Secure the Cities: Cybersecurity 101 for Michigan’s Municipalities

Andy Brush, Michigan DTMB/Michigan Cyber Security, Cybersecurity Partnerships

Jeff Hoffman, Detective Sergeant, Michigan Cyber Command Center
Andy Brush, Michigan DTMB/Michigan Cyber Security, Cybersecurity Partnerships

Andy served Washtenaw County for 17 years in various roles including Webmaster, Knowledge Manager, Innovations Manager, and spent 7 years as the head of the IT organization. Among other things, Andy has worked as a managing consultant, a technical writer, a project manager, a teacher, a cherry shaker operator, and a Peace Corps volunteer in Sri Lanka. Andy Brush works on cyber security partnerships for the State of Michigan. In this new role, Andy is seeking to improve the cyber security posture of governments across the State by finding innovative ways of working together across all sectors.

Jeff Hoffman, Detective Sergeant, Michigan Cyber Command Center

Detective Sergeant (D/Sgt.) Jeff Hoffman is an enlisted member of the Michigan State Police. D/Sgt. Jeff Hoffman joined the State Police in July 1999. He served at the Lakeview Post and Sixth District Fugitive Team. In 2011, D/Sgt. Hoffman was assigned to the Computer Crimes Unit – Grand Rapids. In 2017, he transferred to the Michigan Cyber Command Center (MC3). D/Sgt. Hoffman was promoted in 2018 and is currently the team lead for the MC3.
Secure the Cities: Cybersecurity 101 for Michigan’s Municipalities

Michigan Municipal League
New Orleans Declares State of Emergency After Ransomware Attack

DECEMBER 16, 2019
Cyber Threat Actors: Who Are They and What Do They Want?

**Threat Actors...**
- Cybercriminals,
- Adversary Nation-States,
- Hacktivists
- Employees, Contractors,
- Business Partners
- Compromised Accounts

**Motivated By...**
- Financial gain
- Personal advantage
- Professional revenge
- Outsider influence
- Economic gain
- Corporate or national espionage
- Political or social change
- Military or economic advantage

**Target YOU...**
- Logins & passwords
- Credentials & identifying info
- Emails
- IMs
- Browsing history
- Documents & internal communications
- Photographs
- **Anything** that they can use

**So They Can Get...**
- Access to the corporate network and/or industrial control systems to obtain control and access to sensitive information
- and/or Prevent you from accessing your systems and for ransom or disrupt services for political or military purposes
Successful Attacks are Expensive

- Baltimore spent approx. $10 million to recover from a 2019 ransomware attack
  - Additional $8.2 million in potential lost or delayed income.
- Atlanta’s recovery from a ransomware attack in 218 cost the city $12 million.
- A 2019 ransomware attack on Colorado’s Dept. of Transportation cost approximately $1.5 million to recover, not including National Guard resources.
- These numbers and the cost will continue to grow.
Cyber strike on city hall

By Phil Custodio on September 20, 2018 · No Comment

Computer hackers enjoyed a $13,600 payday after a successful ransomware attack on Clarkston last week. The “cyber incident” happened last Tuesday, Sept. 11. City insurance made the payment on Thursday, and City Council met on the matter at a special meeting, Saturday.

“In this case, the ransomware experts we worked with, including those at the Michigan State Police and FBI, recommended that the ransom be paid as the most efficient and effective way to regain access to our files,” said City Manager Jonathan Smith. “The experts told us that, believe it or not, the attackers take pride in their business and predominately provide the decryption codes once the ransom is paid.”
Coronavirus: Two States Divert to Telework. Are Others Ready?

Work-from-home policies are about to take center stage as public agencies and private corporations around the world prepare unprecedented measures to slow the spread of COVID-19 (coronavirus). Is government ready?

BY ANDREW WESTROPE / MARCH 12, 2020

Local Governments Work Out Kinks for Virtual Public Meetings

Local governments have an obligation to keep conducting business and engaging the public during the global pandemic, but there can often be more to virtual public meetings than meets the eye.

BY JED PRESSGROVE / APRIL 8, 2020

Zoom Rushes to Improve Privacy for Consumers Flooding Its Service

The features that allowed companies to hop on videoconferences also made it easy for trolls to hijack meetings and harass students.
Top 5 Steps to Securely Work from Home*

1. **You**
   - Technology alone cannot fully protect you – **you** are the best defense. Attackers have learned that the easiest way to get what they want is to target you, rather than your computer or other devices.

2. **Home Network**
   - Change Default Passwords
   - Allow Only People You Trust
   - Make Passwords Long and Strong
   - Update Firmware

3. **Passwords**
   - Create strong passwords: the more characters it has, the stronger it is. Using a **passphrase** is one of the simplest ways to ensure that you have a strong password. Like: “Withers&PrineL0st.”

4. **Updates**
   - Make sure computers, mobile phone devices, programs and apps are running the latest version of its software.

5. **Kids & Guests**
   - Make sure family and friends understand they cannot use your work devices.
   - Make sure you know that you should only use your work device for work.

---

*SANS Institute
https://www.sans.org/sites/default/files/2020-03/02-SSA-WorkingFromHome-FactSheet.pdf
What’s My Role?

LEADERSHIP

STRUCTURED APPROACH

ASK QUESTIONS

RECOGNIZE RISK CONVERSATION

BALANCE SECURITY AND CONVENIENCE

BE PREPARED
Cybersecurity is a Team Sport
<table>
<thead>
<tr>
<th>Do Things</th>
<th>The Right Things</th>
</tr>
</thead>
</table>

Do More of the Right Things!
Address Left of Boom and Right of Boom

Prevent bad things
Evaluate
Plan
Upgrade Infrastructure
Build capacity
Build relationships
Prepare for bad things

Contain the damage
Preserve evidence
Restore services
Learn the lessons
A Model that Supports the Whole State

Counties

Cities, Villages, Townships

School Districts

2000+ Local Entities
Engage Partners Across Sectors

Prevention, Protection, & Mitigation

- Michigan Cyber Partners
  - Learn
  - Collaborate
  - Share

- Cyber Readiness Service
  - Expert advice and support
    - Assess
    - Plan
    - Coach

Response & Recovery

1-877-MI-CYBER
mc3@Michigan.gov

- Cyber 911

State of Michigan

Federal Government

Cyber Companies
<table>
<thead>
<tr>
<th>Basic</th>
<th>Foundational</th>
<th>Organizational</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Inventory and Control of Hardware Assets</td>
<td>7. Email and Web Browser Protections</td>
<td>17. Implement a Security Awareness and Training Program</td>
</tr>
<tr>
<td>5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers</td>
<td>11. Secure Configuration for Network Devices, such as Firewalls, Routers and Switches</td>
<td></td>
</tr>
<tr>
<td></td>
<td>13. Data Protection</td>
<td></td>
</tr>
<tr>
<td></td>
<td>14. Controlled Access Based on the Need to Know</td>
<td></td>
</tr>
<tr>
<td></td>
<td>15. Wireless Access Control</td>
<td></td>
</tr>
<tr>
<td></td>
<td>16. Account Monitoring and Control</td>
<td></td>
</tr>
</tbody>
</table>
Cyber Partners 2020 Outcomes

• Build Relationships and Trust
• 12 Monthly Meetings
  – Monthly Participation from Local Public Entities and Combined Cyber Team from State & Federal Government
• 6 Remotely Hosted (not Lansing)
• Cybersecurity Framework Training
• Large Scale Cyber Exercise – state-hosted
• Cyber Incident “In a Box” Exercise – regional/local
• Think, Plan, and Build for the Long Term
Cyber Readiness Service 2020

- Cybersecurity Assessment, Planning, and Coaching Service
- Use CIS Controls Self-Assessment Tool to Measure Maturity
- State-Run Pre-Qualification Process for Cyber Assessors
  - Multiple Vendors
  - Available Across the State
  - Available to All Public Entities via MIDEAL
Response and Recovery 2020

- Coordinated Incident Response
- Reporting Standards for Local Incidents
- Actionable Threat and Intelligence Sharing
- Participate in Incident Response Scenarios and Exercises
- Shared Basic IR Plan – part of assessments
Outreach and Expansion

• Insurers
  – MMRMA
  – MML

• Statewide Associations – leadership side of Local Government
  – MML
  – Michigan Association of Counties
  – Michigan Townships Association
  – Michigan Association of School Administrators
  – Many more...

• National Organizations
  – NASCIO
  – NACO
Questions?
Thank You!

D/Sgt. Jeff Hoffman
Michigan Cyber Command Center
HoffmanJ@michigan.gov
877-MI-CYBER
mc3@Michigan.gov

Andy Brush
Michigan DTMB/Michigan Cyber Security
Cybersecurity Partnerships
BrushA1@Michigan.gov
Upcoming Webinars

Register for the upcoming webinars here: http://www.mml.org/coronavirus

• MML Monday Morning Live, Monday April 13, Noon – 1 PM

• COVID-19 Updates and Resources for Local Governments, April 20, 2 PM – 3PM