



Cyber Security Best Practices and Recommendations: How to Make it Work for Your Municipality

Connell Price
ElectriCities of NC, Inc.





As municipalities strive to integrate technology, it becomes increasingly important for these technology “systems” to remain viable...even through catastrophic events.



Cyber Breach, A 21st Century Catastrophic Event...

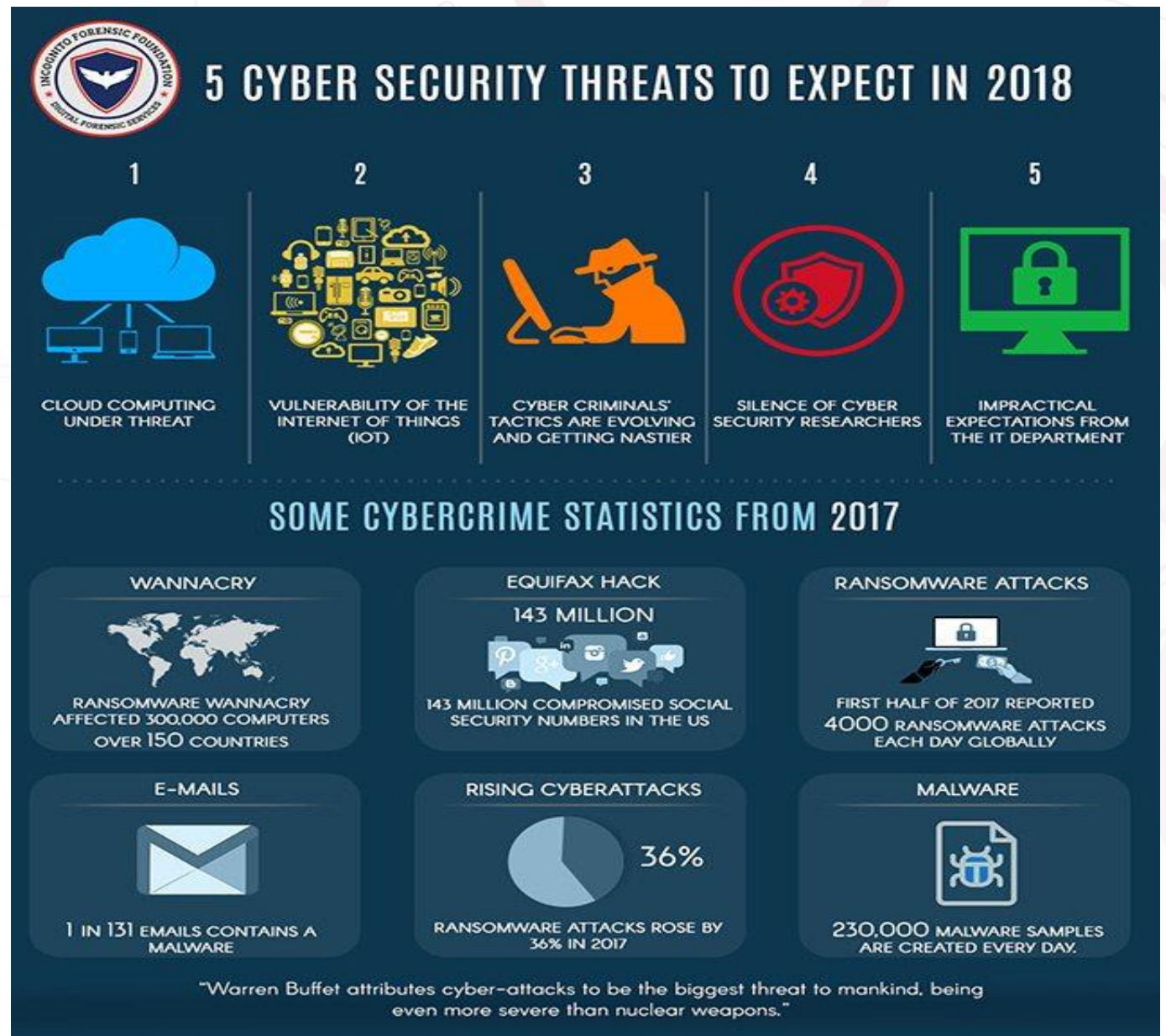
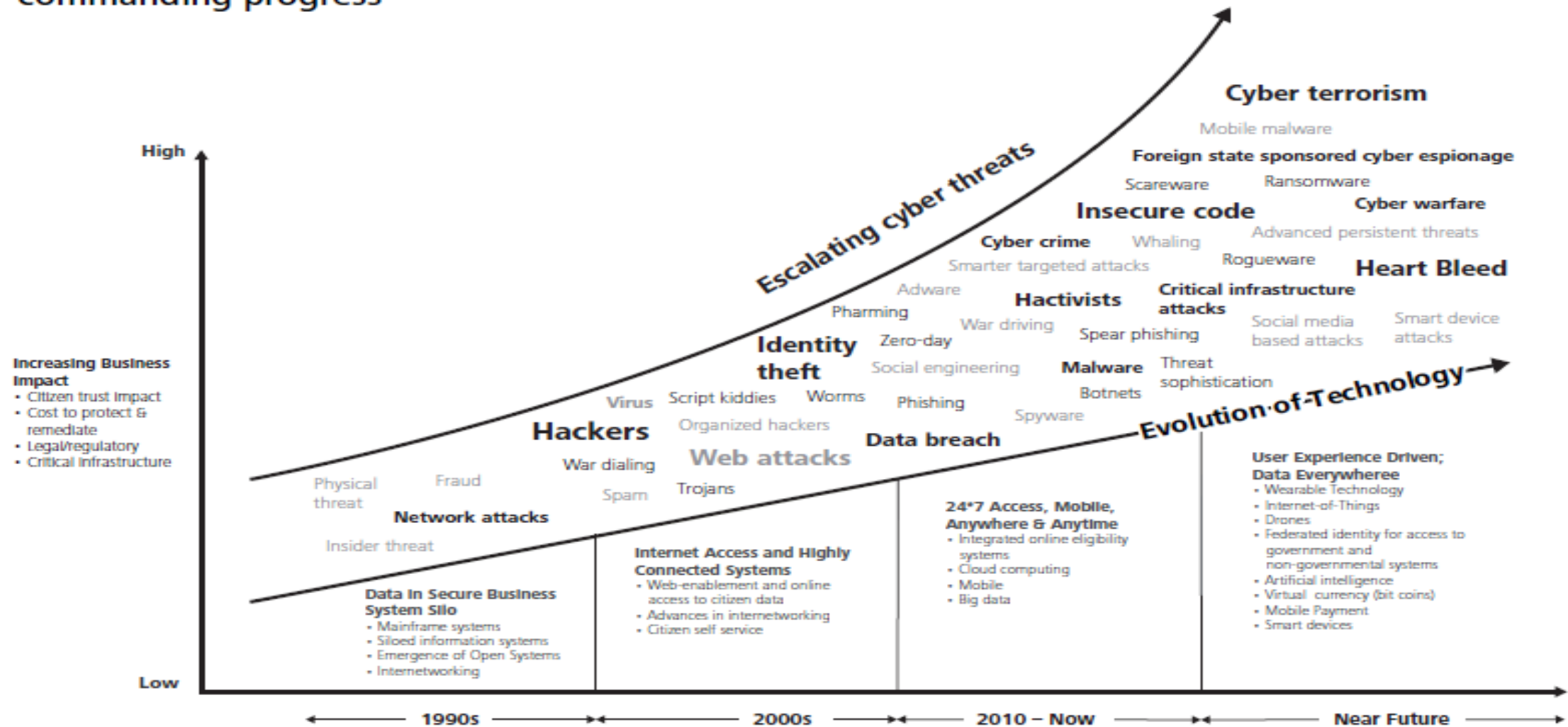




Figure 29: Evolving technology and rapidly escalating cyber threats call for a deliberate approach to make commanding progress



Reproduced from the 2014 Deloitte-NASCIO Cybersecurity Study
 “State governments at risk: Time to move forward”

Introduction

Organizations today face four main types of cyber adversaries

Adversary	Motives	Targets	Impact
 Nation State	<ul style="list-style-type: none">• Economic, political, and/or military advantage	<ul style="list-style-type: none">• Trade secrets• Sensitive business information• M&A information• Critical financial systems	<ul style="list-style-type: none">• Loss of competitive advantage• Regulatory inquiry/penalty• Disruption to critical infrastructure
 Organized Crime	<ul style="list-style-type: none">• Immediate financial gain• Collect information for future financial gains	<ul style="list-style-type: none">• Financial / payment systems• Personally identifiable information• Payment card information• Protected health information	<ul style="list-style-type: none">• Regulatory inquiry/penalty• Consumer and shareholder lawsuits• Brand and reputation• Loss of consumer confidence
 Hacktivists	<ul style="list-style-type: none">• Influence political and /or social change• Pressure business to change their practices	<ul style="list-style-type: none">• Corporate secrets• Sensitive business information• Critical financial systems	<ul style="list-style-type: none">• Disruption of business activities• Brand and reputation• Loss of consumer confidence
 Insiders	<ul style="list-style-type: none">• Personal advantage, monetary gain• Professional revenge• Patriotism• Bribery or coercion	<ul style="list-style-type: none">• Sales, deals, market strategies• Corporate secrets• Business operations• Personnel information• Administrative credentials	<ul style="list-style-type: none">• Trade secret disclosure• Operational disruption• Brand and reputation• Loss of consumer confidence

Why Should Municipalities Plan...

Charlotte Housing Authority suffers data breach, hundreds impacted

Exclusive: Charlotte Housing Authority suffers data breach, 341 employees impacted

January 22, 2018

NOTICE OF DATA BREACH

Dear Staff:

I am writing to inform you that the Charlotte Housing Authority (CHA) was targeted by an email spoofing attack and that the security of information contained on an Internal Revenue Service (IRS) Tax Form was compromised as a result of this incident. While our investigation is ongoing and we have no evidence this information has been misused, we feel it is important to inform you of this incident, encourage you to file your tax return as soon as possible on or before the 2017 W-2, and provide you with the information below that you can use to protect against identity theft and fraud.

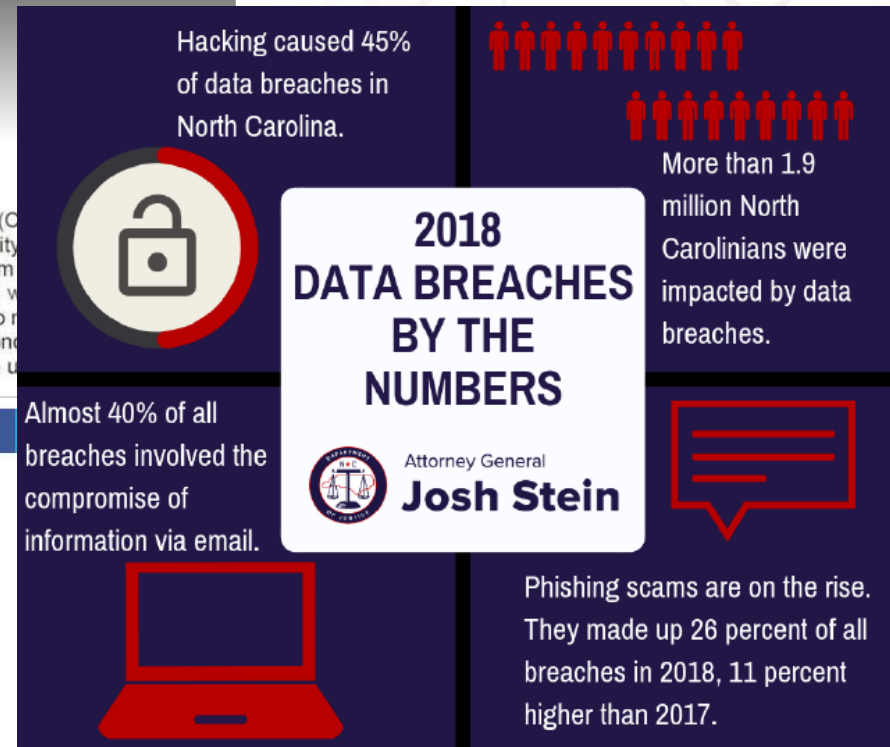
By: Matthew Grant, FOX 46 Charlotte

POSTED: JAN 26 2018 06:28PM EST
VIDEO POSTED: JAN 26 2018 07:08PM EST
UPDATED: JAN 26 2018 11:01PM EST

NEWS

Ransomware attack hits North Carolina water utility following hurricane

A North Carolina water utility still recovering from Hurricane Florence became the victim of a ransomware attack.




By David E. Sanger, New York Times

Cyber Security Strategies and Initiatives Must Be...

- Integrated into your overall Business Resiliency plan
- More than a “set and forget it” activity
- Included in your Risk Management function
- Inclusive of the human factor as it is equally important.

Cyber Security...So Many Methods, So Many Plans...

How do I start with a focus...


Information Technology

CYBERSECURITY

NIST implements practical cybersecurity standards and best practices necessary for the nation's security.

- Computer Security Resource Center
- Cybersecurity Framework
- National Cybersecurity Center of Excellence
- National Initiative for Cybersecurity Education (NICE)
- Privacy Framework



International Organization for Standardization
When the world agrees

English

Taking part | Store

Certification & conformity | SDGs

Search

Search...

Account Log-In/Register | Contact Us

Newsroom | Resource Center

and approved them for adoption by the NERC Board of

mise of critical cyber assets (computers, software and

IEC 27001 Information security...

family - Information security management systems

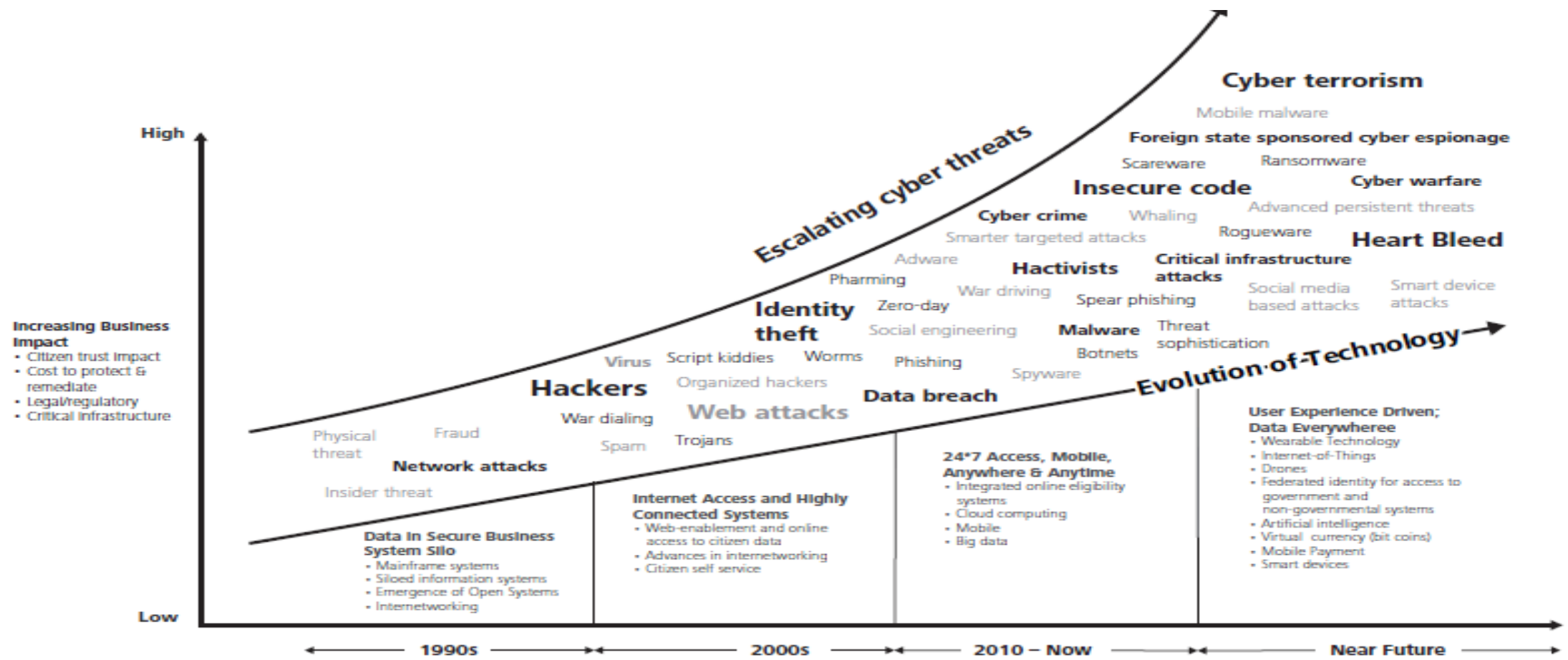
communication networks) that support those systems.

Draft	Action	Dates	Results	Consideration of Comments
Draft 4 Cyber Security Standards CIP-002-1 through CIP-009-1 Cyber Security Standards Implementation Plan	Posted for NERC Board of Trustees Adoption	May 2, 2006		

Best Practice Strategy 1:

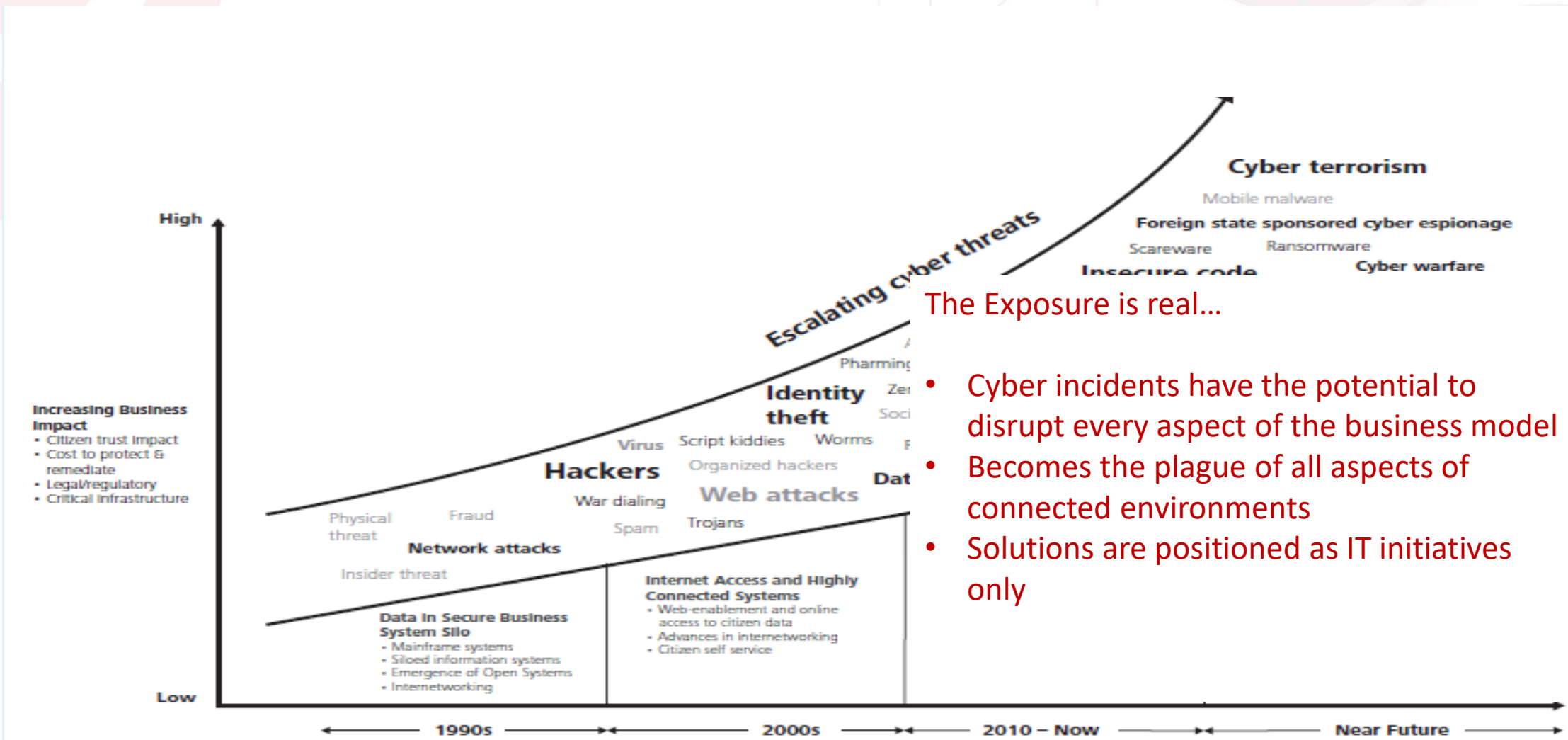
***Incorporate Cyber Security into you
formal Business Resiliency plan.***

Best Practice Strategy 1:



Reproduced from the 2014 Deloitte-NASCIO Cybersecurity Study
"State governments at risk: Time to move forward"

Best Practice Strategy 1:



The Exposure is real...

- Cyber incidents have the potential to disrupt every aspect of the business model
- Becomes the plague of all aspects of connected environments
- Solutions are positioned as IT initiatives only

Reproduced from the 2014 Deloitte-NASCIO Cybersecurity Study
"State governments at risk: Time to move forward"

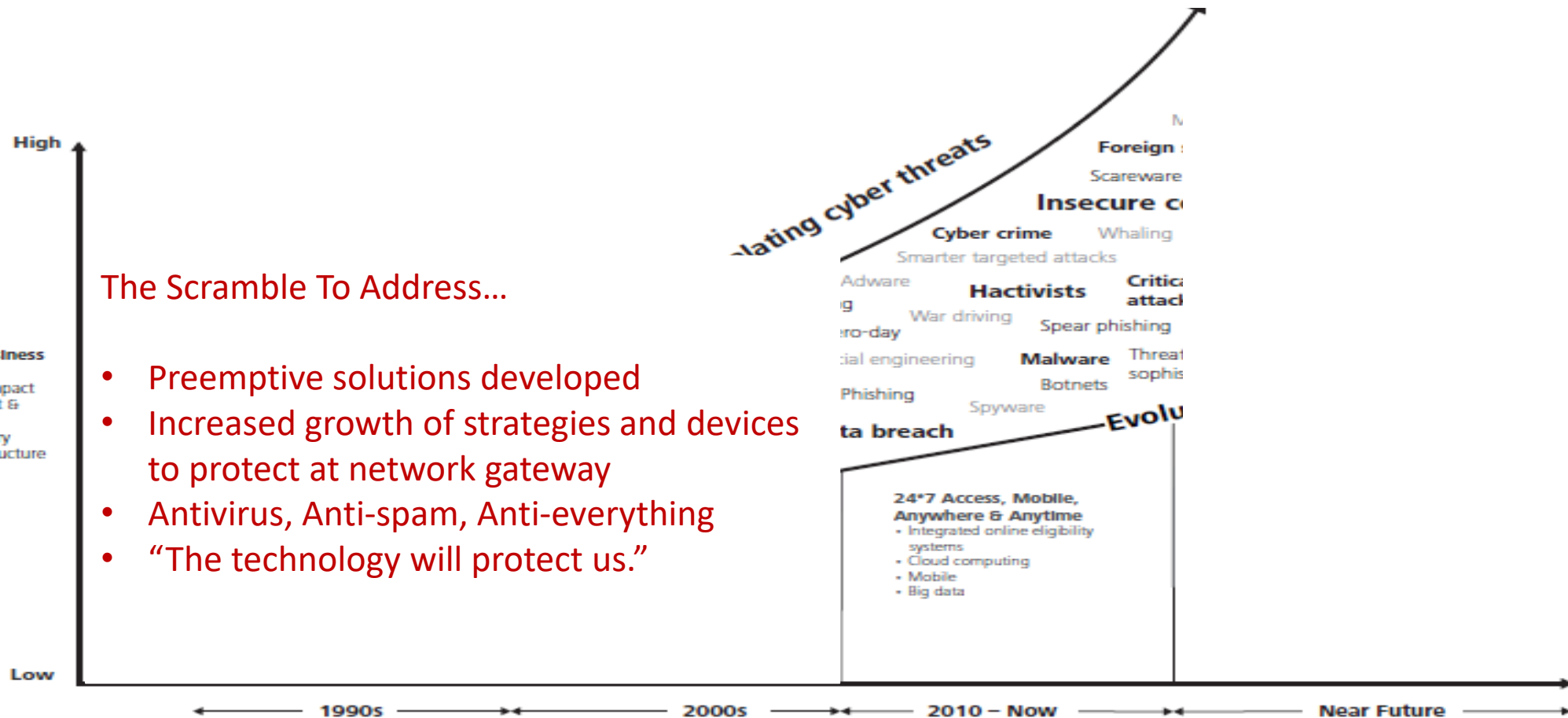
Best Practice Strategy 1:

The Scramble To Address...

- Preemptive solutions developed
- Increased growth of strategies and devices to protect at network gateway
- Antivirus, Anti-spam, Anti-everything
- “The technology will protect us.”

Increasing Business Impact

- Citizen trust impact
- Cost to protect & remediate
- Legal/regulatory
- Critical infrastructure



Reproduced from the 2014 Deloitte-NASCIO Cybersecurity Study
“State governments at risk: Time to move forward”

Best Practice Strategy 1:

Mitigate the Risk...

- Cyber security policy and initiatives adopted to business resiliency plan (BRP)
- Cyber is an enterprise initiative not just an IT problem
- Cyber risk management moves from an IT/Technical issue to a core business process
- Business risk avoidance and mitigation are the focus of technology solutions
- Resiliency and recoverability are equally as important as prevention
- Awareness and training are major efforts in mitigating risks

Increasing Business Impact

- Citizen trust Impact
- Cost to protect & remediate
- Legal/regulatory
- Critical infrastructure

High

Low

← 1990s → 2000s → 2010 - Now → Near Future →

Cyber terrorism

Mobile malware

n state sponsored cyber espionage

re Ransomware

code Cyber warfare

g Advanced persistent threats

Rogueware

Heart Bleed

ical infrastructure

icks

3

eat

histication

Evolution of Technology →

User Experience Driven;

Data Everywhere

- Wearable Technology
- Internet-of-Things
- Drones
- Federated identity for access to government and non-governmental systems
- Artificial intelligence
- Virtual currency (bit coins)
- Mobile Payment
- Smart devices

Reproduced from the 2014 Deloitte-NASCIO Cybersecurity Study
"State governments at risk: Time to move forward"

The background of the slide features a light pink and white color scheme. On the left, there is a large, faint gear. Across the top and right, there are intricate circuit-like lines and nodes. On the right side, there is a large, detailed circular component that resembles a camera lens or a mechanical part of a machine.

Best Practice Strategy 2:

Use the CDC approach...

Best Advice...Adopt the CDC Approach

CDC Organization

[Español \(Spanish\)](#)

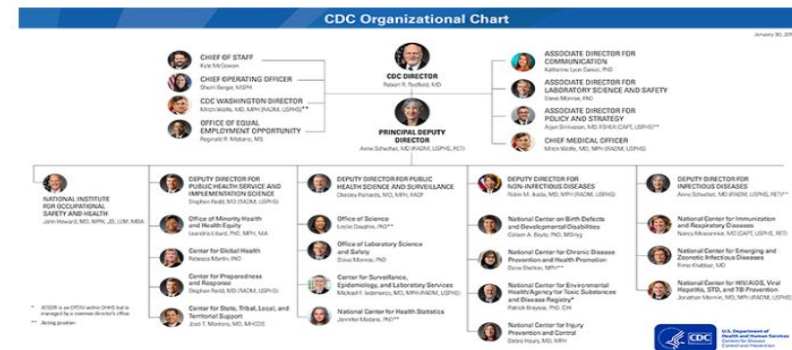
CDC is one of the major operating components of the Department of Health and Human Services. View [CDC's Official Mission Statements/Organizational Charts](#) to learn more about CDC's organizational structure.



CDC's Mission

CDC [works 24/7](#) to protect America from health, safety and security threats, both foreign and in the U.S. Whether diseases start at home or abroad, are chronic or acute, curable or preventable, human error or deliberate attack, CDC fights disease and supports communities and citizens to do the same.

CDC Organization Chart



The CDC Approach...

Control the Environment:

- Data Classification
- Physical/Digital Barriers
- Policies & Procedures
 - ✓ Intrusion Detection
 - ✓ Incident Management



Centers for Disease Control and Prevention
CDC 24/7: Saving Lives, Protecting People™



The CDC Approach...

Control the Behavior:

- Awareness
- Training
- Best Practices
 - ✓ Intrusion Detection
 - ✓ Incident Management

The focus is on behavior modification.



Centers for Disease Control and Prevention
CDC 24/7: Saving Lives, Protecting People™



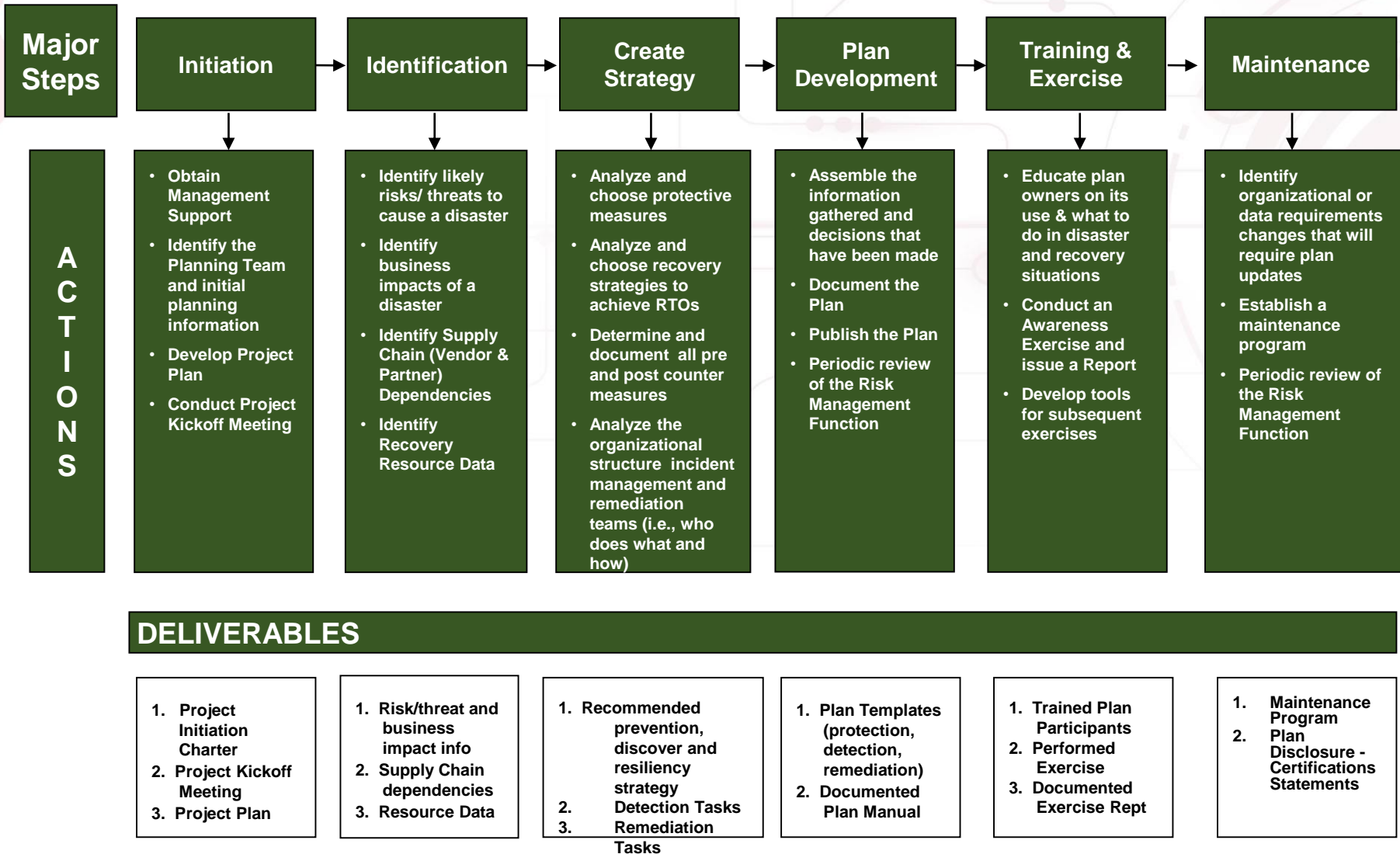
The background of the slide features a light pink and white color scheme. On the left, there are faint, large-scale gear shapes. Overlaid across the right side is a complex network of thin, light pink lines that resemble a circuit board or a data flow diagram, with various nodes and circular elements.

Best Practice Strategy 3:

Build a plan...



How to Start. The Right Way...



The background of the slide features a light pink and white color scheme. On the left, there is a large, faint gear. Across the top and right, there are intricate circuit-like lines and nodes. On the right side, there is a large, detailed circular graphic resembling a camera lens or a complex mechanical component. The overall aesthetic is technical and modern.

Best Practice Strategy 4:

Realize, you can't do it alone.

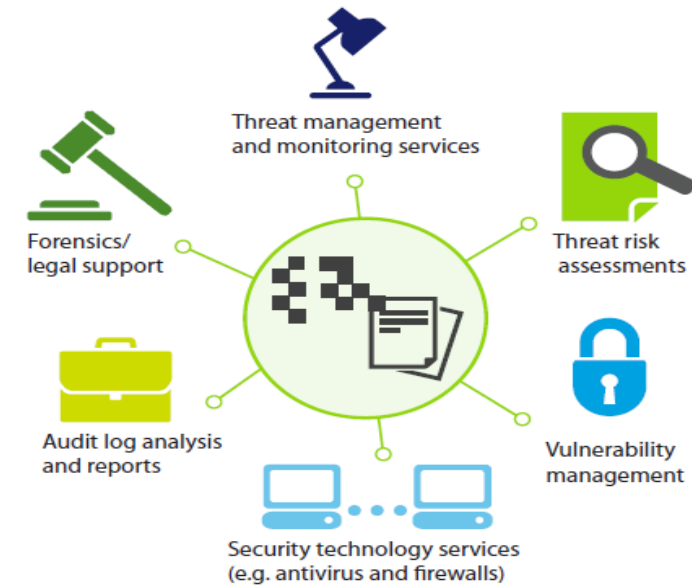
Best Practice Strategy 4:

Consider outsourcing...

“Outsourcing is one way to compensate for talent gaps. For CISOs who are restricted in their ability to hire workers, or who are having trouble attracting employees with the required skill sets, outsourcing certain aspects of cybersecurity work is an option.”

Reproduced from the 2014 Deloitte-NASCIO Cybersecurity Study
“State governments at risk: Time to move forward”

Figure 22: Leading outsourced cybersecurity functions



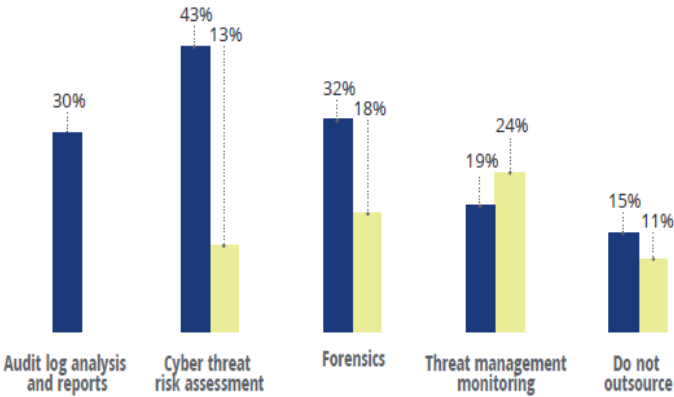
Reproduced from the 2014 Deloitte-NASCIO Cybersecurity Study
“State governments at risk: Time to move forward”

FIGURE 8

While outsourcing has increased for certain functions, more than half of US states have yet to outsource many of them

Select the cybersecurity functions that your state outsources. (47 respondents)

■ 2018 ■ 2010



Source: 2010 and 2018 Deloitte-NASCIO Cybersecurity Studies.

Cyber Security Strategies and Initiatives Must Be...

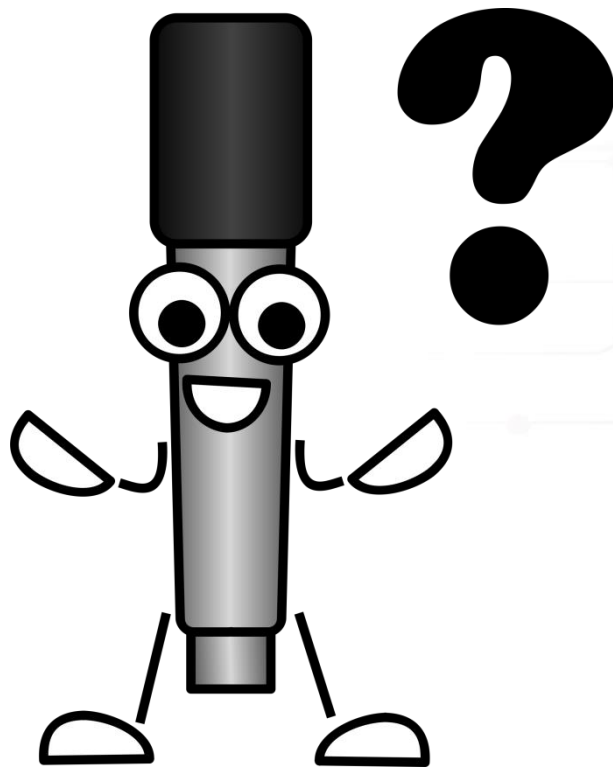
- Integrated into your overall Business Resiliency plan
- More than a “set and forget it” activity
- Included in your Risk Management function
- Inclusive of the human factor as it is equally important.

To All of The Dragon Slayers...



"Oh, don't hurt it. Can't you trap it under a glass, or something?"

Conquer the Cyber Dragon...!



Cyber Security Best Practices and Recommendations: How to Make it Work for Your Municipality





The energy behind public power

www.electricities.com

FOLLOW US ON SOCIAL MEDIA:



@ncpublicpower



facebook.com/Electricities



@ElectriCitiesNC