2024 Wisconsin Counties Association ANNUAL CONFERENCE

8:00 – 9:00 AM

Inside Cyber Incidents: Exploring County Response Teams

Aegis
a Charles Taylor Company

Inside the Cyber Incidents

Exploring County Response Team Member's Minds

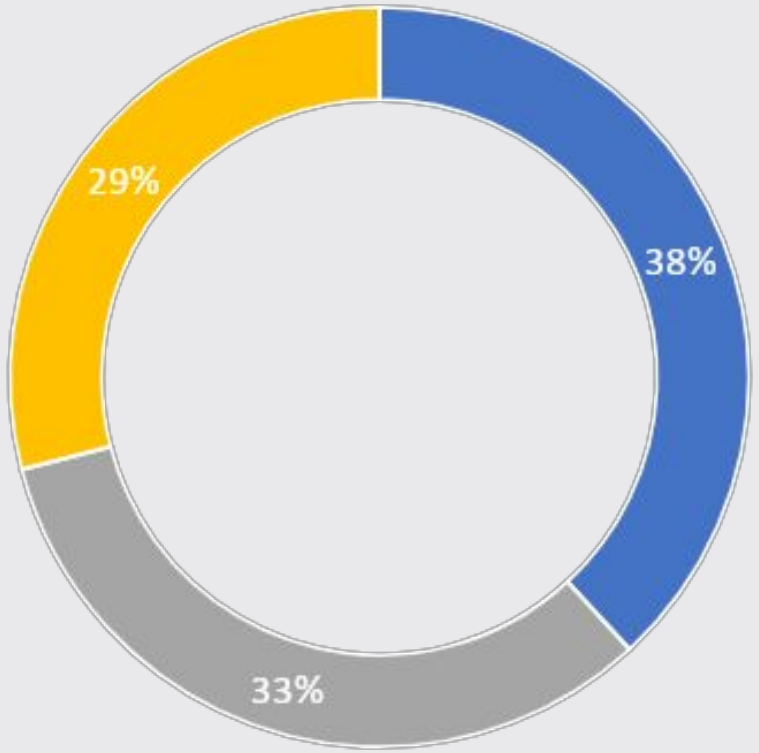
Presented by: **Seth Johnson**, Senior Cyber Risk Professional

Agenda

- *Understanding the Concerns of Incident Response*
- *Understanding the Costs of Incident Response*
- *Cyber Incidents & Response Perspectives (6)*
- *Key Focus Areas Following the Incident*
- *Ongoing Focus Areas for Response Planning*

Aegis
a Charles Taylor Company

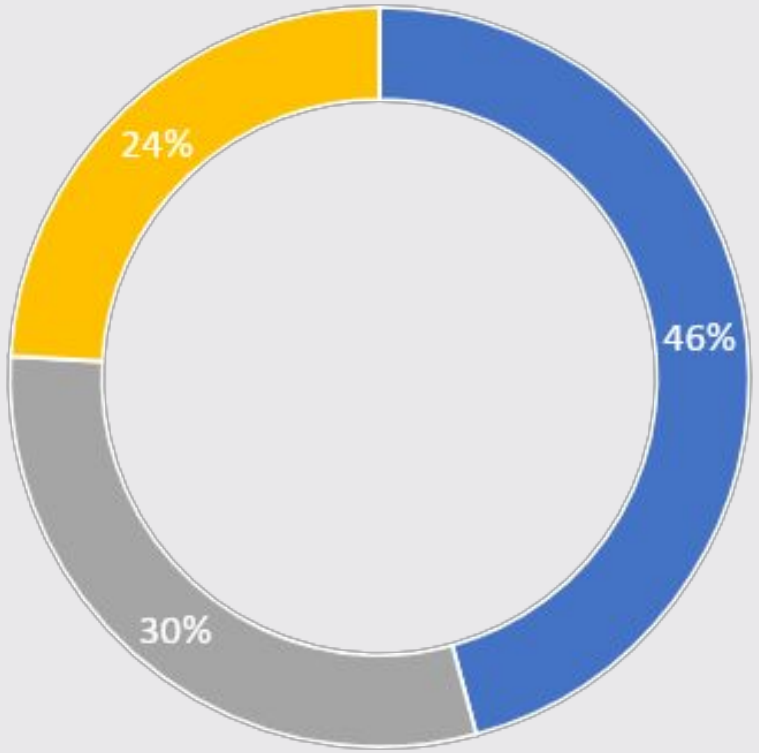
Understanding the Concerns of Incident Response



Top County Concerns

- Loss of access to county-critical information
- Staff prevented from carrying out their day-to-day work
- Erosion of public trust

Understanding the Costs of Incident Response



Top Cost Categories

- Ransom Payment
- Recovery
- Data Mining + Notifications

The **Newcomer**

As the new IT Director, he found himself facing a situation he hadn't anticipated. He was still familiarizing himself with the environment, the team members, and the county's existing cyber program.

- **Takeaway**: Incident response methodologies and team members should be dynamic and adaptable; capable of evolving alongside the county's circumstances.

- **Takeaway**: The lack of preparation will likely add to the complexity of an already complex process.

The **Improviser**

"We do not have any existing processes or procedures in place to guide our work, which means that the ability to improvise and adapt is absolutely crucial in order to meet our objectives and navigate the challenges we encounter."

-Anonymous County CSIRT Member

- **Takeaway:** Improvision is enabled by preparation.

The **Outsourcer**

“We’re covered because IT outsourcing providers take on responsibility for our IT-related functions.”

-Anonymous County CSIRT Member

- **Outsourcing**: Engaging outside entities to provide cyber incident response services that the county otherwise provides for itself.

- **Takeaway**: Counties are responsible for managing the relationship and monitoring the provider’s performance.

The **Reporter**

“I am hyper-focused on the communication aspect of this incident! I will send emails, make phone calls, and even send carrier pigeons if necessary. This incident will not be a mystery to anyone. Shakespeare himself will be jealous.”

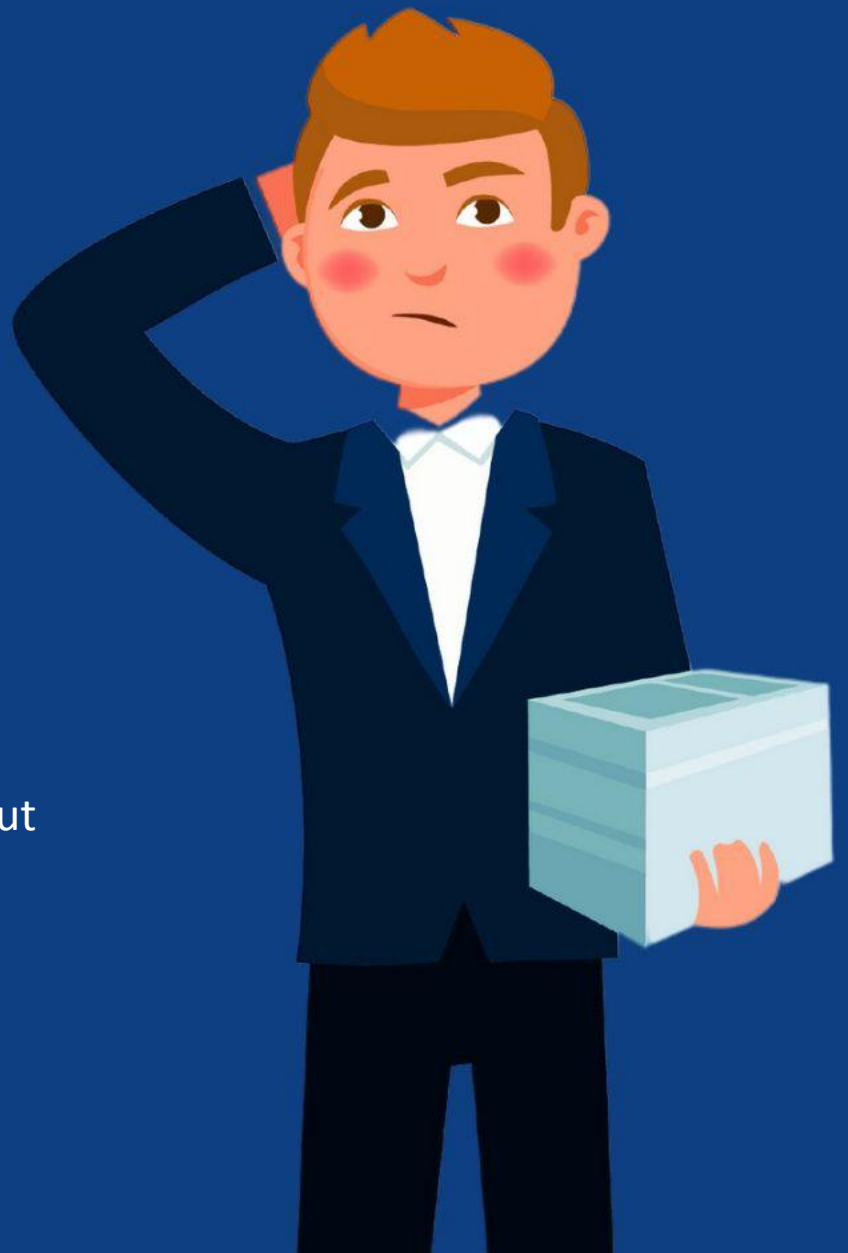
-Anonymous County CSIRT Member

- **Takeaway**: Messages should be created quickly but not hastily.

The **Worrier**

“It’s important we don’t expose our county to incorrect actions taken. There are many ways that our county can get into trouble when it comes to cyber incidents.”

-Anonymous County CSIRT Member



- **Takeaway:** Assumptions should drive the investigation forward, but don’t turn assumptions into facts without verification.

The **Automater**

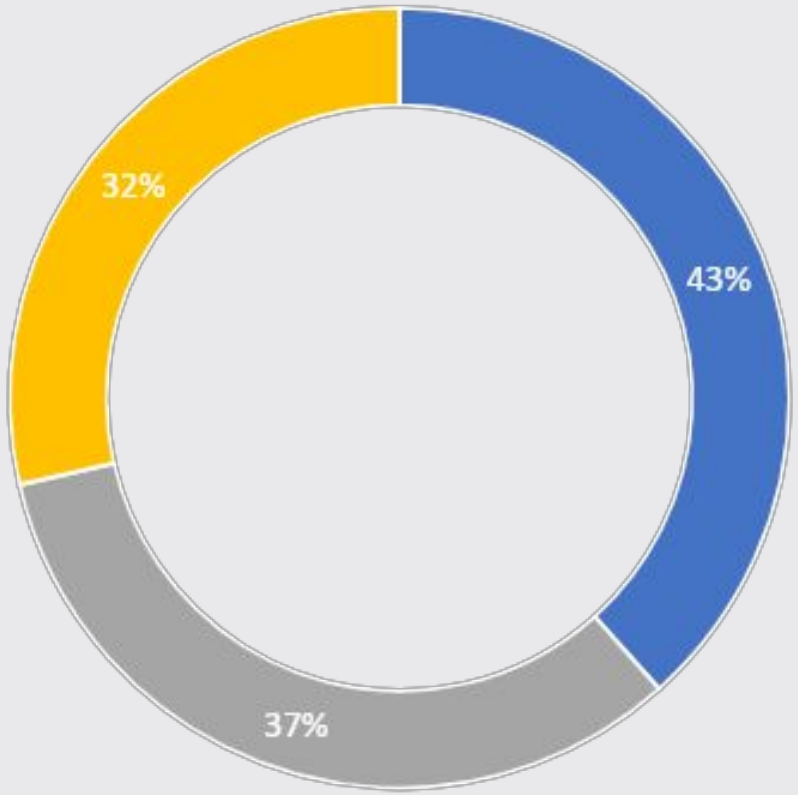
“We don’t have to worry because we’ve made our response procedures more efficient by simplifying and automating them.”

-Anonymous County CSIRT Member

- **Automation**: Automating cyber incident response processes means using technology to perform response tasks without manual intervention.

- **Takeaway**: Find a balance between use of immediate automated response actions and reasoning of human evaluation.

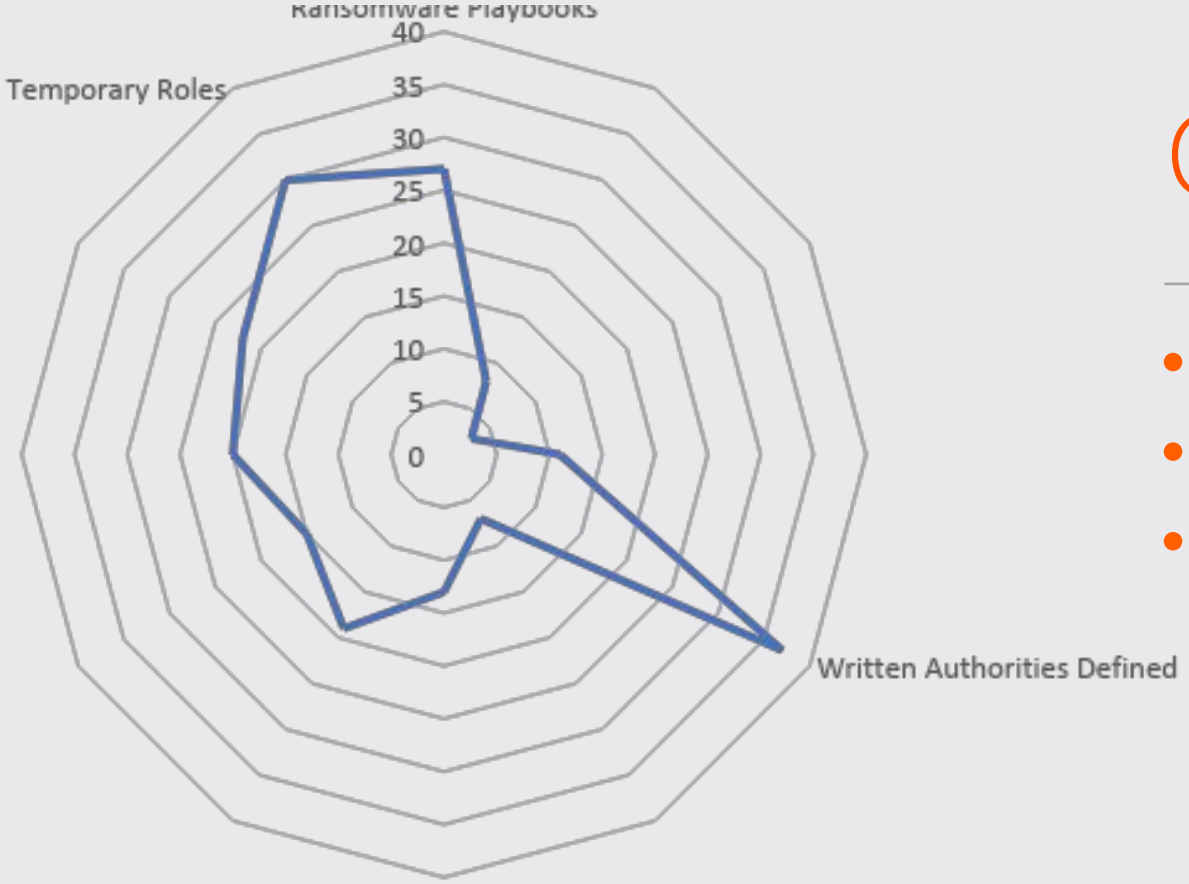
Key Focus Areas Following the Incident



Post-Incident Changes

- Enhanced identity & access management practices
- Implementation of risk assessments
- Establishment of configuration baselines

Ongoing Focus Areas for Response Planning



Current Focus Areas

- Defining formal authorities
- Temporary role integration
- Ransomware playbooks

ctplc.com

Charles Taylor plc

@ctaylorplc

@Charlestaylorplc

Aegis

a Charles Taylor Company