Cybersecurity: Threats, Prevention and Preparation

Phil Bertolini
Co-Director, Center for Digital Government

CENTER FOR DIGITAL GOVERNMENT

Phil Bertolini

Co-Director, Center for Digital Government

CENTER FOR DIGITAL GOVERNMENT

Agenda

- Cybersecurity Issues & Trends
- Cybersecurity Mitigation Tactics
- Where to Start & Cybersecurity Resources
- Virtual Q&A

CENTER FOR DIGITAL GOVERNMENT

Cyber Security Issues and Trends

CENTER FOR DIGITAL GOVERNMENT

Not logged in Talk Contributions Create account Log in

Article Talk | Read Edit View history | Search Wikipedia

WIKIPEDIA
The Free Encyclopedia

Main page
Contents
Featured content
Current events
Random article
Donate to Wikipedia
Wikipedia store

Interaction

Help
About Wikipedia
Community portal

Wiki Loves Love: Documenting festivals and celebrations of love on Commons.
Help Wikimedia and win prizes by sending photos.

2018 Atlanta cyberattack

From Wikipedia, the free encyclopedia

This page's infobox may require expansion, verification, or otherwise need cleanup. Please make sure that the infobox meets Wikipedia's guidelines for infoboxes. There might be relevant comments on the talk page. You may also want to view the infobox template page to view the full parameter list and read guidance on usage of that infobox. *(November 2018)*

The city of Atlanta, Georgia was the subject of a **massive cyberattack** which began in March 2018.[2] The city recognized the attack on Thursday, March 22, 2018,[1][3] and publicly acknowledged it was a e attack.

nta's national importance as a transportation and economic hub, the attack received wide and was notable for both the extent and duration of the service outages caused. Many city d programs were affected by the attack, including utility, parking, and court services.[5] City re forced to complete paper forms by hand.[6]

ber 26, a grand jury indicted two Iranian hackers, Faramarz Shahi Savandi and Mohammad h Mansouri, for the attack. The Department of Justice alleged that Savandi and Mansouri are SamSam group; that the SamSam group is based out of Iran; and that the pair created ansomware, the malware used in the attack. There are no affiliations with the government of

2018 Atlanta cyberattack

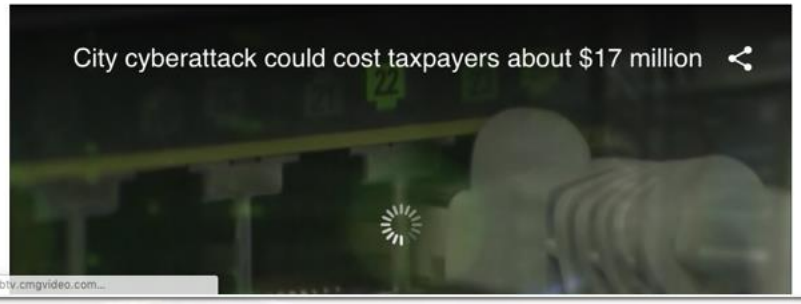
Date	22 March 2018[1]
Location	Atlanta, Georgia, United States
Type	Cyberattack
Theme	Ransomware encrypting files with $51,000 demand (via Bitcoin)
Cause	SamSam Ransomware
Outcome	Multiple municipal services down, including databases and wi-fi Years' worth of data destroyed City spends $2.7 million in recovering services

AJC

40° Search

News Politics County by County Things to do Life Sports More Subscribe Now Log in

CONFIDENTIAL REPORT: Atlanta's cyber attack could cost taxpayers $17 million



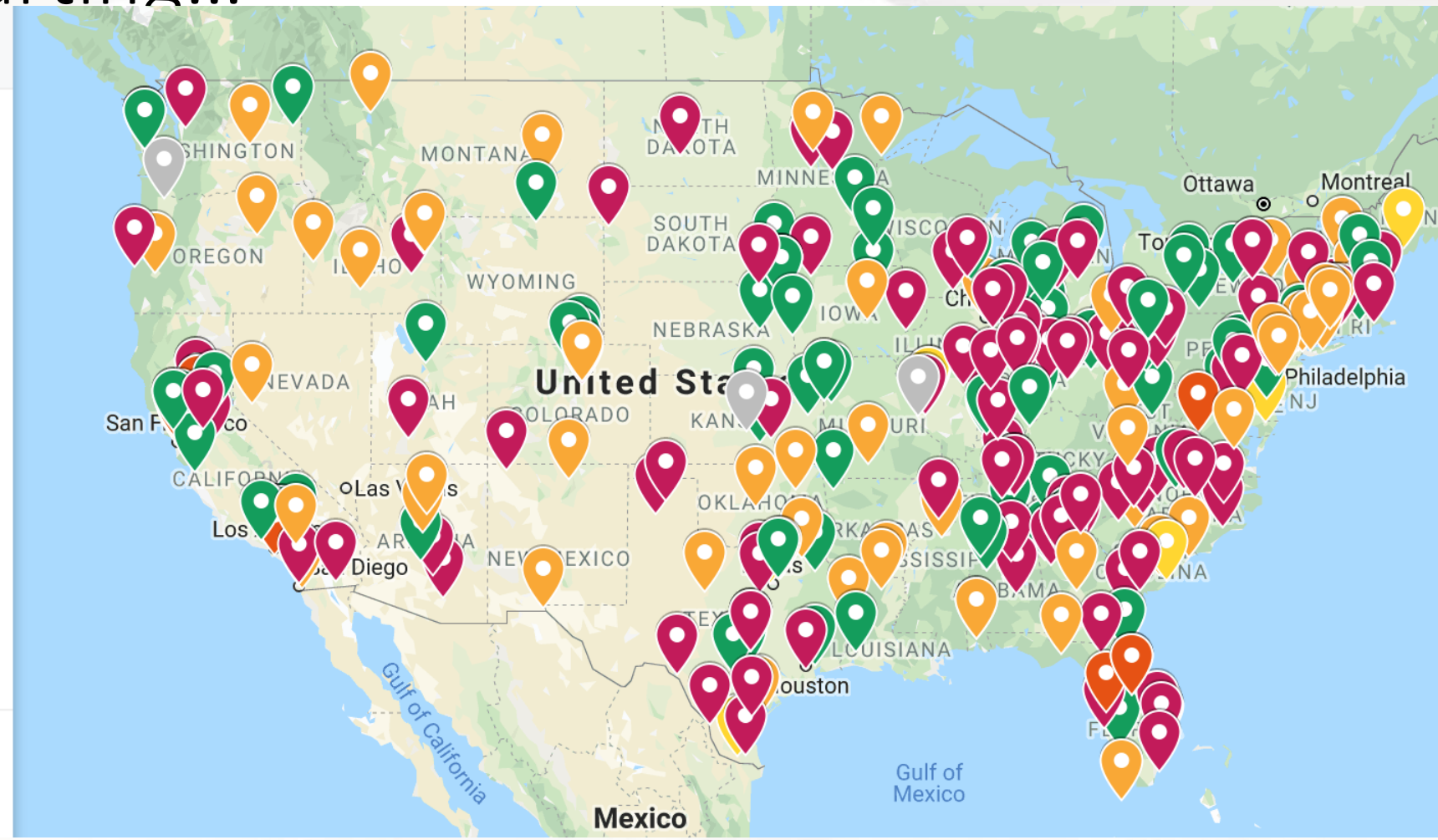
CENTER FOR DIGITAL GOVERNMENT

And It’s Just Starting…

SHARE

Ransomware Map

- Municipality
- Medical
- Education
- Other
- Law Enforcement
- Federal Government
- Other / No data



Data Source: The Ransomware War by PC Matic

CENTER FOR DIGITAL GOVERNMENT

Community cybersecurity will become a new government service.

CENTER FOR DIGITAL GOVERNMENT

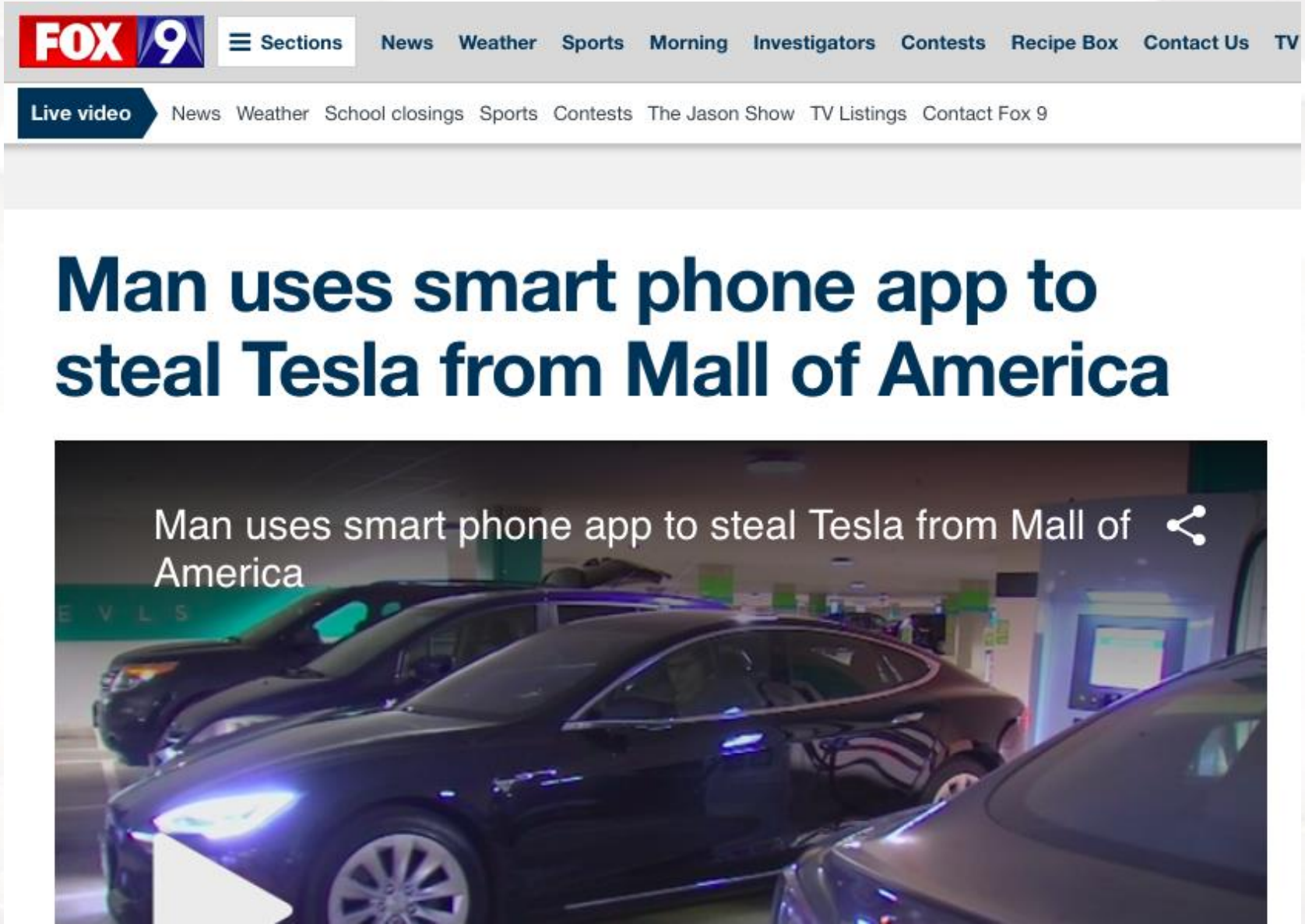
51,471 views | Sep 25, 2016, 10:00am

How Hacked Cameras Are Helping Launch The Biggest Attacks The Internet Has Ever Seen

Thomas Brewster Forbes Staff
Security
I cover crime, privacy and security in digital and physical forms.

The Rio Olympics was targeted with epic DDoS attacks, but shrugged them off. But attacks are getting bigger, sites are falling and voices being silenced. / AFP / Odd ANDERSEN (Photo credit

From IoT-enabled cars…



CENTER FOR DIGITAL GOVERNMENT

Smart Cities, Big Problems? The Risk of Malware in IoT-Enabled Infrastructure

April 27, 2017 @ 6:31 AM

T

Cities are notoriously inefficient. As populations rise, everything from mass transit and road maintenance to power generation and garbage collection becomes more complex and costly. Beyond ballooning budgets, there's also a push among residents for smarter services driven by Internet of Things (IoT)-enabled infrastructure.

Why drive around aimlessly in search of a parking spot when sensor-enabled apps could simply point users in the right direction? Why leave streetlights on when they're not needed, or

Pushing Cybersecurity To The Top of IT Priorities

CENTER FOR DIGITAL GOVERNMENT

2020 County CIO Priorities

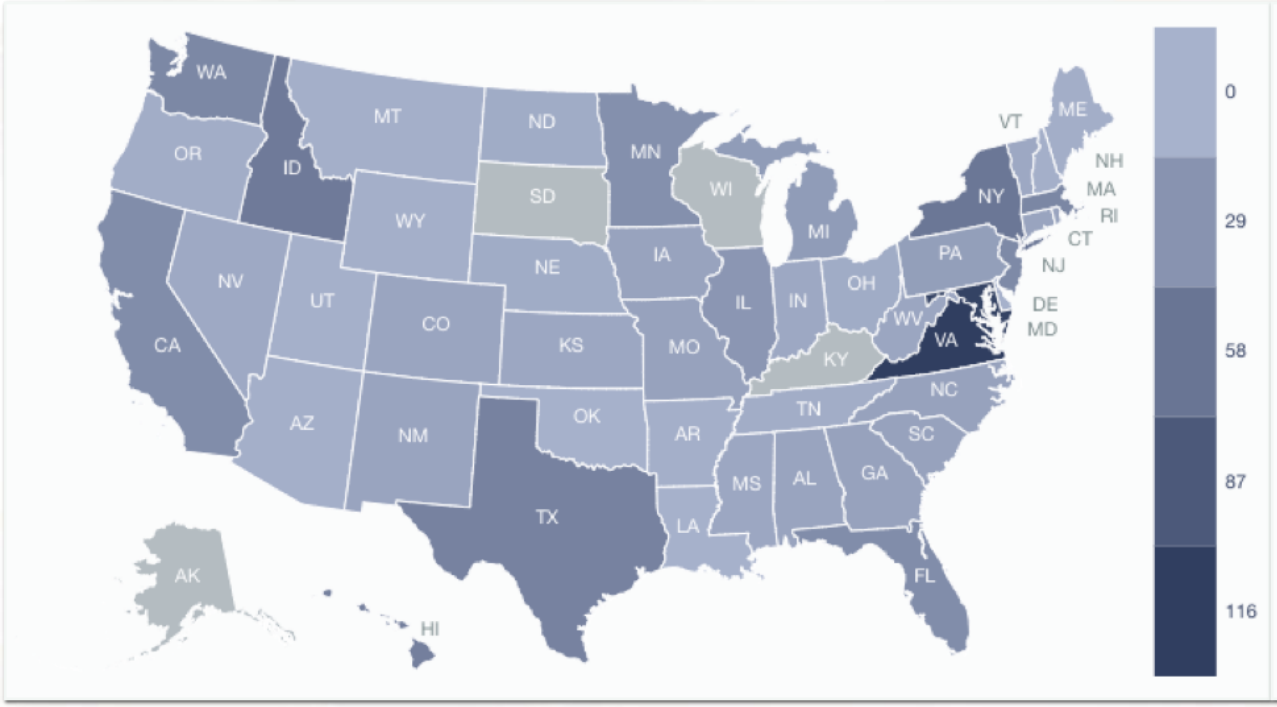
1. Cybersecurity
2. Citizen Experience/E-Services provision
3. Hire and Retain IT Personnel
4. Business Intelligence/Analytics
5. Disaster Recovery/Continuity of Operations
6. Data Governance
7. Infrastructure Modernization
8. Cloud Computing
9. Budget and Cost Control/Increased Agency/ Department/IT Collaboration
10. Shared or Collaborative Services

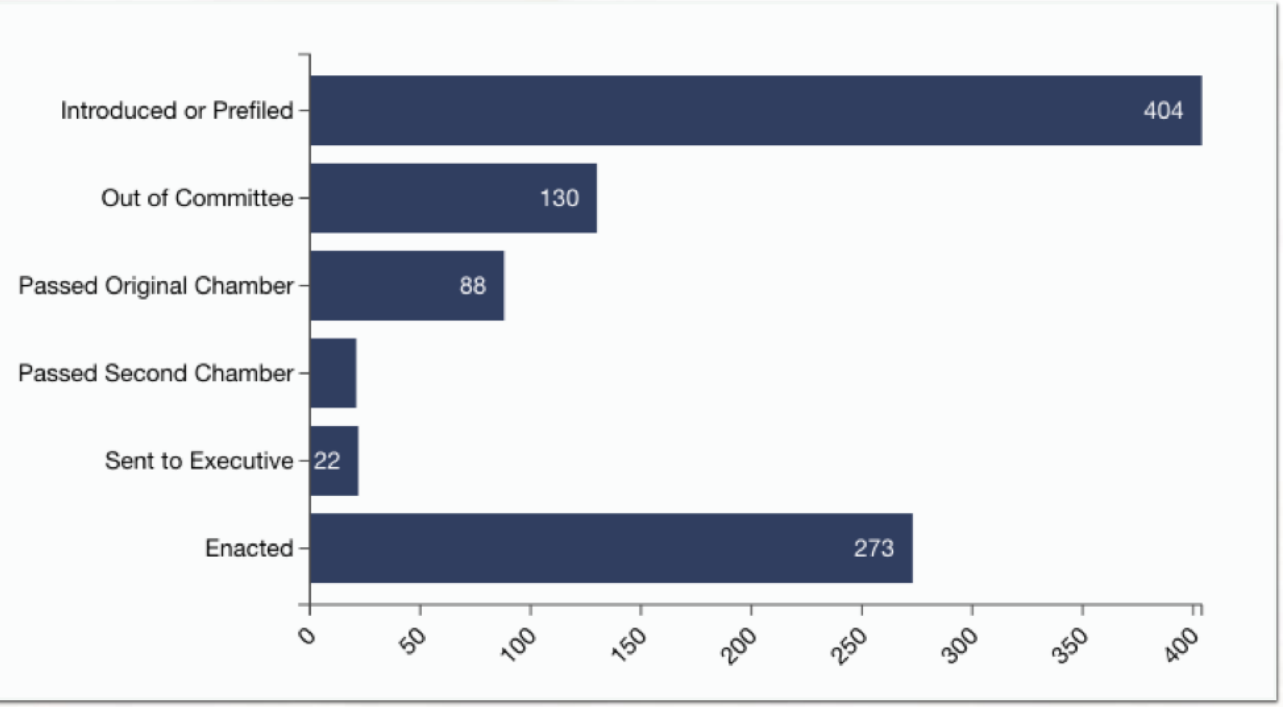
Source: Center for Digital Government 2020

CENTER FOR DIGITAL GOVERNMENT

And forcing legislators to respond…

Cybersecurity





Data Source: Quorum

CENTER FOR DIGITAL GOVERNMENT

Evolving cybersecurity to a
function that spans beyond government walls.

CENTER FOR DIGITAL GOVERNMENT

SECURITY

Arizona Governor Launches Cybersecurity Task Force

The Arizona Cybersecurity Team, created by an executive order on March 1, is expected to foster a collaborative approach to cybersecurity and education throughout the state.

BY THEO DOUGLAS / MARCH 2, 2018

State + Business Task Force

State of Arizona

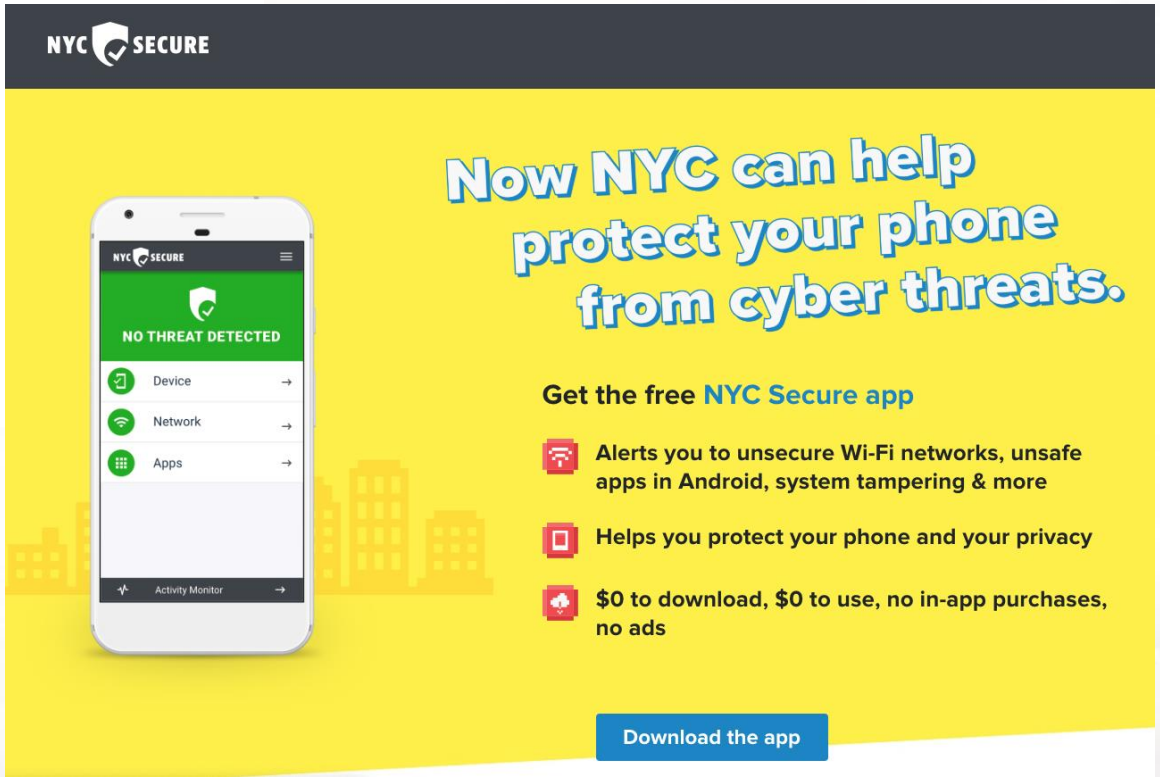
CENTER FOR DIGITAL GOVERNMENT

Mayor de Blasio Announces NYC Secure, The City's First-Ever Cybersecurity Initiative to Protect New Yorkers Online

March 29, 2018

Free smartphone app to launch this summer and new security for public Wi-Fi networks deploying now

NEW YORK – Mayor de Blasio today announced the launch of *NYC Secure*, a pioneering cybersecurity initiative aimed at protecting New Yorkers online. Using a steadily evolving suite of solutions, *NYC Secure* will defend New Yorkers from malicious cyber activity on mobile devices, across public Wi-Fi networks, and beyond. The first *NYC Secure* programs will include a free City-sponsored smartphone protection app that, when installed, will issue warnings to users when suspicious



Citizen Cybersecurity

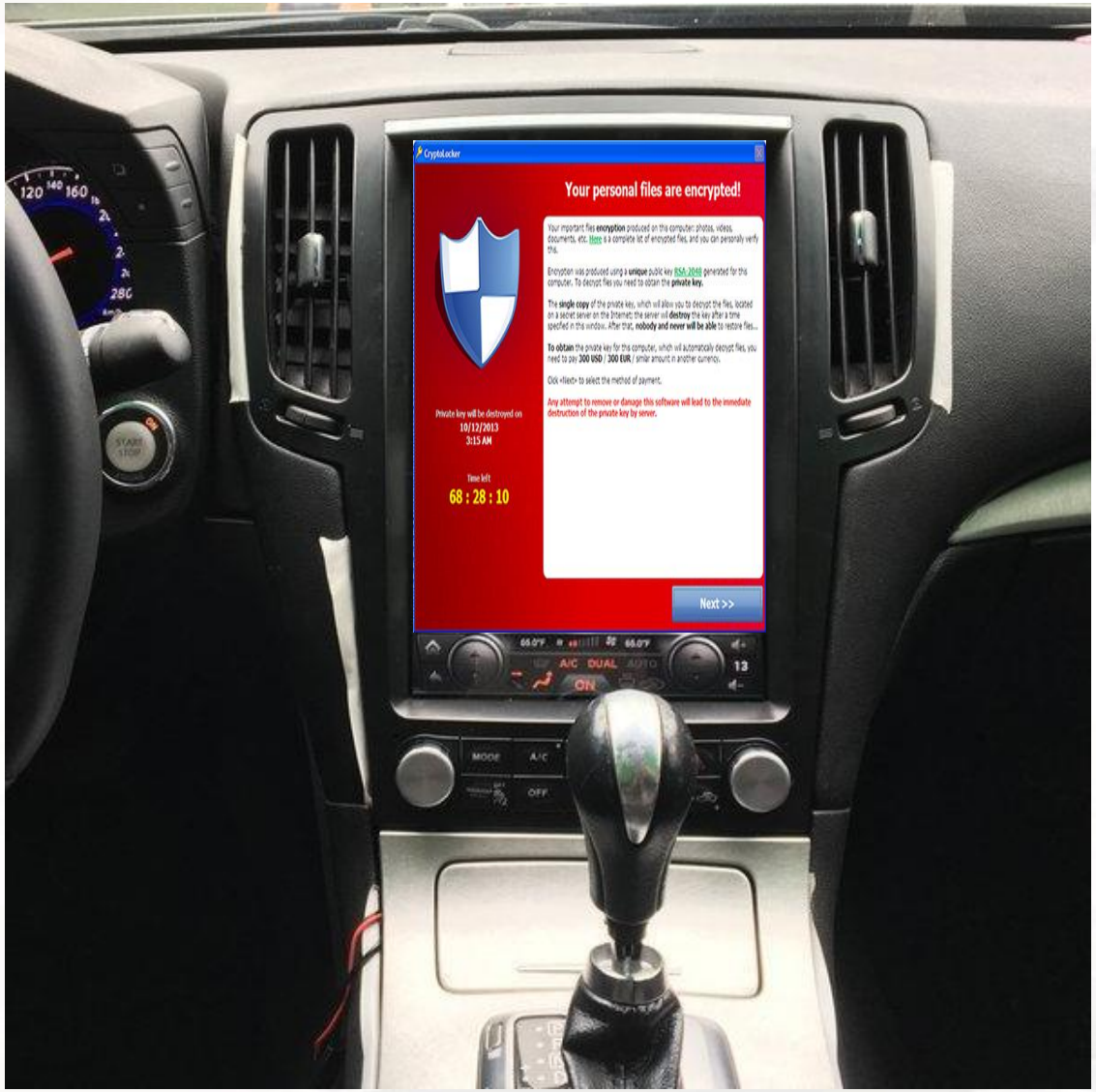
New York City, NY

CENTER FOR DIGITAL GOVERNMENT

Cybersecurity predictions for the future.

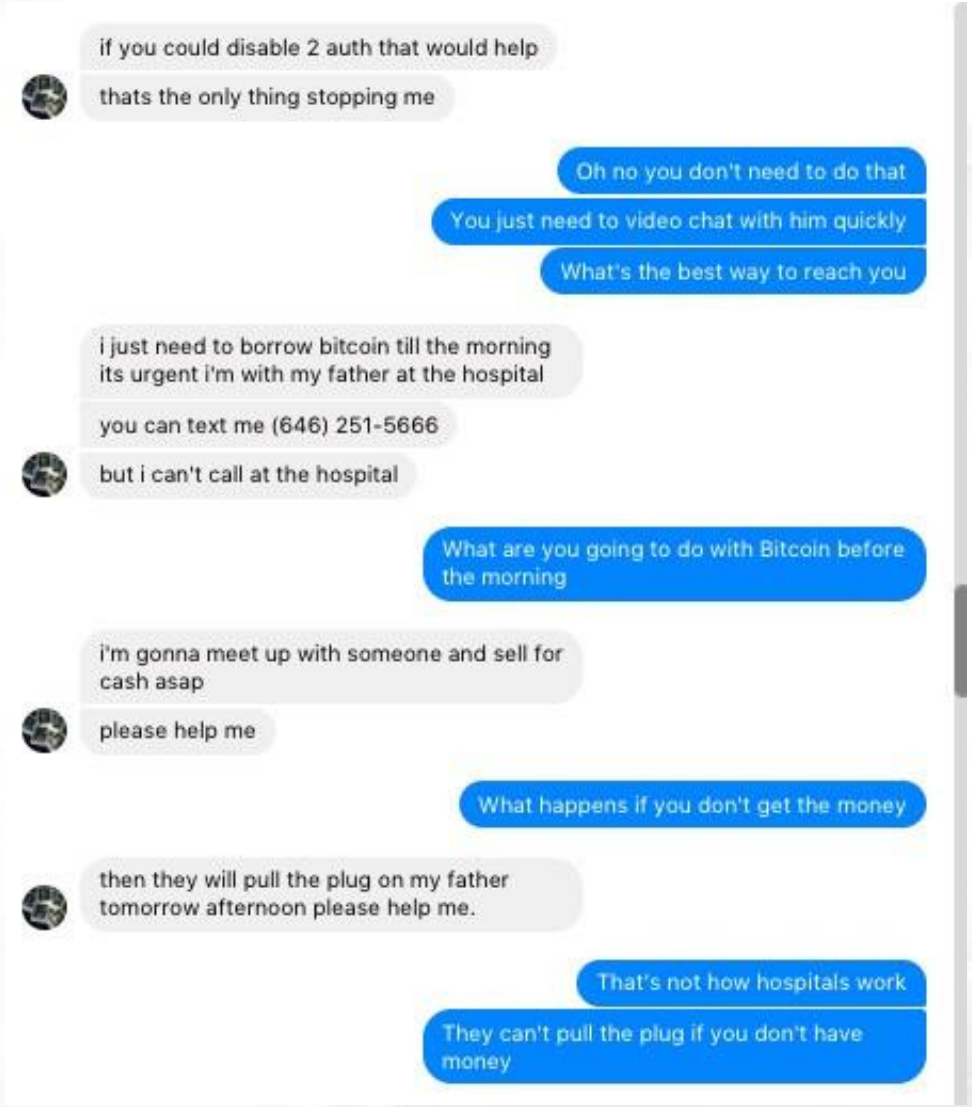
CENTER FOR DIGITAL GOVERNMENT

Ransomware will have a **bigger impact** on consumers.



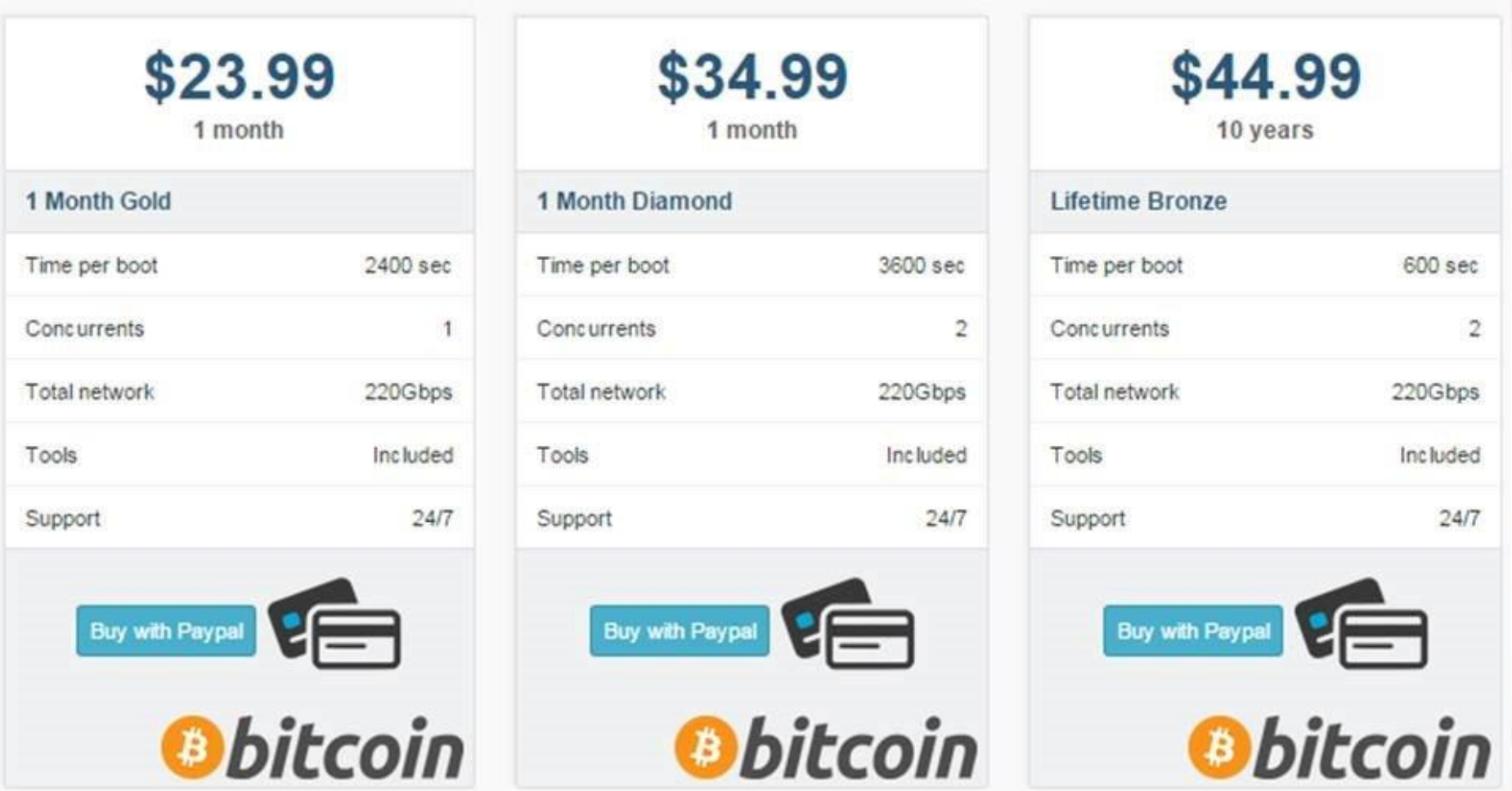
CENTER FOR DIGITAL GOVERNMENT

Social engineering will leverage **Artificial Intelligence.**



CENTER FOR DIGITAL GOVERNMENT

Cyber attack tools will get **exponentially easier and cheaper** to use.



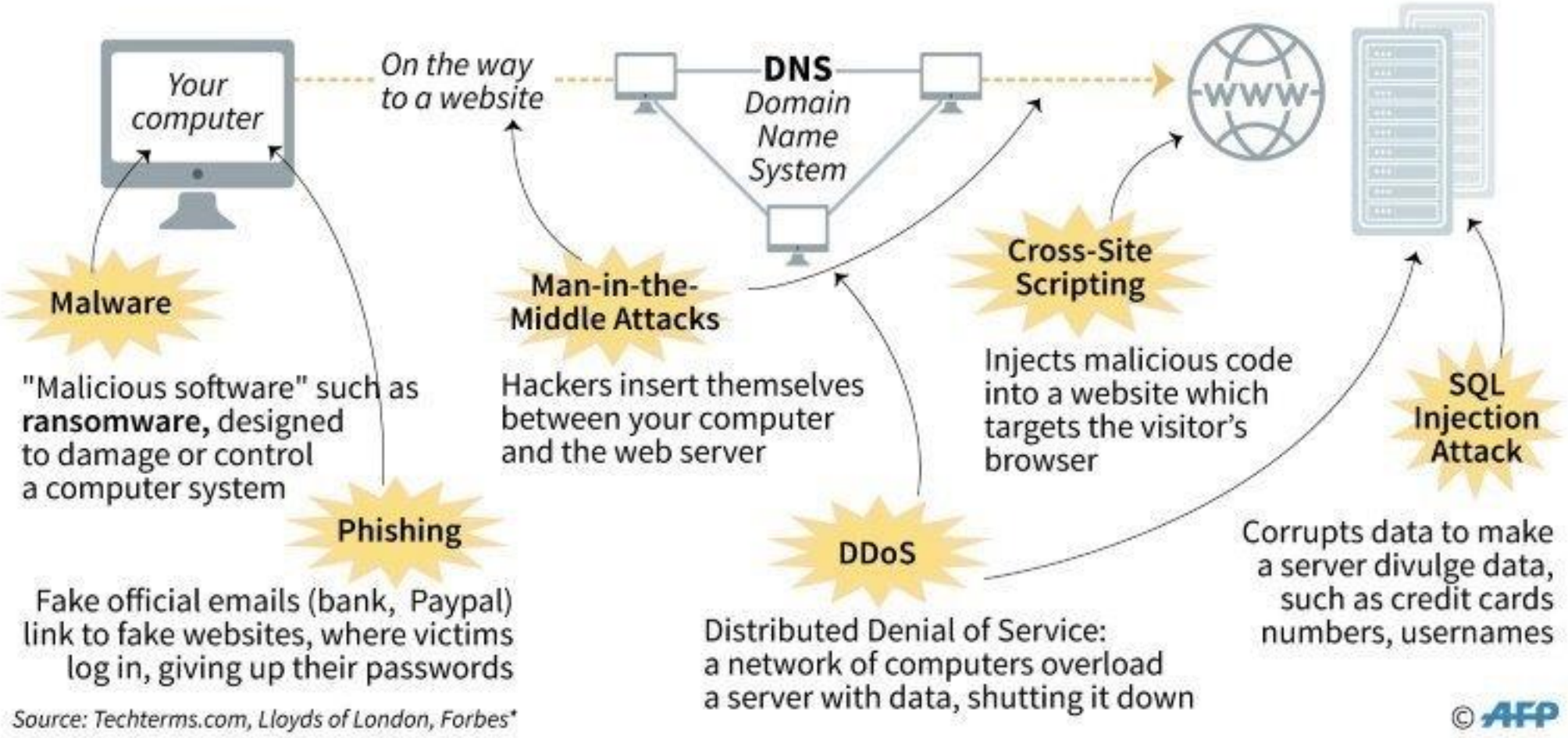
CENTER FOR DIGITAL GOVERNMENT

Types of Cyber Attacks

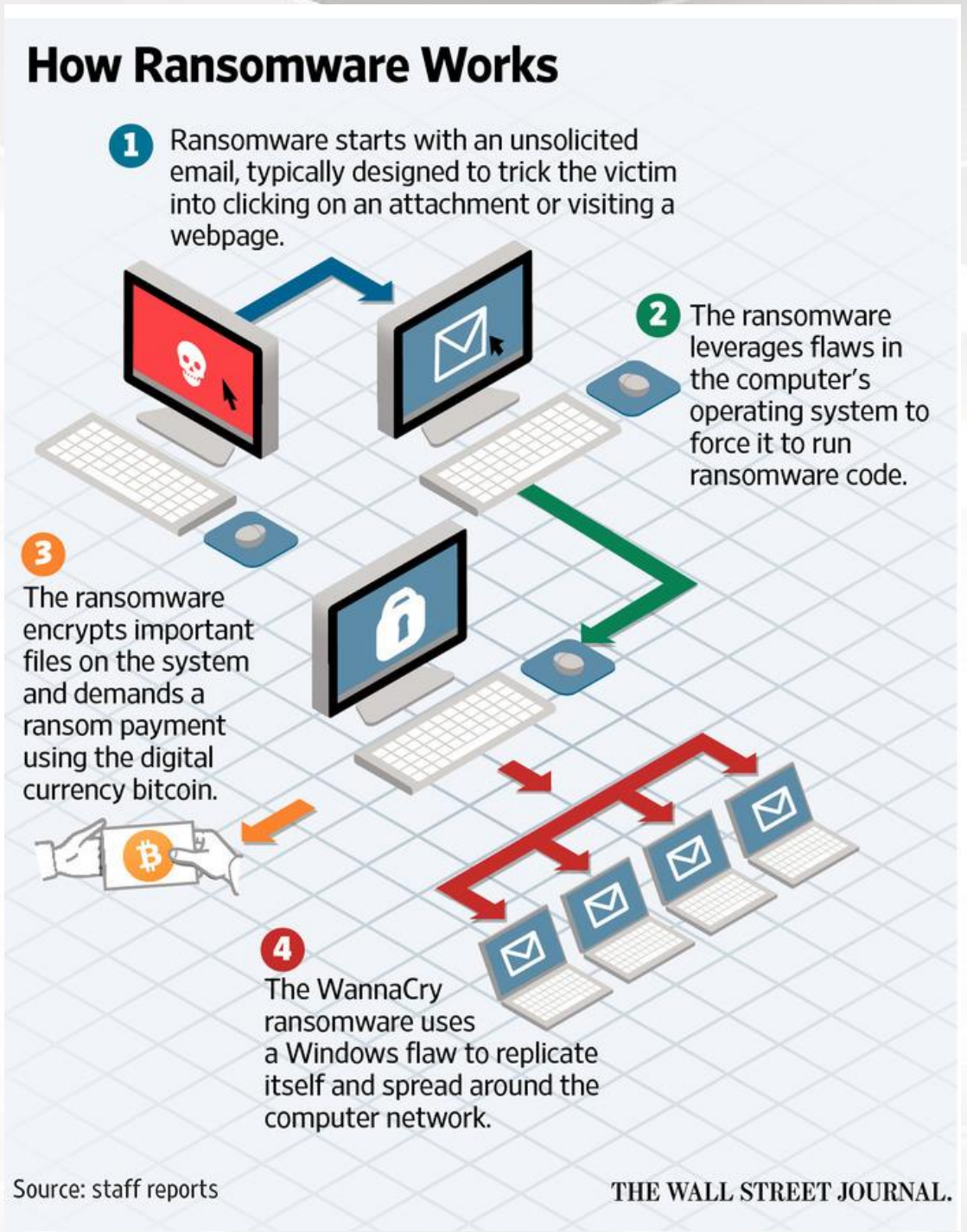
CENTER FOR DIGITAL GOVERNMENT

The different types of cyber attacks

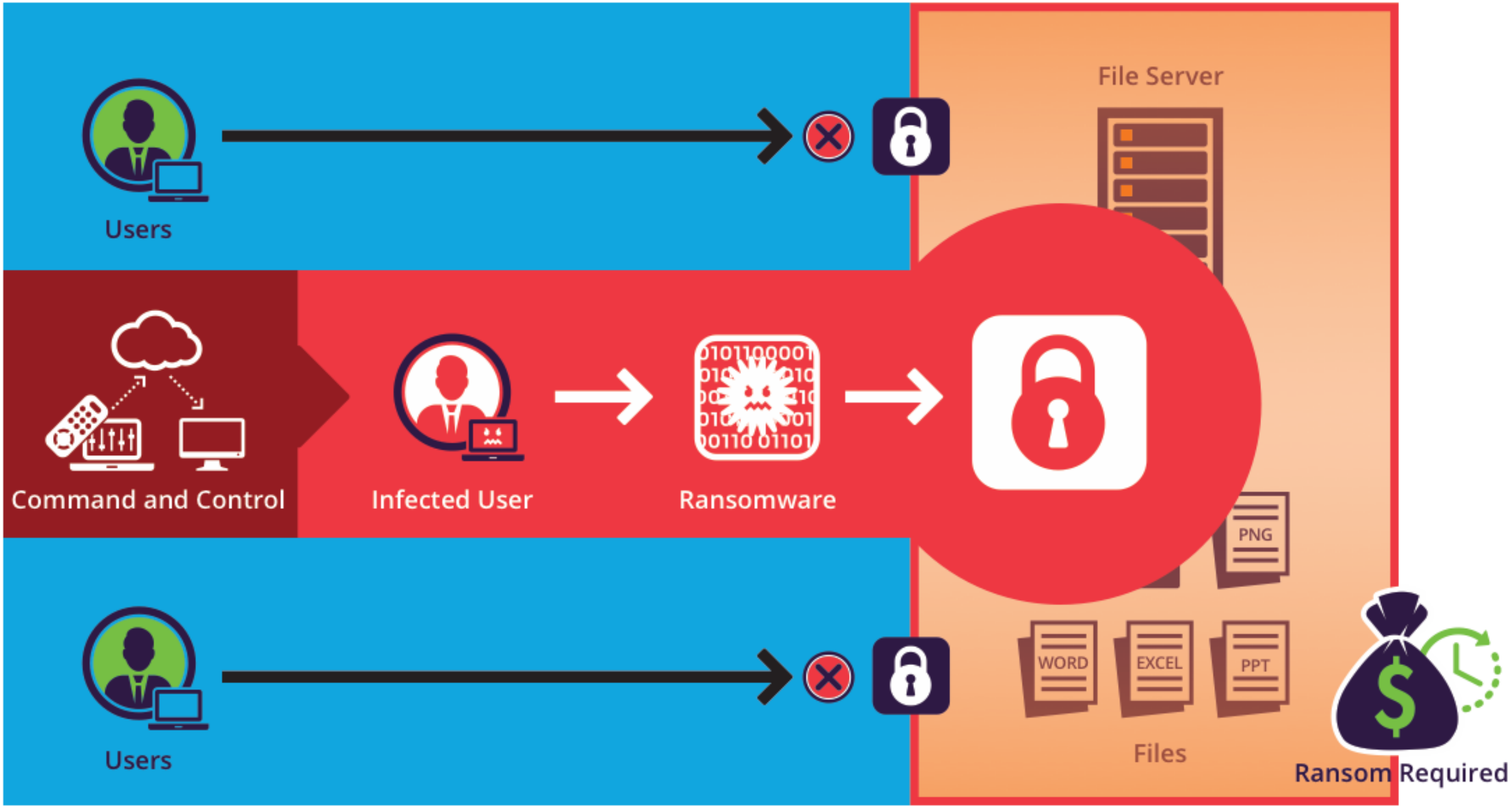
Cyber crime worldwide cost $400 billion in 2015 and is forecast to reach $2 trillion in 2019*



Ransomware



CENTER FOR DIGITAL GOVERNMENT


File Server
Users
Command and Control
Infected User
Ransomware
PNG
WORD
EXCEL
PPT
Files
Users
Ransom Required

Cybersecurity

Cyber-Attack Hits U.S. Health Agency Amid Covid-19 Outbreak

By Shira Stein and Jennifer Jacobs

Updated on

- NSC tweet on disinformation Sunday was connected to attack
- Cyber intrusion comes as U.S. battles the coronavirus pandemic

New COVID-19 Cyber Risks

CENTER FOR DIGITAL GOVERNMENT

Cyber Security Mitigation Tactics

CENTER FOR DIGITAL GOVERNMENT

Why is the current technology vulnerable?

The complexity of today's technology means vulnerabilities exist – think of iPhone updates across all 'computers' on the network.

Why is the current technology vulnerable?

Every device on the network has the potential to create a ‘hole’ for a cyber attack – from desktops to laptops to tablets to mobile phones and now to IoT devices.

Why is the current technology vulnerable?

Every change to the technology opens up the potential for a new ‘hole’.

CENTER FOR DIGITAL GOVERNMENT

What technology should you buy?

Cyber tools are available but they aren't the fix – and there are lots of them.

Cyber tools require skills and funding.

What technology should you buy?

Cyber Insurance – do I need it?

- Having the proper controls in place.
- Understand the risk to your operations.
- Understand what is covered.
- Is it a sound financial decision?

What technology should you buy?

IT Outsourcing provides outside support but requires different management skills

Moving to the Cloud can be more secure but means moving to a services, operating expense model

A Framework To **Prepare** & **Respond**

Source: NIST.gov

CENTER FOR DIGITAL GOVERNMENT

1 IDENTIFY

Identify and control who has access to your business information

Conduct background checks

Require individual user accounts for each employee

Create policies and procedures for cybersecurity

2 PROTECT

Limit employee access to data and information

Install Surge Protectors and Uninterruptible Power Supplies (UPS)

Patch your operating systems and applications routinely

Install and activate software and hardware firewalls on all your business networks

Secure your wireless access point and networks

Set up web and email filters

Use encryption for sensitive business information

Dispose of old computers and media safely

Train your employees

3 DETECT

Install and update anti-virus, anti-spyware, and other anti-malware programs

Maintain and monitor logs

4 RESPOND

Develop a plan for disasters and information security incidents

5 RECOVER

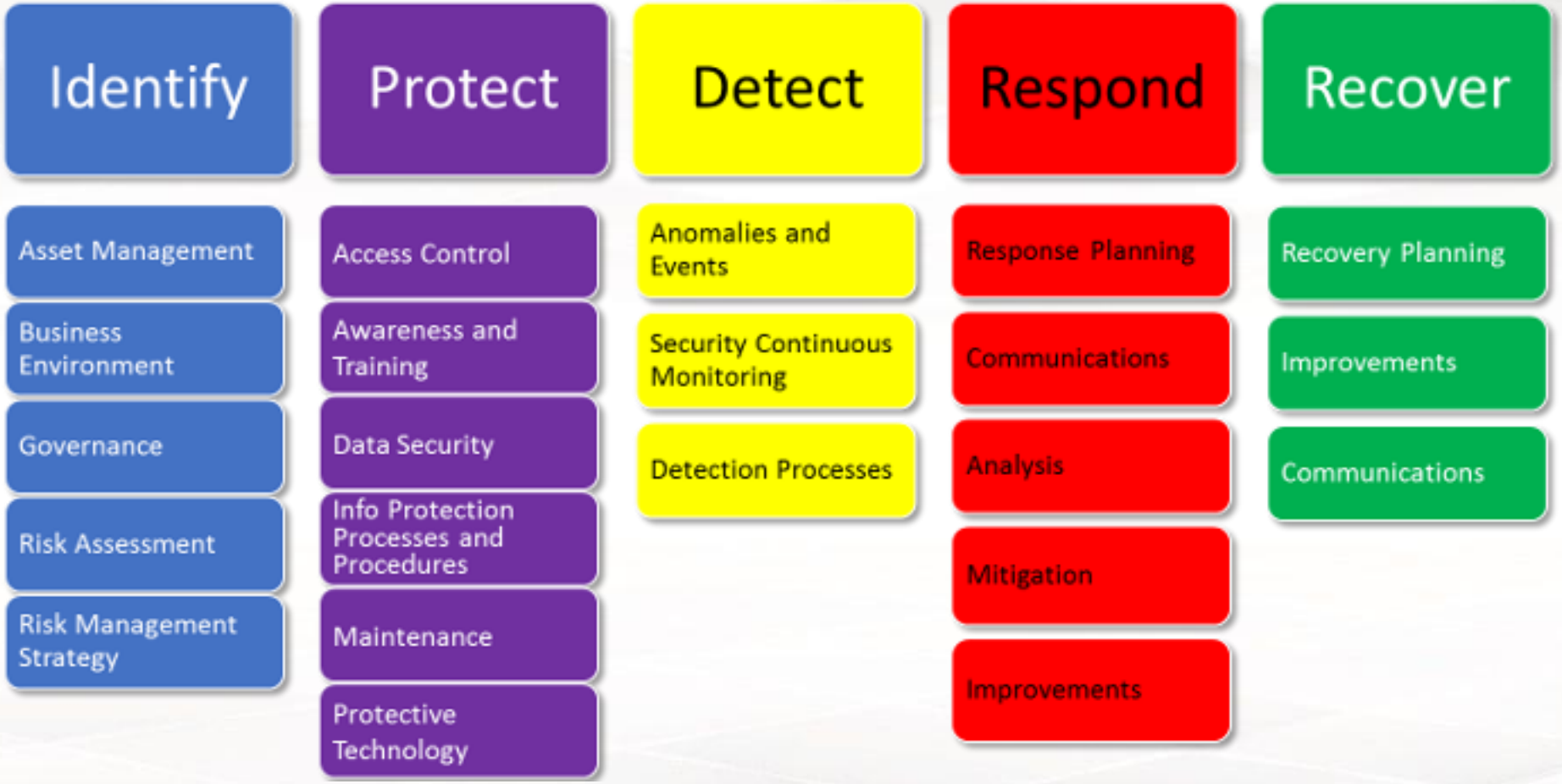
Make full backups of important business data and information

Continue to schedule incremental backups

Consider cyber insurance

Make improvements to processes/ procedures/ technologies

NIST Cyber Security Framework



Source: NIST.gov

CENTER FOR DIGITAL GOVERNMENT

General Preparation Tips

CENTER FOR DIGITAL GOVERNMENT

How do you prepare for a cyber disaster?

Recognize that protection of citizen data is not the sole responsibility of the CIO – it requires department and executive cooperation.

How do you prepare for a cyber disaster?

Treat a cyber disaster in the same way as a physical disaster – with the same planning and coordination.

How do you prepare for a cyber disaster?

Examine current practices for backup and recovery of critical data – treat data like other critical assets – buildings, vehicles, people.

How do you prepare for a cyber disaster?

Allocate the necessary funds over the long term to maintain and upgrade the technology.

How do you prepare for a cyber disaster?

Look for opportunities to share cyber expertise across state and local resources – develop the relationships ahead of a disaster.

General Response Tips

CENTER FOR DIGITAL GOVERNMENT

How do you respond to a cyber disaster?

Recognize that you won't see it coming – it may already be started.

It will happen quickly and response time must be immediate.

How do you respond to a cyber disaster?

Responsibilities between the CIO, Departments and Executives must be established ahead of time and processes in place to evaluate the impact of the disaster.

Decisions must be made by County Executives – not left to the CIO.

How do you respond to a cyber disaster?

A single focal point for public relations must be established and a communication plan developed.

Where To Start

CENTER FOR DIGITAL GOVERNMENT

1

Look at cybersecurity under the lens of enterprise risk management. There is no 100% solution. Cyber Security requires the attention of the executive, departmental and legislative branch.

2 Explore applying a shared services model to cybersecurity capabilities – partnership between state and local government is essential. Establish relationships now.

CENTER FOR DIGITAL GOVERNMENT

3

Evaluate cyber security protections and plans regularly. The technology is growing in importance to your citizens.

CENTER FOR DIGITAL GOVERNMENT

What does this mean to Counties?

Before

- Disaster Recovery Planning
- Continuity of Operations Planning
- Perimeter Defenses
- Intrusion Defenses
- Monitoring
- Employee Training
- Cybersecurity Insurance

During

- Stopping the Attack
- Operationalize Plans
- Finding a Partner
- Notifying Proper Authorities
- Verifying Extent of Attack
- Procuring Technologies to Assist
- Engaging Cybersecurity Insurance Provider

After

- Post Attack Forensics
- Plan to Avoid Future Attacks
- Enhance Perimeter Defenses
- Enhance Intrusion Defenses
- Enhance Monitoring
- Enhance Employee Training
- Re-evaluate Cybersecurity Insurance

CENTER FOR DIGITAL GOVERNMENT

What does this mean to Counties?

Everything has a cost!!

CENTER FOR DIGITAL GOVERNMENT

Cybersecurity Resources

CENTER FOR DIGITAL GOVERNMENT

Federal Resources for State & Local Agencies

https://www.cisa.gov/cisa/cybersecurity-assessments This is a general listing of CISA's cyber assessments.

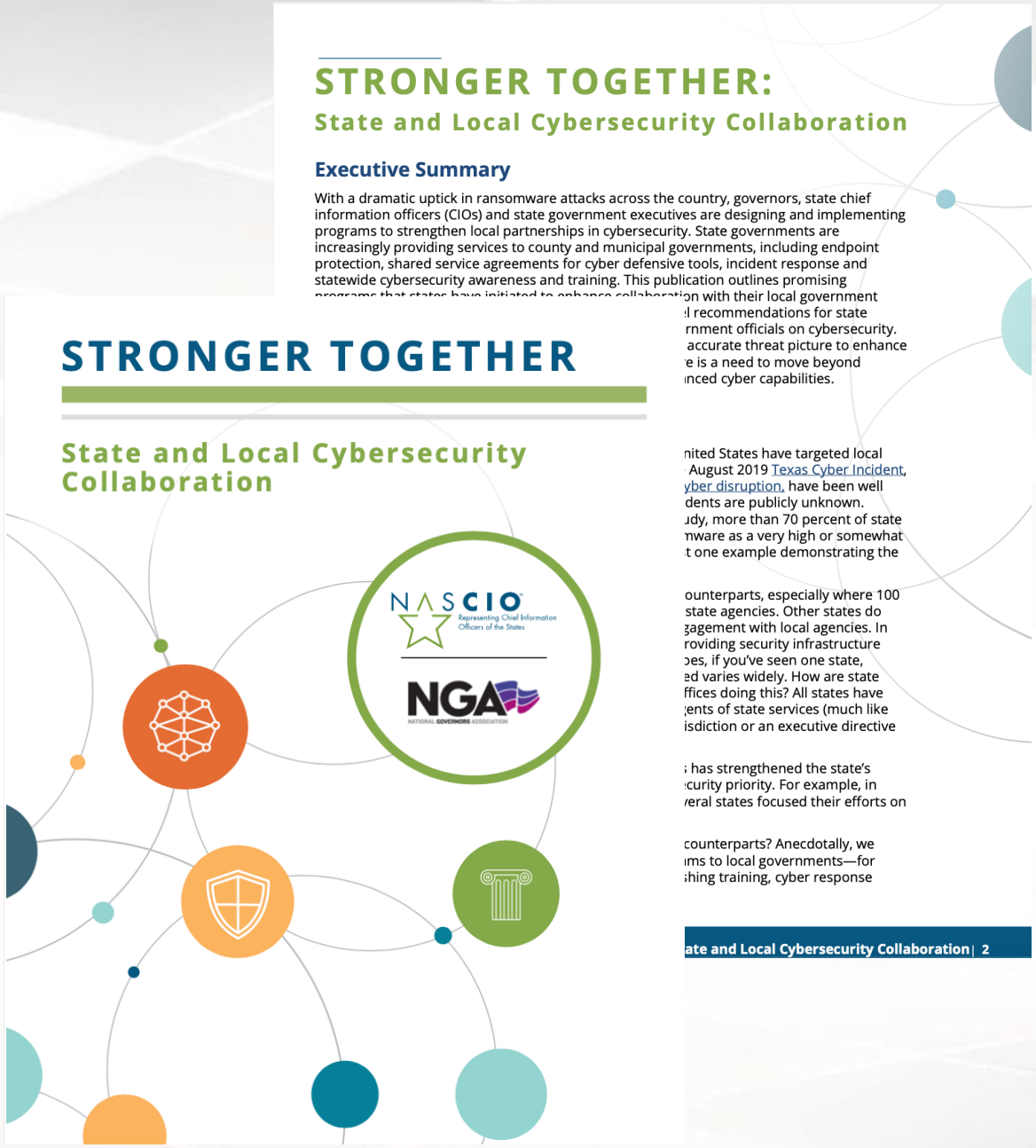
https://www.us-cert.gov/resources/ncats This URL has sample reports for our NCATS Assessments.

https://www.us-cert.gov/resources/assessments This URL has specifics about the Cyber Resilience Review and associated resource guides.

https://www.us-cert.gov/ics/Downloading-and-Installing-CSET To download the Cybersecurity Evaluation Tool (CSET). The CSET has resource library with sample policies and procedures.

https://www.stopthinkconnect.org/ For National Cybersecurity Awareness Month (NCSAM)

CENTER FOR DIGITAL GOVERNMENT



NASCIO Report

State and Local Government Collaboration with Cybersecurity

CENTER FOR DIGITAL GOVERNMENT

Government Finance Review
April 2020 Edition

BY PHIL BERTOLINI

Be Ready When *(Not If)* You're Hit with a Cyber Attack

Our world today can be a scary place, especially when we look at the role of technology in our everyday lives. People use technology for just about everything today, including managing their finances, protecting their property, or simply starting their car. There is an app for everything, or so they say, but are the apps secure enough to make sure that no one steals our identities or our hard-earned money? Will our personal information be protected, or are we willing to accept the risk in order to have an easier way of life?

These questions are top of mind for most people—and governments have these same questions, coupled with the necessity of managing technologies that provide services for the betterment of their citizens. Many of these services, like those provided by law enforcement, are crucial to saving lives every day. Governments rely on technology, but they also have limited funding for developing these technologies. Funding priorities do not always put cybersecurity at the top of the list, prompting the "bad actors" of the world to prey on those that are less protected. The harsh reality is that the battle against cyber criminals may change over and over, but it will never end.

The Latest Scourge

The latest scourge on government technology is the emboldened process of locking up technology resources and forcing governments to pay a ransom, better known as ransomware. The criminals harvest information from unsuspecting government workers by using phishing scams or by simply providing inviting but malicious links. They prey on the technically weak because they can. Local governments have moved up the list of organizations targeted by criminals because in many cases they are the weak and because of their lack of funding coupled with limited cyber protections.

These criminals are often characterized as misguided 16-year-olds working out of their parents' basements when in reality, they are part of organized crime and/or nation-states that see cybercrime as a way to crush the finances of their enemies. They often use mechanized attacks that pound on government systems relentlessly, sometimes reaching into the millions of attempts. They look for holes left as governments frequently change their systems to keep up with the needs of the organization. In fact, the ransomware phenomena represents an estimated $7.5 billion enterprise, making criminals wealthy beyond belief. Data published by the *MIT Technology Review* illustrates the level of impact ransomware is having on governments across the nation. The study estimates that approximately 966 government agencies were affected in 2019, along with 89 universities and 1,233 individual schools.

"Most American local governments do a poor job practicing cybersecurity," according to a study by the University of Maryland. This study also found that a little more than one-third of governments did not know how frequently security incidents occurred, and that approximately two-thirds of governments did not know how often their systems were breached. A cyber criminal could in fact be buried within a target's systems for hundreds of days before striking. The lack of awareness by government is exactly what the criminals count on and is why it is not "if" a government will be successfully attacked, but "when."

The harsh reality is that the battle against cyber criminals may change over and over, but it will never end.

Fast and Furious

These attacks are coming at a rate so fast and furious that governments cannot keep up. Governments of all sizes, especially local governments, are ill-equipped to handle the problem, especially with many budgets declining annually. Services are adversely affected by ransomware. For example, some governments recently saw their 911 systems go down, failures of computer-aided dispatch, website crashes, and phone system malfunctions, along with the severe financial impact of paying ransoms or recovering systems.

Many organizations will focus on technology but soon realize that ransomware is predominantly a "people" problem. According to some estimates, more than 80 percent of attacks are people-related—to put it simply, they are caused by the questionable behavior of people. And governments are aware that the problem is a priority, but the funding doesn't always get to where it needs to go. Data gathered by the Center for Digital Government show that cybersecurity is the top priority for states, cities, and counties. At the

CENTER FOR DIGITAL GOVERNMENT

Virtual Q&A

Phil Bertolini | pbertolini@erepublic.com
Co-Director, Center for Digital Government

CENTER FOR DIGITAL GOVERNMENT