



Agenda for Delaware Continuity Coordinator Council

May 16, 2024

1 p.m. – 2:30 p.m.

Attendees (98): Antoniette Agregado, Mindy Anthony, Patricia Atwood, Michael Bacu, Andrea Bayline, Tiffany Bennett, Ashley Blok, Brian Bauer, Dan Cahall, Lester Carlisle, Cathleen Carter, Michael Chionchio, Timothy Collins, Kenneth Cool, Gemini Cornish, Sam Cucinotta, Cynthia Diaz, Maridelle Dizon, Cherie Dodge Biron, Robert Dreibelbis, Dylan Lee, Denise Elliott, Karin Faulhaber Sheeron Fuller, Christine Gannon, Dale Goodine, Dawn Gordon, Lori Gorman, Linda Graves-Crocker, Christopher L Hall, Isaac Harris, Deborah Hawkins, John Healy, Erich Heintz, Tomi Helojoki, Kim Hicks, Robert Hill, Fern Holland, Christopher Horton, Robert Hudson, Alyssa Huenke, Carrie Hyla, Daniel Isom, Matthew Jamison, Geneer Johnson, Heather Johnson, Tracy Jones, Joseph Simmons, Samara Kaminski, Griffin Kanich, Ken Maloney, Andy Kloepfer, Patti Kozerski, Brianna Kresse, Michael Krumrine, William Lankford, Debra Lawhead, DeWayne Lehman, Carol Lewis, Tameka M Lewis-Sterling, Tim Li, Sarah Lindauer, Yun-Fei Lou, Tanya Lyons, Melissa Marlin, Tracy Mattson, Chris McGonigle, Shamika McLean, Cynthia Mercer, Jennifer Miles, Mark Miller Hannah Morgan, Lori Murray, Lora Nacrelli, Rebecca Noe, Jessie Ogden, Henry Ortiz, Jerome Passon, Bobbie Pearson, Coleen Ponden, Danka Prilepkova, Sruthi Raghunathan, Janet Roberson, John Rudd, Jordan Seemans, Devashree Singh, Robert Sisk, Andrew Sumner, Rachel Surratte, Taylor Burkett, Terri Thomas, Mickie Troubetaris, Victoria Vazquez, James Wagner, Sherine White, Jessica Wurzel, Claudette Wus

AGENDA

- **Welcome/Introductions**
- **DECCC Updates**
 - NEW Plan Builders
 - Upcoming opportunities
 - COOP News
 - Statewide COOP Exercise
 - BCIC News
 - Assessment Results
- **MD Cyber Incident Response and Recovery- Best Practices/Lessons Learned: see ppt slides**

A speaker from the Maryland Emergency Management Agency will share some of their experiences and lessons learned around a cyber incident that impacted their state over the past few years including a major State agency, local jurisdiction impacting 911 and a local school system.
- **Kent County Cyber Incident: see ppt slides**

Joseph Simmons, Director of Information Technology from the Kent County Levy Court will be sharing some of their lessons learned and answering questions regarding their

cyber incident. This is a great time to learn from someone first-hand the impacts to day-to-day operations, and the recovery involved with a cyber incident.

- **Making the Lessons Learned work for you- Ran out of time: see DECC ppt slides**
Now that we have heard some of the lessons learned and best practices, how do we incorporate these into our current plans? Lori will walk through a few possible ways of incorporating what you learned today into your COOP projects.

DECCC Steering Committee members:

Christine Beste – Co-Chair

Lori Gorman – Co-Chair

Tim Li – Disaster Preparedness Officer

Jennifer Coverdale– Facilities Officer

Cherie Dodge Biron- Vice-Chair

Vanessa Briddell- Education & Training Officer

Dan Cahall- IT Systems Officer

Alvin Jones- Vital Records Officer

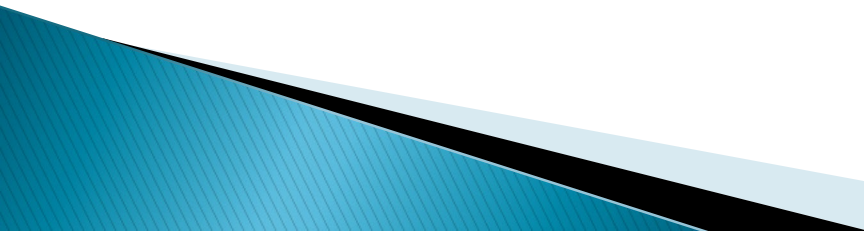


Delaware Continuity Coordinator
Council (DECCC)

2nd Quarter Meeting

May 16, 2024

Agenda

- **Welcome/Introductions**
 - **DECCC Updates**
 - New plan builders
 - Upcoming Opportunities
 - COOP News
 - Statewide COOP Exercise
 - BCIC News
 - Assessment Results
 - **MD Cyber Incident Response & Recovery**
 - **Kent County Cyber Incident**
 - **Making Lessons Learned Work for You**
- 

DECCC Updates

- ▶ Roll Call– New COOP Plan builders
 - Jessie Ogden– DSHS Communications
 - Patricia Atwood– DOF Lottery
 - Tracy Jones– DELDOT Finance
 - Christine Cosgrove– DELDOT Finance
 - Desiree Klein– DHR Statewide Benefits

- ▶ Monthly trainings are currently available for new or existing plan builders:
 - 3rd Tuesday of each Month: COOP plan building
 - 3rd Wednesday of each Month: Crisis Communications

Training

- ▶ **ICS-200: Basic ICS: Single Resources and Initial Action Incidents**
May 29-30: 0830-1630, DEMA
- ▶ **E/L/K 105: Public Information Basics**
June 4-6: 0830- 1630, DEMA
- ▶ **ICS 300: Intermediate ICS for Expanding Incidents**
July 9-11: 0830- 1630, DEMA
- ▶ **L-O146: Homeland Security Exercise/Evaluation Program (HSEEP)**
August 7-8: 0830 - 1630, DEMA
- ▶ **G-191: ICS/EOC Interface**
August 13: 0830 - 1630, DEMA
- ▶ **ICS-400: Advanced ICS for Command and General Staff**
August 21-22: 0830 - 1630, DEMA

DEMA Trainings

<https://dema.delaware.gov/training/dema/index.shtml?dc=demaTrainingCalendar#tabsBox3>

<https://training.fema.gov/is/crslist.aspx>

<https://extranet.coop.state.de.us/index.shtml?dc=training>

Looking for volunteers to review BCIC training recordings for updates.

COOP News

- ▶ 2024 Meeting Schedule:
 - 1st Quarter: February 22, 2024
 - 2nd Quarter: May 16, 2024
 - 3rd Quarter: Statewide COOP Drill–
August 22, 2024
 - 4th Quarter: November 14, 2024



Continuity of Operations Plan (COOP) Exercise

August 22, 2024

The 10th Annual Statewide COOP Tabletop Exercise will be held for Organization Leaders, Emergency Services Coordinators, Public Information Officers, Information Security Officers, Information Technology personnel, Continuity Coordinators/Plan Builders and Local Municipalities on August 22, 2024. This event, presented by DEMA, DECC and DTI, will explore the preparatory measures and continuity of essential functions within the State as they relate to a variety of incidents. The exercise will utilize each organization's COOP plan and permit collaborative discussion of interdependencies amongst agencies.

- What:** Statewide COOP Exercise
- Who:** Continuity Coordinators, Plan Builders, Emergency Services Coordinators, Information Security Officers, IT personnel, HR Managers, Public Information Officers and Management
- Where:** Modern Maturity Center
1121 Forrest Ave, Dover, DE 19904
- When:** August 22nd, 2024
- Time:** 8:30am – 3:00pm
- Cost:** FREE!

[Register Here](#)

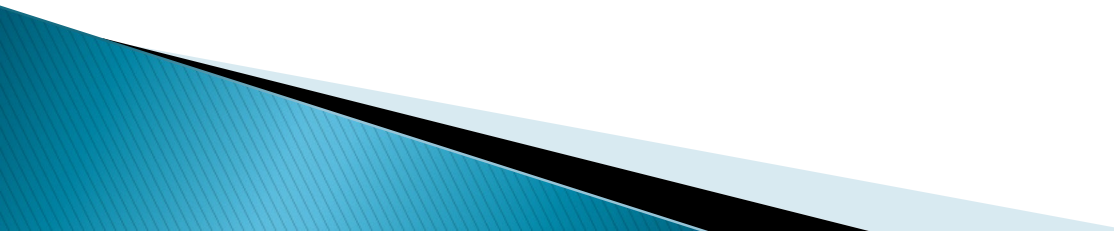
If you have any questions, please send an email to DTI_COOP_Project_Team@state.de.us

What New in BC in the Cloud or MIR3?

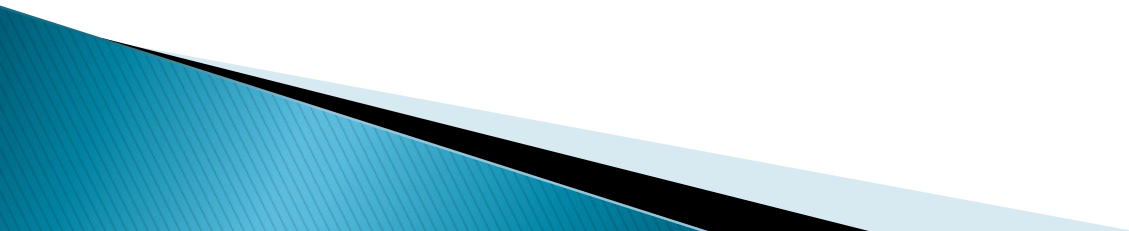
BCIC:

- ▶ Some updates are being requested but have not yet been approved. Waiting on Statement of work approval.

MIR3:

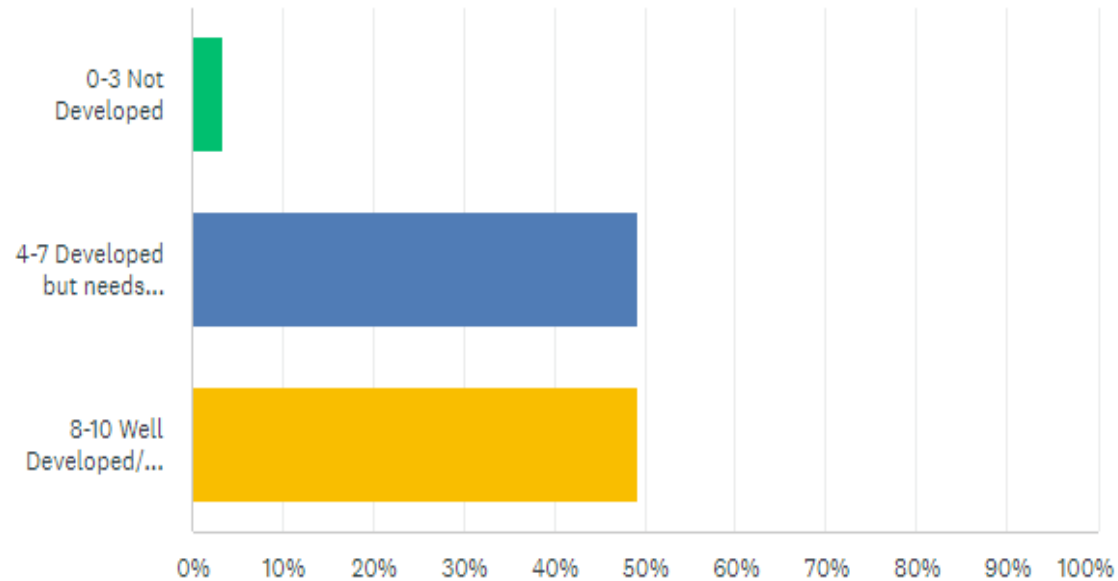
- ▶ Please encourage your staff to add your Agency name and Division ANI (Caller ID) to their Cell phones. Some cell phones/carriers are instituting blocks for calls from unrecognized numbers and this can impact your users.
- 

COOP Planning/ FEMA Assessment Results



COOP Project- Initiating Phase

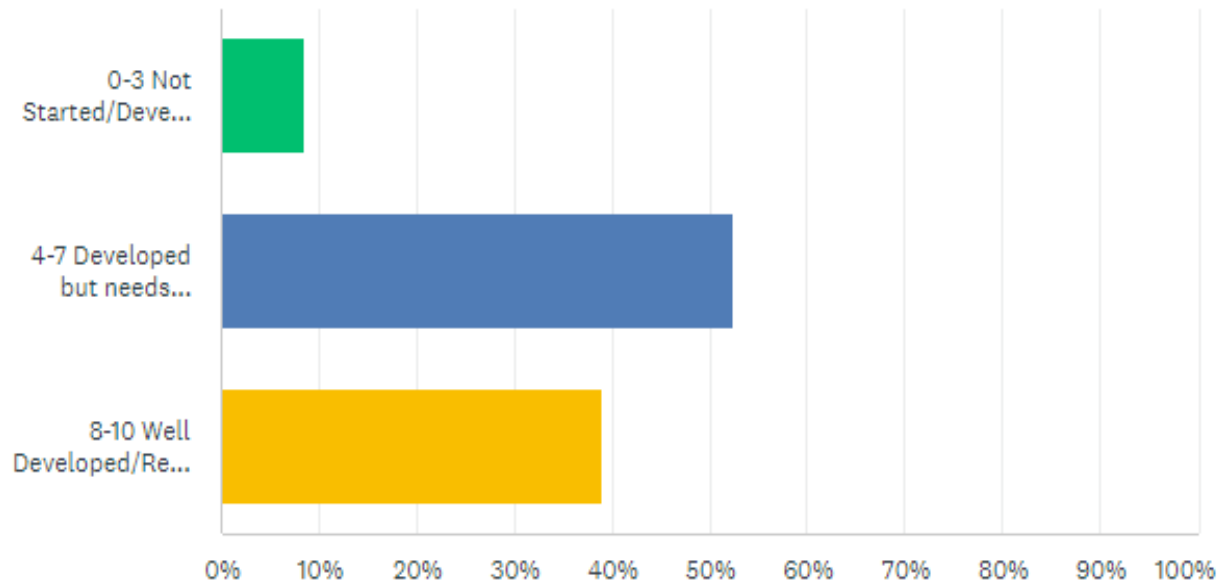
Answered: 59 Skipped: 0



ANSWER CHOICES	RESPONSES
▼ 0-3 Not Developed	3.39% 2
▼ 4-7 Developed but needs Improvement	49.15% 29
▼ 8-10 Well Developed/ Realized	49.15% 29
Total Respondents: 59	

COOP Project: Building Phase

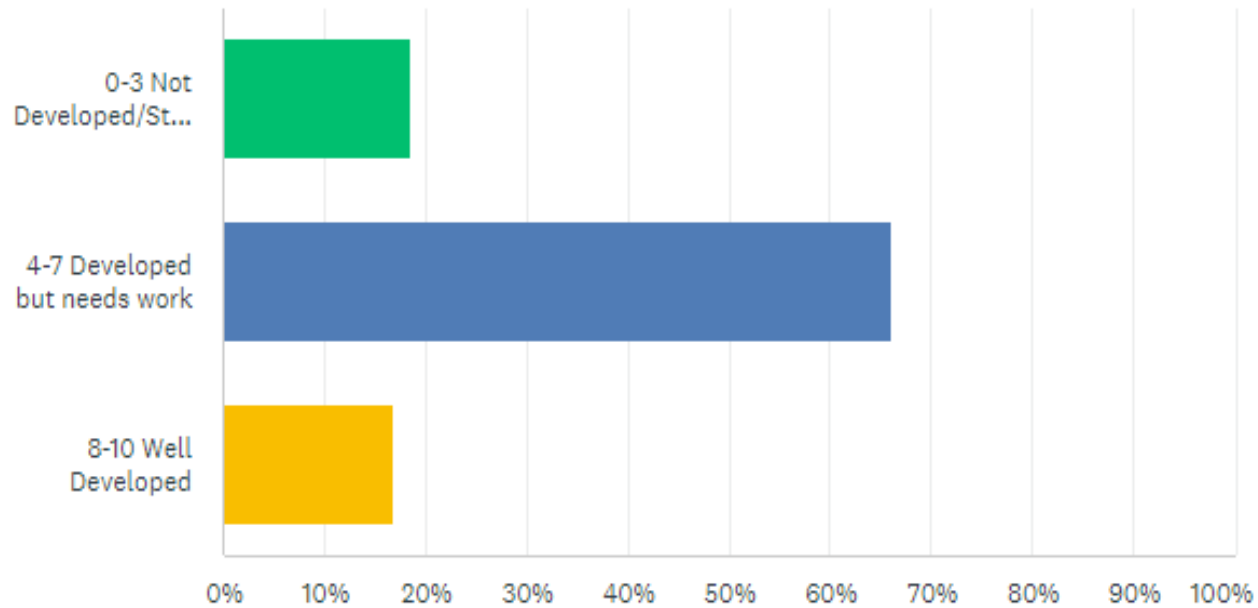
Answered: 59 Skipped: 0



ANSWER CHOICES	RESPONSES
▼ 0-3 Not Started/Developed	8.47% 5
▼ 4-7 Developed but needs further work	52.54% 31
▼ 8-10 Well Developed/Realized	38.98% 23
Total Respondents: 59	

COOP Project: Maintaining Phase

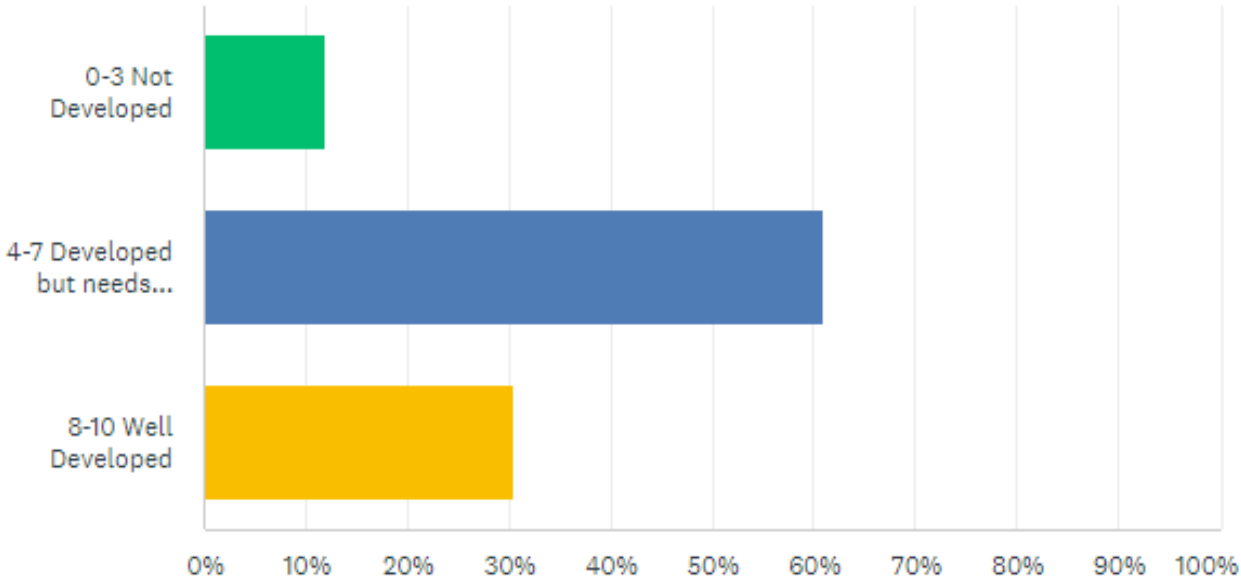
Answered: 59 Skipped: 0



ANSWER CHOICES	RESPONSES
▼ 0-3 Not Developed/Started	18.64% 11
▼ 4-7 Developed but needs work	66.10% 39
▼ 8-10 Well Developed	16.95% 10
Total Respondents: 59	

Over-all COOP Assessment

Answered: 59 Skipped: 0



ANSWER CHOICES	RESPONSES
0-3 Not Developed	11.86% 7
4-7 Developed but needs Improvement	61.02% 36
8-10 Well Developed	30.51% 18

Total Respondents: 59

MD Cyber Incident Response and Recovery

MD Presentation Questions

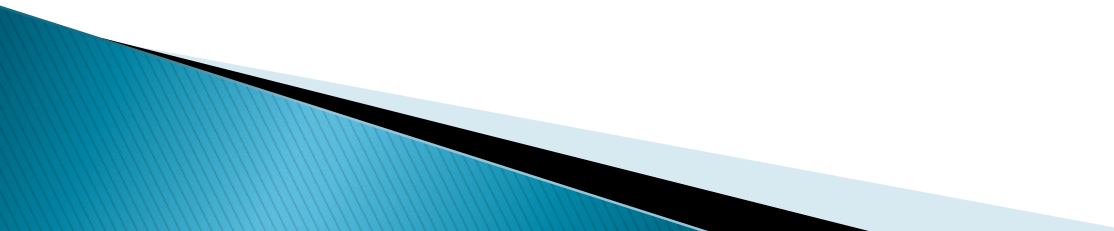
Q: What are the primary preventative steps you would recommend in the area of education for non-technical staff?

A: Continuous cyber awareness education is great, but there is only so much you can do. It's more a matter of being prepared on how to respond on when something happens (because no matter how careful you are, it can happen). **Back-ups and DR planning are key and Incident Command (ICS) Training is critical for all parties that play role in response.**


MD Presentation Questions

Q: With the increase in remote work do you recommend additional anti-spyware software for non-state issued devices to protect information?

A: MD is not aware of any authority or specific anti-spyware software for non-state issued devices that can be leveraged by the state. It is best practice to issue state resources for anyone requiring access to the state network for security purposes.



Key Notes

- ▶ ICS training is critical among all different parties responding to an incident (when responders understand their roles in ICS, and how they fit into those roles– recovery moves faster.)
 - ▶ Exercising together and knowing your counterparts in other agencies smooths the recovery process significantly.
 - ▶ During one event, pairing Vendor/External ICS participants with internal ICS roles worked to ensure everyone had the right information and could respond accordingly.
- 

MD Presentation Questions

NOTE: Delaware's reporting requirement for any breach of an application supporting state processes is to notify the Insurance Coverage Office immediately. They are the vehicle through which the state's cyber insurance is called in and that coverage does require specific steps to be taken. DTI should also be notified and will be the vehicle through which additional resources may be leveraged to help with digital forensics, data recovery, etc.

Kent County Cyber Incident



Kent County

Presentation Questions

Q: What have you done differently now on training?

A: Employee response to training is better received– Most fully accept and see the need. There were a lot of things that just weren't being done before this incident because the focus wasn't there or the funding – now we have a much stronger focus on security, disaster recovery, and cyber education than in the past.

Kent County

Presentation Questions

Q: Any key take-aways you want to highlight?

A: Make sure you know what back-ups exist for your data, but more importantly that you can recovery your system (DR). Just having a back-up copy of the data isn't enough.

Kent County

Presentation Questions

Q: How was HR tied into the response process?

A: HR was closely tied into the command team– they held town halls in order to ensure necessary information was shared to stakeholders and employees.

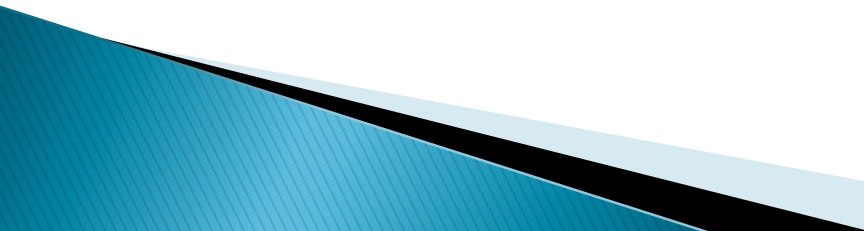
Kent County

Presentation Questions

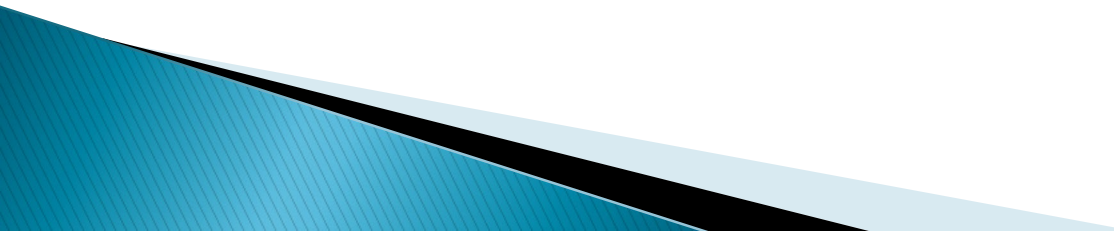
Q: Did you find that the technology dependence hindered recovery and that perhaps moving back to a less technology dependency would be helpful?

A: No, found that moving to better and more advanced technology would have resulted in better protection and recovery. The more antiquated processes tend to be labor-heavy and less streamlined. For example, processes that required faxes and spreadsheets were out of date and couldn't be easily recovered.

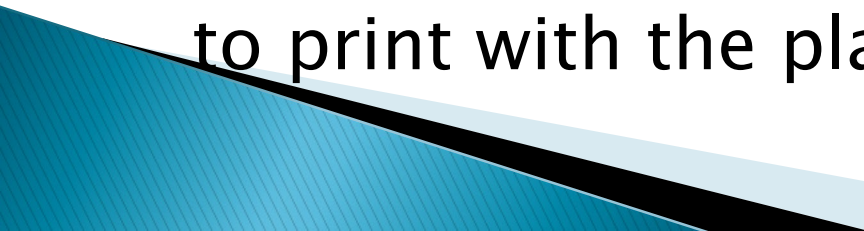
Key Notes:

- ▶ Incident Management is critical to recovery (all the stakeholders have a place and a role and need to know how to work together). This is helped through exercising together.
 - ▶ Succession Planning is a must– stressful situations tend to result in loss of staff (especially those that are eligible for retirement).
 - ▶ Consider tying in Stress Management options as a part of the recovery process.
- 

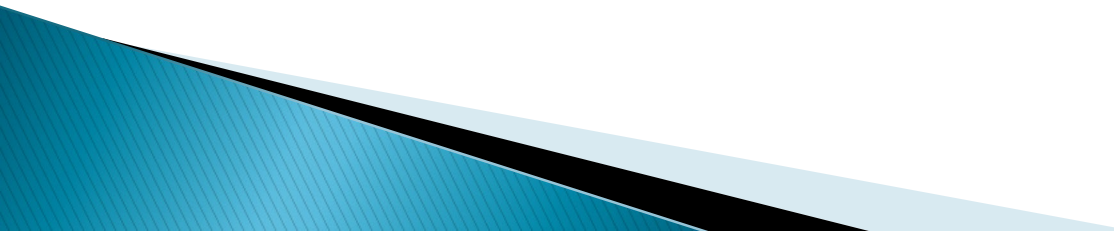
Key Notes:

- ▶ Hardest part of the incident was evaluating how it happened and exactly what went wrong (digital forensics)
 - ▶ Finding ways to ensure it doesn't happen again (bad actors share malware and information on who pays/doesn't pay, and will often exploit first access to your data, then black-mail on sharing that same data).
- 

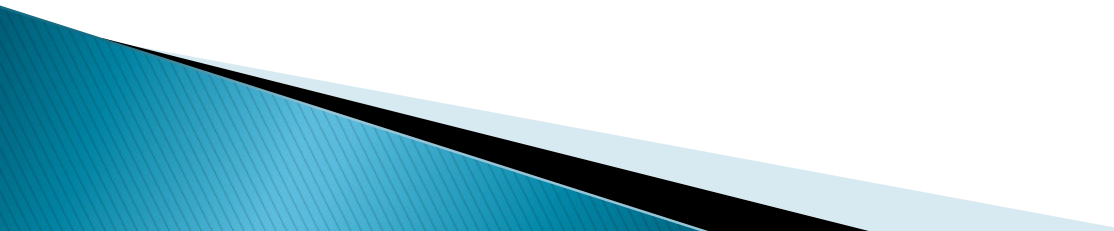
Applying what you learned...

- ▶ Cyber Incident Response Plan– can be added as a document attachment;
 - ▶ Create a Cyber Response Team (plan team) and link staff, customers/partners, and vendors that you anticipate needed for response;
 - ▶ Add tasks to ensure key actions, and reporting requirements are not missed;
 - ▶ Consider adding forms that should be added to your documents section (they don't need to print with the plan);
- 

Applying what you learned...

- ▶ Look at your Processes – are there work around procedures and are these documented;
 - ▶ Be sure you linked all of your applications and vital records to your processes (fill in any blanks for VR locations);
 - ▶ Review your last DR risk assessment with your IT/Leadership, are there area's where you can improve or mitigate risks;
- 

Applying what you learned...

- ▶ Ensure your ISO, Legal, HR, and PIO are all included in your Cyber discussions;
 - ▶ If interested in cyber insurance, reach out to the Insurance Coverage Office.
 - ▶ Review your latest cyber security training results with your ISO (if it isn't you) and encourage your staff to be cyber aware;
 - ▶ Attend Secure Delaware 2024 this fall!
- 

Steering Committee

- ▶ DTI Co-Chair: Lori Gorman
- ▶ DEMA Co-Chair: Christine Beste
- ▶ Vice-Chair: Cherie Dodge-Biron
- ▶ Education and Training Officer: Vanessa Briddell
- ▶ IT Systems Officer: Dan Cahall
- ▶ Vital Records: Tim Li
- ▶ Disaster Preparedness Officer: Alvin Jones
- ▶ Facilities Officer: Jennifer Coverdale

**Thank you and
see you at the Next Meeting!**



Maryland Perspective on Cyber Incidents

Delaware COOP Coordinators Council
May 16, 2024



Maryland
DEPARTMENT OF
EMERGENCY MANAGEMENT

Wes Moore | Governor

Aruna Miller | Lt. Governor

Russell J. Strickland | Secretary

[MDEM.MARYLAND.GOV](https://mdem.maryland.gov)

Introduction

Brian Bauer, MPIA, MBCP, CBCLA, CC, CCRP, CEM, CRMP, PCP

- Preparedness Branch Manager
 - State Continuity Unit
 - Cyber Preparedness Unit
- Agency Chief Information Officer

Ken Maloney, MA, MBCP, MCP, CBCLA, CCRP, CRMP, CHPCP

- State Continuity Unit Supervisor
- Agency Chief Data Officer

Recent Maryland Cyber Disruption Incidents

Incident/Event	Year	Cascading Impacts
Baltimore City Government	2019	<ul style="list-style-type: none">● Email● End-User Devices & Hardware● Government Services
Baltimore County Public Schools	2020	<ul style="list-style-type: none">● End User Devices & Hardware● Records & Data● Education Platforms
Maryland Department of Health	2021	<ul style="list-style-type: none">● Email● End-User Devices & Hardware● Records & Data● Government Services● Healthcare Services
Washington County Cybersecurity Incident	2022	<ul style="list-style-type: none">● 911 Center● Email● State Service Connectivity● Inmate Release Delays

Observations

- Command & Coordination (Crisis Management)
- Parallel Operations
 - Continuity
 - Continuity of Operations (Essential Functions)
 - Business Continuity (Revenue & Reputation)
 - IT Disaster Recovery
 - Cyber Incident Response
 - Data Privacy
 - Crisis Communications
 - Consequence Management
- Cyber Insurance Utilization & Engagement
- Technical vs Non-Technical
- Law Enforcement Engagement

Questions





The mission of the Maryland Department of Emergency Management is to proactively reduce disaster risks and reliably manage consequences through collaborative work with Maryland's communities and partners.



KENT COUNTY

LEVY COURT

Sometimes in life you don't know what you
don't know

Director, Information Technology



Known

Things we are aware of and understand

Things we are aware of but don't understand

Unknown

Things we understand but are not aware of

Things we are neither aware of nor understand

Knowns

Unknowns



July 8, 2023

Kent County was hit by a cyber incident by the Black Cat Ransomware Group, which deployed a ransomware virus within the County's network environment, rendering most county services and multiple servers and employee workstations inoperable.



KENT COUNTY LEVY COURT
DELAWARE

Timeline of Events

June 14
WinRM Sessions

June 20
Remote Desktop Protocol (RDP)
RDClient.exe

June 22
WinRM Sessions
Authentication of an Employee

June 30
Remote Utilities
ADRecon.exe

July 6
Execution
Connection
Service Creation
MSI Installation
Defender Detection
New User Created

July 8
Execution
Connection
Evasion
Clean-Up (Anti-Forensics Tactics)

Listen

Control

Disguise

Reporting
&
Extraction

Evasion

Execution of
Ransomware





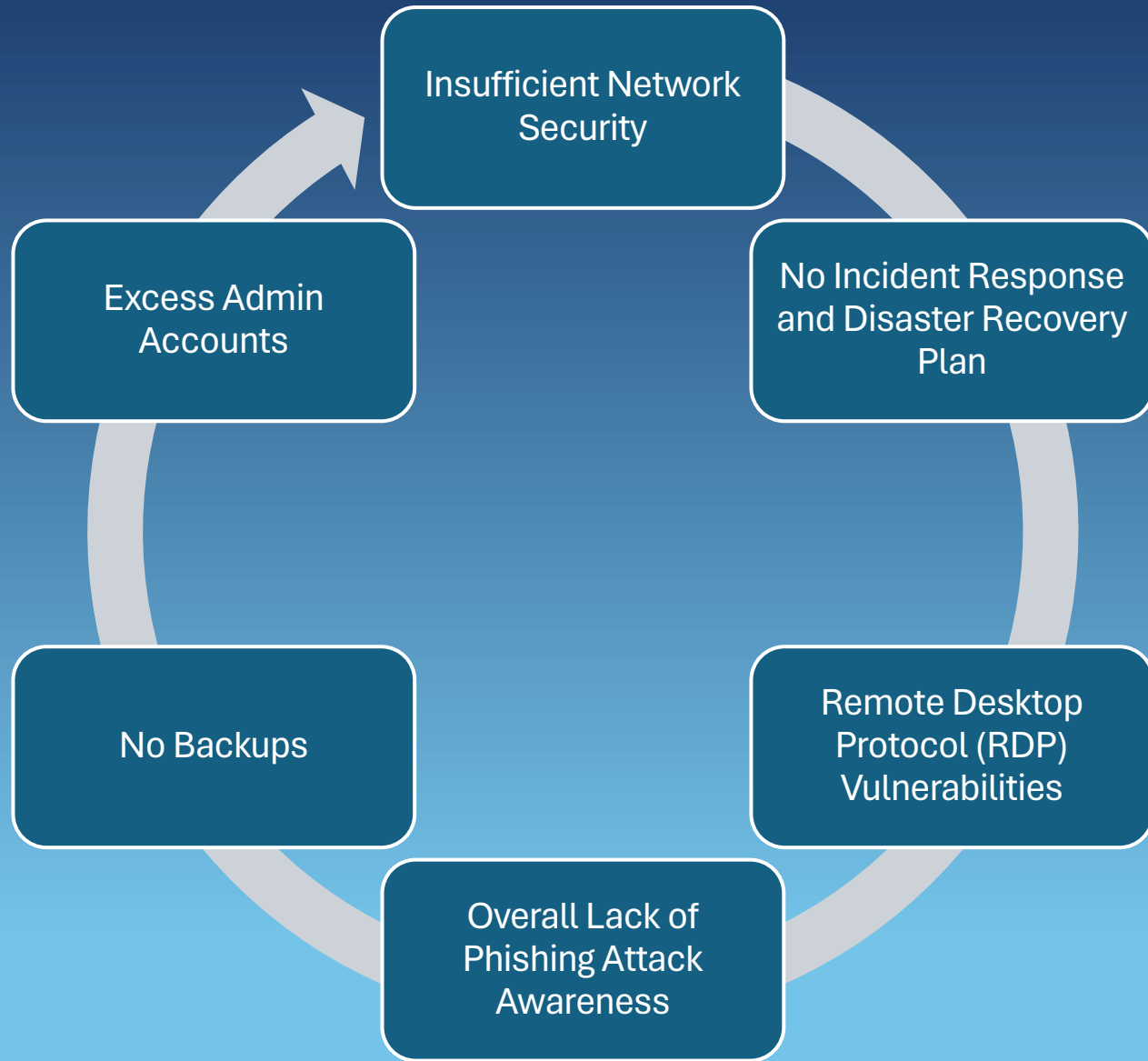
KENT COUNTY LEVY COURT
DELAWARE

FACTORS THAT CONTRIBUTED TO THE ATTACK

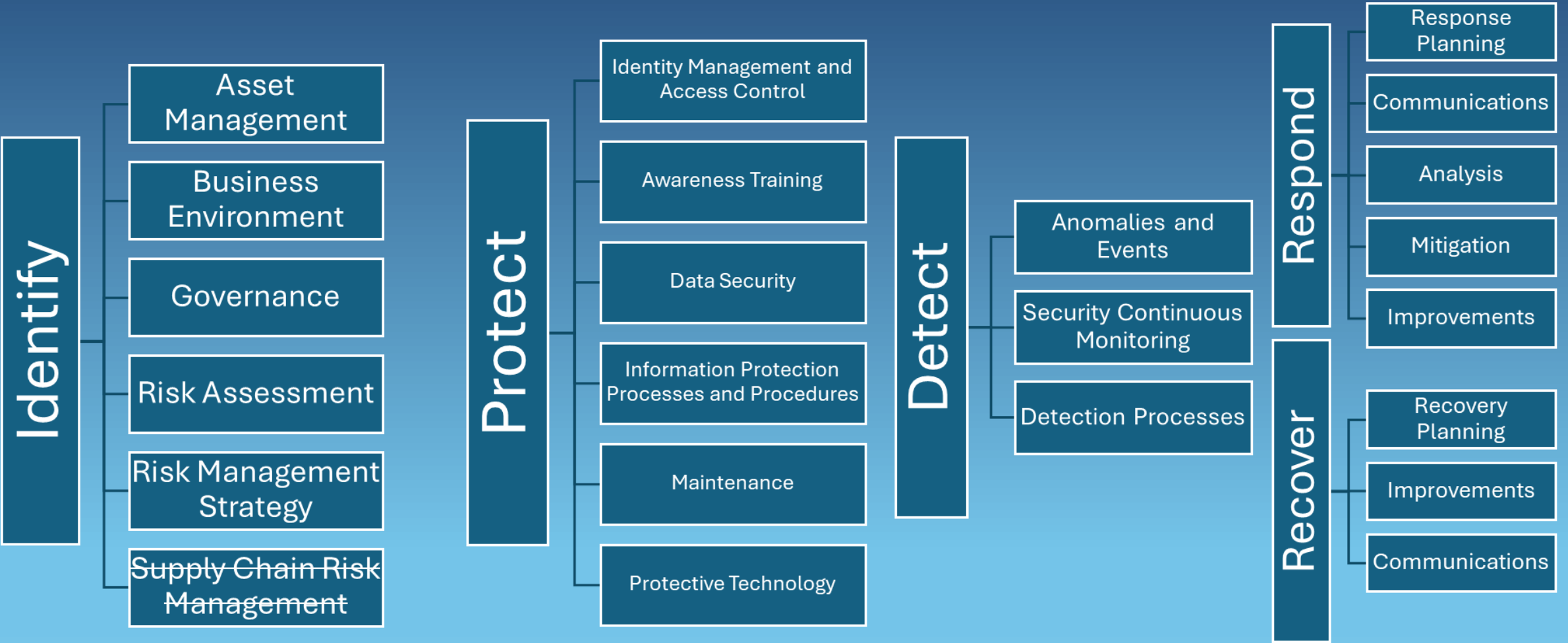
- Lack of Modern Advanced Security Tools
- Unpatched and Outdated Software and Systems
- Lack of Data Backup and Recovery
- Lack of Network Segmentation
- Lack of Employee Training



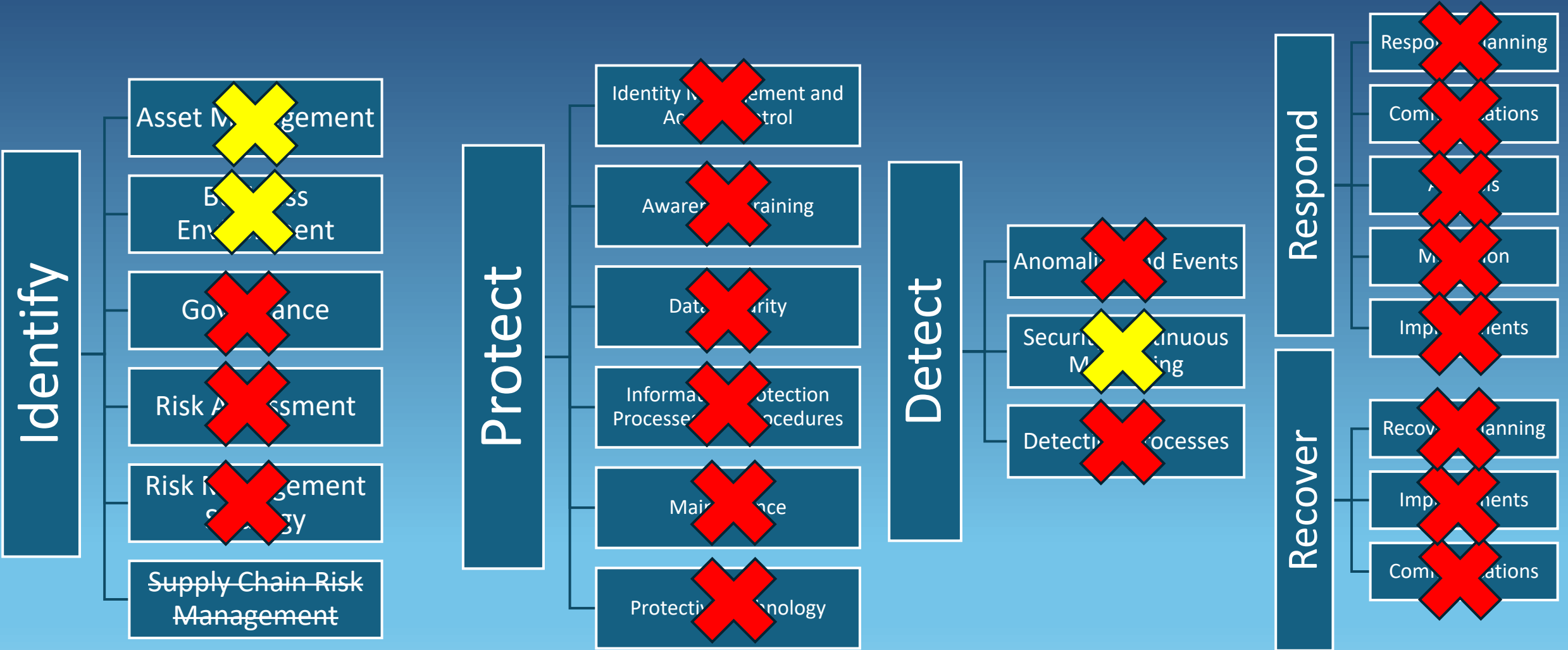
Any one of these factors leaves you vulnerable



NIST Framework



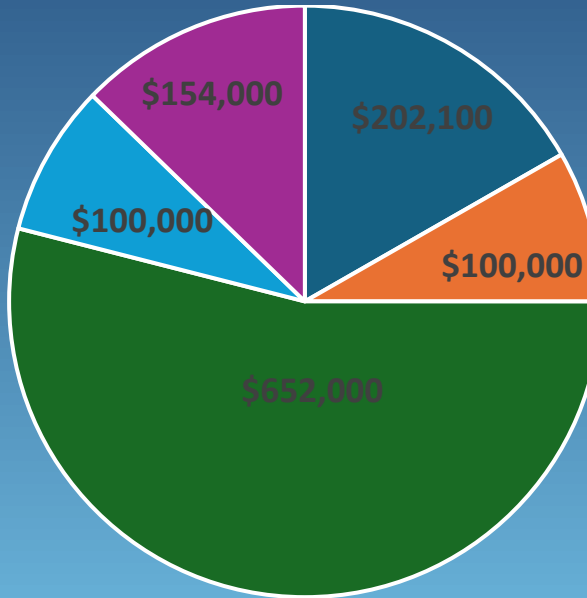
Prior to July's Incident



RECOVERY COST

\$950,100

Without SCADA Recovery/Update



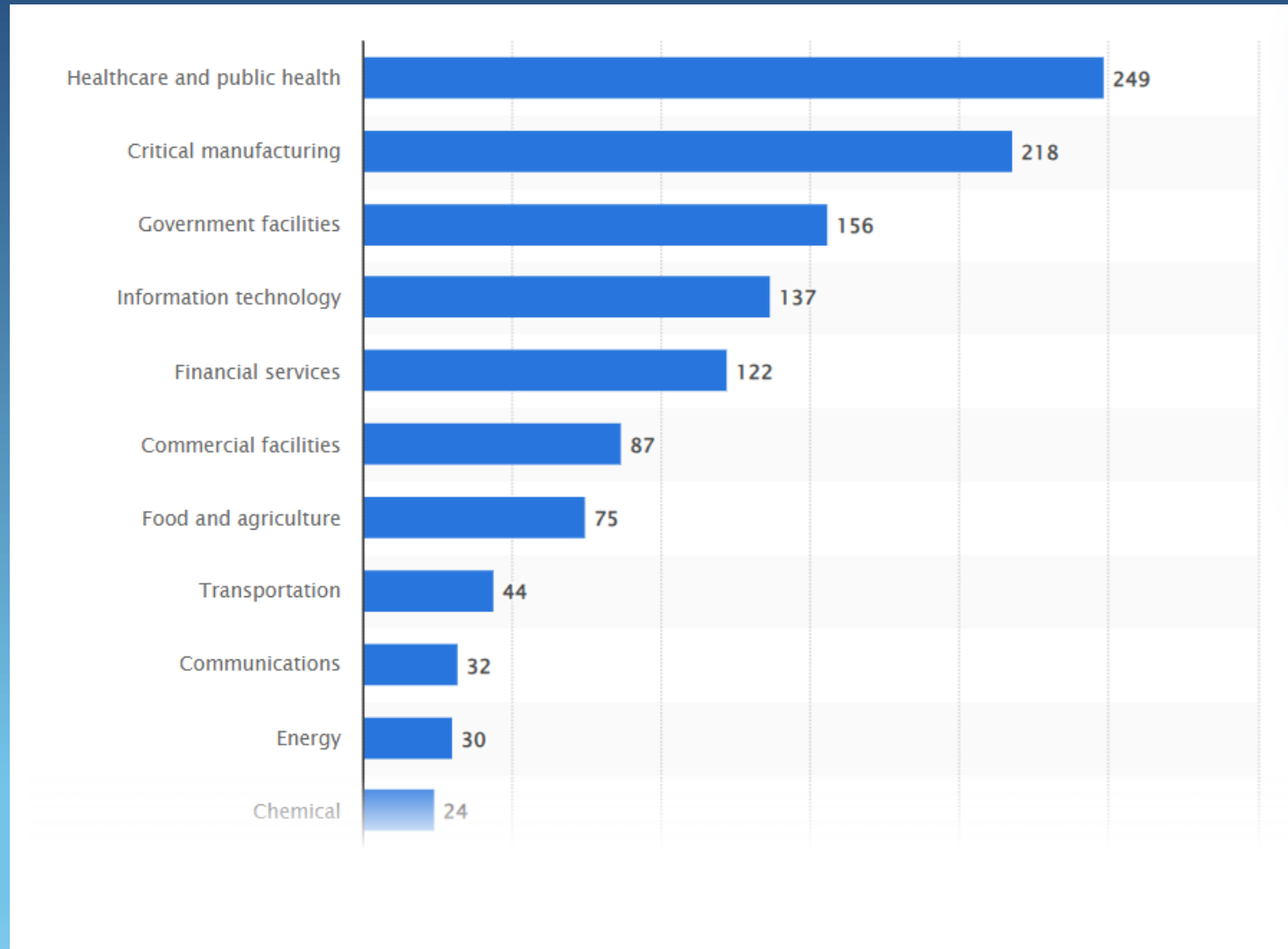
\$1,204,100

With SCADA Recovery/Update

■ Hardware ■ Software ■ Professional Services ■ Microsoft Server Lic ■ SCADA



Industry sectors most targeted by ransomware attacks in the United States in 2023



Ransomware FACTS

- Ransomware attacks frequently target State and Local governments.
- Ransomware attacks can disrupt essential government services such as public safety
- Recovering from a ransomware attack can be financially burdensome
- Ransomware attacks raise concerns about the security of sensitive citizen data.
- Local governments typically have limited budgets and IT resources available for cybersecurity.



Ransomware Stats

- The average ransom payment in Q2 2023 was \$704,144. Up 126% from Q1 2023 (Source: Coveware)
- The median ransom payment in Q2 2023 was \$190,424. Up 20% from Q1 2023
- The average cost of a ransomware insurance claim \$352,000 (Source: SouthPoint Risk)
- The average ransomware attack causes 16.2 days of downtime. (Source: Comparitech Ltd.)
- 25% of small businesses hit by ransomware go out of business, while 66% faced significant revenue loss. (Source: ALG)



The Big 5

2FA/MFA

Endpoint Detection and Response

Email Security

Data Backup

Incident Response Plan



Resources



**DELAWARE DEPARTMENT OF
TECHNOLOGY & INFORMATION**



KENT COUNTY
LEVY COURT

INFORMATION TECHNOLOGY OFFICE

**CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY**



AMERICA'S CYBER DEFENSE AGENCY



KENT COUNTY LEVY COURT
DELAWARE



KENT COUNTY

LEVY COURT

So, now you know,
what are you going to do about it?

Thank You
