

Cyber Disaster Recovery

What's the Hype All About?

Teri Takai and Phil Bertolini

Co-Directors, Center for Digital Government



What we will cover today

- A brief history of cyber attacks.
- Why is the current technology vulnerable?
- Will counties need more technology?
- What technology should the county buy?
- How do you prepare for a cyber disaster?
- How do you respond to a cyber disaster?

What we won't cover today

What is needed in a robust cyber security plan focused on prevention and remediation.

Brief History of Cyber Attacks

Cyber security attacks in 2000-2010 focused on Disruption of Service – mainly, defacing and shutting down websites

Then came the theft of intellectual property

Brief History of Cyber Attacks

Perpetrators were largely individuals or groups

And then it moved to nation states and organized crime

\$\$\$

\$\$\$

\$\$\$

Cyber Attacks are now Big Business

\$\$\$








\$\$\$

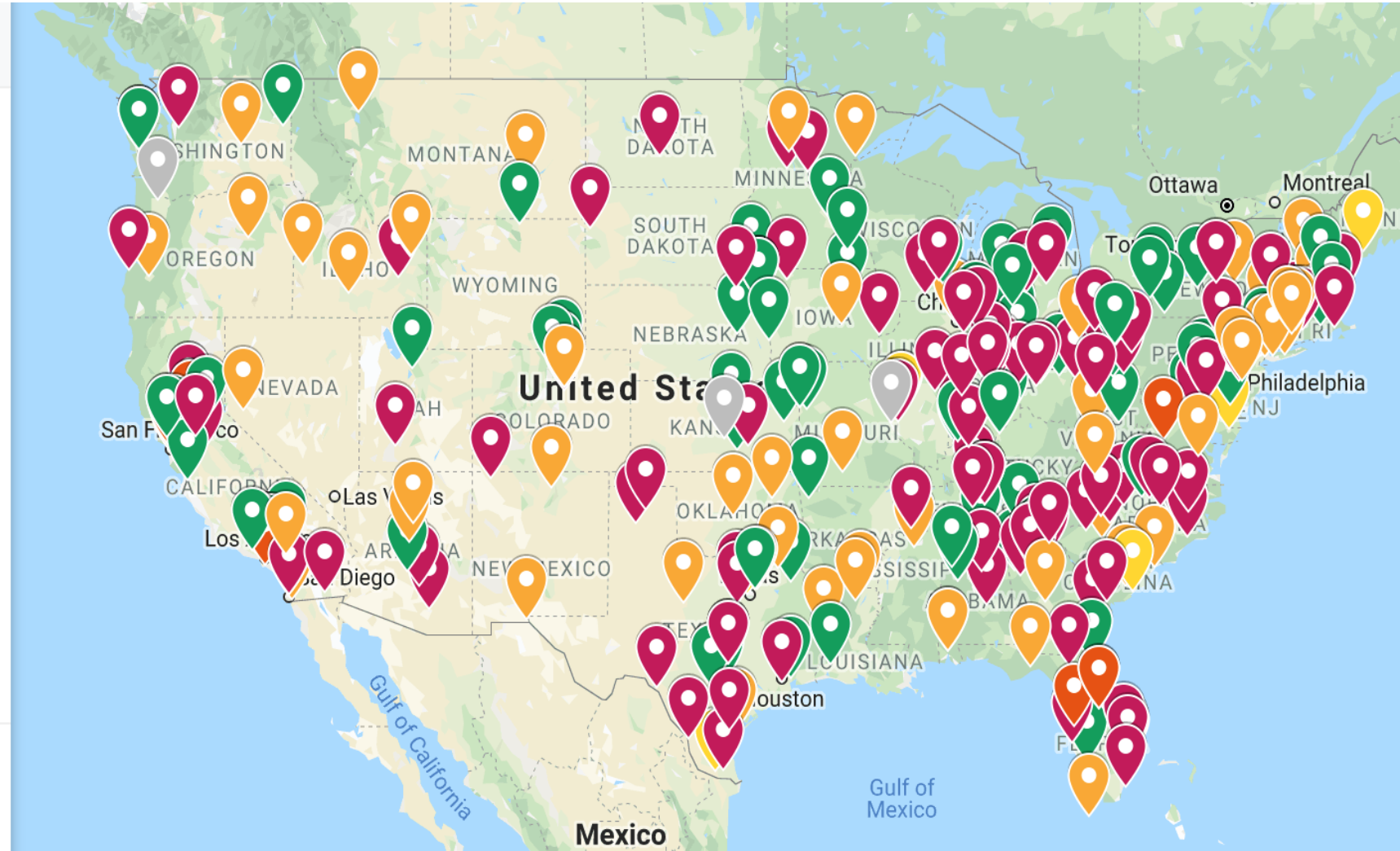
\$\$\$

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

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

\$23.99 1 month	\$34.99 1 month	\$44.99 10 years
1 Month Gold	1 Month Diamond	Lifetime Bronze
Time per boot2400 sec	Time per boot3600 sec	Time per boot600 sec
Concurrents1	Concurrents2	Concurrents2
Total network220Gbps	Total network220Gbps	Total network220Gbps
ToolsIncluded	ToolsIncluded	ToolsIncluded
Support24/7	Support24/7	Support24/7
Buy with Paypal 	Buy with Paypal 	Buy with Paypal 
 bitcoin	 bitcoin	 bitcoin

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'.

Will counties need more technology?

The focus for government is to become more citizen centric – to provide services on multiple devices to reduce the need for citizens to 'wait in line'.

Will counties need more technology?

This means more dependence on citizen access through the internet.

Will counties need more technology?

County governments are becoming more and more dependent on their data to operate.

What technology should the county buy?

Ensure a steady stream of technology spending to keep up to date.

What technology should the county 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 the county buy?

Cyber Insurance – do I need it?

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

What technology should the county buy?

IT Outsourcing

Moving to the Cloud

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.

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.

And....

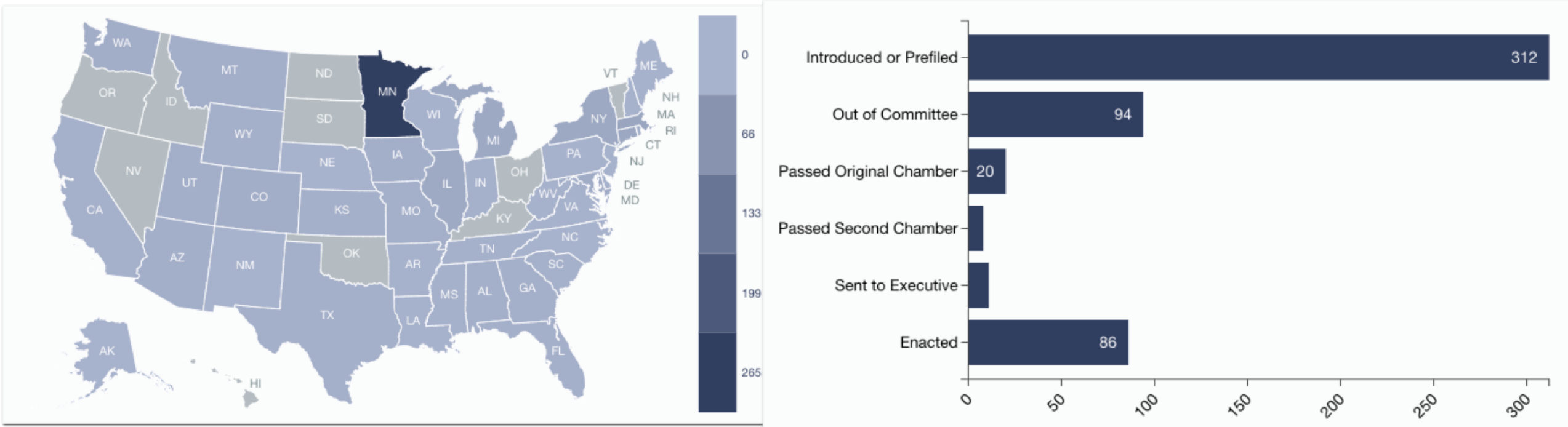
Don't start by firing the CIO.....

Right behind Cyber Security is the growing concern over Data Privacy

How much is your data worth per year?



Data Privacy



Data Source: Quorum

In the future, the role of the citizen defining their right to control data will drive further change in policies and technologies.

What are next steps?

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

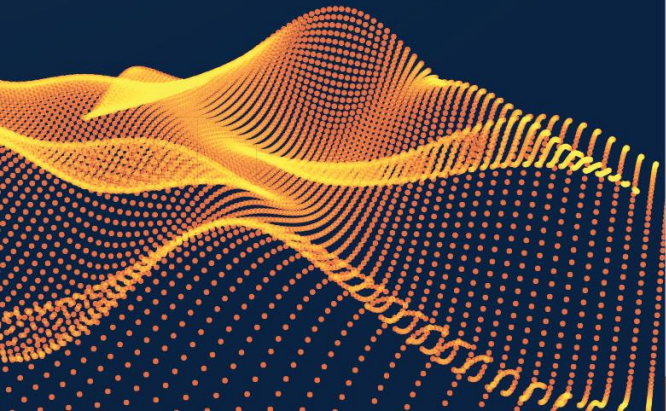
Explore applying a shared services model to cybersecurity capabilities – partnership between state and local government is essential. Establish relationships now.

3

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

Cyber Disaster Recovery

Q&A



Cyber Disaster Recovery

What's the Hype All About?

Teri Takai and Phil Bertolini

Co-Directors, Center for Digital Government

