# The STAGEnet Security Model

Peeling Away the Layers

March 17, 2015

NDSU Memorial Union

Rose Room

## NDSU 2015 Cyber Security Conference

# Art Bakke

Enterprise Information Security Administrator / Security Architect

## Goal

- To describe how security is strategically developed and implemented for STAGEnet enterprise network based on the needs of the various stakeholders.

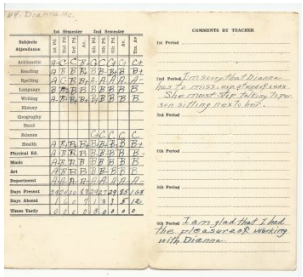
## Agenda

- The Crown Jewels
- Roles and Responsibilities
- STAGEnet
- Cybersecurity Framework

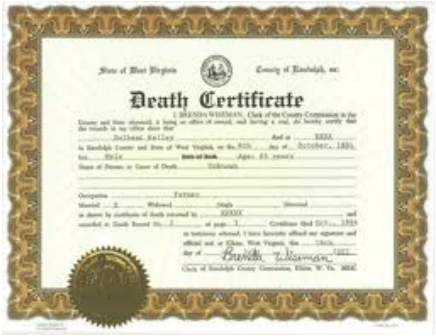
# The Crown Jewels

## From Cradle




## To Grave




## And Bevond!

North Dakota
L • O • T • T • E • R • Y

## ITD's Roles and Responsibilities

- Per NDCC 54-59-05.2 and 54-59-05.14 ITD has the authority and responsibility for information systems security surrounding State of North Dakota information technology assets.
- ITD is responsible for protecting the availability, integrity, and confidentiality of the state's information systems and the data stored in information systems that are managed by ITD.
- ITD also directs the development of standards, policies and guidelines for enterprise security. This is done in collaboration with state agencies through the Enterprise Architecture process.
  - **Centralized Model**

## ITD Security Administrator Roles and Responsibilities

- Lead enterprise information security team; manage and provide oversight for information security projects and programs
- Develop security direction for ITD, State of North Dakota, political subdivisions & K-12 schools
- Provide guidance to meet technical & legal requirements for access to 1,700+ servers, 10,000+ endpoints for 100,000+ users

## What is STAGEnet?

# STAGEnet

- The North Dakota Statewide Technology Access for Government and Education network (STAGEnet) provides broadband connectivity, Internet access, video conferencing and other networking services to all state agencies, colleges and universities, local government, and K-12.

## What is STAGEnet? (continued)

- STAGEnet is governed as a partnership between government and education that consists of three committees*, which aid in planning, prioritizing, approving standards, policies and procedures. Because of the varied nature and the variety of resources that use this network, security for it is built based on layers much like those of an onion.
  - *Executive Committee (State CIO, NDUS CIO, K12 Director, ITD Network Services Director)
  - *Management Committee (State, NDUS, ITD, IVN)
  - *Technical Committee (State, NDUS, ITD, K12)

# Cybersecurity Framework

State of North Dakota
Information Technology Department
Cybersecurity Framework
April 4, 2014

Chief Information Officer

Mike J. Ressler

Mike J. Ressler

Deputy CIO/Director of ITD

Daniel E. Sipes

Daniel E. Sipes

# Cybersecurity Framework

Table of Contents

## Cybersecurity Framework

- Security Framework Roles and Responsibilities
  - ITD Executive and Information Security Management
    - CIO/Deputy CIO Responsibilities
    - Enterprise Security Administrator
    - ITD Virtual Security Team
  - Information/Application Owners
    - Agency Directors
    - Agency IT Coordinators
    - Agency Security Officers

## Cybersecurity Framework

- Security Framework Roles and Responsibilities
  - Technology Providers
    - ITD Architects
    - Project Managers
    - Developers
    - Network and System Administrators
  - Supporting Functions
    - Audit, Physical Security, Contingency Planning
    - Quality Assurance, Training, Procurement
    - Human Resources, Facilities
  - Users of Information and Systems

# Cybersecurity Framework Core

- Security Areas
  - Network Security
  - Host Security
  - Application Security
  - User Security

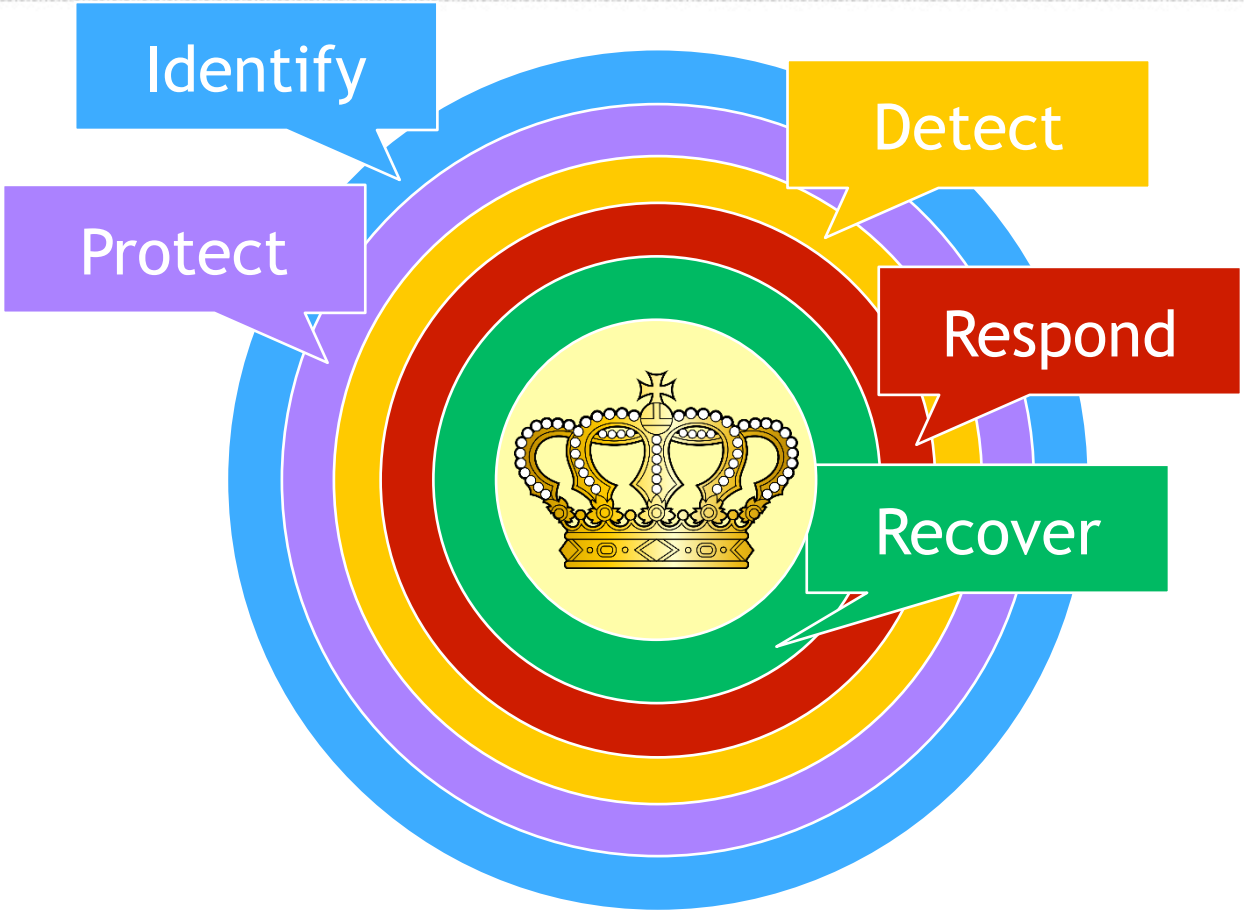
| Function Unique Identifier | Function | Category Unique Identifier | Category |
|---|---|---|---|
| ID | Identify | ID.AM | Asset Management |
| | | ID.BE | Business Environment |
| | | ID.GV | Governance |
| | | ID.RA | Risk Assessment |
| | | ID.RM | Risk Management |
| PR | Protect | PR.AC | Access Control |
| | | PR.AT | Awareness and Training |
| | | PR.DS | Data Security |
| | | PR.IP | Information Protection Processes and Procedures |
| | | PR.PT | Protective Technology |
| DE | Detect | DE.AE | Anomalies and Events |
| | | DE.CM | Security Continuous Monitoring |
| | | DE.DP | Detection Processes |
| RS | Respond | RS.CO | Communications |
| | | RS.AN | Analysis |
| | | RS.MI | Mitigation |
| | | RS.IM | Improvements |
| RC | Recover | RC.RP | Recovery Planning |
| | | RC.IM | Improvements |
| | | RC.CO | Communications |

# Cybersecurity Framework

*Appendix A – Framework Core*

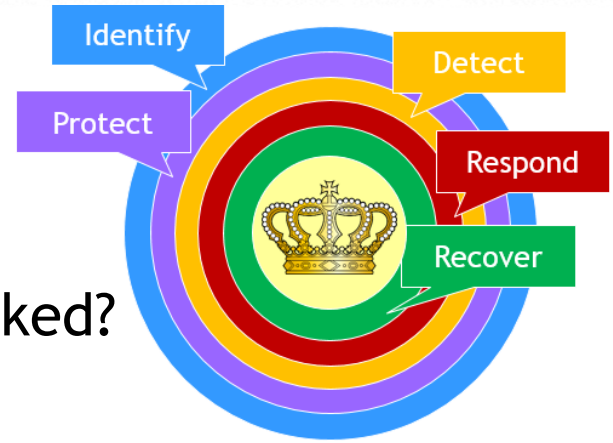
| Function | Category | Subcategory | Policies | Informative Resources |
|---|---|---|---|---|
| RESPOND (RS) | **Response Planning (RP):** Response processes and procedures are maintained and tested to ensure timely response of detected cybersecurity events | **RS.PL-1:** Response plan is implemented during or after an event. | • ITD.IR | • **ISA 99.02.01** 4.3.4.5.1<br>• **NIST SP 800-53** Rev. 4 CP-10, IR-4<br>• **CCS CSC** 18 |
| | **Communications (CO):** Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from federal, state, and local law enforcement agencies | **RS.CO-1:** Personnel know their roles and order of operations when a response is needed | • ITD.IR | • **ISO/IEC 27001** A.13.2.1<br>• **ISA 99.02.01** 4.3.4.5.2, 4.3.4.5.3,<br>• 4.3.4.5.4<br>• **NIST SP 800-53** Rev 4 CP-2, IR-8 |
| | | **RS.CO-2:** Events are reported consistent with established criteria | • ITD.IR | • **ISO/IEC 27001** A.13.1.1, A.13.1.2<br>• **ISA 99.02.01** 4.3.4.5.5<br>**NIST SP 800-53** Rev 4 IR-6, IR-8 |
| | | **RS.CO-3:** Detection/response information, such as breach reporting requirements, is shared consistent with response plans, including those related to privacy and civil liberties | | **ISO/IEC 27001** A.10 |
| | | **RS.CO-4:** Coordination with stakeholders occurs consistent with response plans, including those related to privacy and civil liberties | • ITD.IR | • **ISO/IEC 27001** A.8.1.1, A.6.1.2, A.6.1.6, A.10.8.2<br>**NIST SP 800-53** Rev. 4 CP-2, IR-8 |
| | | **RS.CO-5:** Voluntary coordination occurs with external stakeholders (ex, business partners, information sharing and analysis centers, customers) | | **NIST SP 800-53** Rev. 4 PM-15, SI-5 |

# Cybersecurity Functions - The basis for our Framework



## Cybersecurity Functions - The basis for our Framework

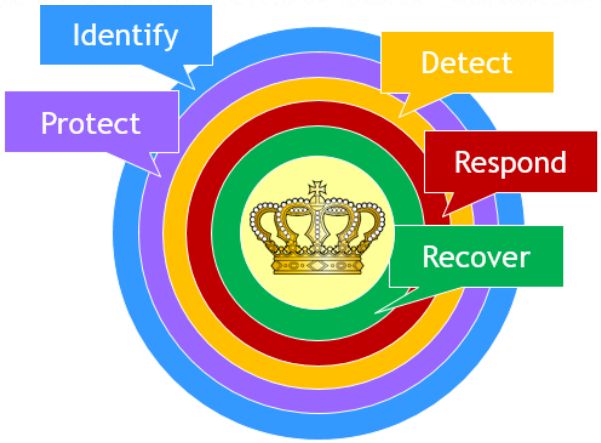
- **Identify** - What do I need to protect?
- **Protect** - What controls do I use?
- **Detect** - How do I know I am being attacked?
- **Respond** - What actions do I take?
- **Recover** - How do I return to normal operations?



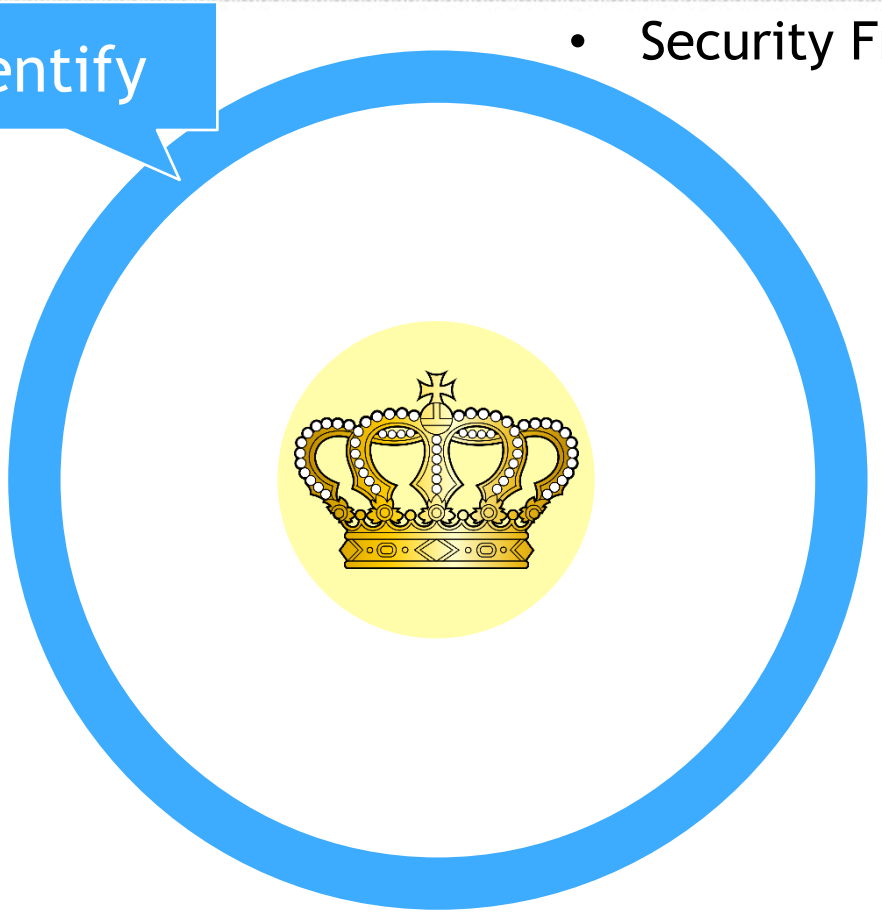

- Effective security encompasses the relationship between all five functions - it is a process, not a product.

## Cybersecurity Principles

- Security by Design
- Defense in Depth
- Compartmentalize
- Utilize Control Points (Choke) Points
- Fail Securely
- Secure the Weakest Link



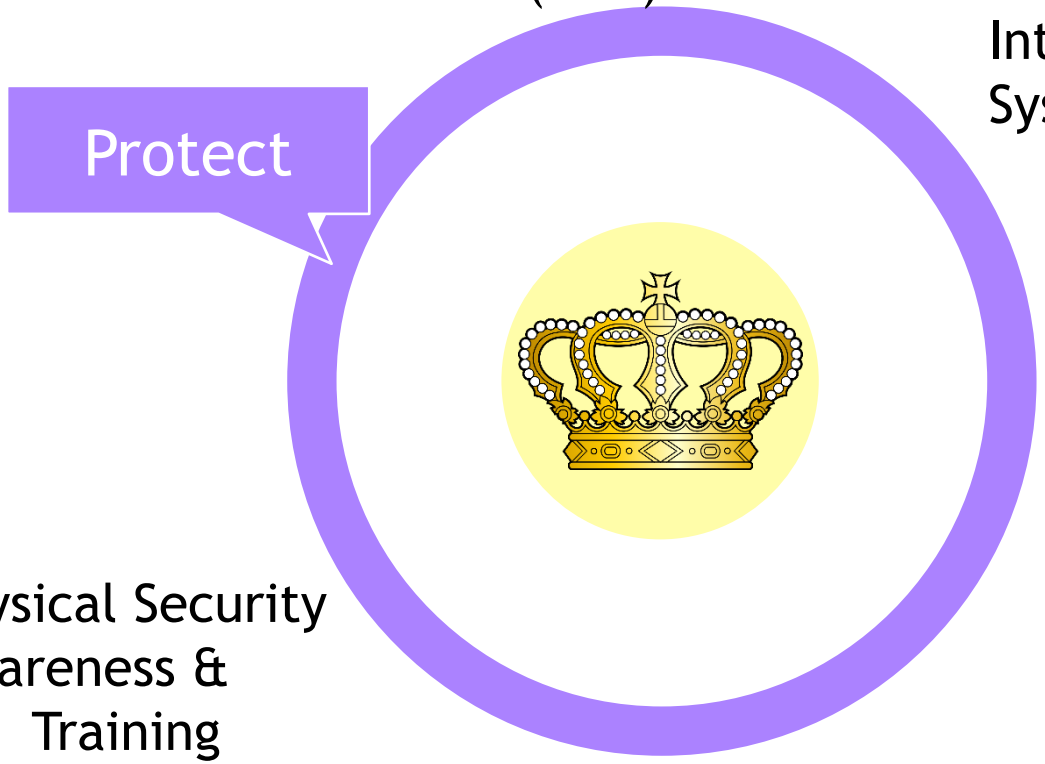
# What Do I Need to Protect?




- Security Frameworks
- Audits/Risk Assessments
- Data Classification

## What controls do I use?

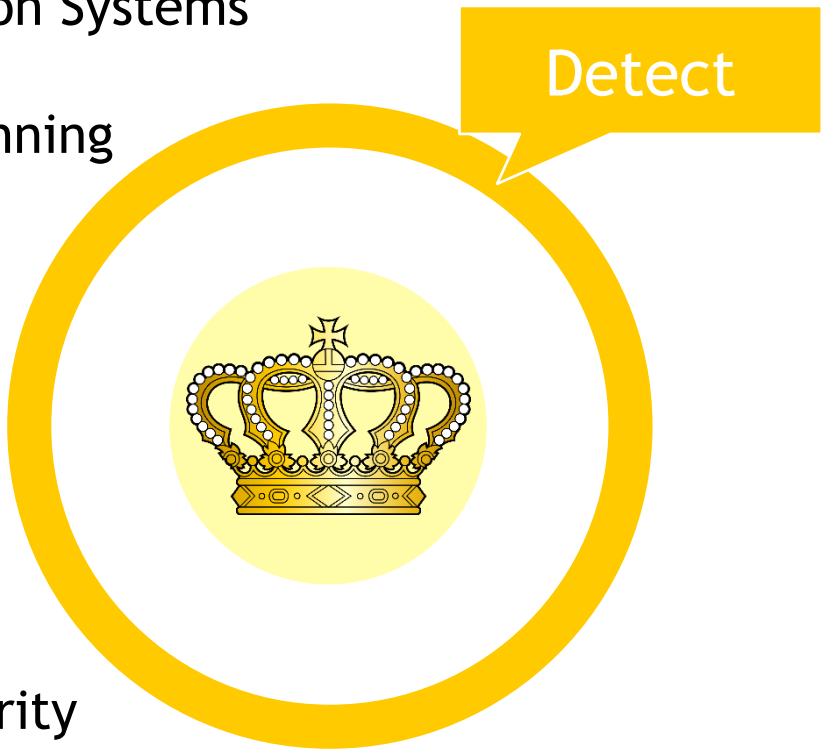
- Encryption
- Virtual Private Networks (VPN)
- Advanced Firewalls & Intrusion Prevention Systems (IPS)




- Physical Security
- Awareness & Training
- Identity & Access Management

# How do I know I am being attacked?

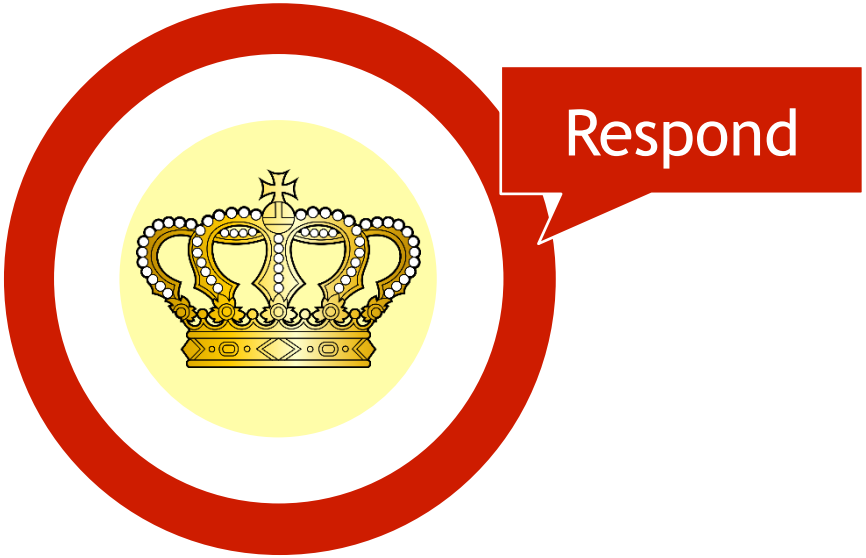
- Intrusion Detection Systems (IDS)
- Vulnerability Scanning




- Audit Logs – Security Information and Event Management (SIEM) Systems

## What actions do I take?

- Security Incident Response Team and processes
- Cybersecurity Forensics
- Proactive Vulnerability Management



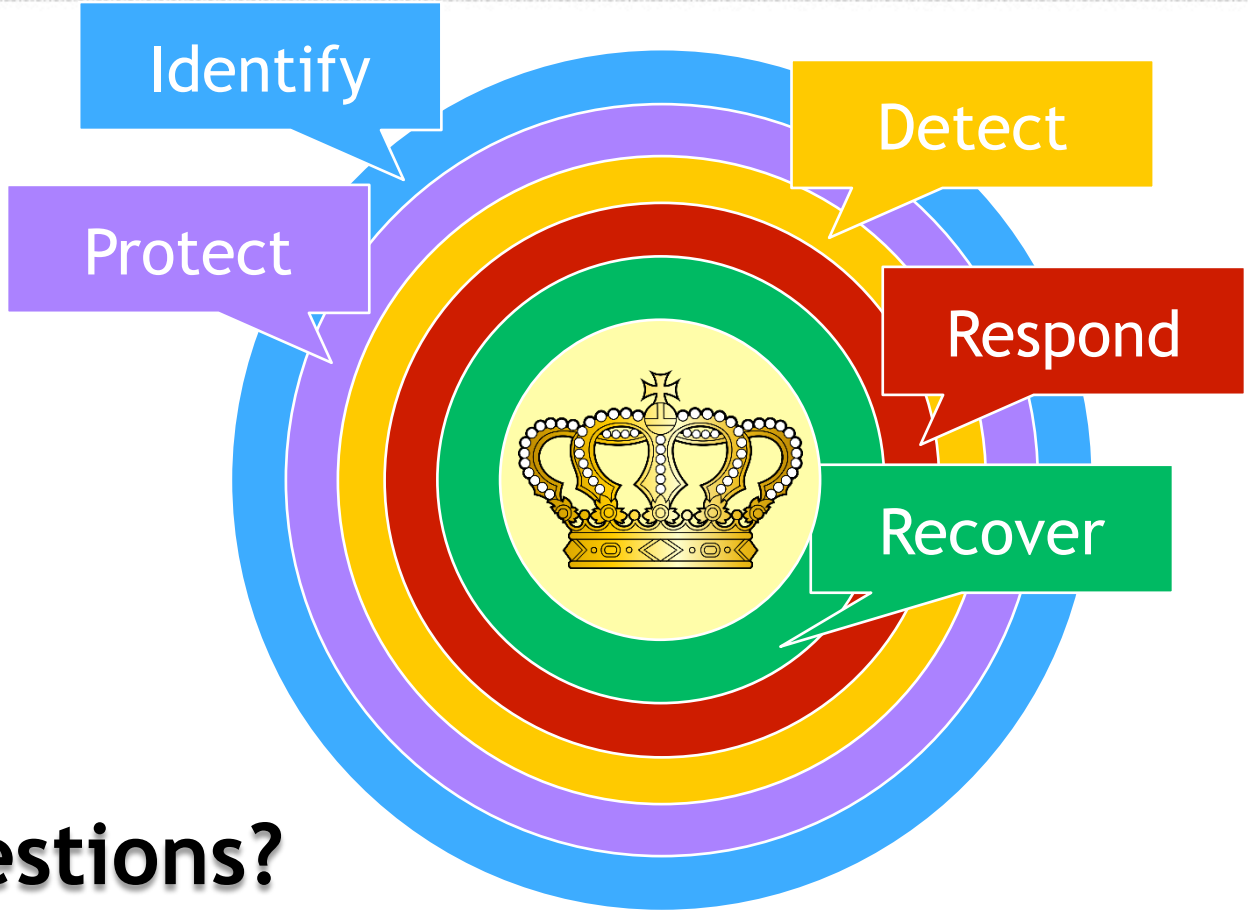
## How do I return to normal operations?

- Contingency Planning
- Data Backups and High Availability Systems
- Secondary Data Centers

## Conclusion

- The Crown Jewels
- Roles and Responsibilities
- STAGEnet
- Cybersecurity Framework

## Cybersecurity Functions - The basis for our Framework




# Questions?

# Thank you!

Art Bakke
Enterprise Information Security Administrator / Security Architect
State of North Dakota
ambakke@nd.gov