



Mat-Su Borough

2018 Cyber Attack

- What Happened
- Why It Happened
- The Response
- Going Forward

- Late April eMail phishing
- Late May heavy activity
- June dormant
- July Discovery and **Crypto-Locked**

Zero Day

*Theoretical
Exploit*

- Trojan- Emotet
- Credential Stealing - Dridex
- PowerShell Empire
- Ransom Ware - BitPaymer

Victim 210

Data Gathering

Disruption

Ransom

Staffing

Funding

Priorities

Complacency



Incident Response

Vendors

Project Management

Volunteers

Minimum Viable Product
(MVP)

Long hours

Emergency funding

Communication

Communication

COMMUNICATION

**Take Care Of
Your Users**

Communication
Communication
COMMUNICATION

Partnering

Federal

State

Local

Commercial

MS-ISAC

DHS – US Cert

InfraGard

CIO Council

Smart Community Forum

Take Care Of
Each Other
We Can't Do This Alone

Security Portfolio



