GLOBAL CITY TEAMS CHALLENGE

SMART AND SECURE CITIES AND COMMUNITIES CHALLENGE (SC3)

A Starting Point for Smart Cities and Communities on Managing Ransomware Risk

A whitepaper from the Cybersecurity and Privacy Advisory Committee (CPAC) Public Working Group

May 2020

Purpose and Intended Audience

This whitepaper from the Cybersecurity and Privacy Advisory Committee (CPAC) of the Global City Teams Challenge (GCTC) program aims to raise awareness of the critical impact of ransomware in the context of Smart Cities and Communities, demonstrate the importance of these ransomware-related issues, and show how they are relevant to the missions and responsibilities of a broad range of stakeholders. This document provides a summary of the ransomware risk that Smart Cities and Communities currently face and identifies key, existing resources and references that can help Smart City stakeholders begin to prepare for and manage ransomware risk.

The primary audience for this document includes municipal policymakers, leaders, officials, and implementers actively involved in or considering the development of Smart City capabilities. Suppliers providing critical products and services should also be aware of the ransomware risk and collaborate with their customers to properly manage associated risks.

Disclaimer

This document is not intended to endorse any commercial products or services or any particular approach, implementation, or solution for addressing ransomware risk. Similarly, this document identifies numerous organizations and associated publications relevant to managing ransomware; these are intended to be examples and/or potential references and are not intended to be endorsements of specific organizations or their respective guidance, products, or services.

When addressing ransomware and other cybersecurity and privacy risks, Smart Cities and Communities should identify the risk management processes and associated products, services, and solutions that best fit your environment and requirements.

Executive Summary

Cities are becoming increasingly complex as the number and types of systems and data used in providing city services grow. Smart Cities and Communities aim to leverage ubiquitous connectivity, increased digitization and automation, and vast amounts of data to improve the delivery of city services and address key areas of concern (e.g., traffic congestion, public safety, energy efficiency and sustainability). Additionally, cities and communities are approaching these ambitions with generally limited resources, including financial and human resources.

This environment is characterized by technological complexity, delivery of critical city services, and constrained budgetary and technical resources, which makes cities perfect targets for cyber-attacks, including ransomware. Ransomware is defined as "[a] type of malware that blocks access to a system, device, or file until a ransom is paid" and is becoming an increasingly prevalent cybersecurity threat that has cyber-physical implications as well as potentially substantial monetary consequences – upwards of hundreds of thousands or tens of millions of dollars in some recent cases.

Cities that are affected by ransomware face the difficult decision of (a) seeking to restore data, systems, and services independently; (b) paying the ransom out-of-pocket without any assurance of data/system/service restoration; or (c) attempting to transfer response and recovery costs to a third-party, namely a cyber insurance provider – each of which entails short- and long-term risks and benefits. The risk that ransomware poses to aspiring Smart Cities and Communities warrants proactive attention to adequately understand the risk, prevent attacks, and be prepared to respond to and recover from attacks. Malicious actors will continue to seek out vulnerable cities, and those who are unprepared and most likely to pay will serve as particularly attractive targets

There are three broad categories of ransomware-related considerations particularly pertinent to Smart Cities and Communities when approaching the ransomware problem: (1) Planning and Process; (2) Technical Controls; and (3) Education and Training. The key considerations for Smart Cities and Communities are listed here and supplemented in the body of the document with lists of existing references for readers to seek further, more in-depth information and guidance. These considerations and the associated references are not intended to be comprehensive or exhaustive but provide a useful starting point.

Planning and Process Considerations

- Establish, exercise, and maintain cyber incident response, continuity of operations, and disaster recovery plans
- Consider and develop processes and policies for managing supply chain risk
- Carefully consider cyber insurance as a risk transfer component of broader cyber incident response, continuity of operations, and disaster recovery plans

Technical Control Considerations

- Select and implement technical controls to combat ransomware as dictated by the risk management process
- Recognize that Smart City environments are technologically diverse, which may limit which and how technical controls can be implemented
- Assess, authorize, and monitor implemented controls and associated policies to ensure proper operation in current risk environment

Education and Training Considerations

- Perform tailored cybersecurity and privacy awareness training and outreach for leadership, employees, partners, and constituents to help build a risk-aware environment and population
- Provide tailored training for those developing, deploying, operating, and maintaining Smart City systems
- Collaborate with and leverage expertise from partner governments, academia, and private sector organizations

Ransomware is one particularly harmful source of cybersecurity and privacy risk and needs to be managed in a manner consistent with overall cybersecurity and privacy risk management processes. The key considerations and references presented in this document can be used in conjunction with a developing cybersecurity and privacy risk management approach or to complement an existing one. While these considerations are especially germane to ransomware risk, they are similarly applicable to cybersecurity and privacy risks, in general.

1. What is Ransomware?

Everyday, there seems to be another occurrence of a ransomware attack on a large metropolitan area, a group of counties, a small city, a hospital, a school, or some other critical infrastructure organization. While there are many ransomware variants and a wide range of targeted organizations, ransomware attacks generally operate in a similar fashion with a clear and consistent objective – monetary gain.

The Center for Internet Security (CIS) defines ransomware as

> *[A] type of malware that blocks access to a system, device, or file until a ransom is paid. This is achieved when the ransomware encrypts files on the infected system (crypto ransomware), threatens to erase files (wiper ransomware), or blocks system access (locker ransomware) for the victim.*

Organizations affected by ransomware are ultimately forced to decide whether to pay the ransom – which does not guarantee restoration of access to all targeted data – or to independently attempt to rebuild systems and restore services.

2. What is Ransomware Risk?[1]

Ransomware attacks can be opportunistic or targeted and can be executed by both sophisticated (e.g., nation-state) and unsophisticated threat actors. The rise of ransomware-as-a-service offerings has made it possible for virtually anyone with malicious intent to participate in the increasingly popular digital extortion market.

While the threat of ransomware is clear, it may be even more evident that cities are vulnerable and attractive targets. In fact, research from Barracuda Networks, Inc. has indicated that, in 2019 to date, two-thirds of ransomware attacks in the U.S. have targeted state and local government organizations. Research from Coveware, Inc. suggests that "public sector victims paid an average ransom of $338,700, almost 10x the global enterprise average," highlighting the lucrativeness of state and local government targets.

The events, media headlines, and associated government publications below are just a small sample of major, highly-publicized ransomware events that have affected U.S. cities of all demographics and geographies.

The Baltimore, Maryland, ransomware event that started in May 2019 was characterized by the degradation of a broad range of city services, the high cost of

[1] Risk (R) is commonly considered a function of three factors: vulnerability (V), threat (T), and consequence (C). A common mathematical expression of risk is that risk is the product of vulnerability, threat, and consequence – or R = V x T x C.

incident response and disaster recovery, and the ineffectiveness and poor implementation of existing controls.[2]

- "Baltimore introduces 'manual workaround' for homebuying during ransomware attacks" (WYPR - May 22, 2019)
- "Baltimore's bill for ransomware: Over $18 million, so far" (Ars Technica - June 5, 2019)
- "Baltimore acknowledges for first time that data was destroyed in ransomware attack" (The Baltimore Sun - September 11, 2019)
- "Baltimore IT department uses 'mind-boggling,' outdated data storage method, audit finds" (The Baltimore Sun - September 27, 2019)

Commencing in August 2019, over 20 Texas communities were affected by ransomware. This event highlighted the ability of ransomware to have a negative impact across a distributed set of organizations and also raised questions about interdependencies and supply chain risks; however, this event also demonstrated the importance of coordinated incident response and ability of small organizations to manage ransomware risk.[3]

- "22 Texas towns hit with ransomware attack in 'new front' of cyberassault" (NPR - August 20, 2019)
- "How Texas used its disaster playbook after a huge ransomware attack" (StateScoop - October 15, 2019)
- "Managed service providers a growing target for ransomware attacks" (StateScoop - November 1, 2019)

Multiple small Florida cities were affected by ransomware during the summer of 2019. In several cases, the local governments relied on existing insurance policies to help bring services back online. This demonstrates the mission/business decision that small organizations may face as a result of ransomware; accordingly, this also alludes to the need for organizations to incorporate cybersecurity and privacy considerations into normal mission/business planning and decision-making processes.

- "Florida city pays hackers $600,000 after ransomware attack" (StateScoop - June 20, 2019)
- "Another Florida city is making a ransomware payment, worth nearly $500,000 this time" (CyberScoop - June 26, 2019)

The March 2018 Atlanta, Georgia, ransomware event was notable due to the size of the municipality affected, the scope of services impacted, and the time and cost

[2] More information from the City of Baltimore government is available at https://mayor.baltimorecity.gov/ransomware-frequently-asked-questions.
[3] More information from the State of Texas government is available at https://dir.texas.gov/View-About-DIR/Information-Security/Pages/Content.aspx?id=155.

required to restore city functions. Given the continuing ransomware problem around the globe, it is clear that practices and processes have not matured sufficiently to manage the ransomware risk.

- "Confidential Report: Atlanta's cyber attack could cost taxpayers $17 million" (The Atlanta Journal-Constitution - August 1, 2018)
- "Atlanta U.S. Attorney charges Iranian nationals for City of Atlanta ransomware attack" (United States Department of Justice - December 5, 2018)
- "Atlanta CIO worries city employees will forget ransomware attack" (StateScoop - October 24, 2019)

These events and headlines begin to demonstrate the criticality of the ransomware issue, the range of threat actors, and the potential consequences of an attack.

Recent Ransomware Attacks in the United States

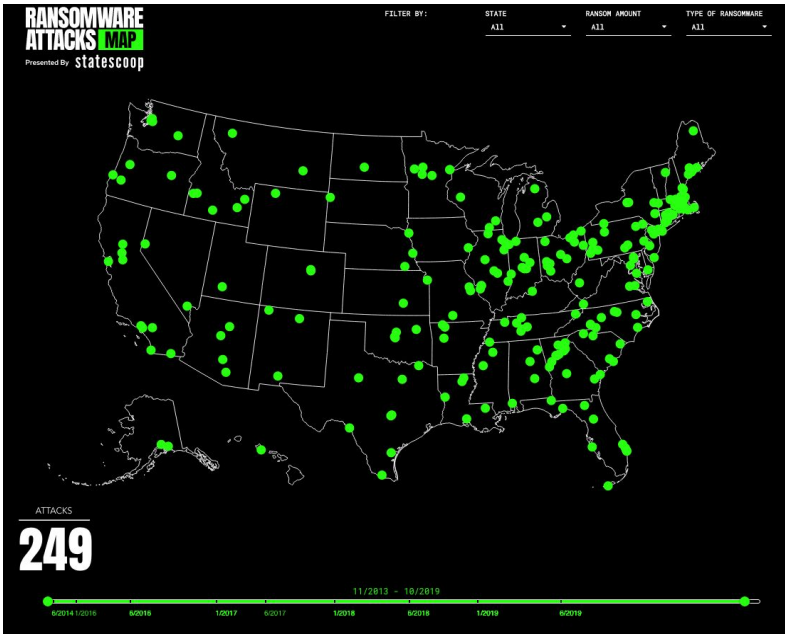

Image from https://statescoop.com/ransomware-map/, as of November 2019.

3. What are the Potential Consequences for Smart Cities and Communities?

Many benefits of Smart Cities are dependent on the generation, collection, and analysis of data as well as increased digitization, connectivity, integration, and automation. The consequences of ransomware can potentially be amplified in such an environment characterized by greater cyber-physical convergence and system interdependencies. New smart technologies – including IoT devices – can potentially serve as a target for ransomware attacks as well as a new attack surface for ransomware attacks to exploit.

The consequences for Smart Cities are many, though they may be able to be simplified and categorized into three primary categories:

- Denial or degradation of Smart City services (e.g., public WiFi or services dependent on public WiFi infrastructure; smart transportation infrastructure; smart building safety and security systems; public safety cameras and footage)
- Monetary loss attributable to either a ransom payout and/or response and recovery costs
- Degradation of trust in government and Smart City services

There are both immediate consequences that may be limited in duration as well as longer-term consequences that may require a considerable amount of time to restore – namely the trust in government and associated services. The inability to manage ransomware – and other cybersecurity and privacy risks – can have the potential to inhibit the success of long-term Smart City missions and objectives.

Ultimately, Smart Cities and cities striving to develop Smart City capabilities need to manage cybersecurity and privacy risk – understanding that ransomware is just one, albeit significant, threat. This necessitates having a proper and thorough understanding of the environment and mission, establishing a risk management strategy, conducting risk assessments, prioritizing missions and systems, and systematically and continually conducting the risk management process (i.e., Prepare; Categorize; Select; Implement; Assess; Authorize; Monitor).[4]

NIST Risk Management Framework (RMF) Process

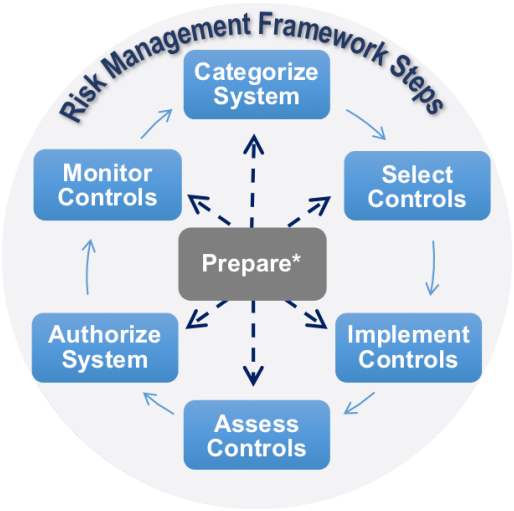

Image from https://csrc.nist.gov/Projects/risk-management/rmf-overview.

[4] In-depth discussion of cybersecurity and privacy risk management for Smart Cities is available in the Cybersecurity and Privacy Advisory Committee's *A Risk Management Approach to Smart City Cybersecurity and Privacy* available at https://pages.nist.gov/GCTC/uploads/blueprints/2019_GCTC-SC3_Cybersecurity_and_Privacy_Advisory_Committee_Guidebook_July_2019.pdf.

4. Smart City Considerations and Existing Resources for Mitigating Ransomware Risk

Smart City stakeholders should consider how the following broad sets of capabilities are applicable to addressing ransomware-specific risk and can assist in achieving overall cybersecurity and privacy risk management objectives. These categories generally align with the traditional people-process-technology construct for approaching specific problem sets.

- Planning and Process
- Technical Controls
- Education and Training

4.1 Planning and Process Considerations

Instituting plans and processes to consistently and systematically manage cybersecurity and privacy risk and aspects thereof - including ransomware risk - is essential and can enable Smart Cities and Communities to fully leverage technical and human assets. Specific to addressing the ransomware risk, Smart Cities and Communities should pay heed to the following considerations.

Establish, exercise, and maintain cyber incident response, continuity of operations, and disaster recovery plans – For managing ransomware risk, it is particularly important that Smart Cities and Communities have well-crafted incident response,[5] continuity of operations,[6] and disaster recovery[7] plans and that these plans have been exercised with relevant internal and external stakeholders. These plans should consider how different organizations and resources from different levels of government - in particular state and local law enforcement and in addition to new and existing relationships with private sector and academic partners - could be leveraged for effective response and recovery. It is important that these relationships are nurtured outside of and prior to disaster events and that these select entities are involved in the planning and exercise processes.

Some example organizations and resources include the following:

- U.S. Federal Government
    - Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) National Cybersecurity and Communications Integration Center (NCCIC)

[5] NIST defines *incident response plan* as "the documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyber attacks against an organization's information system(s)."
[6] NIST defines *continuity of operations plan (COOP)* as "a predetermined set of instructions or procedures that describe how an organization's mission essential functions will be sustained within 12 hours and for up to 30 days as a result of a disaster event before returning to normal operations."
[7] NIST defines *disaster recovery plan (DRP)* as "a written plan for processing critical applications in the event of a major hardware or software failure or destruction of facilities."

    - Federal Bureau of Investigation (FBI) Field Offices
    - Secret Service Electronic Crime Task Force (ECTF) and Field Offices
- U.S. State- and Local-Level
    - Multi-State Information Sharing & Analysis Center
    - National Guard and the 91st Cyber Brigade
    - Fusion Centers
    - State-level cyber coordination/operations centers, incident response teams, and support resources (e.g., Louisiana Cyber Coordination Center, Wisconsin Cyber Response Teams)
    - State and local law enforcement
- International
    - The No More Ransom Project – and participating international government and law enforcement organizations

Indeed, in the recent ransomware attack that affected numerous entities – including local governments – in the State of Texas, the state government has identified no fewer than half a dozen state-level government organizations,[8] an academic organization,[9] and multiple U.S. Federal government agencies[10] that were involved in the incident response efforts.

The process of developing and exercising these post-incident plans is important not only for ensuring efficient restoration of systems and services but also for enabling the design and engineering of cybersecurity, privacy, and resiliency into these Smart City systems and services from conception.

[8] Texas Department of Information Resources; Texas Division of Emergency Management; Texas Military Department; Texas Department of Public Safety; Texas Commission of Environmental Quality; and the Texas Public Utility Commission
[9] The Texas A&M University System's Security Operations Center/Critical Incident Response Team
[10] DHS; FBI – Cyber; and the Federal Emergency Management Agency (FEMA)

Cyber Incident Response, Continuity of Operations, and Disaster Recovery Planning Resources

While jurisdictions may have incident response, continuity of operations, and disaster recovery plans for natural disasters and other physical threats, the cyber domain may necessitate alternate actions and may involve other, additional stakeholders. There are numerous existing resources for developing such plans that have been made available by various State government-oriented organizations as well as the Federal government. The following are five example references:

Organization	Resource/Service	URL
National Association of State Chief Information Officers (NASCIO)	*Cyber Disruption Response Planning Guide*	https://www.nascio.org/Portals/0/Publications/Documents/2016/NASCIO_CyberDisruption_072016.pdf
National Governors Association (NGA)	Issue Brief on "State Cyber Disruption Response Plans"	https://www.nga.org/wp-content/uploads/2019/04/IssueBrief_MG.pdf
NIST	*Special Publication (SP) 800-34 Rev. 1: Contingency Planning Guide for Federal Information Systems*	https://csrc.nist.gov/publications/detail/sp/800-34/rev-1/final
DHS CISA	Cybersecurity Training & Exercises offerings - including incident response planning *Elections Cyber Tabletop Exercise Package*	https://www.dhs.gov/cisa/cybersecurity-training-exercises https://www.cisa.gov/sites/default/files/publications/Elections-Cyber-Tabletop-Exercise-Package-20200128-508.pdf

Consider and develop processes and policies for managing supply chain risk – Smart Cities should consider how operational partners and interdependencies (e.g., neighboring jurisdictions, critical infrastructure owners and operators) and as well as product and service providers may introduce risk to ransomware and other cybersecurity and privacy threats. As systems and capabilities become increasingly integrated in Smart Cities and across jurisdictions, understanding the cybersecurity posture of other organizations in the supply chain becomes increasingly difficult. In fact, remote access/management connections (e.g., remote desktop protocol), often used by outsourced or managed service providers, have been identified as a frequently-exploited attack vector.

Supply Chain Risk Management Resources The resources listed below provide frameworks for working through the supply chain risk management process and also include a free service for assessing interdependency risk – an aspect of supply chain risk that is particularly pertinent to Smart Cities.		
Organization	Resource/Service	URL
Healthcare and Public Health Sector Coordinating Council (HSCC) Joint Cybersecurity Working Group (JCWG)	*Health Industry Cybersecurity Supply Chain Risk Management Guide (HIC-SCRiM)*	https://healthsectorcouncil.org/hic-scrim/
National Cyber Security Centre (UK)	"Supply Chain Security Guidance"	https://www.ncsc.gov.uk/collection/supply-chain-security
DHS/CISA	External Dependencies Management Assessment[11]	https://www.dhs.gov/cisa/cybersecurity-assessments
NIST	Cyber Supply Chain Risk Management project NCCoE Supply Chain Assurance project *SP 800-161: Supply Chain Risk Management Practices for Federal Information Systems and Organizations*	https://csrc.nist.gov/projects/supply-chain-risk-management/ https://www.nccoe.nist.gov/projects/building-blocks/supply-chain-assurance https://csrc.nist.gov/publications/detail/sp/800-161/final

Carefully consider cyber insurance as a risk transfer component of broader cyber incident response, continuity of operations, and disaster recovery plans – In the context of ransomware, cyber insurance is frequently mentioned as a means to mitigate the financial burdens associated with paying ransoms and/or responding and recovering from ransomware attacks. Cyber insurance is an important risk management tool that can play a critical role in a Smart City's planning processes. However, it is just one tool and should not be viewed as a means of completely transferring ransomware risk to a third-party – nor does it prevent ransomware events. There are several key considerations when assessing the utility of cyber insurance:

- Explicitly understand what is and is not covered by cyber insurance, as some policies may exclude acts of "war" and "terrorism"

[11] The External Dependencies Management Assessment is just one of many cybersecurity assessment services offered by CISA to state and local jurisdictions.

- Public knowledge of cyber insurance coverage can increase probability of ransomware attack as there may be a perception of greater ability or propensity to pay the ransom
- Paying ransoms, whether through cyber insurance or otherwise, can contribute to perpetuating ransomware attacks and the supporting industry
- Utilizing insurance payouts to expedite restoral of services (whether through paying the ransom or covering other incident response and disaster recovery costs) can lead to increased long-term costs through higher insurance premiums, a consequence that was highlighted in the Florida ransomware example

Cyber Insurance Resources
The following are example resources that can help cyber insurance purchasers assess and determine proper coverage for their organization and associated risk environment.

Organization	Resource/Service	URL
Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC)	*Purchasers' Guide to Cyber Insurance Products*	https://fsscc.org/files/galleries/FSSCC_Cyber_Insurance_Purchasers_Guide_FINAL-TLP_White.pdf
Federal Trade Commission (FTC)	"Cybersecurity for Small Business: Cyber Insurance" planning tool	https://www.ftc.gov/system/files/attachments/cyber-insurance/cybersecurity_sb_cyber-insurance.pdf
NGA	"Cyber Liability Insurance for States"	https://www.nga.org/wp-content/uploads/2019/09/Cybersecurity-Insurance-Two-Pager-Final.pdf

4.2 Technical Control Considerations

Technical controls and mitigations have an important role to play in managing any particular cybersecurity and privacy risk. As Smart Cities and Communities tackle the ransomware problem, they should consider how the following points pertain to existing, new, and future capabilities and technologies.

Select and implement technical controls to combat ransomware as dictated by the risk management process – Many of the often recommended technical controls to mitigate ransomware risk can be considered basic cyber hygiene. Many of the various resources on combating ransomware recommend a similar set of controls to consider.

- Data backup and disaster recovery

- Patch and vulnerability management
- Anti-malware and endpoint protection
- E-mail filtering, e-mail security, and anti-phishing
- Application whitelisting
- Network segmentation
- Identity and access management – and more specifically, privileged access management

As with other cybersecurity and privacy risks, it is important to ensure that the basics are being done; being done properly; and conducted in a risk-informed manner prior to devoting resources to more complex capabilities.

Recognize that Smart City environments are technologically diverse, which may limit which and how technical controls can be implemented – While there are many traditional IT technologies involved in the development of Smart City solutions and capabilities, many implementations also depend on newer, Internet-connected sensors (i.e., IoT devices). In many cases, functionality may not exist to implement specific controls, and other limitations (e.g., connectivity, power consumption) may affect the practicality of certain cybersecurity and privacy measures. When selecting Smart City capabilities and solutions, it is important to consider whether the security and/or securability of those technologies or services align with the overarching risk management strategy.

Assess, authorize, and monitor implemented controls and associated policies to ensure proper operation in current risk environment – Beyond selecting and implementing controls to mitigate ransomware risk, it is critical to ensure that the controls and the policies associated with the controls are evaluated for proper implementation and performance (i.e., is the intended risk outcome achieved?) and are adjusted, as necessary, to accommodate changes in the risk environment. In rapidly evolving Smart City environments, the ability to continually assess control implementation and performance and to continually monitor the risk environment is critical.

Indeed, in the Baltimore ransomware incident, it was discovered that Baltimore's data backup policies were only applied to its server environment. As a result, some data stored on personal computers may not have been backed up and may have been lost as a result of the incident. Baltimore's CIO acknowledged that "more rigorous processes and testing are needed."

Technical Control Resources
The following resources provide commentary on controls and how to implement them; along with more technical information on example implementations and use cases with commercial technologies from the National Cybersecurity Center of Excellence (NCCoE) at NIST:

Organization	Resource/Service	URL
DHS/CISA	"Ransomware" security publication	https://www.us-cert.gov/security-publications/Ransomware
	"Security Tip (ST19-001): Protecting Against Ransomware"	https://www.us-cert.gov/ncas/tips/ST19-001
	"How to Protect Your Networks from Ransomware" technical guidance document	https://www.us-cert.gov/sites/default/files/publications/Ransomware_Executive_One-Pager_and_Technical_Document-FINAL.pdf
FBI and Internet Crime Complaint Center (IC3)	"High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations" public service announcement	https://www.ic3.gov/media/2019/191002.aspx
	"Ransomware" brochure	https://pdf.ic3.gov/Ransomware_Trifold_e-version.pdf
NIST/NCCoE	Data Security program	https://www.nccoe.nist.gov/projects/building-blocks/data-security
	SP 1800-11: Data Integrity: Recovering from Ransomware and Other Destructive Events	https://csrc.nist.gov/publications/detail/sp/1800-11/draft
	SP 1800-25: Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events	https://www.nccoe.nist.gov/projects/building-blocks/data-integrity/identify-protect
	SP 1800-26: Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events	https://www.nccoe.nist.gov/projects/building-blocks/data-integrity/detect-respond

Technical Control Resources (cont.)
Given the importance of IoT in the Smart City context, the following provide frameworks for assessing the security and securability of IoT devices. These can play a role in the selection, procurement, and implementation of devices, systems, and solutions and should also be considered in the supply chain risk management planning process.

Organization	Resource/Service	URL
DHS CISA	*Internet of Things Security Acquisition Guidance*	https://www.cisa.gov/sites/default/files/publications/20_0204_cisa_sed_internet_of_things_acquisition_guidance_final_508_0.pdf
NIST	Interagency or Internal Report (NISTIR) 8259 - *Core Cybersecurity Feature Baseline for Securable IoT Devices: A Starting Point for IoT Device*	https://csrc.nist.gov/publications/detail/nistir/8259/draft
Council to Secure the Digital Economy (CSDE)	*C2 Consensus on IoT Device Security Baseline Capabilities*	https://securingdigitaleconomy.org/projects/c2-consensus/
European Union Agency for Cybersecurity (ENISA)	*Good Practices for Security of IoT*	https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-1
CTIA	IoT Cybersecurity Certification Program	https://www.ctia.org/about-ctia/certification-resources

4.3 Education and Training Considerations

While it is unreasonable to expect all Smart City and Community participants to become cybersecurity or privacy experts, it is important to continue to increase the overall level of awareness. Consideration of cybersecurity and privacy issues should not be delegated solely to subject matter experts but rather should be common considerations integrated in all decision-making.

Perform tailored cybersecurity and privacy awareness training and outreach for leadership, employees, partners, and constituents to help build a risk-aware environment and population – At a minimum, Smart Cities should leverage cybersecurity and privacy education, awareness, and training tools to promote a risk-aware community. Instilling basic cyber hygiene principles among the Smart City system owners and operators as well as the users/customers can assist in reducing overall risk. However, relying on human users as a primary means of mitigating ransomware risk is likely not an effective strategy; technical, policy, and

process considerations can serve to reduce the cybersecurity and privacy burden on humans (e.g., utilizing remote browsing solutions versus anti-phishing training; mandating multi-factor authentication versus an opt-in approach).

Provide tailored training for those developing, deploying, operating, and maintaining Smart City systems – Smart Cities should facilitate cybersecurity and privacy training for employees and partners involved throughout the system or capability lifecycle. This should include traditionally non-technical roles – e.g., procurement, legal, financial. Basic understanding of cybersecurity and privacy risks and available resources to address cybersecurity and privacy risks can help better ensure their consideration throughout the lifecycle.

Collaborate with and leverage expertise from partner governments, academia, and private sector organizations – Smart Cities are largely about integration to create better outcomes. Limited cybersecurity and privacy expertise and human capital necessitates cooperation and collaboration to attain the desired cybersecurity and privacy risk outcomes. A recent example of state-wide collaboration includes MassCyberCenter's announcement of "a series of statewide workshops that will provide municipalities with the tools to develop or review their cyber incident response plans and facilitate collaboration with neighboring communities."[12] As another example, the Atlanta ransomware event demonstrated how on-going and pre-existing collaboration and relationship-building can be useful in the event of a cyber incident; Atlanta leveraged Federal government resources from the FBI, DHS, and USSS as well as the expertise of private sector companies, including Secureworks, Microsoft, and Cisco.

[12] NASCIO has made available a compilation of successful cross-jurisdictional collaboration projects and models at https://www.nascio.org/Advocacy/Collaboration. More recently, NASCIO and NGA jointly published a report on state and local cybersecurity collaboration projects available at https://www.nga.org/wp-content/uploads/2020/01/NASCIO_NGAStatesLocalCollaboration.pdf.

Education, Training, and Awareness Resources
While education, training, and awareness can cover a very broad range of topics, there are many existing resources to help organizations assess and address their human capital and community needs.

Organization(s)	Resource/Service	URL
DHS/CISA	National Initiative for Cybersecurity Careers and Studies (NICCS) Education and Training Catalog	https://niccs.us-cert.gov/training/search
Texas Department of Information Resources (DIR)	Certified [Cybersecurity] Training Programs	https://dir.texas.gov/View-About-DIR/Information-Security/Pages/Content.aspx?id=154
Anti-Phishing Working Group (APWG), National Cyber SEcurity Alliance (NCSA), and DHS	STOP. THINK. CONNECT. Campaign	https://www.stopthinkconnect.org/
NIST	*SP 800-50: Building an Information Technology Security Awareness and Training Program*	https://csrc.nist.gov/publications/detail/sp/800-50/final
NIST National Initiative for Cybersecurity Education (NICE) Working Group	"Cybersecurity is Everyone's Job" Workforce Management Guidebook	https://www.nist.gov/sites/default/files/documents/2018/10/15/cybersecurity_is_everyones_job_v1.0.pdf
DHS/CISA	Phishing Campaign Assessment[13]	https://www.dhs.gov/cisa/cybersecurity-assessments

5. Conclusion

There are many aspects to managing ransomware risk – as there are aspects and considerations to the broader practice of cybersecurity and privacy risk management. Cities are already prime targets for ransomware, and the increased digitization, automation, and integration foundational to Smart Cities will continue to make them ripe targets for threat actors. It is important to systematically address and integrate cybersecurity and privacy risk management practices and processes into the Smart City planning, development, and operation/maintenance processes. While ransomware is a particularly difficult and prominent cybersecurity problem, there are many existing resources to help Smart Cities manage this risk.

[13] The Phishing Campaign Assessment is just one of many cybersecurity assessment services offered by CISA to state and local jurisdictions.

References

Allyn, Bobby. "22 Texas Towns Hit with Ransomware Attack in 'New Front' of Cyberassault." *NPR*, 20 August 2019, https://www.npr.org/2019/08/20/752695554/23-texas-towns-hit-with-ransomware-attack-in-new-front-of-cyberassault.

"Atlanta U.S. Attorney Charges Iranian nationals for City Of Atlanta ransomware attack." *The United States Attorney's Office for the Northern District of Georgia*, United States Department of Justice, 5 December 2018, https://www.justice.gov/usao-ndga/pr/atlanta-us-attorney-charges-iranian-nationals-city-atlanta-ransomware-attack.

"Baker-Polito Administration Announces New Program to Assist Municipalities in Bolstering Cyber Resiliency." *MassCyberCenter at MassTech*, 17 October 2019, https://masscybercenter.org/press-releases/baker-polito-administration-announces-new-program-assist-municipalities-bolstering.

Broadwater, Luke. "Baltimore IT department uses 'mind-boggling,' outdated data storage method, audit finds." *The Baltimore Sun*, 27 September 2019, https://www.baltimoresun.com/politics/bs-md-ci-audit-it-20190927-23hrwbtdyzcu7lmmwdqzbmzja4-story.html.

"Certification Resources." *CTIA*, https://www.ctia.org/about-ctia/certification-resources.

City of Baltimore. "Baltimore City Information Technology Biennial Performance Audit Report: Fiscal Years Ended June 30, 2018 and 2017," September 2019.

Council to Secure the Digital Economy, *The C2 Consensus on IoT Device Security Baseline Capabilities*, September 2019.

"Cyber Incident Response." *Cybersecurity & Infrastructure Security Agency*, Department of Homeland Security, 26 November 2018, https://www.cisa.gov/cyber-incident-response.

Cybersecurity and Infrastructure Security Agency, *Elections Cyber Tabletop Exercise Package*, January 2020.

Cybersecurity and Infrastructure Security Agency, *Internet of Things Security Acquisition Guidance*, February 2020.

"Cybersecurity Assessments." *Cybersecurity & Infrastructure Security Agency*, Department of Homeland Security, https://www.dhs.gov/cisa/cybersecurity-assessments.

"Cybersecurity Training & Exercises." *Cybersecurity & Infrastructure Security Agency*, Department of Homeland Security, https://www.dhs.gov/cisa/cybersecurity-training-exercises.

"Cyber Supply Chain Risk Management." *Computer Security Resource Center*, National Institute of Standards and Technology, 30 September 2019, https://csrc.nist.gov/projects/supply-chain-risk-management/.

"Data Security." *National Cybersecurity Center of Excellence*, National Institute of Standards and Technology, https://www.nccoe.nist.gov/projects/building-blocks/data-security.

Deere, Stephen. "Confidential Report: Atlanta's cyber attack could cost taxpayers $17 million." *The Atlanta Journal-Constitution*, 1 August 2018, https://www.ajc.com/news/confidential-report-atlanta-cyber-attack-could-hit-million/GAIjmndAF3EQdVWlMcXS0K/?icmp=np_inform_variation-control#.

Douglas, Theo. "What can we learn from Atlanta?" *Government Technology*, October/November 2018, https://www.govtech.com/security/What-Can-We-Learn-from-Atlanta.html.

Duncan, Ian. "Baltimore acknowledges for first time that data was destroyed in ransomware attack." *The Baltimore Sun*, 11 September 2019, https://www.baltimoresun.com/politics/bs-md-ci-data-lost-20190911-i6feniyk5nd3pereznpdxwsf7a-story.html.

European Union Agency for Cybersecurity, *Good Practices for Security of IoT*, November 2019.

Federal Bureau of Investigation, "Ransomware," April 2016.

Federal Trade Commission, "Cybersecurity for Small Business: Cyber Insurance," October 2018.

"Field Offices." *Federal Bureau of Investigation*, U.S. Department of Justice, https://www.fbi.gov/contact-us/field-offices.

"Field Offices." *United States Secret Service*, Department of Homeland Security, https://www.secretservice.gov/contact/field-offices/.

Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security, "Purchasers' Guide to Cyber Insurance Products," April 2016.

Freed, Benjamin. "Atlanta CIO worries city employees will forget ransomware attack." *StateScoop*, Scoop News Group, 24 October 2019, https://statescoop.com/atlanta-cio-worries-city-forget-ransomware-attack/.

Freed, Benjamin. "Florida city pays hackers $600,000 after ransomware attack." *StateScoop*, Scoop News Group, 20 June 2019, https://statescoop.com/florida-city-pays-hackers-600000-after-ransomware-attack/.

Freed, Benjamin. "How Texas used its disaster playbook after a huge ransomware attack." *StateScoop*, Scoop News Group, 15 October 2019, https://statescoop.com/texas-ransomware-emergency-declaration-nascio-19/.

"Fusion Centers." *Department of Homeland Security*, 19 September 2019, https://www.dhs.gov/fusion-centers.

Gallagher, Sean. "Baltimore's bill for ransomware: Over $18 million, so far." *Ars Technica*, 5 June 2019, https://arstechnica.com/information-technology/2019/06/baltimores-bill-for-ransomware-over-18-million-so-far/.

"Glossary." *Computer Security Resource Center*, National Institute of Standards and Technology, https://csrc.nist.gov/glossary.

Healthcare and Public Health Sector Coordinating Council Joint Cybersecurity Working Group, *Health Industry Cybersecurity Supply Chain Risk Management Guide*, October 2019.

"High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations." *Federal Bureau of Investigation Internet Crime Complaint Center*, Department of Justice, 2 October 2019, https://www.ic3.gov/media/2019/191002.aspx.

"Investigation." *United States Secret Service*, Department of Homeland Security, https://www.secretservice.gov/investigation/#field.

Johnston, Ryan. "Managed service providers a growing target for ransomware attackers." *StateScoop*, Scoop News Group, 1 November 2019, https://statescoop.com/ransomware-managed-service-providers-local-government/.

"MS-ISAC." *Center for Internet Security*, https://www.cisecurity.org/ms-isac/.

NASCIO, *Cyber Disruption Response Planning Guide*, April 2016.

National Governors Association, "Cyber Liability Insurance for States," September 2019.

National Governors Association, "State Cyber Disruption Response Plans," July 2019.

National Initiative for Cybersecurity Education Working Group Subgroup on Workforce Management at the National Institute of Standards and Technology, *Cybersecurity is Everyone's Job*, October 2018.

National Institute of Standards and Technology, *NISTIR 8259 (Draft): Core Cybersecurity Feature Baseline for Securable IoT Devices: A Starting Point for IoT Device Manufacturers*, July 2019.

National Institute of Standards and Technology, *NIST SP 1800-11 (Draft): Data Integrity: Recovering from Ransomware and Other Destructive Events*, September 2017.

National Institute of Standards and Technology, *NIST SP 1800-25 (Draft): Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events*, January 2020.

National Institute of Standards and Technology, *NIST SP 1800-26 (Draft): Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events*, January 2020.

National Institute of Standards and Technology, *NIST SP 800-161: Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, April 2015.

National Institute of Standards and Technology, *NIST SP 800-34 Rev. 1: Contingency Planning Guide for Federal Information Systems*, November 2010.

National Institute of Standards and Technology, *NIST SP 800-50: Building an Information Technology Security Awareness and Training Program*, October 2003.

"NICCS Education and Training Catalog." *Cybersecurity & Infrastructure Security Agency*, Department of Homeland Security, https://niccs.us-cert.gov/training/search.

"Ransomware Amounts Rise 3x in Q2 as Ryuk & Sodinokibi Spread." *Coveware, Inc.*, 15 July 2019, https://www.coveware.com/blog/2019/7/15/ransomware-amounts-rise-3x-in-q2-as-ryuk-amp-sodinokibi-spread.

"Ransomware." *Cybersecurity & Infrastructure Security Agency*, Department of Homeland Security, 11 April 2019, https://www.us-cert.gov/security-publications/Ransomware.

"Ransomware Attacks Map." *StateScoop*, Scoop News Group, https://statescoop.com/ransomware-map/.

"Ransomware Frequently Asked Questions." *City of Baltimore*, https://mayor.baltimorecity.gov/ransomware-frequently-asked-questions.

"Ransomware Tips and Information." *Texas Department of Information Resources*, https://dir.texas.gov/View-About-DIR/Information-Security/Pages/Content.aspx?id=155.

"Risk Management Framework (RMF) Overview - FISMA Implementation Project." *Computer Security Resource Center*, National Institute of Standards and Technology, 29 October 2019, https://csrc.nist.gov/Projects/risk-management/rmf-overview.

"Security Awareness Training Certification (HB 3834)." *Texas Department of Information Resources*, https://dir.texas.gov/View-About-DIR/Information-Security/Pages/Content.aspx?id=154.

"Security Primer – Ransomware." *Center for Internet Security*, https://www.cisecurity.org/white-papers/security-primer-ransomware/.

"Security Tip (ST19-001): Protecting Against Ransomware." *Cybersecurity & Infrastructure Security Agency*, Department of Homeland Security, 11 April 2019, https://www.us-cert.gov/ncas/tips/ST19-001.

Shi, Fleming. "Threat Spotlight: Government Ransomware Attacks." *Journey Notes*, Barracuda Networks, Inc., 28 August 2019,

https://blog.barracuda.com/2019/08/28/threat-spotlight-government-ransomware-attacks/.

"State Websites." *National Guard*, https://www.nationalguard.mil/Resources/State-Websites/.

Stone, Jeff. "Another Florida city is making a ransomware payment, worth nearly $500,000 this time." *CyberScoop*, Scoop News Group, 26 June 2019, https://www.cyberscoop.com/ransomware-lake-city-florida-payment/.

"Stop.Think.Connect." *STOP. THINK. CONNECT. Campaign*, https://www.stopthinkconnect.org/.

Sullivan, Emily. "Baltimore introduces 'manual workaround' for homebuying during ransomware attacks." *WYPR*, 22 May 2019, https://www.wypr.org/post/baltimore-introduces-manual-workaround-homebuying-during-ransomware-attacks.

"Supply Chain Assurance." *National Cybersecurity Center of Excellence*, National Institute of Standards and Technology, https://www.nccoe.nist.gov/projects/building-blocks/supply-chain-assurance.

"Supply chain security guidance." *National Cyber Security Centre*, https://www.ncsc.gov.uk/collection/supply-chain-security.

"The No More Ransom Project." *The No More Ransom Project*, https://www.nomoreransom.org/.

"Update on Texas Local Government Ransomware Attack." *Texas Department of Information Resources*, 5 September 2019, https://dir.texas.gov/View-About-DIR/Article-Detail.aspx?id=213.

United States Government, "How to Protect Your Networks from Ransomware," July 2016.

"91st Cyber Brigade Archive." *Virginia National Guard*, https://vaguard.dodlive.mil/category/armyguard/91stcyberbrigade/.

Background and Acknowledgements

The National Institute of Standards and Technology (NIST) launched the Global City Teams Challenge (GCTC) program in 2014 as a means to encourage collaboration across the global Smart Cities community. NIST subsequently partnered with the Department of Homeland Security Science and Technology Directorate (DHS S&T) to initiate the Smart and Secure Cities and Communities Challenge (SC3) and encourage the consideration of cybersecurity and privacy in designing and implementing Smart City solutions.

The Cybersecurity and Privacy Advisory Committee (CPAC) was established as a public working group of cybersecurity and privacy professionals and practitioners across the GCTC community. The CPAC has representation from all levels of government, non-profit organizations, academia, and the private sector.

The CPAC public working group is intended to provide a forum for members to share their expertise, leverage industry best practices, and further collaborate with relevant organizations. The CPAC also serves as a cybersecurity and privacy resource for the GCTC-SC3 SuperClusters and Action Clusters.

This whitepaper has been developed by the CPAC to provide a starting point for Smart City and Community leaders and stakeholders to tackle the growing ransomware problem.

We would like to recognize the following CPAC participants for their contributions to this whitepaper:

- *David Balenson, SRI International*
- *Pamela Gupta, OutSecure*
- *Lan Jenson, Adaptable Security*
- *Matthew Rosenquist, Eclipz.io*
- *Peter Wong, The Soter Group*