experiencing cybersecurity incidents on an hourly basis.[xvii] Similarly, according to an information systems research firm, these kinds of public sector attacks are increasing at a faster pace than those targeting the private sector, and frequently city officials are often unprepared to deal with the consequences.[xviii] The research firm estimates that based on a sample of 300-400 public-sector entities, 38% of the public entities will suffer a ransomware attack this year, up from 31% last year and 13% in 2016.[xix]

The increase is also likely contributed to the fact that cities like Leeds are paying the ransom rather than making efforts to rebuild the affected systems as evidenced by Figure 2.[xx] Furthermore, the cost of the ransom itself is further compounded by the cost of recovery efforts and cybersecurity improvements. For instance, after a ransomware attack Madison County, Indiana will spend more than $200,000 to recover, which includes paying the ransom and securing additional IT contracts to help prevent future attacks and improve recovery and continuance efforts, including off-site data storage, a backup court system and protections against future infections.[xxi]

Year	Police Department	Ransom Paid
2018	Wasaga Beach, ON	USD 35,000
	Midland, ON	Amount Undisclosed
	Shiawassee County, MI	USD 50,000
	Leeds, AL	Ransom demanded USD 12,000 in bitcoin, paid USD 8,000 after negotiating down
	Leominster, MA	USD 10,000
2017	Bingham, ID	USD 3,500
	Brownsburg County, IL	USD 1,000
2016	Madison County, IN	USD 21,000
2015	Chicago, IL	USD 500

Figure 2. Recent Instances of Municipalities Paying Ransom Demands

Overall, the resource-scarcity problem that prevents many small counties from proactively fortifying their cybersecurity — a lack of funds to outsource threat monitoring and recovery and a depleted talent base for knowledgeable IT professionals — is compounded by the absence of a federal database local governments can report cyber attacks to. A report released in 2018 by the University of Maryland, Baltimore County (UMBC) and the International City/County Management Association (ICMA) detailing the cybersecurity practices of local governments found that the agencies struggled to fund and staff their cybersecurity programs.[xxiv]

CITY OF ATLANTA

A notable example of a crippling effect a ransomware attack can have on a city and its critical municipal services is the 2018 Atlanta cyber attack acknowledged by the city on March 22, 2018, in which hackers demanded $51,000 worth of bitcoin for the release of encrypted city data.

This attack was notable as it was the largest successful breach of security for a major American city by ransomware, potentially affecting up to 6 million people.

The attack caused widespread city-run program outages and raised fears about the security of financial and personal data belonging to government workers and residents who have used online services provided by the City of Atlanta. Among the services impacted by the attack were the Atlanta Police Department records system (the Department lost years of dashcam footage as a result), warrant issuances, water service requests, new inmate processing, court fee payments and other online bill-pay programs across a range of city departments.[xxx] Specifically, attackers took down at least a third of the city's 424 software programs, about 30% of which were considered "mission critical."

Security researchers report that the ransomware used in the attack comes from the SamSam family, which has been operating and executing similar attacks since at least 2015.[xxviii] Unlike most other forms of high-profile ransomware, SamSam targets sectors that cannot afford downtime and have the financial resources to pay the ransom as security researchers estimate that the ransomware has earned its creator(s) more than $5.9 million since late 2015. The majority of the known victims (74%) are based in the United States, although other regions known to have suffered attacks include Canada, the UK and the Middle East.[xxix] Unlike most other ransomware, SamSam encrypts not only document files, images and other personal or work data, but also configuration and data files required to run applications (e.g., Microsoft Office). Victims whose backup strategy only protects the user's documents and files will not be able to recover a machine without reimaging it.

Historically, SamSam attacked organizations in the Healthcare, Government and Education sectors (Figure 3).[xxxi] However, security researchers have found that these three sectors account for fewer than half of the total number of organizations that have been victims of SamSam and it is the private sector who have suffered the most (and disclosed the least).[xxxii] The reason that the Healthcare, Government and Education sectors dominate the headlines is that they have been, so far, more likely to go public about a SamSam attack than any companies in the private sector.

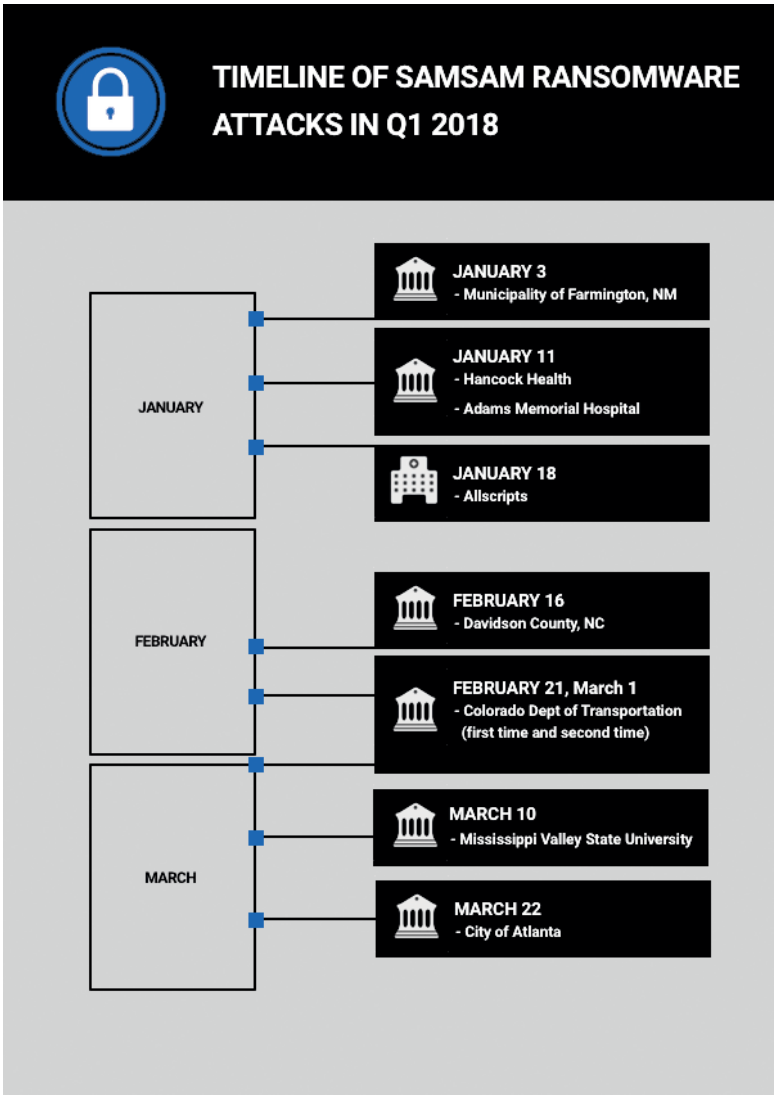


Figure 3. SamSam Ransomware Attacks in Q1 2018
(https://blog.barkly.com/atlanta-ransomware-attack-2018-samsam)

Although the city officials declared that there was little to no evidence that personal data had been compromised, later studies show that the breach was worse than initially estimated. In April, city officials said the investigation and system restore had cost $2.7 million — more than 50 times the original ransom demand. In addition, many legal documents and police dashcam video files were permanently deleted, although the police department was able to restore access to all its investigation files.[xxxiii]

In June, however, Reuters reported that Atlanta Information Management head Daphne Rackley requested another $9.5 million — putting the total at 250 times the hacker's demand.[xxxiv] By early August, a "confidential report" obtained by the Atlanta Constitution Journal and a local TV station estimated the total at $17 million — $6 million in existing contracts for security services and software upgrades and $11 million in associated potential costs, including new desktops, laptops, smartphones, and tablets. That is 333 times the original ransom demand.[xxxv]

HACKTIVISM

LAW ENFORCEMENT

When it comes to traditional hacktivist tactics, techniques and procedures targeting the public safety sector, as early as 2012, hackers gained access to the Salt Lake City Police Department and claimed to have acquired information on the identities of confidential informants and operations.[xxxvii]

This operation dubbed "OpPiggybank" was led by a now-defunct hacktivist collective CabinCr3w and targeted several other police departments nationwide in protest of police brutality, as well as several other topics including immigration.[xxxvi] Multiple police departments across the country were hacked, their websites defaced and usernames along with the passwords of police officers were leaked to the public. In one instance hackers claimed that the information was obtained "because of police being lazy when

it comes to data security" and allegedly included social security numbers, license plate numbers, dates of birth and addresses of residents. In addition, as part of the Operation, hackers also gained access to over 15,000 police warrants, hundreds of thousands of court summons, over 40,000 social security numbers of citizens, anonymous tips of criminal informants pertaining to narcotics, criminal informant information and thousands of online police reports attempting to prove the police lack of care for the security of the citizens. The hacktivists were subsequently arrested.[xxxviii]

Image 1. Message sent by Hacktivist Collective CabinCr3w

Some attacks on police departments by hacktivists have taken the form of Distributed Denial of Service (DDoS), which disrupts websites by channeling an overwhelming amount of web traffic in their direction. In August 2017, James Robinson in Akron, Ohio executed a DDoS attack against Akron Police Department, Ohio Department of Public Safety and the Department of Defense (DoD). Robinson's attack reportedly disrupted emergency operations at the Akron Police Department after he targeted multiple domains belonging to the department.[xxxix] Similarly, during the events in Ferguson, the St. Louis County Police Department's website was taken offline for several hours as a result of a DDoS attack in retaliation of the police shooting of Michael Brown and in support of ongoing physical protests.[xl] In addition, the Anonymous collective that took responsibility for the attacks published hours of alleged police dispatch tapes on Twitter and YouTube from the day Brown was shot. While some attacks were politically motivated, other police departments like San Jose[xli] and Newark[xliv] have been forced to shut down their websites after DDoS attacks that had no apparent trigger.[xli] [xlii]

In 2015, police in Arizona arrested a man who claimed responsibility for a DDoS attack on the city of Madison and Dane County's Internet resources following the fatal shooting of a 19-year-old man by a Madison, WI police officer. The attacker claimed affiliation with the Anonymous hacktivist collective and combined off-the-shelf DDoS tools with a series of publicity stunts that included attempts to present himself as part of an Anonymous hacking collective and demanded that a police officer is fired. In addition to disabling the City of Madison's website, the attack crippled the city's Internet-connected emergency communication system, causing delays and outages in the ability of emergency responders to connect to the 9-1-1 center and degraded the system used to automatically dispatch the closest unit to a medical, fire, or other emergency.[xliii] In the aftermath of the attack, the city's IT department began a review to see if any changes can further protect the city's network infrastructure and the results are still pending. In 2018, Randall Charles Tucker, aka "Bitcoin Baron," 23, of Apache Junction, Arizona, was sentenced to serve 20 months in prison by U.S. District Judge Douglas L. Rayes of the District of Arizona.[xliv]

PHISHING

LAW ENFORCEMENT

As of 2017, phishing has been identified by security researchers as the most common vector of compromise. In 2018, 70% of phishing attempts have become more targeted and selective.[xlv] For state and local governments, including state-level law enforcement organizations, spear phishing is the third most common vector of compromise.[xlvi]

Cyber attacks on municipal systems across the U.S. appear to be rising faster than those in the private sector, a threat exacerbated by the lack of adequate security awareness, educational programs, and overall lower cybersecurity posture, compared to other industries.[xlvii] [xlviii] [xlix] Through phishing and spear phishing attack vectors, malicious actors have successfully compromised the computer networks of local municipalities and first responders, including the examples we referenced under the ransomware section, disrupting vital municipal and emergency response operations in multiple cities.[l] [li] [lii] [liii]

For instance, in 2016, the Cockrell Hill Police Department fell victim to ransomware after a malicious attachment was opened by one of the staff members, which locked a police server containing documents, videos, and photos dating back to 2009. The attackers demanded roughly $4,000 worth of bitcoin to unlock the files, however, after consulting the FBI and the department's IT staff and taking into account the possibility that the files might not be unlocked even if the ransom was paid, the decision was made to wipe the server and delete all its contents.[liv]

Phishing attacks, as well as malware infections, frequently result from employee carelessness. While phishing incidents have been making headlines for years and education around avoiding opening suspicious attachments has been going on for considerably longer, sometimes a well-crafted and a believable piece of social engineering can trick the most cautious of users.

Such emails often intend to psychologically manipulate victims into performing a certain action or divulging confidential information and are often laden with malicious links and attachments. These emails often use clever tactics to get victims' attention and employ effective personalized messages. Consequently, even high-ranking targets within organizations, like top executives, can find themselves opening emails they thought were safe, thereby exposing their personal computers or those of their organizations to potential intrusion and hacking. For instance, a staff member at the Midlothian Police Department opened an infected email, inadvertently downloading malware, which then shut down the computer. In 2013, cyber criminals used CryptoLocker to infiltrate and lock more than 12,000 computers, including some belonging to Swansea Police Department in Massachusetts, which handed over $750 to unlock its files.[lv] Malware like CryptoLocker typically spreads via email attachments, typically a PDF that claims to be from a government department or delivery service and is especially damaging to police departments that do not back up important and sensitive files. Even though local police departments may have limited IT needs and restricted budgets, the Swansea incident highlights the need for proper staff training and a robust security awareness program to thwart attacks of these type. First responders, in general, should consider intensifying employee training to combat the increasing craftiness of phishers who are working harder to obtain personal details on targets in order to trap them in scams.[lvi]

DISTRIBUTED DENIAL-OF-SERVICE (DDOS)

PUBLIC SAFETY ANSWERING POINTS/9-1-1 CALL CENTERS

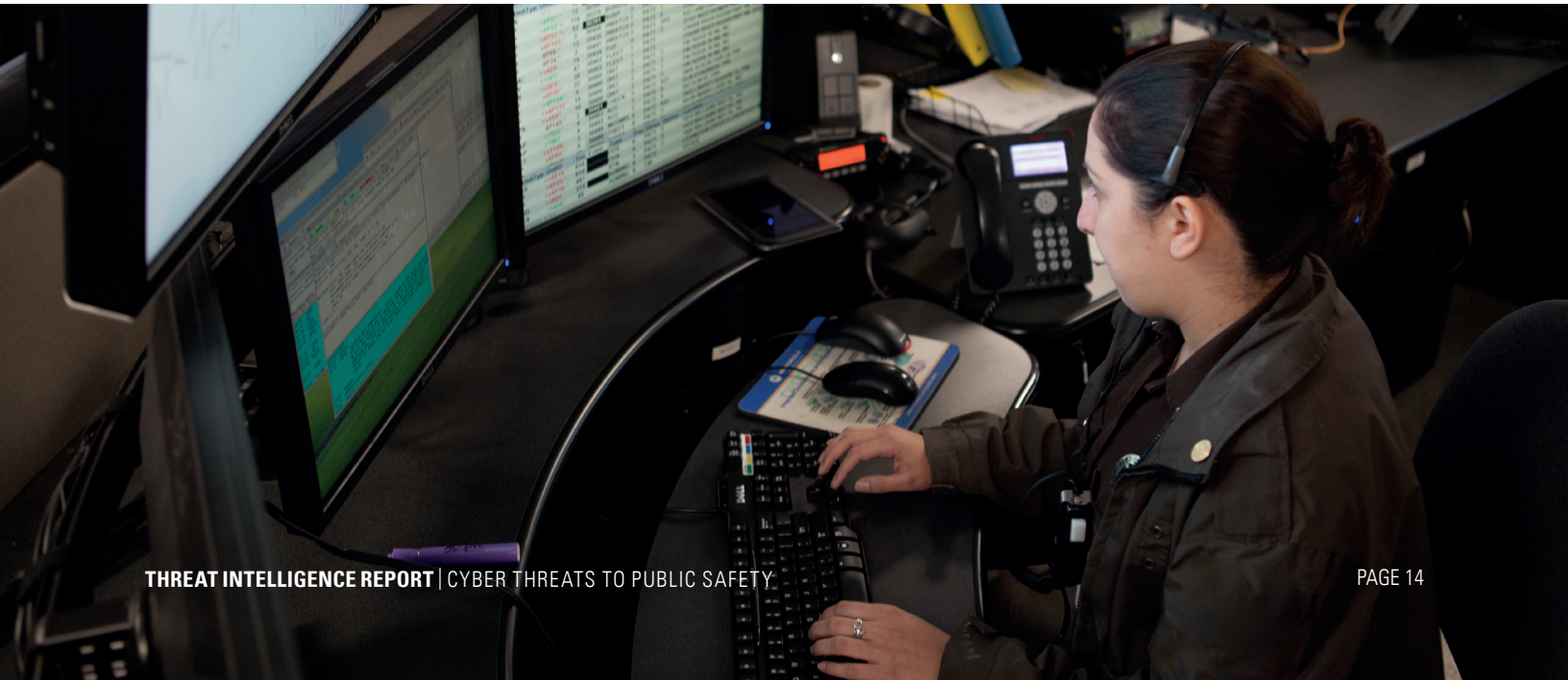
9-1-1 communication systems are a critical component of emergency response and preparedness, which make them an attractive target for criminal activity and specifically Distributed Denial-of-Service (DDoS) attacks in which multiple compromised computer systems attack a target and cause a denial of service for legitimate users of the targeted resource.

Similarly, Telephone Denial-of-Service (TDoS) attacks originate from or are directed towards a telephone system with the intent of bringing down the targeted system. These attacks commonly focus on commercial businesses and may often include ransom requests. In reality, these attacks can affect anyone, including the nation's 9-1-1 infrastructure. The flood of incoming messages, connection requests or phone calls to the target system overwhelms its capacity to process further connections and forces it to slow down or even crash and shut down, thereby denying service to legitimate users or systems.[lvii]

Such attacks against US 9-1-1 emergency operators are relatively easy to perform, as shown in the 2016 TDoS attack on Arizona's 9-1-1 emergency call system. The attack was the result of a simple code written by an 18-year-old student and posted on Twitter and demonstrated the ability of an individual, or small group, to impact 9-1-1 networks, systems, and facilities, even in their current legacy state. Since then, similar attacks affected the 9-1-1 emergency systems in Tennessee, Texas, and Ohio.

A DDoS attack launched from a mobile phone botnet is a significant threat to the availability of 9-1-1 services. In such attacks, frequent fraudulent calls made to 9-1-1 by a botnet comprised of many mobile phones, since many Public Safety Answer Points (PSAPs) work at full capacity and cannot handle this large volume of calls. Moreover, this call volume can disrupt the telephony network itself, preventing legitimate 9-1-1 calls from ever reaching a PSAP. In 2013, the U.S. Department of Homeland Security (DHS) and Federal Bureau of Investigation (FBI) issued an alert stating that various public services may be vulnerable to DDoS attacks.[lviii] This warning was triggered due to a DoS attack launched against the administrative line of a PSAP. In 2014, security researchers presented "Hacking 9-1-1" at DEF CON and provided a general description of attack vectors on 9-1-1 services broadly discussing line-cutting, cell phone jamming, and DDoS attacks.[lix]

Although no comprehensive vulnerability assessment of the nation's 9-1-1 emergency system has been conducted, industry experts approximate 80% of the country's Public Safety Answer Points (PSAPs) in the United States are vulnerable to DDoS attacks. Furthermore, the vulnerability is exacerbated by the second order effect of legitimate callers, frustrated by their emergency calls being dropped, repeatedly calling 9-1-1. In 2016, a group of academic researchers simulated statewide and nationwide DDoS attacks on the 9-1-1 emergency systems and concluded a 50% call-drop rate could be caused by infecting 6,000 and 200,000 mobile phones, respectively, with the proper malware.[lx] This number stands in contrast with the 500,000+ routers controlled by Russian Advanced Persistent Threat (APT) and discovered in May 2018, highlighting malicious actor's ability to compromise the necessary number of devices to mount an effective DDoS attack.



Overall, the DDoS/TDoS threat is evolving. Attacks have evolved to the point where, as with any DDoS attack, automation is almost always used with most automated attacks being fairly low volume and simple. In the case of TDoS, attackers do not need to generate many calls, because their victims are not entire organizations or sites. The attacker has the advantage because it is easy to generate the attack, the target usually has a small number of critical lines and the victim has very limited capability to deal with the attack.

The impact of DDoS/TDoS attacks on 9-1-1 emergency systems can range from mild to catastrophic, depending on the targeted system(s), the size and scale of the attack, the timing of the attack and the response of local and national citizens and governments. The longer the system is inaccessible due to an attack, the more dangerous it is for those in need of critical care, creating physical consequences to cyber attacks. In 2017, a 6-month-old Dallas boy died after his babysitter's 9-1-1 calls were delayed during an apparent DDoS attack.[lxi] It is also dangerous for public safety professionals, as paramedics cannot request police support and firefighters cannot call for mutual aid.

Additionally, a small-scale DDoS attack, such as the 2018 attack on Baltimore's 9-1-1 emergency system, can cause the 9-1-1 emergency system to become inoperable for tens of hours at a time.[lxii] The actual impact of this operational disruption, however, can increase in orders of magnitude during times of heightened threat levels, such as natural disasters and public unrest. The impact can also vary depending on local and national emergency response assets, protocols and effectiveness. Such events could erode the public's trust in their local and national governments' ability to maintain order and safety, further challenging our efforts to accurately estimate the impact of DDoS attacks on first responders.

While the Department of Homeland Security has allocated millions of dollars since 2017 to find a solution that could protect the 9-1-1 emergency systems from DDoS attacks, malicious actors are also evolving. In September 2018, security researchers revealed that the average scale of DDoS attacks has increased by 500% in the past year alone, outpacing the DHS' efforts to implement effective protection measures.[lxiii] Amplifying the threat, nation-state threat actors continue to demonstrate willingness and capability to conduct malicious cyber campaigns against U.S. critical infrastructure during periods of heightened political tension.

PERPETRATOR OVERVIEW

Over the years, cyber attacks against first responders have become more sophisticated, targeted, and frequent. Threat actors behind ransomware and phishing improve their capabilities by developing new attack methods and evolving malware strains.

Security researchers indicate that since 2017, the number of existing malware families increased by 25% and unique malware variants grew 19%, which not only indicates a dramatic growth in volume but in the evolution of malware itself. As seen in the case of SamSam, ransomware now has the ability to encrypt not only data on a network but also backup files and data – rendering this common security strategy obsolete. Moreover, traditional threat detection tools and signature-based antivirus programs are frequently unable to keep pace with the volume, variety, and velocity of today's malware.

Modern phishing emails have become incredibly advanced and very often are difficult to spot. As organizations do a better job of educating users not to click on suspicious links, threat actors are shifting and improving their tactics, techniques, and procedures. Instead of a link, they use a document attachment that might be a PDF, Microsoft Word, or other common file types.[lxiv] Some hackers also use official-looking company logos and terse language in order to trick people into clicking on an attachment. In some instances, attackers follow up fake emails with calls, urging the victims to open malicious attachments. Frequently, malicious emails are not only tailored to the specific organization, they often are sent directly to the individual who would normally field that kind of request, indicating that threat actors engage in reconnaissance and research of their targets for maximum impact.[lxv]

Furthermore, with the evolution of the attacks and their seemingly increased profitability, barriers to entry into criminal underground have been lowered. Increasingly security researchers observe the "as-a-service" business model adopted by cyber criminals that enable any willing buyer to get involved in criminal endeavors without needing to be technically proficient. As a result, a wide range of malicious tools used to carry out attacks are now available to wider audiences, including tools needed to launch ransomware and DDoS attacks. Moreover, as this practice has grown widespread, criminals are taking a more aggressive approach in marketing their offerings. While previously such services were only available in closed-off environments and the dark web, attackers are now being more brazen with promoting their products out in the open using mainstream marketing tactics, professionally produced video advertisements and heavily designed websites. Such aggressive marketing only further highlights how widespread this approach is becoming. As the more high-profile ransomware attacks happen, the more likely it is for the would-be attackers with limited skills to take advantage of the offerings, while malware authors continue to share their products for the most potential income.

Since 2017

25%

existing malware families increase

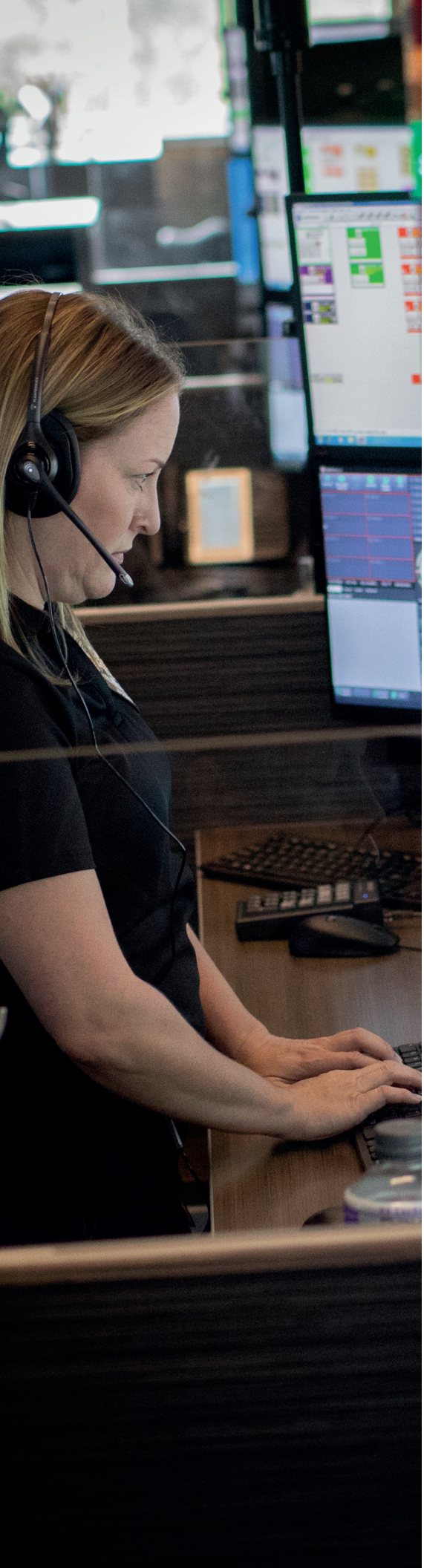
19%

unique malware variant growth

BEST PRACTICES

Phishing and ransomware are very serious threats that can cause enormous damage to an organization's finances, data assets and reputation. They can cause vast disruptions and have a national security impact.

However, there are steps that first responders can take to address these threats so that the chances of infection – and the consequences that will arise from it – can be mitigated. First responders 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 users themselves. Cyber crime is an industry with significant technical expertise, extensive funding, and a rich target environment and therefore it is essential to understand the risks that first responders face.



TRAIN YOUR USERS AND TEST THEIR KNOWLEDGE

Employees are part of an organization's attack surface and ensuring they have the know-how to defend themselves and the organization against threats is a critical part of a comprehensive security awareness program, especially as attackers often target organizations through employees by a variety of phishing attacks with embedded malware. [lxvi]

As a preventive effort, organizations should conduct regular trainings to help employees avoid common malware pitfalls and implement an overall policy which mandates that employees submit any suspicious-looking emails to IT staff before opening attachments. It is essential to remind employees to avoid clicking on unknown links or open unsolicited email attachments. In addition, security researchers recommend collecting examples of the types of phishing emails users are likely to see and educate them on what to watch out for.[lxvii] To improve workforce awareness, the internal security team may test the training of an organization's workforce with simulated phishing emails. For instance, after experiencing a ransomware attack in 2014, the Tewksbury police department holds staff meetings where examples of phishing emails and other potential sources of infection are shown.[lxviii] The department also sends out staff-wide alerts any time something suspicious is discovered. Police departments should identify staff member who will ensure the agency's network is operating effectively, efficiently, and safely.

A third party may be used to assist with security awareness training services if internal security resources and expertise are not adequate or available. Regardless of whether outside assistance is leveraged, an organization's leaders should understand what goes into building a security awareness training program, get involved and offer feedback throughout the process.[lxix]

If defenses fail and networks become compromised by a ransomware attack, most experts say to never pay the ransom because there are no guarantees your files will be returned or the malware will even be removed.[lxx] In the event your network is impacted by ransomware or other types of compromises, employers should immediately notify local police, FBI and their insurance company. Once the authorities are involved, employers should follow the advice they receive from the experts.[lxxi]

MONITOR YOUR NETWORK

Diligent network monitoring by analyzing logs, clearing out alerts and processing potential threat feeds is an essential prevention method. If the infection or malicious activity is detected quickly and the workstation is disabled immediately, the data can typically be recovered within 24 hours. Organizations should constantly update the operating systems and other software on their systems with the latest patches, as they serve as a common entry point for malware. Patching commonly exploited third-party software such as Java, Flash and Adobe will significantly reduce the likelihood of these attacks from being successful in the first place. Every organization should have a standardized and well-versed patching process, which includes testing the patches prior to deploying them. Additionally, it is best to have a multi-faceted security solution that employs additional protective technologies such as heuristics, firewalls, behavioral-based threat prevention, etc.

MAINTAIN ROBUST BACKUP AND RECOVERY

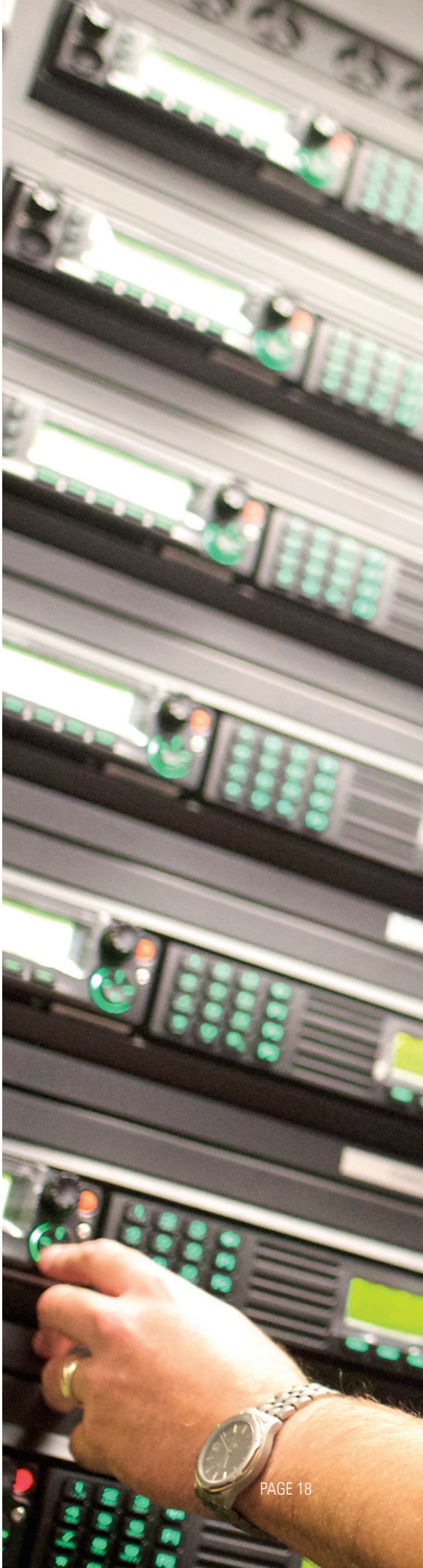
One of the most important defenses against ransomware is to have a robust backup strategy in place that includes off-site storage and regular testing of images and other saved data to ensure their integrity.[lxxii] If ransomware manages to install and execute on a machine, a recent, comprehensive backup is an essential remedy. Rather than attempting to remove the malware and attempt to decrypt affected files, the infected machine can be wiped and restored from the clean backup with minimal impact on operations.[lxxiii] Backups should be performed regularly and stored on media that is not connected to the machine, as new ransomware variants like WannaCrypt0r and CryptoLocker are known to destroy all shadow copies and restore point data. 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 examples in this report.

HAVE AN INCIDENT RESPONSE PLAN

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 data and normal operations. 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 can get 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.

DEVELOP ADEQUATE POLICIES

A step for any organization should be 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.[lxxiv] 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.[lxxv]



APPENDIX A: INDUSTRY STANDARDS FOR SYSTEM SECURITY

Department of Justice:
https://www.justice.gov/criminal-ccips/file/872771/download

Department of Homeland Security:
https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_0.pdf

Federal Bureau of Investigation:
https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-ceos.pdf/view

---

SOURCES:

[i] https://www.bbc.com/news/world-europe-42511133

[ii] https://www.theregister.co.uk/2018/09/21/cctv_ransomware_trump_washington_dc/

[iii] https://www.bbc.com/news/world-europe-42511133

[iv] https://www.bbc.com/news/world-europe-42511133

[v] https://www.wfaa.com/article/news/cockrell-hill-police-lose-years-worth-of-evidence-in-ransom-hacking/392673232

[vi] https://www.nbcnews.com/news/us-news/ransomware-hackers-blackmail-u-s-police-departments-n561746

[vii] https://www.bostonglobe.com/metro/2013/11/19/swansea-police-pay-ransom-open-files-locked-hackers/7bOdi8i7foNkTmdnokMAkP/story.html

[viii] https://www.mydaytondailynews.com/news/local/riverside-police-lost-access-crime-fighting-tool-cyberattack/eaFlb0FunQ88rRNXng5IGP/

[ix] http://www.govtech.com/security/Multiple-Ransomware-Attacks-Cut-Off-Police-Access-to-Crime-Database-in-Riverside-Ohio.html

[x] https://www.bleepingcomputer.com/news/security/police-dept-loses-10-months-of-work-to-ransomware-gets-infected-a-second-time/

[xi] https://www.mydaytondailynews.com/news/crime--law/investigation-ransomware-costs-riverside-thousands-hinders-access-police-systems/WpSa08YrLMRdgL0Uue8g5L/

[xii] https://www.nbcnews.com/news/us-news/ransomware-hackers-blackmail-u-s-police-departments-n561746

[xiii] https://www.nbcnews.com/news/us-news/hackers-have-taken-down-dozens-911-centers-why-it-so-n862206

[xiv] https://www.wraltechwire.com/2018/04/05/ibm-human-error-is-biggest-reason-for-data-breaches-as-ransomware-attacks-surge/

[xv] https://www.baltimoresun.com/news/maryland/crime/bs-md-ci-hack-folo-20180328-story.html

[xvi] https://www.baltimoresun.com/news/maryland/crime/bs-md-ci-hack-folo-20180328-story.html

[xvii] https://blog.barkly.com/local-government-cybersecurity-2018-ransomware-attacks

[xviii] https://blog.barkly.com/local-government-cybersecurity-2018-ransomware-attacks

[xix] https://blog.barkly.com/local-government-cybersecurity-2018-ransomware-attacks

[xx] https://blog.barkly.com/local-government-cybersecurity-2018-ransomware-attacks

[xxi] https://www.csoonline.com/article/3148274/security/after-attack-indiana-county-will-spend-220000-on-ransomware-recovery.html

[xxii] https://www.bleepingcomputer.com/news/security/police-dept-loses-10-months-of-work-to-ransomware-gets-infected-a-second-time/

[xxiii] https://www.dispatch.com/news/20170207/ransomware-cyberattack-keeps-licking-county-vigilant

[xxiv] https://ebiquity.umbc.edu/blogger/2018/04/14/umbc-icma-survey-of-local-government-cybersecurity-practices/

[xxv] https://www.dispatch.com/news/20170207/ransomware-cyberattack-keeps-licking-county-vigilant

[xxvi] http://www.govtech.com/security/GT-OctoberNovember-2017-The-Case-for-Ransomware-Insurance.html

Center for Internet Security: https://www.cisecurity.org/controls/

National Emergency Number Association: https://cdn.ymaws.com/www.nena.org/resource/resmgr/Standards/NENA_04-503.1_Network_ System.pdf

[xxvii] https://www.kansas.com/news/local/article173254491.html

[xxviii] https://www.secureworks.com/research/samsam-ransomware-campaigns

[xxix] https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/SamSam-The-Almost-Six-Million-Dollar-Ransomware.pdf

[xxx] https://www.bleepingcomputer.com/news/security/years-of-police-dashcam-video-lost-in-atlanta-ransomware-incident/

[xxxi] https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/SamSam-The-Almost-Six-Million-Dollar-Ransomware.pdf

[xxxii] https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/SamSam-The-Almost-Six-Million-Dollar-Ransomware.pdf

[xxxiii] https://siliconangle.com/2018/06/07/city-atlanta-ransomware-attack-far-worse-initially-thought/

[xxxiv] https://www.synopsys.com/blogs/software-security/samsam-ransomware/

[xxxv] https://securityboulevard.com/2018/09/samsam-ransomware-keeps-striking-victims-still-unprepared/

[xxxvi] https://www.databreaches.net/salt-lake-city-police-department-hacked-in-oppiggybank/

[xxxvii] https://www.databreaches.net/salt-lake-city-police-department-hacked-in-oppiggybank/

[xxxviii] https://www.dailydot.com/news/anonymous-hacker-kahuna-sentence/

[xxxix] https://www.news5cleveland.com/news/local-news/akron-canton-news/man-charged-in-federal-court-for-ddos-attack-on-akron-police-department

[xl] https://www.cnet.com/news/st-louis-police-website-suffers-ddos-attack/

[xli] https://mashable.com/2015/11/11/san-jose-police-sites-hacked/#mu.JuL8MMsq2

[xlii] https://www.nj.com/essex/index.ssf/2016/04/cyber_attack_shuts_down_newark_police_computer_sys.html

[xliii] https://www.justice.gov/opa/pr/arizona-man-sentenced-prison-distributed-denial-service-attacks-against-emergency

[xliv] https://www.justice.gov/opa/pr/arizona-man-sentenced-prison-distributed-denial-service-attacks-against-emergency

[xlv] https://www.databreachtoday.com/phishing-attacks-get-more-targeted-a-11129

[xlvi] https://www.nascio.org/events/sponsors/vrc/Advanced%20Cyber%20Threats%20in%20State%20and%20%20Local%20Government.pdf

[xlvii] https://cdn2.hubspot.net/hubfs/533449/Images/SecurityScorecard%202017%20Govt%20Cybersecurity%20Report.pdf

[xlviii] https://blog.barkly.com/local-government-cybersecurity-2018-ransomware-attacks

[xlix] https://www.pymnts.com/news/security-and-risk/2018/38-percent-local-government-cyberattack

[l] https://www.businesswire.com/news/home/20171113005006/en/Arctic-Wolf-Networks-Protects-City-Sparks-Ransomware

[li] https://blog.barkly.com/local-government-cybersecurity-2018-ransomware-attacks

[lii] https://arcticwolf.com/blog/awn-cybersoc-makes-a-difference-in-protecting-first-responder-networks/

[liii] https://www.detroitnews.com/story/news/local/michigan/2018/06/02/mich-county-official-falls-phishing-scam-quits/35640183/

[liv] https://www.motherjones.com/politics/2017/02/police-department-loses-years-worth-evidence-ransomware-attack/

[lv] https://www.nbcnews.com/news/us-news/ransomware-hackers-blackmail-u-s-police-departments-n561746

[lvi] https://www.csoonline.com/article/2466621/data-protection/why-it-is-time-to-intensify-employee-education-on-phishing.html

[lvii] https://www.ntia.doc.gov/files/ntia/publications/forescout_response_to_rfc_on_botnets_and_other_automated_threats_final.pdf

[lviii] https://www.scribd.com/document/325062076/911-DDoS-Cyber-Security-Report

[lix] https://arxiv.org/pdf/1609.02353.pdf

[lx] https://www.bleepingcomputer.com/news/government/us-911-emergency-services-can-be-shut-down-by-ddos-attacks-from-mobile-botnets/

[lxi] https://www.nbcnews.com/news/us-news/hackers-have-taken-down-dozens-911-centers-why-it-so-n862206

[lxii] https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet

[lxiii] https://www.businesswire.com/news/home/20180912005347/en/Nexusguard-research-reveals-500-percent-increase-average

[lxiv] https://www.csoonline.com/article/3267544/ransomware/11-ways-ransomware-is-evolving.html

[lxv] https://www.wired.com/story/fin7-wild-inner-workings-billion-dollar-hacking-group/

[lxvi] https://www.rapid7.com/fundamentals/security-awareness-training/

[lxvii] https://manage.carbonite.com/blog/article/2016/08/protect-your-company-from-ransomware-six-best-practices-for-it-pros/

[lxviii] https://efficientgov.com/blog/2016/10/31/why-ransomware-threat-protect-police/

[lxix] https://www.rapid7.com/fundamentals/security-awareness-training/

[lxx] https://www.openonline.com/Resources/News/News-Article-View/cyber-lessons-for-employers-after-the-atlanta-ransomware-attack

[lxxi] https://www.openonline.com/Resources/News/News-Article-View/cyber-lessons-for-employers-after-the-atlanta-ransomware-attack

[lxxii] https://digitalguardian.com/blog/ransomware-protection-attacks

[lxxiii] https://www.swordshield.com/2018/08/locked-out-ransomware-prevention-incident-response/

[lxxiv] https://www.knowbe4.com/phishing

[lxxv] https://www.knowbe4.com/phishing

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

Disclaimer
LookingGlass and Motorola Solutions, Inc. have co-authored this report. Reference to products or services not provided by Motorola Solutions, Inc. is for information purposes only and constitutes neither an endorsement nor a recommendation. All information provided by LookingGlass is provided without warranty of any kind, either expressed or implied.

MOTOROLA SOLUTIONS

LOOKINGGLASS

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