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

Connell Price
ElectriCities of NC, Inc.
As technology continues to change, its rate of adoption increases exponentially. 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...

Internet of Everything...

"Warren Buffet attributes cyber-attacks to be the biggest threat to mankind, being even more severe than nuclear weapons."
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”
### Organizations today face four main types of cyber adversaries

<table>
<thead>
<tr>
<th>Adversary</th>
<th>Motives</th>
<th>Targets</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nation State</td>
<td>• Economic, political, and/or military advantage</td>
<td>• Trade secrets</td>
<td>• Loss of competitive advantage</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Sensitive business information</td>
<td>• Regulatory inquiry/penalty</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• M&amp;A information</td>
<td>• Disruption to critical infrastructure</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Critical financial systems</td>
<td></td>
</tr>
<tr>
<td>Organized Crime</td>
<td>• Immediate financial gain</td>
<td>• Financial / payment systems</td>
<td>• Regulatory inquiry/penalty</td>
</tr>
<tr>
<td></td>
<td>• Collect information for future financial gains</td>
<td>• Personally identifiable information</td>
<td>• Consumer and shareholder lawsuits</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Payment card information</td>
<td>• Brand and reputation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Protected health information</td>
<td>• Loss of consumer confidence</td>
</tr>
<tr>
<td>Hacktivists</td>
<td>• Influence political and/or social change</td>
<td>• Corporate secrets</td>
<td>• Disruption of business activities</td>
</tr>
<tr>
<td></td>
<td>• Pressure business to change their practices</td>
<td>• Sensitive business information</td>
<td>• Brand and reputation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Critical financial systems</td>
<td>• Loss of consumer confidence</td>
</tr>
<tr>
<td>Insiders</td>
<td>• Personal advantage, monetary gain</td>
<td>• Sales, deals, market strategies</td>
<td>• Trade secret disclosure</td>
</tr>
<tr>
<td></td>
<td>• Professional revenge</td>
<td>• Corporate secrets</td>
<td>• Operational disruption</td>
</tr>
<tr>
<td></td>
<td>• Patriotism</td>
<td>• Business operations</td>
<td>• Brand and reputation</td>
</tr>
<tr>
<td></td>
<td>• Bribery or coercion</td>
<td>• Personnel information</td>
<td>• Loss of consumer confidence</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Administrative credentials</td>
<td></td>
</tr>
</tbody>
</table>
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 the target of an email spoofing attack and that the sensitive personal information contained on an Internal Revenue Service (IRS) Tax Form was as a result of this incident. While our investigation is ongoing and there is no evidence this information has been misused, we feel it is important to report this incident, encourage you to file your tax return as soon as possible on or before 2017 W-2, and provide you with the information below that you can use against identity theft and fraud.

By: Matthew Grant, FOX 46 Charlotte

POSTED: FEB 20 2018 12:30PM EST
VIDEO POSTED: FEB 20 2018 12:30PM EST
UPDATED: FEB 20 2018 12:50PM 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.

2018 DATA BREACHES BY THE NUMBERS

Attorney General Josh Stein

Almost 40% of all breaches involved the compromise of information via email.

Hacking caused 45% of data breaches in North Carolina.

Phishing scams are on the rise. They made up 26 percent of all breaches in 2018, 11 percent higher than 2017.

More than 1.9 million North Carolinians were impacted by data breaches.

Russian hackers appear to shift focus to U.S. power grid

Tags: cyber security, hacking, Russia

Posted July 27, 2018
Updated July 28, 2018

By David E. Sanger, New York Times

CONNECTIONS SUMMIT
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...
Best Practice Strategy 1:

Incorporate Cyber Security into your 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
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.”
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

Reproduced from the 2014 Deloitte-NASCO Cybersecurity Study

“State governments at risk: Time to move forward”
Best Practice Strategy 2:

*Use the CDC approach...*
Best Advice...Adopt the CDC Approach

CDC Organization

E 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.
The CDC Approach...

Control the Environment:
• Data Classification
• Physical/Digital Barriers
• Policies & Procedures
  ✓ Intrusion Detection
  ✓ Incident Management
The CDC Approach...

Control the Behavior:
• Awareness
• Training
• Best Practices
  ✓ Intrusion Detection
  ✓ Incident Management

The focus is on behavior modification.
Best Practice Strategy 3:

Build a plan...
How to Start. The Right Way...

**Major Steps**

1. **Initiation**
   - Obtain Management Support
   - Identify the Planning Team and initial planning information
   - Develop Project Plan
   - Conduct Project Kickoff Meeting

2. **Identification**
   - Identify likely risks/threats to cause a disaster
   - Identify business impacts of a disaster
   - Identify Supply Chain (Vendor & Partner) Dependencies
   - Identify Recovery Resource Data

3. **Create Strategy**
   - Analyze and choose protective measures
   - Analyze and choose recovery strategies to achieve RTOs
   - Determine and document all pre and post counter measures
   - Analyze the organizational structure, incident management and remediation teams (i.e., who does what and how)

4. **Plan Development**
   - Assemble the information gathered and decisions that have been made
   - Document the Plan
   - Publish the Plan
   - Periodic review of the Risk Management Function

5. **Training & Exercise**
   - Educate plan owners on its use & what to do in disaster and recovery situations
   - Conduct an Awareness Exercise and issue a Report
   - Develop tools for subsequent exercises

6. **Maintenance**
   - Identify organizational or data requirements changes that will require plan updates
   - Establish a maintenance program
   - Periodic review of the Risk Management Function

**Deliverables**

1. Project Initiation Charter
2. Project Kickoff Meeting
3. Project Plan

1. Risk/threat and business impact info
2. Supply Chain dependencies
3. Resource Data

1. Recommended prevention, discover and resiliency strategy
2. Detection Tasks
3. Remediation Tasks

1. Plan Templates (protection, detection, remediation)
2. Documented Plan Manual

1. Trained Plan Participants
2. Performed Exercise
3. Documented Exercise Report

1. Maintenance Program
2. Plan Disclosure - Certifications Statements
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"
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...

Conquer the Cyber Dragon...!
Cyber Security Best Practices and Recommendations: How to Make it Work for Your Municipality
FOLLOW US ON SOCIAL MEDIA:

@ncpublicpower
facebook.com/Electricities
@ElectriCitiesNC