

# Managing Technology in Local Government: Cybersecurity, Risk and Proficiency

---

## Guidance for Local Government and Other Organizations

Issue Paper #9 | March 2020  
Bloustein Local Government Research Center

Marc H. Pfeiffer, MPA  
Assistant Director and Senior Policy Fellow  
Bloustein Local Government Research Center  
Edward J. Bloustein School of Planning and Public Policy  
Rutgers, The State University of New Jersey

# The Bloustein Local Government Research Center

New Jersey is served by more than 1,500 distinct local government agencies: municipalities, school districts, utilities, counties, and more. Yet, even with this wealth of opportunity, precious little substantive research has been done within the local government environment to inform some of our state's most pressing policy issues.

The **Bloustein Local Government Research Center**, or **Bloustein Local** <http://blousteinlocal.rutgers.edu/>, serves as a focal point and engages in a range of services, including:

- Encouraging and conducting applied and academic research on local government fiscal and administrative issues, emphasizing application and support to New Jersey local government.
- Developing resources that can assist others in conducting research and analysis.
- Organizing and hosting conferences and symposia on New Jersey local government fiscal and administrative issues.
- Supporting New Jersey local government fiscal and administrative policy development, implementation, and analysis through contract research and on-call advice for organizations and institutions that engage in local government policy setting and policymaking.
- Promoting and increasing public understanding of local government issues by partnering with and supporting civic and media organizations that inform and educate the public on local government matters.

A list of the Center's current projects may be found online at <http://blousteinlocal.rutgers.edu/projects/>.

## About the Author

**Marc H. Pfeiffer retired in 2012 from a 37-year career in New Jersey local government administration, having served as a municipal administrator in several municipalities, and 26 years of service in the State's local government oversight agency, the Division of Local Government Services. At DLGS he served as Deputy Director for 14 years, and periodically as Acting Director.**

**Marc has broad experience in many areas of local government policy and administration, including specific expertise in areas such as finance and property taxation, public procurement, shared services and consolidation, technology, energy, labor relations, and general local and**

**state government administration. He also has deep experience in the legislative process and as a regulatory officer. He is currently engaged in research concerning the use of technology in local government.**

**In addition to participating in Bloustein Local, Marc makes his extensive government experience available as a guest lecturer at the Bloustein School and other collaborative efforts. He is also assisting the Rutgers School of Public Affairs and Administration with the State's Certified Public Manager Program in curriculum development and instruction. He can be reached at [marc.pfeiffer@rutgers.edu](mailto:marc.pfeiffer@rutgers.edu).**

# Contents

Introduction . . . . .	2
<b>Part 1 – Managing Technology Risks</b>	
1. When It Comes to Managing Technology, Being Cyber Secure Is Not Enough . . . . .	4
2. Managing Technology Risks Through Technological Proficiency . . . . .	6
3. Are Your Municipality’s Technology Management Practices Putting It at Risk?. . . . .	9
4. Technology Leadership Bytes. . . . .	12
<b>Part 2 – Minimum Technological Proficiency Standards</b>	
5. Minimum Technology Standards Overview . . . . .	14
6. Getting Started . . . . .	16
7. Minimum Technological Proficiency Standards . . . . .	17
<b>Appendices</b>	
1. Model Information Technology Practices Policy Guidance . . . . .	19
2. Model Information Technology Practices Policy . . . . .	20
3. Model Cybersecurity Incident Response Plan & Claim Roadmap . . . . .	22
4. Additional Security Practices to Consider . . . . .	24
Infographic of Minimum Technology Standards . . . . .	25

# Introduction

In the last five years, Bloustein Local Government Research Center has undertaken several local government technology initiatives; this report is based on those findings and recommendations.<sup>1</sup> While focused on and applicable to small- and medium-sized New Jersey local government agencies, the principles and policies put forward may be applicable to all small and medium sized local governments, as well as similarly sized businesses and not-for-profit organizations.

Technology is complicated, as is managing it. And like any other activity, technology requires management time, attention, and financial resources. This report focuses not on technology itself, but on the challenges presented to senior managers and elected officials who have the decision-making responsibility for their organizations.

After setting the stage with an overview in section 1, guidance is provided from three perspectives:

1. Section 2 draws attention to the range of risks organizations face when they adopt today's digital technologies. While cybersecurity is by far the most significant, there are five other risks that require management's attention.
2. Section 3 provides technology management guidance to agency governing boards and their senior managers. This covers the elements of technological leadership, planning, decision-making, and budgeting; ensuring technical competence when it comes to maintaining the agency's technology; and cyber hygiene, making sure agency employees understand their role in ensuring cyber safety.
3. Part 2 (sections 4-6 and the Appendices) promotes a set of minimum technology standards that when applied, provides a floor level of technological proficiency within the organization.

Taken together, the full report comprises a set of minimum standards and management practices that will provide a reasonable level of proficiency, protection, and sustainability for small and medium-sized government organizations.<sup>2</sup> While the specifics can be debated or modified, they set a practical and achievable starting point upon which organizations can then improve.

The author hopes readers will find this report helpful and supportive as technology becomes even more deeply ingrained in everyday activities. This has particular application for those places looking to embrace the concepts of smart cities, which place great reliance on technology to meet public needs.

---

<sup>1</sup> Some of material in this report has been edited from its original form to reflect changes in technology and to provide context.

<sup>2</sup> There are various cybersecurity frameworks and practices promulgated by government and private organizations that are well suited for large, sophisticated organizations. These approaches are highlighted in Appendix 4.

# Thanks and Acknowledgments

The Principal Investigator, developer, and author of this work is Marc Pfeiffer, MPA, Assistant Director of the Bloustein Local Government Research Center. Mr. Pfeiffer is grateful for the efforts and support of:

- The NJ Municipal Excess Liability Joint Insurance Fund (MEL), led by the MEL's founding executive director, David Grubb; executive director, Joseph Hrubash; and Edward Cooney, a vice president of the insurance firm Conner, Strong, and Buckelew. The MEL provided the funding to conduct research into the issues of technological risk, proficiency, and the minimum standards.
- Guidance for the specific technology recommendations were provided by a group of local government technology managers from the New Jersey Chapter of GMIS International, led by Justin Heyman and Robert McQueen.
- Dr. Alan R. Shark, Ph.D., the Executive Director of the Public Technology Institute provided invaluable guidance and support in the development of technological risk concepts.
- Dr. Raphael Caprio, Ph.D., Director of the Bloustein Local Government Research Center for his overall guidance and organizational support.
- Debra Meltzer for her editing skill, Tamara Swedberg for her graphic choices, and Karyn Olsen for her publication design efforts.

The author welcomes comments and evaluations of the work at [marc.pfeiffer@rutgers.edu](mailto:marc.pfeiffer@rutgers.edu).

# PART ONE

## 1. When It Comes to Managing Technology, Being Cyber Secure Is Not Enough

As with all technological revolutions, the constantly evolving digital technologies of the 21st century have brought new possibilities, goods, services, and opportunities to society. History has shown, however, that most new technologies bring a dark side that presents risks and threats to the society (air and water pollution, climate change).

Digital technologies, as reflected by data processing (information), communications (fiber optic networks and cellular phone services), and operational “things” (video cameras, sensors) all have risks attached to them. And the most significant one is cybersecurity; which is “the state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this.”<sup>3</sup>

Without question, the threats to cybersecurity challenge all of society. These threats have evolved over the years from hackers in basements to sophisticated criminal networks and nation-states (and newer generations of hackers in basements). They look to monetarily gain from or manipulate or disrupt the societies and cultures that have become critically dependent upon digital technology.

**New technologies bring new threats that require new solutions to respond to them.** Businesses, government agencies, and educational institutions around the world have responded with a wide range of products,

services, guidance, and networking and training opportunities to help organizations manage their cybersecurity risks.

Agency leaders must have their cybersecurity risks assessed and allocate resources to mitigate and manage them. Making cybersecurity assessments is something new and challenging to many organizations. This is because the risk is new and evolving, and leadership may not understand or fully appreciate them. Expertise to assess and advise on actions may need to be acquired.

Sound management requires expenditure of the three resources that organization have available; time, attention, and money. And these resources are inherently limited in supply and must be allocated among all organizational needs. If more resources are required, they must come from the customers, clients, and constituent/owners of the organization, usually through increased fees, costs, taxes, or reduced services or investment returns, as relevant to the agency.

Organizations of every size are working to meet these challenges and allocate their scarce resources effectively. Based on needs and sometimes limited understanding of the risks, leaders balance hiring staff and contracting with service providers; try to keep current with the latest in hardware and software; train (and retrain) employees in safe practices (cyber hygiene); network with like organizations to

<sup>3</sup> <https://www.lexico.com/en/definition/cybersecurity>

learn and share expertise; and sometimes engage in wishful thinking that they will not become the next headline of a hacker success story. As is said in cybersecurity circles: the hacker has to be successful only once, the target's defenses have to work 100 percent of the time.

The cybersecurity world is awash with constantly evolving technological solutions, sophisticated management frameworks, detailed lists of controls, marketing of goods and services, and professional advice that reflect the needs of the moment. Bloustein Local has observed that despite this wealth of guidance, when balancing technology management challenges along with other organization needs, many organizations are challenged to provide the resources required by technology best practices, frameworks, and checklists.

Further, cybersecurity is the most critical of the multiple risks that digital technology presents to all organizations. Digital technology also presents organizations with *operational, financial, legal, reputational, and societal risks*. Focusing only on cybersecurity and ignoring the others, leaves organizations open to the other threats.<sup>4</sup> These very real risks warrant that organizations pay attention to them. This makes managing

technology all the more difficult, but still requires time, attention, and money.

To address these real and practical challenges the concept of *minimum technology standards* is presented as a practice to raise the proficiency of technology management in smaller and medium sized organizations. Of course, a challenge of setting minimum standards is that they become a floor and there may be few incentives to exceed the minimum. That may be true but setting a minimum at least gets to a responsible level of proficiency and protection, from which improvement can follow. That is better than floundering around with incomplete solutions they do not address the range of technology risks that face a given organization.

The minimum standards in this report reflect the three primary elements of technological proficiency: *technical competence, leadership* (budgeting, decision-making, and planning), and *cyber hygiene*. Cybersecurity practices are at the core and meeting all the minimum standards goes a long way to address and mitigate the other risks. It is a practical starting point that if met, places organizations in a strong position to understand its technology, reduce its threat level and attack points, and be able to successfully recover from a successful attack.




<sup>4</sup> These risks are reported on in the 2015 Bloustein Local report on Technological Proficiency and Risks prepared for the N.J. Municipal Excess Liability Fund: <http://blousteinlocal.rutgers.edu/managing-technology-risk/>

## 2. Managing and Mitigating Technology Risks Through Technological Proficiency

### *A Leadership Summary*

**Technology Has Risks.** Digital technology permeates everything we do. It goes beyond cyber security issues such as data breaches and network intrusions. This project identifies the risks that face local governments and the steps they can take to manage and mitigate them.

**What is Digital Technology?** Today's technology can be broken down into three areas of concern:

-  Information technology – computers, applications, and security services
-  Communications technology –voice, video and data that move over wired and wireless networks
-  Operational technology – digitally driven devices such as video cameras, process controllers at water treatment plants, ice-detecting road sensors, meters, drones, video doorbells, and fitness recorders: the “internet of things.”

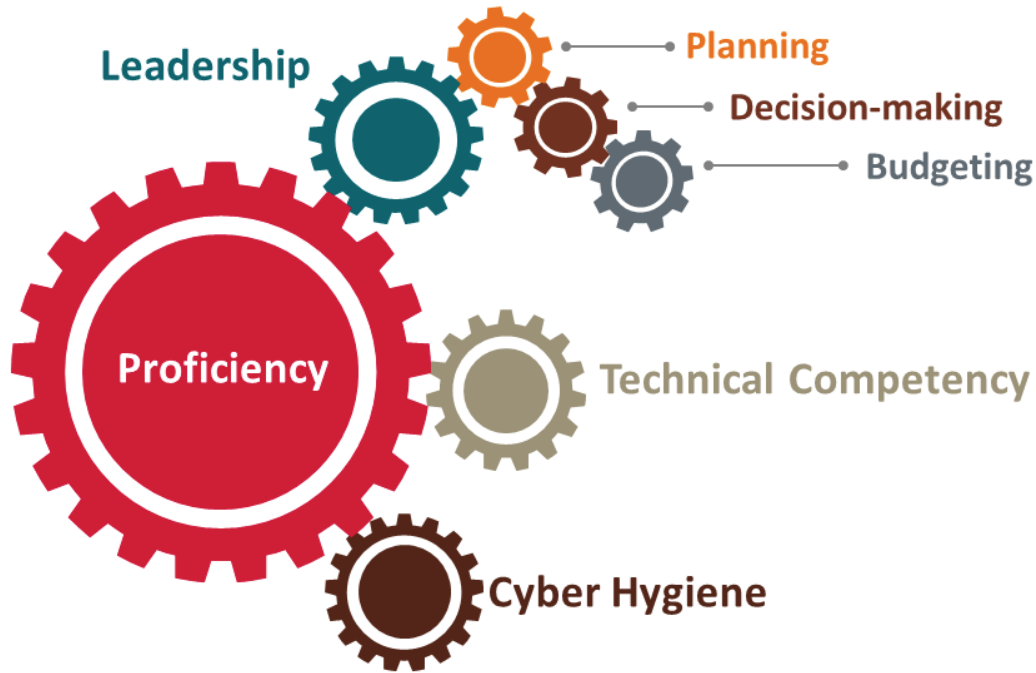
**Impact of Digital Technology on Local Governments:** Citizens are driving government to adopt new technologies (web pages, social media, and online services). The challenge is that citizens and businesses want their government to use more technology, but they don't want to pay more for it. A further challenge is that managing technology is an ongoing process; it is not a short-term project that can be completed and then ignored.

**Technology risks:** The effects of these risks are significant; they overlap, and break down into six categories:

**Cybersecurity:** data breach/theft and disclosure of personally identifiable information, data loss/file corruption, network intrusion, cyber-extortion, website/social media attacks.







**Legal:** third party liability for denial of services, discrimination, litigation costs, OPRA liability, police system failures, employee misuse

**Operational:** loss of capacity to manage work, compromised physical security of technology, electrical system failures, contractor failures, failed backup systems

**Financial:** cost of cyber insurance, responses to breaches (time and money), procurement delays, change from capital to operating expenses

**Reputational:** loss of public trust, media risk, social media, political responses, bond rating agency evaluations

**Societal:** differing expectations of the next generation of workers, speed of change and ability to manage it, increased expectations of government transparency that are rooted in technology.

**How Technological Proficiency manages and mitigates risks:** Becoming technologically proficient enables governments to understand, mitigate, and manage their risks. This will provide assurance that their technology will work when it needs to and protect themselves from compromise. Technological proficiency has three interconnected elements:

**1. Leadership has three elements:**

*Planning:* governance and technology managers combine to approve a technology plan that implements long- and short-term goals and recommends risk management strategies.

*Decision-making:* governing body and executive management provide overall technology policy goals and guidance, evaluate risks, approve and fund plans, and monitor activities.

*Budgeting:* ensuring that the agency budget supports the decisions made through the planning process. When it doesn't, the process cycles back to planning and iterates.

2. **Cyber Hygiene:** all employees understand and practice safe use of technology (cyber hygiene) and receive ongoing training to prevent technology compromise.
3. **Technical Competence:** staffing, management attention, and financial resources necessary for the development and implementation of sound technology strategies are properly and adequately deployed to fulfill the plan.

In addition, given the range of today's technology risks, a key element of risk management is cyber insurance. Sound cyber insurance coverage is necessary to mitigate a range of financial, legal, and operational risks. This includes responding to and recovering from a successful ransomware attack, or the managing the impact of the theft of personally identifiable information stored by the agency. Implementation practices and techniques

based on this approach were adopted by the NJMEL as its "Cyber Risk Management Program." That program (discussed later in this report) is targeted to small and medium sized organization that do not have the technological maturity or capacity of large, complex organizations.

*This article summarized key elements of the 2015 report, **Managing Technology Risks Through Technological Proficiency** produced by the Bloustein Local Government Research Center, Rutgers University. That report was supplemented with a resources guide. Some elements of the 2015 resources guide have been superseded by more contemporary resources but it continues to have value at a basic level. Both documents can be found at: <http://blousteinlocal.rutgers.edu/managing-technology-risk/>. The MEL Cyber Risk management program is at <https://njmel.org/wp-content/uploads/2017/12/Cyber-Risk-Management-Program.pdf>*

### 3. Attention Elected Officials: Are Your Municipality's Technology Management Practices Putting It (and You) at Risk?

**By Marc Pfeiffer. Based on a version originally published in New Jersey Municipalities, October 2019**

Today's technology is solidly embedded in most things that municipalities do. What's more, the public now **expects** technology-based services from its local government. However, as we have seen in recent headlines, technology presents risks that require sound management and ongoing mitigation.

To be clear: IT systems in every municipality around the country are under attack from cyber-criminals who want to steal and extort money, steal and resell data, or use hacked networks to attack and harass other computer users. These criminal networks target every computer user, from individuals whose computer is their smart phone, to tablets and desktop computers used in homes, governments, and business networks of every size.

If you don't already know this, you haven't been paying attention. The news has been full of stories about cybersecurity breaches affecting Equifax, the NSA, and the cities of Atlanta and Baltimore, with more places added to the list each week. You may even have heard rumors that three dozen or more New Jersey municipalities have been the victims of successful hacker attacks in the last two years.

If you are not proactively responding to these threats, you are putting your government,

residents, and businesses in jeopardy and are effectively *negligent in your responsibilities*.

To help you understand what to do, here are some questions and answers about technology issues. As elected officials, you are ultimately responsible for your organization's cyber safety.



*Do you understand your municipality's technology risks?*

There are six primary, inter-related technology risks: cybersecurity, financial, legal, operational, reputational, and societal. Cybersecurity threats present the most immediate, likely, and potentially damaging risk.

Technology risks can never be eliminated, but they can be mitigated. Mitigating cybersecurity risks requires ongoing management, technical attention, and support.

Today, system failures often stem from ransomware, when hackers encrypt software and data files and the "key" to unlock them requires payment over the internet (e.g., bitcoin). But beyond hackers, there are physical threats (e.g., broken HVACs, burst water pipes), power failures, and other disasters to consider.



*How do we manage these?*

There are two things you absolutely must have in place: 1) a trusted employee or consultant who advises the town on technology management, and 2) tested back-up procedures that restore operating systems and data in the event your technology is compromised (e.g., ransomware). There are many backup solutions and yours must meet your specific needs. That's why trusted expertise is a must. Your advisors can be vendors, employees, or even citizens involved in the computer industry.

If you don't have both, remedy that immediately. If you already have them, ask your expert to report on how secure you are, how often your data backup process is tested, and if there are other steps to take that would ensure adequate protection.



*Is it too late to protect my town from cyber threats?*

No, you are not too late because the threats are ongoing. But first, ask your technology staff one key question – what will your town do if its systems get infected by ransomware? If the answer does not give you confidence that recovery time will be reasonable, you need to revise your procedures.

Nevertheless, recovery from a successful ransomware attack doesn't happen overnight (even if a ransom payment is successful). Depending on the sophistication of the system, it will take at least several days or weeks to rebuild and restore systems. Do you have disaster

recovery plans that allow critical operations to continue during that time?



*OK, we have an expert and a sound and tested backup system. What else should we be doing?*

Since every municipality has its own technology profile, each one must forge its own path to successfully mitigate its risks. However, there are three key elements needed to establish technological proficiency\*:

- **Technology Management:** this requires organizational leadership (proactive technology planning, budgeting, and decision-making processes), the development of sound incident response plans and technology policies that establish proficiency.
- **Cyber Hygiene:** this means ensuring that all employees who use computers have had, in the last two years, at least one hour of training to stay safe from phishing attempts and social engineering when using their computer. Cyber hygiene also includes sound computer use policies, smart password construction, and appropriate data encryption practices.
- **Technical Competence:** the more sophisticated the technology system, the greater the number of technical activities there are to do. However, there are some activities that apply to systems of all sizes. They include having sound backup practices, keeping software and hardware current with patches and updates, using defensive software (an anti-virus program at minimum) on all computers, procedures to control who has access to your systems; and maintaining a properly trained staff to manage those systems.

While cybersecurity is of primary importance, do not ignore the five other technology risks listed above. Municipalities must address their complete technology “risk profile” as a management priority.

The Minimum Technology Model is a prudent next step to move your organization along the tech proficiency scale.

No one expects every elected official or senior manager to be an expert in all things municipal. That is why there are police chiefs, public works directors, engineers, finance officers, health officers and experts in every field. Today, technology managers need to be part of that list.

As a municipal leader, there is no excuse for your town not to manage its technology proficiently. Elected and appointed officials must make the security of their technology and their communities a priority and find ways to get it done well.

If your municipality is already there, kudos for having things under control! Most likely, you discovered that technology management takes more time, attention, and money than you thought it would. You were able to achieve proficiency because you invested in competent, trusted personnel to run your technology and you have supported them with sound decision-making processes. Keep up the good work. Share what you’ve learned with your peers. Staying cyber safe is a team effort.

### Additional Resources/For More Information

- The Municipal Excess Liability Fund’s [Cyber Risk Management Program](https://njmel.org/wp-content/uploads/2017/12/Cyber-Risk-Management-Program.pdf) implementation of Minimum Tech Standards ties compliance with the standards to a reduction in cyber insurance deductibles in the event of a cyber insurance claim. <https://njmel.org/wp-content/uploads/2017/12/Cyber-Risk-Management-Program.pdf>. (The practices are available to anyone and not limited to MEL members.)
- MS-ISAC is a federally sponsored resource center for states and municipalities on cybersecurity management: [www.cisecurity.org/ms-isac/](http://www.cisecurity.org/ms-isac/). It is free to join and each government agency should join. It provides technology managers with valuable resources.
- The NJ Office of Homeland Security and Prevention’s point of contact for cybersecurity threats is [www.cyber.nj.gov](http://www.cyber.nj.gov) (aka, NJ-CCIC). Cybersecurity managers or the technical oriented can sign up for their (slightly technical) free weekly bulletin.
- Government agencies can join GMIS, the professional association of local government technology managers at [www.gmis.org](http://www.gmis.org). Join as a government agency (low fees) and your staff (or contractor) can participate in a local government technology management support group. Joining GMIS automatically enrolls you in the NJ chapter. Anyone can attend the chapter’s annual Technology Education Conference ([www.njgmis.org](http://www.njgmis.org)).
- The [OUCH](http://www.sans.org/security-awareness-training/ouch-newsletter) Newsletter from the SANS Institute is a free monthly newsletter covering safe cyber hygiene, useful for distribution to staff as part of a cyber hygiene training plan: [www.sans.org/security-awareness-training/ouch-newsletter](http://www.sans.org/security-awareness-training/ouch-newsletter)
- [Managing Technology Through Technological Proficiency](http://blousteinlocal.rutgers.edu/managing-technology-risk/): the original Bloustein Local tech management report with implementation guidance. Released in 2015, it provides a overview to help organizations understand and manage technology risks. <http://blousteinlocal.rutgers.edu/managing-technology-risk/>
- [Employee Cyber Hygiene Training Options](https://njmel.org/wp-content/uploads/2018/04/Cyber-Hygiene-Vendor-Report_2-20.pdf), a 2018 report done for the Municipal Excess Liability Fund to assist government agencies in developing cyber hygiene training programs for employees. [https://njmel.org/wp-content/uploads/2018/04/Cyber-Hygiene-Vendor-Report\\_2-20.pdf](https://njmel.org/wp-content/uploads/2018/04/Cyber-Hygiene-Vendor-Report_2-20.pdf)

## 4. Technology Leadership Bytes



### **1. Regrettably, Most Successful Cybersecurity Attacks Can Be Traced to a Management Failure**

Cyberattacks enter a computer or network in two ways; through a user's computer (front door) or a hole or network weakness (back door). The types of attacks are many, but most front door attacks are preventable with sound employee cyber hygiene training, so employees avoid clicking on malware related links or files. Back door attacks are generally prevented by competent network management, routine log and permissions checking, and timely software patching. If management fails to provide adequate resources (e.g., financial, personnel, training, management time and attention) necessary to meet those goals, a successful attack can be traced back to that management failure. Of course, there are exceptions and variations, but most attacks can be avoided by employing this model.



### **2. Agency Leaders Are Not Cybersecurity Experts**

Agency leadership not expected to be cybersecurity experts, nor to plan and execute cyber security plans. That's the responsibility of the agency technology/cyber security experts/managers. Those individuals have the responsibility to assess agency cybersecurity risks and recommend responses to leadership as part of the planning/decision-making/budgeting cycle (and see Item #1 above!). Like most government services, unless they have specific knowledge of the field, those in leadership should avoid second guessing their experts' advice.



### 3. Challenges of Funding Technology

Traditionally, particularly in New Jersey local government, technology costs were treated as a capital cost (buying servers and desk/laptop computers that came loaded with software and licenses). As debt service, those costs are exempt from spending and tax levy caps. While hardware and its software can still be treated that way, today's software markets are less amenable to capital funding as more and more software and services are subscription based, requiring appropriation of operating funds.

But at this stage of technological evolution, tech funding needs to be integral to agency budgeting cycles; it is not a discretionary activity anymore. Then, it is a matter of putting tech (particularly cybersecurity) funding in the mix along with other spending such as employee salaries, insurance and utility costs, and the increases that come along with them, and making priority decisions accordingly (and see Item #1 above!).



### 4. Importance of Verifying Financial Accounts, Payroll, Vendor Direct Payment Changes.

Today, business email and related social engineering compromises are running rampant and the perpetrators are becoming proficient in fooling people. To prevent fraudulent financial transactions, under no circumstance should an email, phone call, online or mailed in form, or dropped off handwritten form authorize specific payments or transfers be made, direct deposit account numbers changed, or payment instructions changed or executed, unless there is some verification that the sender of the email or form was the actual person who sent the email and was authorized to do so.

In this case, *verification* means obtaining confirmation of the request via a separate email sent to a known email address (not using "reply"), or in the case of employee related actions, personal verification by a responsible employee that the employee actually initiated the action.



## PART TWO

# 5. The Minimum Technology Standards: An Overview

Since 2013, the N.J. Municipal Excess Liability Joint Insurance Fund (MEL) has provided its almost 600 local government agency members with cyber insurance coverage. As risks associated with the use of technology by municipalities and affiliated entities has evolved over time, so did the MELs interest in managing the risks.

In 2017 it embarked on a process to assist members in managing this evolving risk through the development of a set of minimum technology proficiency standards. The MEL partnered with the Bloustein Local Government Research Center at Rutgers University to develop standards. The effort was driven by a previous partnership between the MEL and Bloustein Local that developed a risk-management based approach to develop technology management proficiency.<sup>5</sup>

The result was the *MEL Cyber Risk Management Program* with minimum technology goals that fall into three categories of technological proficiency:

1. Achieve a minimum level of technical and cyber security competency with computers and networks;
2. Ensure that employees practice sound cyber hygiene; and
3. Ensure that members have basic technology management leadership, including the adoption of a basic plan to respond to a cybersecurity incident.

The MEL's implementation of the standards incentivized member compliance by offering complying members up to a 75% discount on cyber insurance deductible if a claim is filed.

The program has several goals: to decrease the agency's exposure to the most common technology/cybersecurity risks; plan for successful recovery from a security breach; reduce the potential for loss of critical data; increase awareness of cyber security with employees; and improve management capacity to make technology decisions.

While the standards are noted as minimums, the program identified that lying below the minimums are two basic elemental requirements that everything organization must have. These two requirements are pre-requisites to make survival possible given the risks posed by technology. They are: 1) *having access to an expert that can advise them on technology decisions*, and 2) *having data files and system software routinely backed up in the event they become inaccessible due to physical disaster or a successful cyber-attack*.

The minimum standards package tries to keep technical jargon to a minimum. However, those implementing it should be conversant with technology and it is recommended that the organization's technology expert be consulted on implementation. The expert needs to determine whether the organization is already in compliance with all or some of the program standards and/or what needs to be done to come into compliance. In the event the

<sup>5</sup> See the report on Technological Proficiency prepared for the MEL in 2015 at Bloustein Local: <http://blousteinlocal.rutgers.edu/managing-technology-risk/>



organization does not have a technology expert to advise it, that is Job One and should be resolved before moving on.

The standards are particularly targeted to smaller organizations. Medium and larger organizations should exceed them; if they do not, they are lacking proficiency in managing their technology and are exposing their organizations to unnecessary risks. Gaps in meeting these minimum standards should be addressed promptly; failure to do that in today's environment is arguably nonfeasance.

Some of the minimum standards involve little or no cost (i.e., activating Microsoft Defender software on Windows 10 machines meets the anti-virus requirements). Cloud-based services can also support data backup requirements (e.g., Microsoft Office 365, Google Office, subscription-based cloud backup). One item involves adopting a cyber-incident response plan (a customizable sample is included); if your organization has cyber-insurance coverage, this plan should be coordinated with the incident reporting elements of the policy.

To meet these goals, organizations may incur new one-time and ongoing expenses. This is a trade-off for reducing their security risk profile, improving their ability to respond to an event, and improving their overall technological proficiency.

**Because cybersecurity threats are always changing, "cybersecurity" is not a specific status.** These minimum standards cannot eliminate all cybersecurity and technology management risks. This set of standards is designed to mitigate the majority of cybersecurity risks. It provides an effective pathway to system and data recovery in the event of a cybersecurity incident. It also establishes a core of technology leadership elements. Organizations that meet this standard can and should work to improve their risk profile by taking other actions suggested in the program (Appendix 4).



Minimum  
back-up practices



Patch



Defensive software



Training



Incident  
response plan



Tech  
practices policy

## 6. Getting Started with the Minimum Standards

**Before starting, it is important to review this material with a technology expert.** Whether that person is an employee or an outside consultant, engaging the expert at the beginning of this process will make meeting the standards easier. In addition, each organization will have different considerations and approaches to meeting the standards. Some will already meet various standards, some more, some less. There is no one-size-fits-all plan when it comes to technology, but there are some minimum standards. The goal is to accomplish the following:

- Understand the risks
- Spend the time and attention to develop a plan to address the risks
- Appropriate funds to meet the needs, if necessary
- Manage the implementation
- Establish an ongoing process to review technology and your cybersecurity status.

These steps will get you started, caught up, or confirm your compliance:

1. If the agency does not have one, get a knowledgeable technology expert to provide advice to the governing body and senior management on implementing the *Minimum Technology Proficiency Standards* and technology issues in general. Senior management must have confidence in the expert's advice. The technology expert can be an existing employee, contractor, citizen committee, employee committee, or combination thereof. If not done prior to engaging a technology expert, ensuring computer systems and data are backed up in a way that meets the minimum technology

standard should be the top priority.

2. Have the technology expert review the agency's existing practices against the *Minimum Technology Proficiency Standards Chart* to determine the current status. If you already meet the standards, congratulations!
3. Once this review is complete, work with the expert to develop a plan, timetable, and budget to implement any standards not currently met. Have senior management and the governing body review and obtain their concurrence and funding commitment.
4. Put funding in place, if necessary, and move forward with implementation.
5. Establish a process to periodically (at least annually) review the technology issues (and consider a formal plan).
6. Don't stop here. Conduct a technology risk assessment. Based on the agency's technological sophistication and risks, there are additional risk mitigation activities that can be taken. See Appendix 4 for details.

Want to learn more about technology risks? See the work done by the Bloustein Local Government Research Center on Technology or the MEL Cyber Risk Control webpage:

- Bloustein Local Technology Risks: <http://blousteinlocal.rutgers.edu/managing-technology-risk/>
- NJMEL Cyber Risk Management Plan: <https://njmel.org/mel-safety-institute/resource-center/public-officials/public-officials-cyber-risk-control/><sup>6</sup>

<sup>6</sup> The MEL's plan divides the Standards into two tiers and applies improved cyber insurance benefits to those places that meet both tiers. This document combines the two tiers into one and makes modifications in other elements that were specific to the MEL's environment.

# 7. Minimum Technological Proficiency Standards

Subject	Requirement	Comment
<b>A. TECHNICAL COMPETENCY</b>		
<b>Minimum back-up practices</b>	<ol style="list-style-type: none"> <li>1. <b>Daily incremental backups</b> or the use of standardized system images or virtualized desktops, with at least 14 days of versioning on off-network device for data files.</li> <li>2. <b>Weekly off-network full backups</b> of all devices:                             <ol style="list-style-type: none"> <li>a. Use of non-versioned, synchronized cloud-based drives are not acceptable as backup solutions. Cloud-based drives used for backup must have a minimum of 14 days of versioned files.</li> <li>b. A full backup of non-networked/standalone (desk and laptop) computers must include all storage drives. <b>Alternative:</b> consult with technology professional to assess and make recommendations for agency backup needs.</li> </ol> </li> <li>3. All backups are spot-checked monthly.</li> <li>4. Consult with third party application providers to ensure their data files are part of a backup practice.</li> <li>5. Set the practice as a formal policy, implement and maintain it.</li> </ol>	<p>“Versioning” is where a backup system stores multiple copies of files going back in time. This permits a file encrypted by ransomware to be recovered by going to an earlier version of it.</p> <p>Cloud-based backup solutions include services such as Carbonite, Barracuda, Backblaze, and Crashplan that include several weeks of versioning or similar ransomware protection.</p> <p>Most Office 365 and Google Drive users have at least 14 days of versioning for data files; but it should be verified as being active before using it as a backup plan. If these are used, a separate backup or imaging plan for system and applications files must be in place.</p>
<b>Patch</b>	<p>Adopt a <b>Patch Management Policy</b> for all operating and application software that balances cybersecurity, vulnerabilities and operational needs (use automatic updating where practicable); particularly as related to security patches. Outdated or non-supported operating systems and software are not used.</p>	<p>Security patches should be applied immediately unless testing shows the patch will create application problems. System administrators need to coordinate patch upgrades with applications residing on systems managed by third parties to ensure upgrades will not disable their applications.</p>
<b>Defensive software is used and regularly updated</b>	<ol style="list-style-type: none"> <li>1. For all desktops and laptops: antivirus and firewall enabled</li> <li>2. Mail server: antispam and anti-virus filters</li> <li>3. For network servers that connect to the internet: firewall on all active ports; unused ports closed; and anti-virus and anti-malware software active</li> <li>4. Microsoft Office applications open all downloaded files in “Protected Mode”</li> </ol>	<p>Microsoft Windows 10 includes a built-in firewall (as do earlier versions) and anti-virus software. Third party applications that incorporate combinations of defensive software are available commercially.</p>
<b>Server security</b>	<p>Servers are physically protected from access by unauthorized individuals.</p>	<p>Can be in a cage, locked cabinet (with sufficient airflow), or air-conditioned room where only authorized users have access.</p>
<b>Access privilege controls are in place</b>	<ol style="list-style-type: none"> <li>1. Users with administrator rights are limited to those that need them</li> <li>2. Users only have access only to those services they need</li> <li>3. Access rights are removed when no longer needed or immediately when an employee separates from service</li> <li>4. Access rights are periodically reviewed</li> </ol>	

Subject	Requirement	Comment
<b>A. TECHNICAL COMPETENCY</b>		
<b>Technology support</b>	Staff or contractors are regularly trained, <b>available to support the agency's technology</b> , and respond to security incidents.	
<b>B. SOUND CYBER HYGIENE</b>		
<b>Training</b>	All computer users receive <b>annual training</b> of at least one hour per year. Training includes but is not limited to malware identification (email and websites), password construction, identifying security incidents, and social engineering attacks.	The training can be online, in person lecture or other effective training resource.
<b>Policies</b>	The organization adopts sound government internet and email use <b>Policies</b> .	
<b>Protect Information</b>	Files with personally identifiable and protected health information are <b>password protected or encrypted</b> .	This has specific relevance to human resource and health information.
<b>Password strength</b>	Employees are required to use <b>strong, unique passwords</b> , changed at least annually	<b>Passphrases</b> with at least 9 characters with upper- and lower-case letters and incidental numbers and symbols are highly recommended.
<b>C. TECHNOLOGY LEADERSHIP</b>		
<b>Leadership has expertise</b>	Organization leadership has access to expertise that supports technology decision making (i.e., risk assessment, planning, and budgeting). This should be exercised through a coordinated planning, decision-making, and budgeting process.	This can be any combination of officials, employees, contractors/consultants, or citizen volunteers as appropriate to the organization.
<b>Incident Response Plan</b>	Management/Governing Body adopts a basic cybersecurity incident response plan to direct staff and guide technology management decision making when a cybersecurity incident takes place.	Appendix 3 is a sample plan that is tied to typical cyber insurance coverage program. It should be modified to reflect local circumstances.
<b>Technology Practices Policy</b>	Management/Governing Body adopts a basic Information Technology Practices Policy that outlines the agency's commitment to sound cyber security practices and technology management practices.	Appendix 1 and 2 are guidance and a sample Tech Practices policy that is consistent with the Minimum Standards.

## Appendix 1

# Model Information Technology Practices Policy Implementation Notes

- 1) Appendix 2 is the *Model Information Technology Practices Policy* (Model Policy), a minimum policy template that is consistent with the Minimum Technological Proficiency Standards.
- 2) This assumes that the organization already has basic policies related to Appropriate Use of internet and Email Resources. If not, they are necessary to the organization. Sample policies are readily available from professional government organizations, insurers, or the SANS Institute at [www.sans.org/security-resources/policies/general](http://www.sans.org/security-resources/policies/general); general internet searches for policies will display ones from many different organizations.
- 3) **Organizations are encouraged to amend the model policy to reflect or extend their own practices.** Policies not consistent with, or which do not exceed the model policy do not meet the Minimum Standard.
- 4) The policy includes several terms and phrases that need to be edited to reflect each organization's specific organization and practices. They are all italicized and enclosed in *<brackets>*. The document should be carefully edited prior to adoption to replace those terms with ones appropriate to the organization.
- 5) The backup policy in Section A of the Minimum Standards is highly technical in nature, but its importance is highlighted by formalizing backup practices as a policy. Prior to adopting the policy, it should be adjusted to reflect the organization's specific backup practices; keeping in mind, the practices describe a minimum. It is recommended the advice of a technology expert be obtained to ensure the backup practice meets the agency's needs.
- 6) Elected officials and chief administrators should take careful note of the practices in Section C of the Minimum Standards, as they relate to the processes used to make technology decisions.
- 7) Appendix 3 is a Cybersecurity Incident Response Plan to fulfil that element (in Section C) of the Minimum Standard requirement. This template should be the starting point for the adoption of a plan. It should be adapted to reflect local practices, but if the organization has a cyber insurance or related liability policy, it should be adapted to be consistent with the policy's requirements, and when and how the carrier is notified to ensure the engagement a breach coach and timely computer forensics engagement.
- 8) Underlying the Model Policy is an assumption that individuals will be named to ensure the practices are implemented and maintained. While the term "information technology manager" is sometimes used, the organization should carefully consider who, either employee(s), contactor(s), or a combination thereof, are given responsibilities to implement specific practices.
- 9) To the extent that some practices are not currently in place, the policy can include target dates for their implementation. A planned, but not implemented practice will not meet eligibility for the deductible reimbursement. Overnight implementation is not practical, but planned and focused implementation should be the practice.
- 10) **Keeping up-to-date:** In addition, all organizations should have their technology expert join the MS-ISAC at [www.cisecurity.org/ms-isac/](http://www.cisecurity.org/ms-isac/), a federally funded program that provides a range of cybersecurity services for local government agencies. There is no cost to join MS-ISAC, except a resolution of the governing body is required. A local government agency should also consider joining GMIS, the association of local government IT managers.

## Appendix 2

# Model Information Technology Practices Policy

### <Agency Organization Name>

**Purpose:** To establish as policy certain information technology practices.

#### A. Technical Operations

**1. System and data back-up practices:** <Name of organization> will implement backup practices that meet the following as a minimum standard or will implement recommendations of a qualified information technology expert who, after consideration of <name>'s information technology needs, recommends an alternative, which shall be fully documented.

- a) Daily incremental backups or the use of standardized system images or virtualized desktops, with at least 14 days of versioning on off-network device for data files
- b) Weekly off-network full backups of all devices:
  - a. Use of non-versioned, synchronized cloud-based drives are not acceptable as backup solutions. Cloud-based drives used for backup must have a minimum of 14 days of versioned files
  - b. A full backup of non-networked/standalone desk and laptop computers must include all storage drives
- c) All backups are spot-checked monthly
- d) Consult with third party application providers to ensure their data files are part of a backup practice

**2. Security and system patching:** all operating, and application software shall be updated on a timely basis with latest versions as released, particularly as related to security updates. Outdated or non-supported operating systems and software shall not be used unless there is no practical alternative available, in which case, appropriate steps shall be taken to mitigate potential security threats. System administrators shall coordinate patching with applications maintained or managed by third parties to ensure upgrades will not disable their applications. When upgrades cannot be applied, appropriate action shall be taken to prevent the system or application from security exploitation.

**3. Defensive software** shall be installed and operative on all computing devices as follows:

- a) For all desktops and laptops devices: antivirus and an enabled firewall
- b) Mail server: anti-spam and anti-virus filters
- c) For network servers that connect to the internet: an active firewall on all open ports, unused ports closed; and anti-virus, anti-malware software running
- d) All Microsoft Office applications are set to all downloaded files in "Protected Mode"



**4. Server security:** all servers are protected from unauthorized access by means of a secured cage, locked cabinet (with sufficient airflow) or other physically secure means to ensure that only authorized users have access to it.**5. Access privilege controls and policies** are in place and maintained to ensure that: 1) users with administrator rights are limited to those that need them; 2) that other users only have access to those services they need for day-to-day activities; 3) that access is removed when it is no longer needed or when an employee separates from service; and 4) access rights are periodically reviewed to ensure compliance.

<Human resources officer> shall work with <information technology manager> to ensure that system access needed by new employees is provided on a timely basis, and that notice of termination of employees is provided and acted upon by <information technology manager> prior to notice provided to the employee.

**6. Security Incident response:** Appropriately trained staff or contractors are available to support <name>'s technology and to timely respond to security incidents.

## **B. Employee-based Cyber Security Practices**

1. All computer users shall receive annual training of <at least> one hour, <each year or spread over two years> in email and website malware identification, password construction, identifying security incidents, and social engineering attacks.
2. Employees are required to use unique passwords or passphrases made up of at least 9 characters, changed periodically, but at least annually. Passwords/phrases shall be at least 9 alpha-numeric characters, with incidental upper- and lower-case letters and symbols.
3. Files that contain protected data shall be password protection or be encrypted when the files are stored or transferred to others, regardless of the storage medium or means of transfer. Examples of protected data includes social security numbers, birthdates, driver's license number, health insurance numbers, etc. Practices shall include ensuring that more than one employee is aware of the password or passphrase used to encrypt these files.

## **C. Technology Management Practices**

1. <Mayor and Governing Body> shall ensure that technology policy decisions (i.e., risk assessment, planning, and budgeting) are made with input from staff or advisors that possess appropriate technological expertise. This can be any combination of officials, employees, contractors/consultants, or citizen volunteers as they determine necessary.
2. <Chief administrative officer or Governing Body> shall approve and implement a cybersecurity incident response plan to direct staff and guide IT management decision making when a cybersecurity incident takes place.

## Appendix 3

# Minimum Security Response Plan for Cybersecurity Incidents

**If you suspect a cyber incident has taken place, start your incident response plan.**

*This plan is a minimum. It should be modified to reflect organization-specific circumstances, but it must be consistent with any cyber insurance policy in place.*

### **What is a Cybersecurity Incident?**

For cyber insurance purposes, a **security incident** is an event that is a: **cyber security breach**, or **cyber extortion threat**, or **data breach**.

**What is a Cyber Security Breach:** Any unauthorized: access to, use or misuse of, modification to the network, and/or denial of network resources by attacks perpetuated through malware, viruses, worms, and Trojan horses, spyware and adware, zero-day attacks, hacker attacks and denial of service attacks.

**What is a Cyber-Extortion Threat:** A threat against a network to:

1. disrupt operations;
2. alter, damage, or destroy data stored on the network;
3. use the network to generate and transmit malware to third parties;
4. deface the agency's website; and
5. access personally identifiable information, protected health information or confidential business information stored on the network;

made by a person or group, whether acting alone or in collusion with others, demanding payment or a series of payments in consideration for the elimination, mitigation or removal of the threat.

**What is a Data Breach:** A data breach is the actual or reasonably suspected theft, loss or unauthorized acquisition of data that has or may compromise the security, confidentiality and/or integrity of personally identifiable information, protected health information, or confidential business information.

Employees require training to understand what a security incident is, what they might observe if one is happening, and how to report it. For example, a security incident could include appearance of a ransomware attack screen, the mouse or computer screen acting on its own, an unauthorized user accessing a computer, not being able to access routine services, device theft, or finding a damaged or non-operating computer.

Other security incidents that would be noticed by system administrators include:

- Attempts from unauthorized sources to access systems or data
- Unplanned disruption to a service or denial of a service
- Unauthorized processing or storage of data
- Unauthorized changes to system hardware, access rights, firmware, or software
- Presence of a malicious application, such as ransomware or a virus
- Presence of unexpected/unusual programs
- A denial of service condition against data, network or computer



## Responding to a Security Incident

### Prerequisites to managing a security incident:

- a) The agency has access to technology (tech) support personnel (employee or contractor) that understands how to recognize and respond to security incidents.
- b) Management knows how to contact tech support when a security incident occurs.
- c) Staff has received instruction on how to identify a potential security incident and how to contact tech support when one happens.
- d) Management establishes a chain of command for staff to report a potential security incident.
- e) It is strongly advised that tech support develops a detailed security incident response plan tied to the agency's technology risks.

## What to Do When a Possible Security Incident Takes Place

1. The user aware of a possible security incident should identify the affected device(s) (individual machines or network equipment) and:
  - a) Immediately contact tech support to report the event and follow their instructions. It is now the responsibility of tech support to notify management of the incident and to execute the security incident response plan.
  - b) Continue with Step 2 if tech support is not immediately available.
2. Isolate the affected devices from the network or internet by removing the network cable from the device. If operating via wireless, turn off the wireless connection. Turn the equipment off if tech support is not immediately available or isolation is not possible. If the machine will not let you do that, unplug the power supply.
3. User reports the incident to management.
  - a) If technology support has not been contacted management by this time, management must communicate with support, advise them of the situation, and engage them in the matter.
4. Management or tech support assesses if the incident is a **cyber security breach, cyber extortion threat, or data breach. If it is, or if there is any question that the incident may or may not be one**, management contacts their liability insurance agent. If cyber insurance coverage is in place, follow the incident reporting and response instructions of the carrier.
5. Advise the agency's risk manager, legal counsel, chief operating officer, and chief executive officer (i.e., Mayor, Commission Chair, etc.) of the event and actions taken.
6. Follow advice technology personnel until the issue is resolved.
7. Document all actions as they are taken.

## Appendix 4

### Additional Security Practices to Consider

Subject to adequate budgeting and staffing resources, there are additional technological enhancements that organizations can implement to help reduce their cybersecurity and technology risks. They are also highly recommended for any organization that has a technology staff.<sup>7</sup> These practices include the following suggested actions:

- a) Conduct a security review of third party vendors
- b) Conduct and maintain an inventory of authorized and unauthorized devices
- c) Servers are protected from environmental hazards
- d) Conduct and maintain an inventory of authorized and unauthorized software and whitelisting of approved software
- e) Implement basic internet content filtering
- f) Ensure that a firewall protects the <agency>'s Wi-Fi network from any public Wi-Fi network
- g) Employees receive a total of one hour of annual cyber hygiene training
- h) Implement and maintain the CIS Critical Security Controls (<https://www.cisecurity.org/controls/>)
- .
- i) <For agencies with sophisticate profiles> Consider adopting the NIST Cybersecurity Framework as part of their technology planning practices ([www.nist.gov/cyberframework](http://www.nist.gov/cyberframework))

<sup>7</sup> Including agencies with managed or sophisticated technology profiles.

# MEL Cyber Insurance Reimbursement Plan



- ◆ \$10,000 standard claim deductible
- ◆ \$5,000 reimbursement if TIER 1 requirements are met
- ◆ \$7,500 reimbursement if TIER 1 & 2 requirements are met



## Tier | Technical Competency | Cyber Hygiene | Tech Management

1



Minimum back-up practices



Training



Incident response plan



Patch

Details at:  
[njmel.org/index.php/58-technology-risk](http://njmel.org/index.php/58-technology-risk)



Tech practices policy



Defensive software

2



Controlled server access



Policies



Leadership has expertise



Access privilege controls



Protect information



Technology support



Password strength

## Plus - Improve Your Technical Competency With... |

## Brought to You By

+

- ◆ Safe and secure servers
- ◆ Third party risk assessments
- ◆ Device inventory
- ◆ Software inventory
- ◆ Secure internet usage
- ◆ Wi-Fi controls
- ◆ Additional training
- ◆ Controls and Frameworks



NJ Municipal Excess Liability Joint Insurance Fund



RUTGERS

Edward J. Bloustein School of Planning and Public Policy

# RUTGERS

Edward J. Bloustein School  
of Planning and Public Policy

Bloustein Local Government Research Center  
Rutgers, The State University of New Jersey  
33 Livingston Avenue  
New Brunswick, N.J. 08901

p. 848-932-2830      [blousteinlocal.rutgers.edu](http://blousteinlocal.rutgers.edu)

© 2020, Rutgers, The State University of New Jersey