Office of the
Chief Information Officer
Iowa Department of Management

Cyber Incident Response Program: Preparing organizations for crisis

ISAC Annual Conference

Introductions

State of Iowa Chief Information Security Officer (CISO)

- Principal executive reporting into Iowa’s Executive Branch
- Support government operations against foreign and domestic cyber threats
- Promote and foster a cyber culture across Iowa
- Commoditize cyber operations and improve cyber resiliency
- Participating in national forums including National Association of Chief Information Officers and National Governors Association

Iowa Code 8B allows the OCIO to serve

- Executive, Judicial, and Legislative branches
- Iowa Counties and Cities
- Iowa Educational Institutions
- Iowa not-for-profits

Expected outcomes, key points

Shape to your business

- Sharing the State of Iowa’s practices, one size doesn’t fit all

Defensibility, liability, and risk

- Our teams should
  - Pay attention to the environment
  - Have situational awareness
  - Train for crises
  - Have documented processes

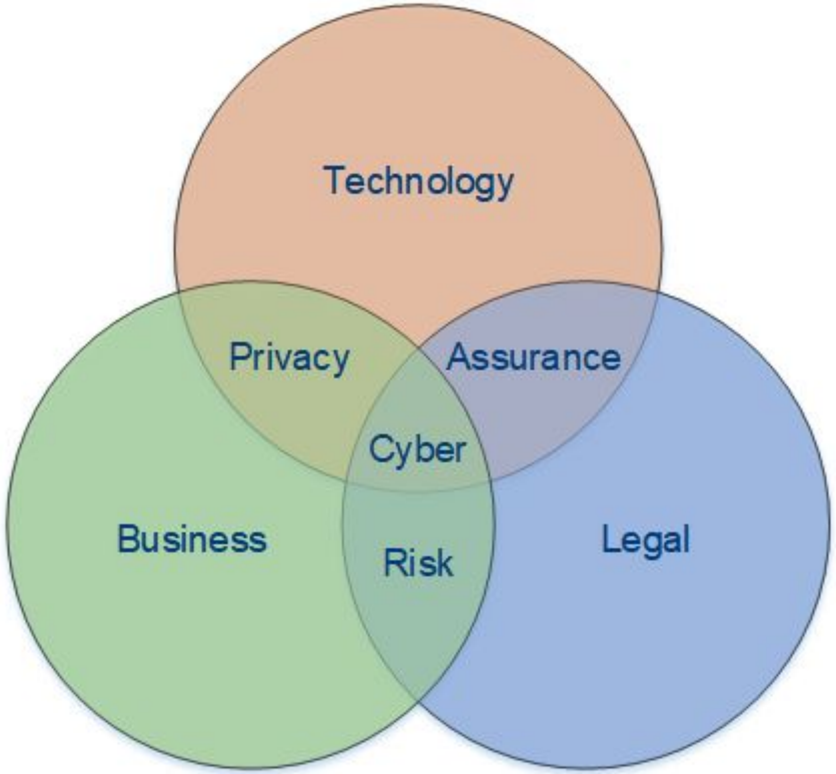
How does the State of Iowa define Cyber?

Infrastructure (on-premise and cloud)

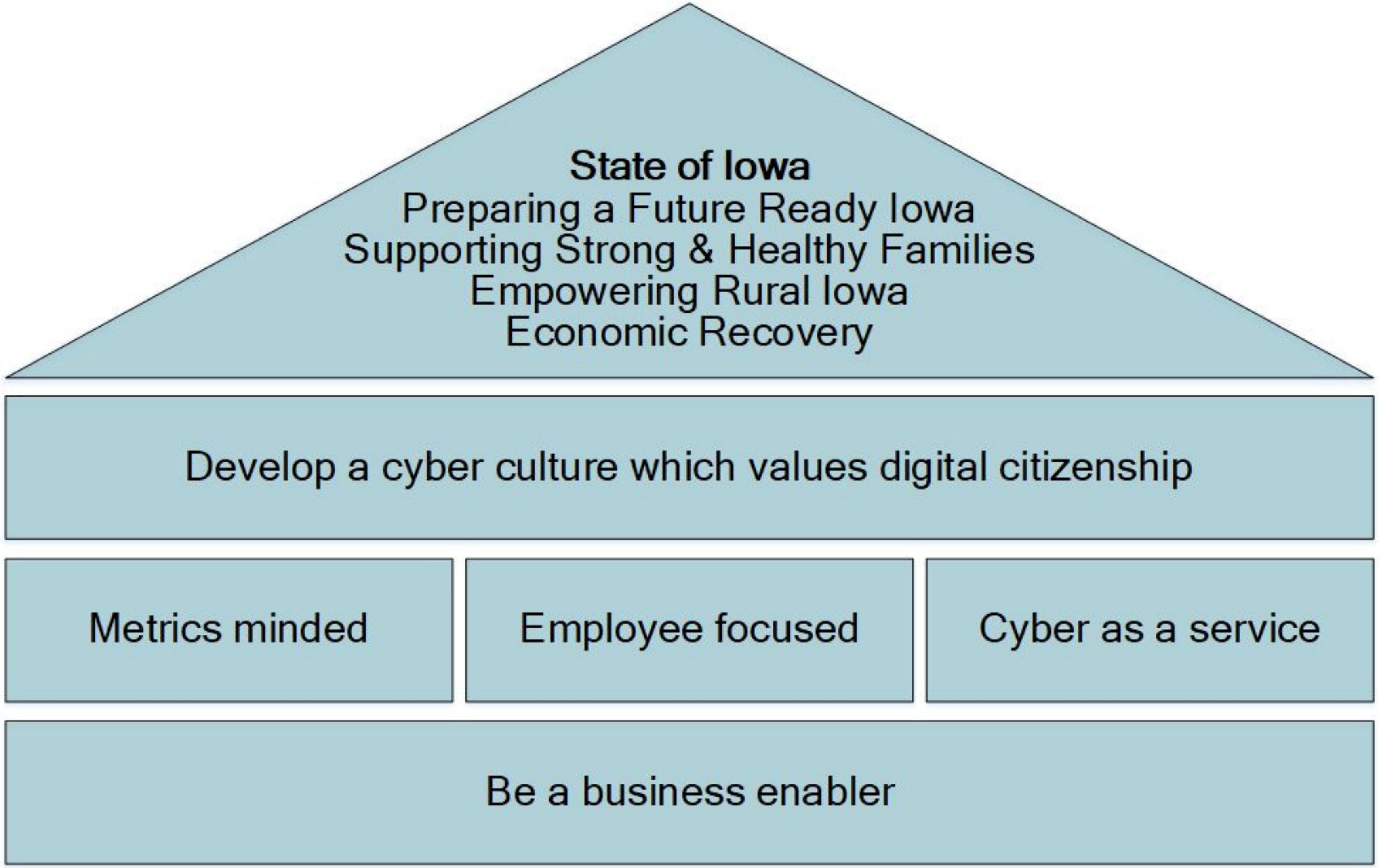
- Servers and disaster recovery
- State internet connections
- Personal computers
- Mobile devices

Information Security

- Organizational security governance
- Security awareness training
- Security operations and risk management
- Audit and compliance



Iowa's Cyber Pillars



State of Iowa
Preparing a Future Ready Iowa
Supporting Strong & Healthy Families
Empowering Rural Iowa
Economic Recovery

Develop a cyber culture which values digital citizenship

Metrics minded

Employee focused

Cyber as a service

Be a business enabler

Fear, Uncertainty, and Doubt (FUD)

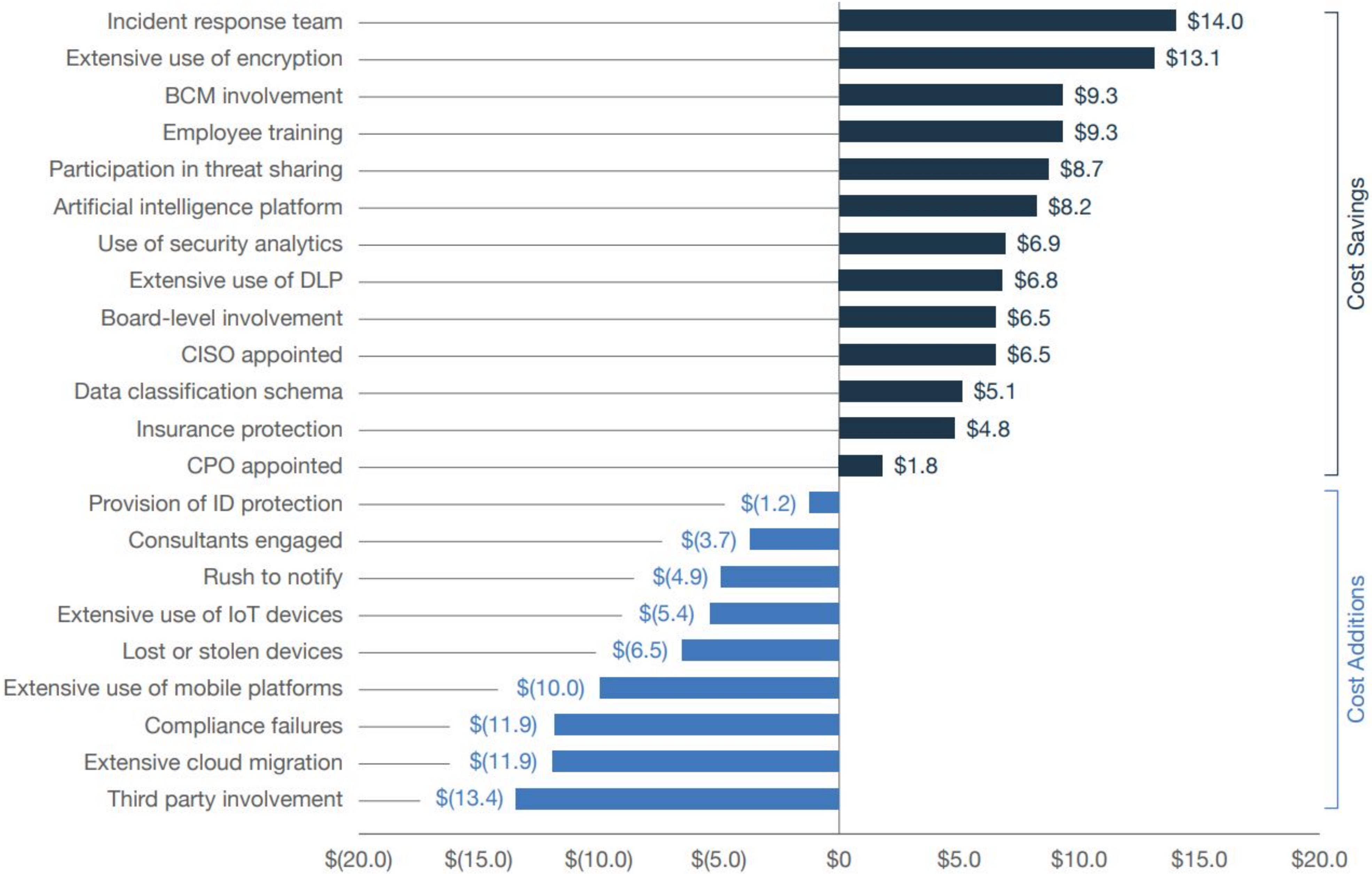
There are two types of organizations; those that know they've been hacked, and those who don't know they've been hacked.

Best way to guard against cyber attacks is to prevent them

~~FUD~~ vs business impact

- Averages per data breach (2021)
  - 26,335 records lost or stolen
  - $4.24 million financial loss of data breach
  - $161 loss per record lost or stolen

Source: IBM Security

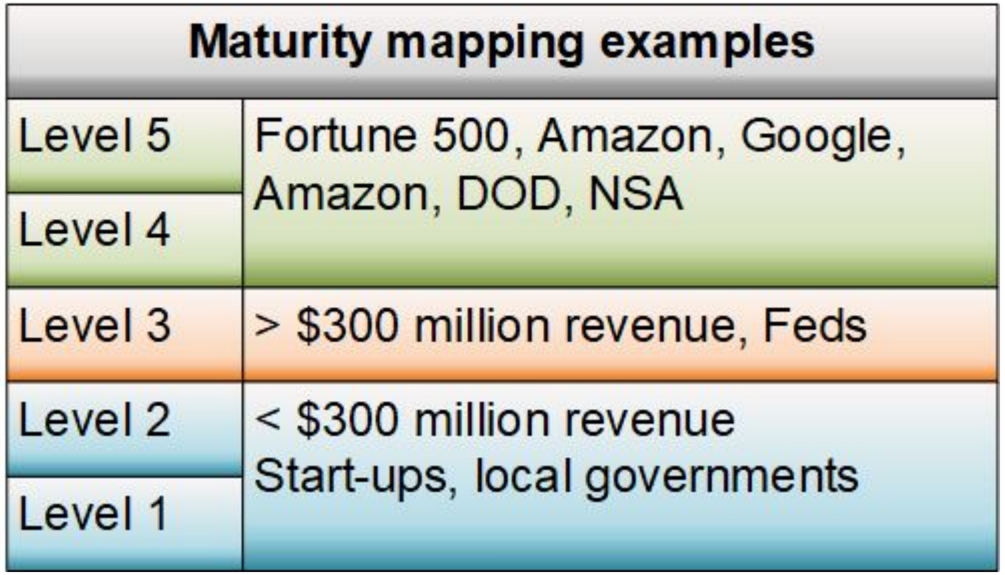


Source: IBM Security and Ponemon Institute

CMMI Framework

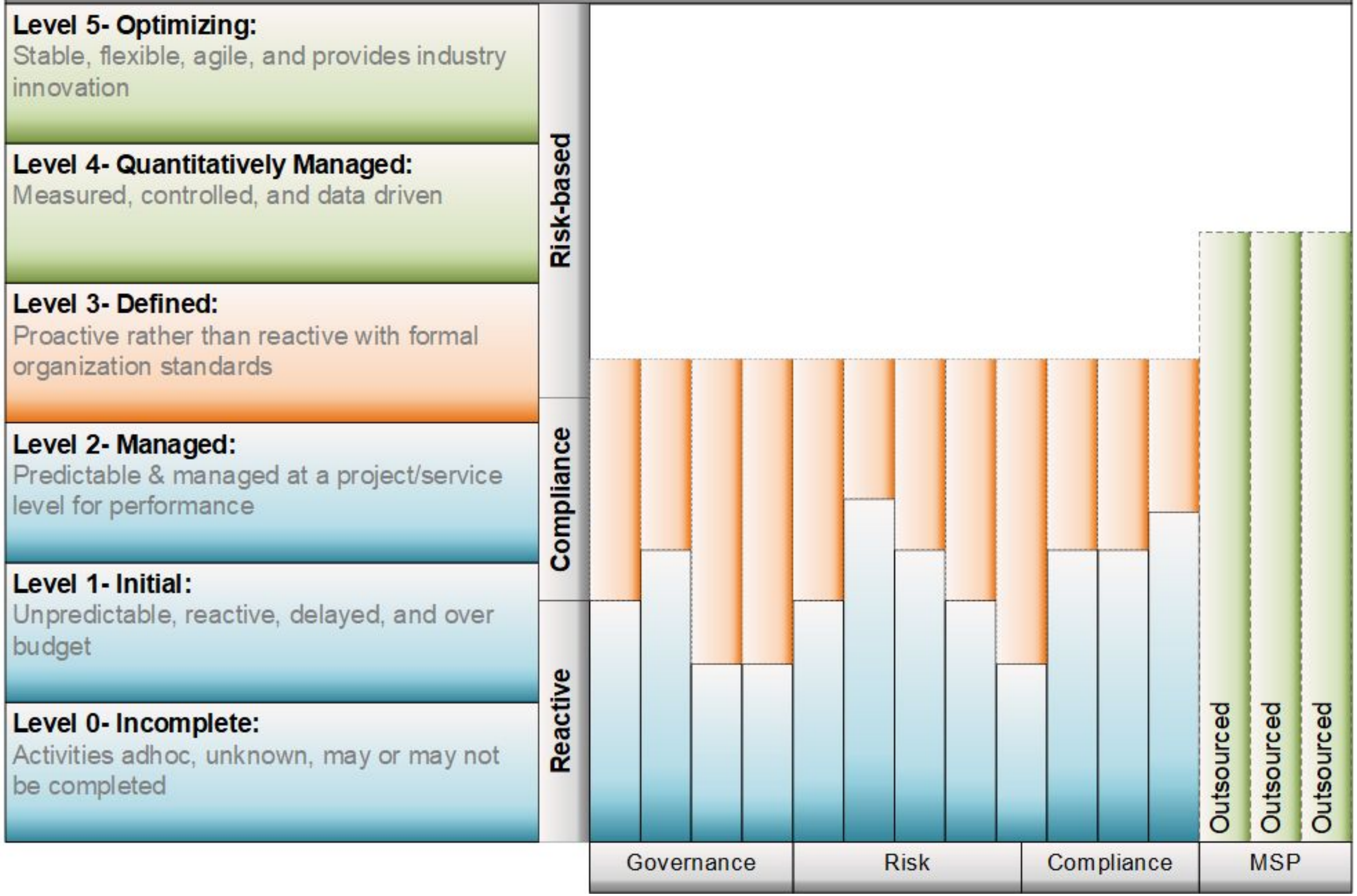
Capability Maturity Model Integration (CMMI)

- Created for the U.S. Department of Defense
- Process and behavioral model
- Build and benchmark key capabilities
- Drive process improvements
- Scale, one to five
- Factor in acceptable levels of risk
- 25+ years old



Maturity mapping examples	
Level 5	Fortune 500, Amazon, Google, Amazon, DOD, NSA
Level 4	
Level 3	> $300 million revenue, Feds
Level 2	< $300 million revenue Start-ups, local governments
Level 1	

CMMI Maturity Levels for Service Catalog



Level 5- Optimizing: Stable, flexible, agile, and provides industry innovation

Level 4- Quantitatively Managed: Measured, controlled, and data driven

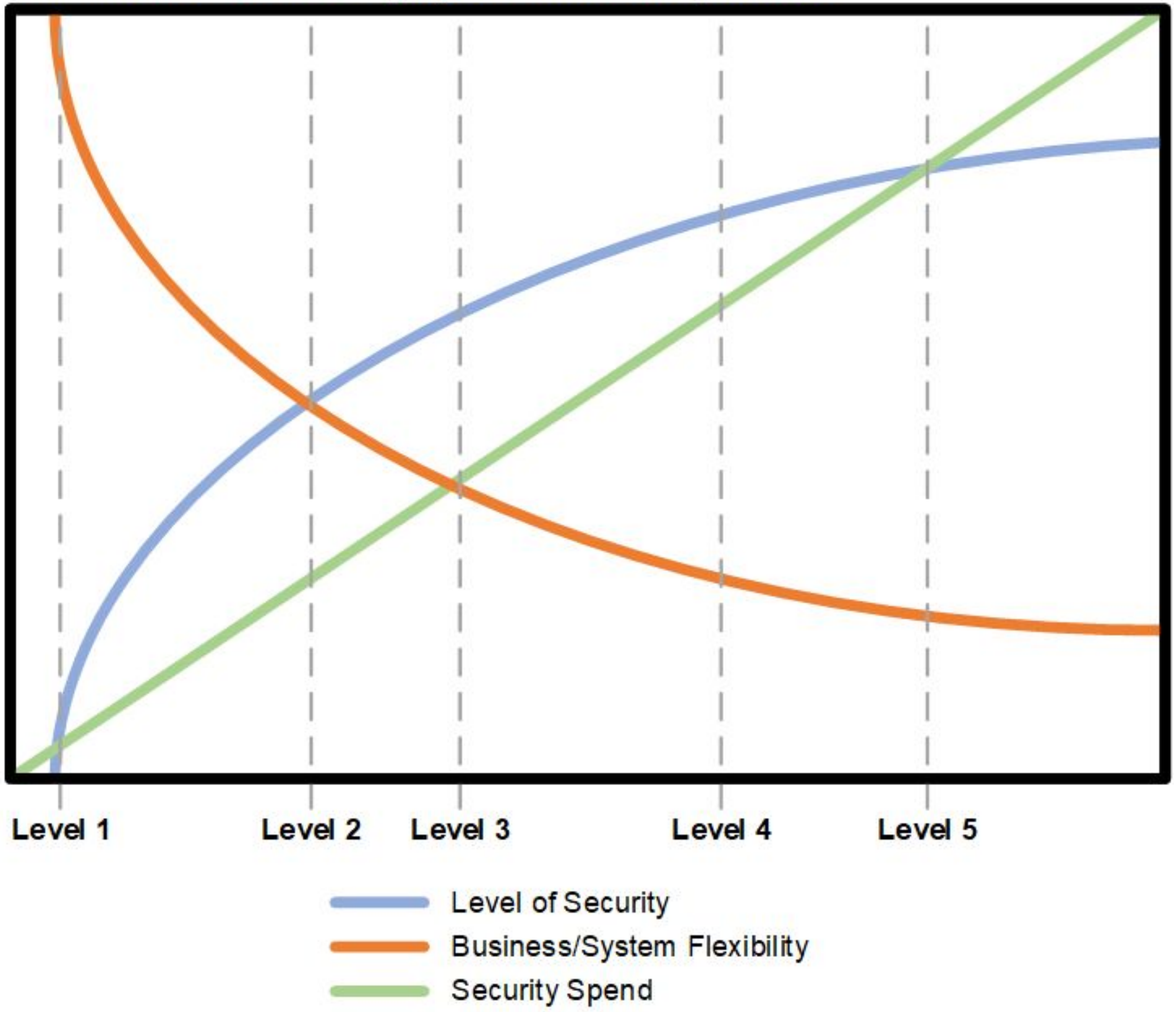
Level 3- Defined: Proactive rather than reactive with formal organization standards

Level 2- Managed: Predictable & managed at a project/service level for performance

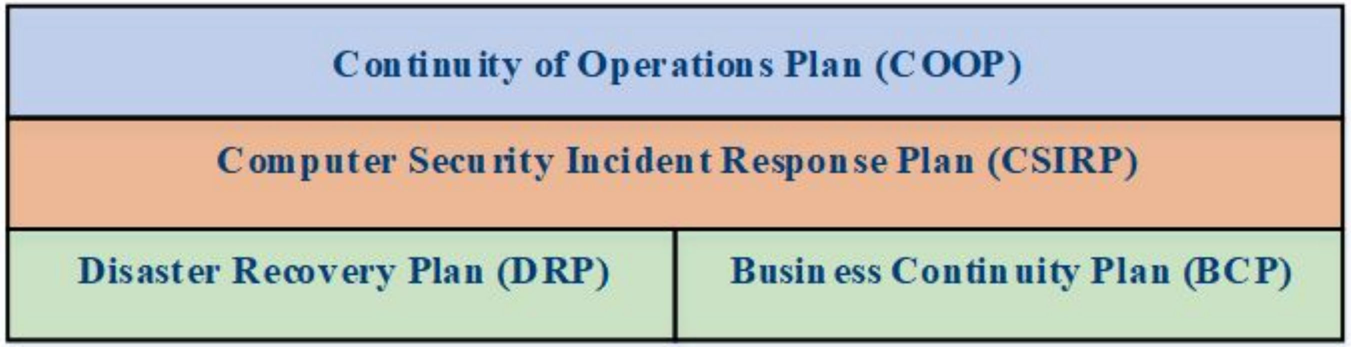
Level 1- Initial: Unpredictable, reactive, delayed, and over budget

Level 0- Incomplete: Activities adhoc, unknown, may or may not be completed

The balance of business agility and information protection



Frameworks and References



Continuity of Operations Plan (COOP)

Computer Security Incident Response Plan (CSIRP)

Disaster Recovery Plan (DRP)

Business Continuity Plan (BCP)

- FEMA National Incident Management System (NIMS)
- NIST SP 800-53, Rev. 4: Security and privacy expectations
- NIST SP 800-61, Rev. 2: Security incident handling
- ISO/IEC 27031:2011: IT Readiness for DRP and BCP
- Electronic Discovery Reference Model (EDRM)

Legal and Regulatory Expectations

Federal expectations

- Tied directly to law (Federal and State)
  - Example: HIPAA of 1996 Pub.L. 104–191
- Tied through law then to us through regulation
  - Example: FISMA 44 U.S.C. § 3541 mapped to NIST SP 800-53 R4

Contractual Expectations

- Recipients or providers

Local expectations (organizational law)

- Work rules, Administrative Directives
- Policy, Standards

Regulations and Contracts

Examples of regulation and contract expectations

- DOD, Defense Manpower Data Center
- U.S. Department of Commerce, NTIS
- U.S. Department of Health and Human Services
  - Administration for Children and Families, Office of Child Support Enforcement
  - Centers for Medicare and Medicaid Services
- U.S. Department of Labor, Bureau of Labor Statistics
- FBI Criminal Justice Information System
- Social Security Administration Data Safeguards
- Internal Revenue Service Publication 1075

Terms to become familiar with

Core Terms

- Computer Security Incident Response Plan (CSIRP)
- Computer Incident Response Team (CIRT)
- Security Operations Center (SOC)

Cyber Incident Response Team (CIRT)

- Indicator incidents
- Precursor incidents

Chief Information Security Officer and/or Chief Legal Counsel

- Security incident, security breach
- Privacy incident, privacy breach

Issues to look for?

- Excess storing and securing of information, costly mandated preservation requirements
- IT Service procurement, information assessments and disposal of information does not include the business, IT, legal, risk and regulatory teams
- The organization does not have business continuity, IT disaster recovery, or Incident response plans
- IT teams do not understanding the underlying business processes and how those processes are automated into technology
- IT teams do not have data flow documentation and architecture diagrams
- The organization does not have a rudimentary data map or data inventory

How to get started?

Get to know your business-enterprise

1. Do you understand the business-enterprise and decision makers (data owner)?
2. Do you understand your business and data sharing agreements?
3. Do you know how it translate into technology operations and requirements?

Get to know your data inventories, data maps, and data flows, look for

- **System Interconnections**
  - Connection between two or more systems
- **Ecosystem (Security Authorization Boundary)**
  - If data is being queried (answer/response)
  - If data is being sent to another information system
  - If data is being reciprocally sent and received (or shared)

Identify stakeholders

Business teams

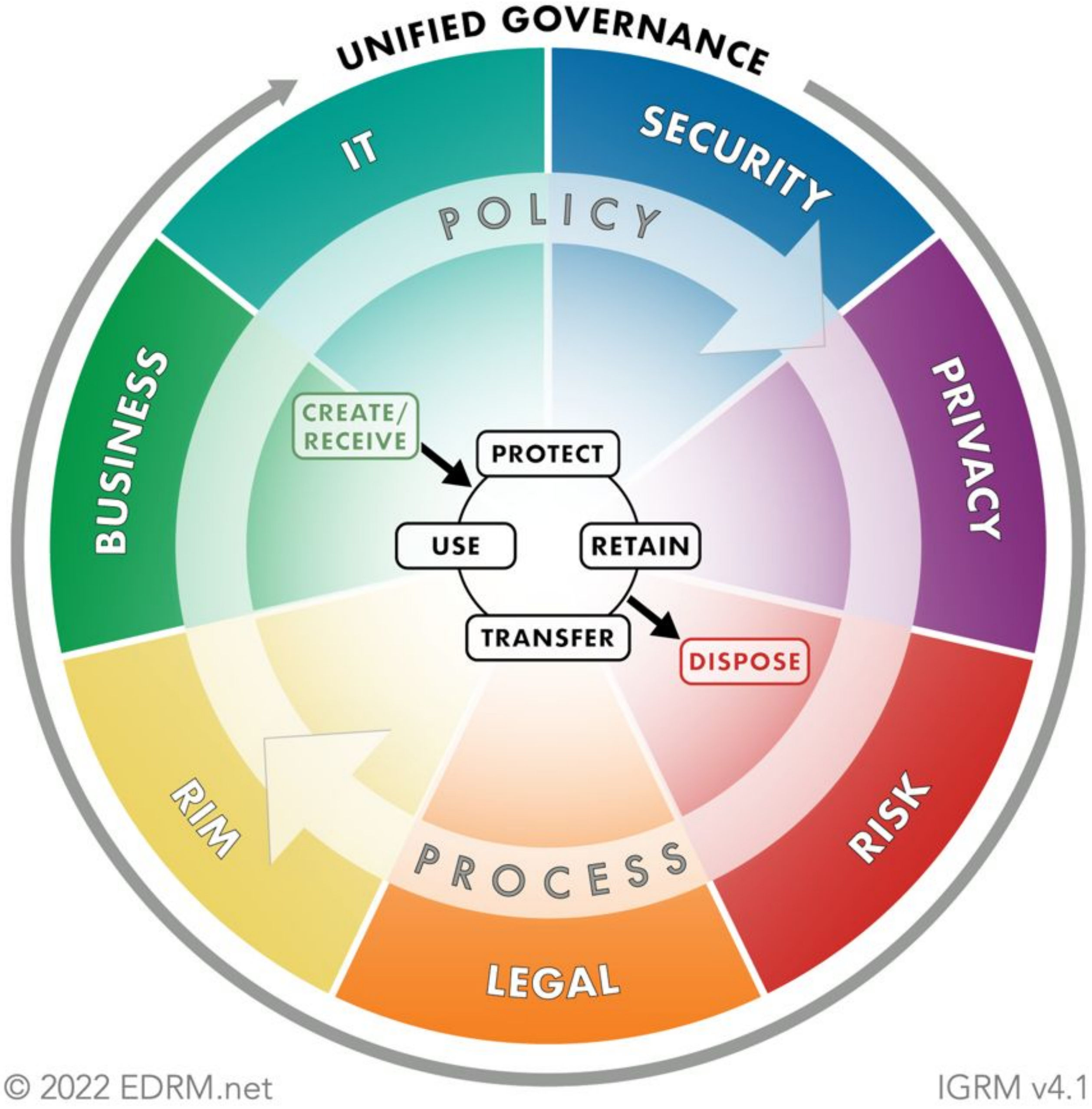
- Business objectives

Information Technology teams

- Knowledge of tools
- Infrastructure management

Legal, Risk and Regulatory teams

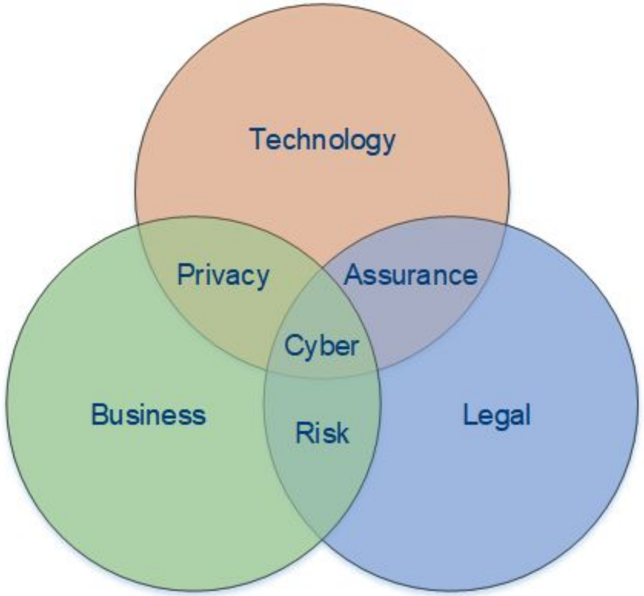
- Legal and regulatory duties
- Constraints and obligations:
  - e-discovery
  - government regulation
  - contractual obligations

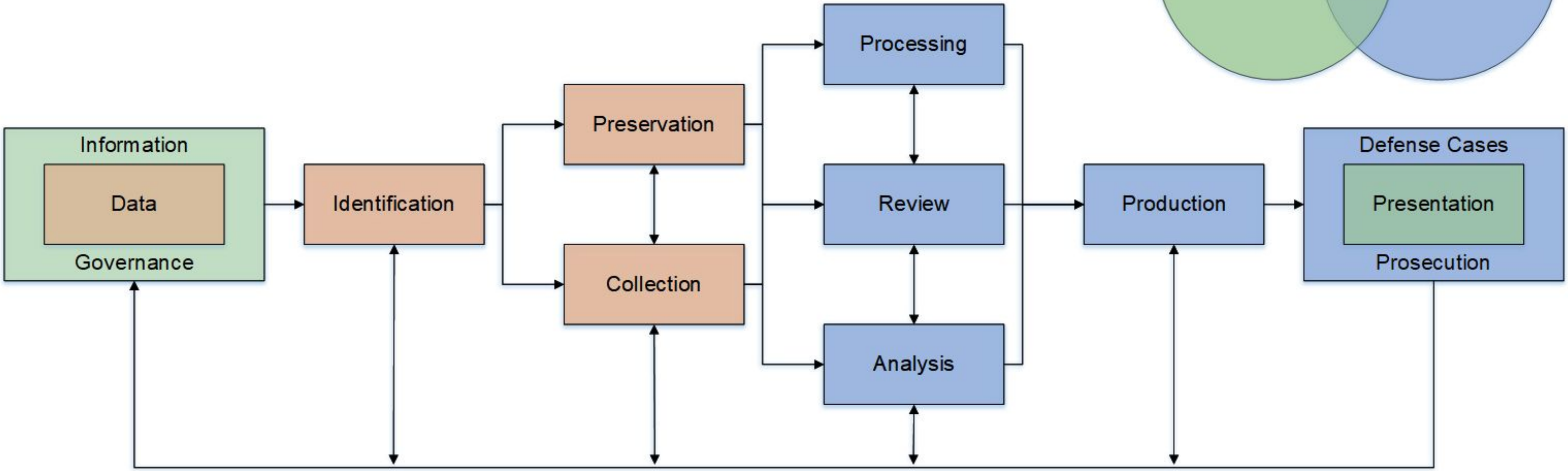


Source: EDRM (EDRM.NET)

Defensibility

Electronic Discovery Reference Model (EDRM)





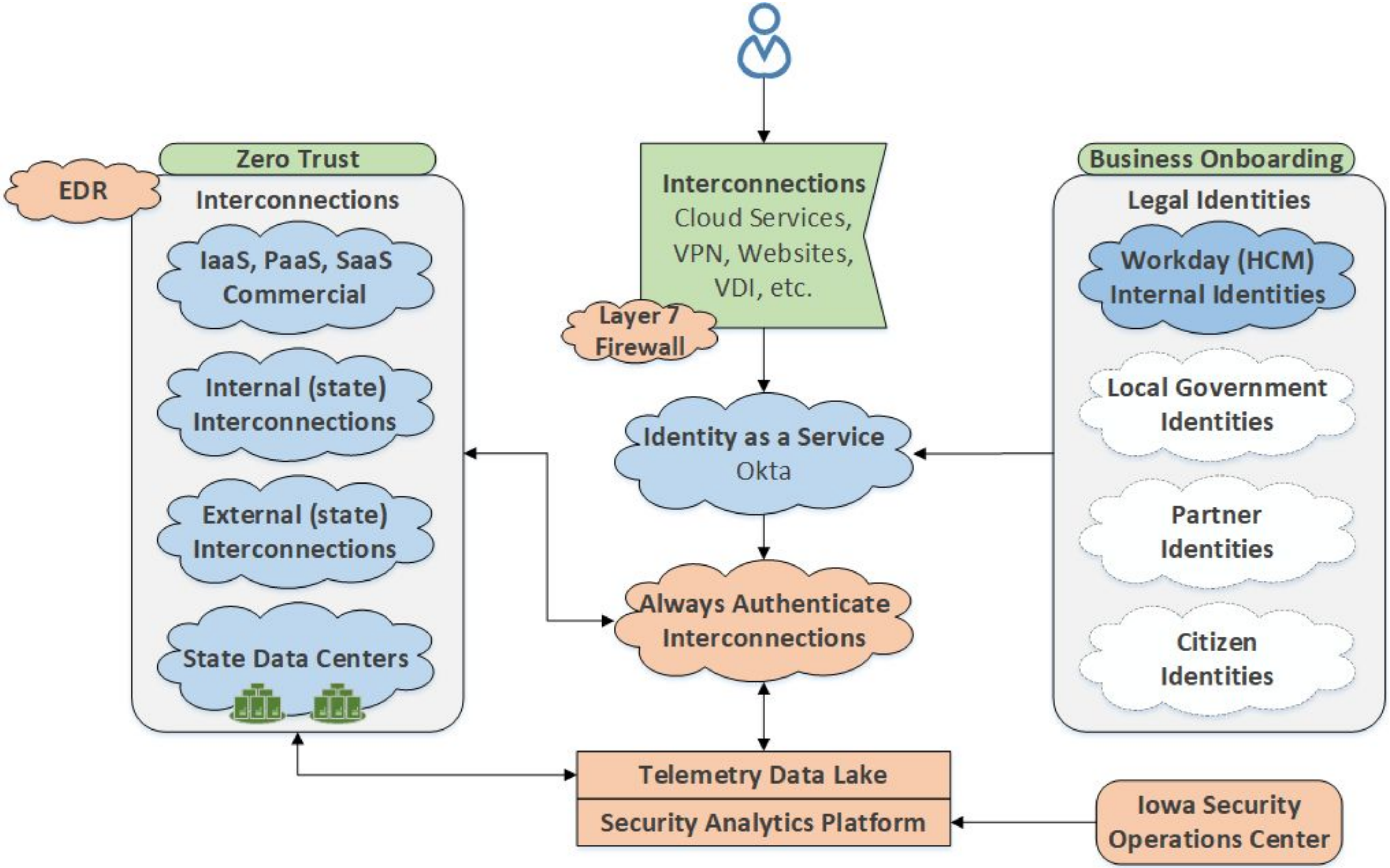
Source: EDRM (EDRM.NET)

Data and Security Classifications

Type of Data	Data Classification	Security Classification
► Public Data	► Open data ► Public data	► NIST Low Risk
► Personally Identifiable Information (PII) ► Protected Health Information (PHI)	► Unrestricted ► Restricted ► Confidential	► NIST Moderate Risk
► Impacts on critical infrastructure, national security, or results in loss of life	► Federal classified data	► NIST High Risk

Iowa’s Preliminary Zero Trust Roadmap

#	Activity	Government Scope
1	Manual inventory information systems and Ecosystems	State | County | City
1.1	Deploy Endpoint Protection and Response (EDR) tool (Prevention Mode)	State | County | City
1.1.1	Enhancement: EDR real-time scanless vulnerability assessment	State | County | City
1.1.2	Enhancement: EDR automated inventory of information systems and software	State | County | City
2	Manual inventory of individual assigned accounts and resource accounts	State | County | City
2.1	Integrate into “Identity as a Service” and apply multifactor authentication	State | County | City
3	Manual inventory of interconnections (website, API, SaaS, PPS, etc.)	State
3.1	Integrate interconnections into security boundaries and Identity as a Services	State
3	Security Analytics Platform	State


Zero Trust
EDR
Interconnections
IaaS, PaaS, SaaS Commercial
Internal (state) Interconnections
External (state) Interconnections
State Data Centers
Interconnections Cloud Services, VPN, Websites, VDI, etc.
Layer 7 Firewall
Identity as a Service Okta
Always Authenticate Interconnections
Business Onboarding
Legal Identities
Workday (HCM) Internal Identities
Local Government Identities
Partner Identities
Citizen Identities
Telemetry Data Lake
Security Analytics Platform
Iowa Security Operations Center

Major Projects - Cyber Security

FY’ 23 Cybersecurity Achievements

State of Iowa Security Operations Center (ISOC):

- Launched the 24/7/365 Security Operations Center (SOC) on April 4, 2022.
- Supports state and local government, education.
- Shares real-time cyber threat intelligence of observed vulnerabilities.

Iowa’s Endpoint Detection and Response Services (EDR):

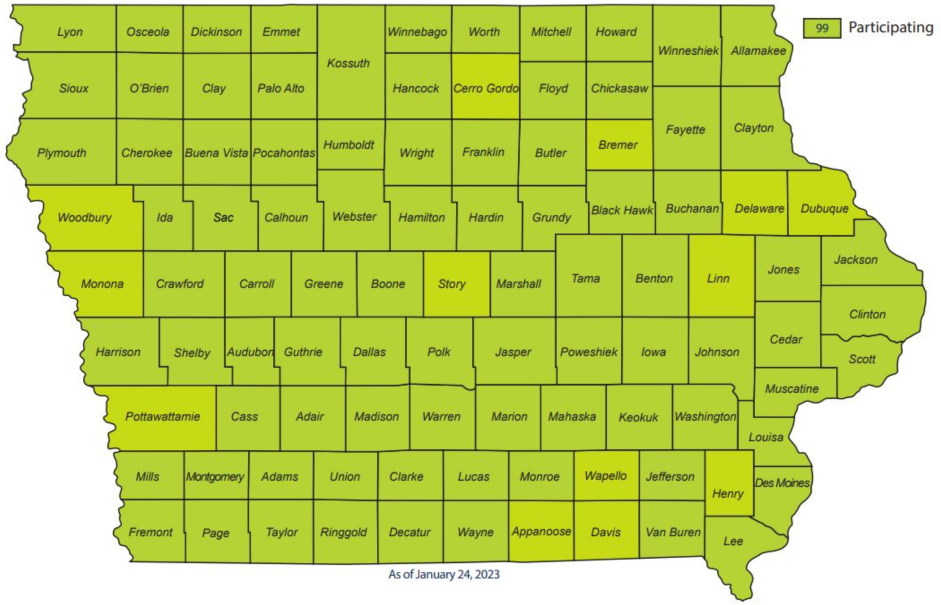
- Security tool which prevents cyber attacks on computers and servers.
- Requires minimal intervention to mitigate cyber threats.
- Shares real-time cyber threat intelligence of observed vulnerabilities.

Major Projects - Cyber Security

FY’ 23 Cybersecurity Achievements (Cont)

Cybersecurity Achievements (cont.):

- Formalize the State of Iowa Cyber Incident Response Team (CIRT).
- Implemented Multi Factor Authentication for all workforce members.
- Deploy additional protections to protect local governments (counties and cities).



As of January 24, 2023

State of Iowa's Cyber Incident Response Team

CIRT serves the State of Iowa in preparing and responding to cybersecurity threats against State, Local, Tribal, and Territorial (SLTT) governments.

The CIRT consists of the following organizations

- Air National Guard, 168th Cyber Operations Squadron
- Iowa Homeland Security and Emergency Management
- Iowa Department of Public Safety, Division of Criminal Investigation
- Iowa Secretary of State
- Iowa State University Board of Regents
- Office of the Chief Information Officer

State of Iowa's Cyber Incident Response Team

The CIRT supports the following organizations

- Executive, Judicial, and Legislative Branches
- Association of Counties and 99 Counties
- League of Cities
- Educational Institutions
- Nonprofits

The CIRT collaborates with the following organizations

- Cybersecurity and Infrastructure Security Agency (CISA)
- Iowa Fusion Center
- Federal Bureau of Investigation (FBI)
- Multi State Information Sharing and Analysis Center (MS-ISAC)
- U.S. Department of Homeland Security (DHS)

Cybersecurity Best Practices

People

Passwords

Patching

Data Backups

Endpoint Detection & Response

Monitoring & Alerting

A successful phishing attack can be so convincing that you won't even know that you were affected.

Cybersecurity: People

3.4 billion phishing emails are sent daily

Cybersecurity: People

- People can be the weakest link in your security
- 95% of successful cyber attacks begin in email
- Annual security awareness training & phishing tests

43%

of adults have shared their password with someone.

Source Google

Cybersecurity: Passwords

70% of people admit they use the same password for more than one account

Cybersecurity: Passwords

43% of people admit they share their passwords with someone

- Password complexity
- Password manager
- State of Iowa Password Standard:

  https://ocio.iowa.gov/authentication-security-standard

blocked by MFA.

Nearly

1/2

of people surveyed say they have never heard of MFA.

Cybersecurity: Multi-Factor Authentication (MFA)

99% of account hacks could have been avoided by using MFA

Cybersecurity: Multi-Factor Authentication (MFA)

MFA is an authentication method that requires the user to provide two or more verification factors to gain access to an account

- Over 80% of breeches leverage stolen or weak passwords
- MFA is number one recommendation to improve cybersecurity posture
- Leverage built-in MFA where offered

1/3
of people say they
or

Cybersecurity: Patching

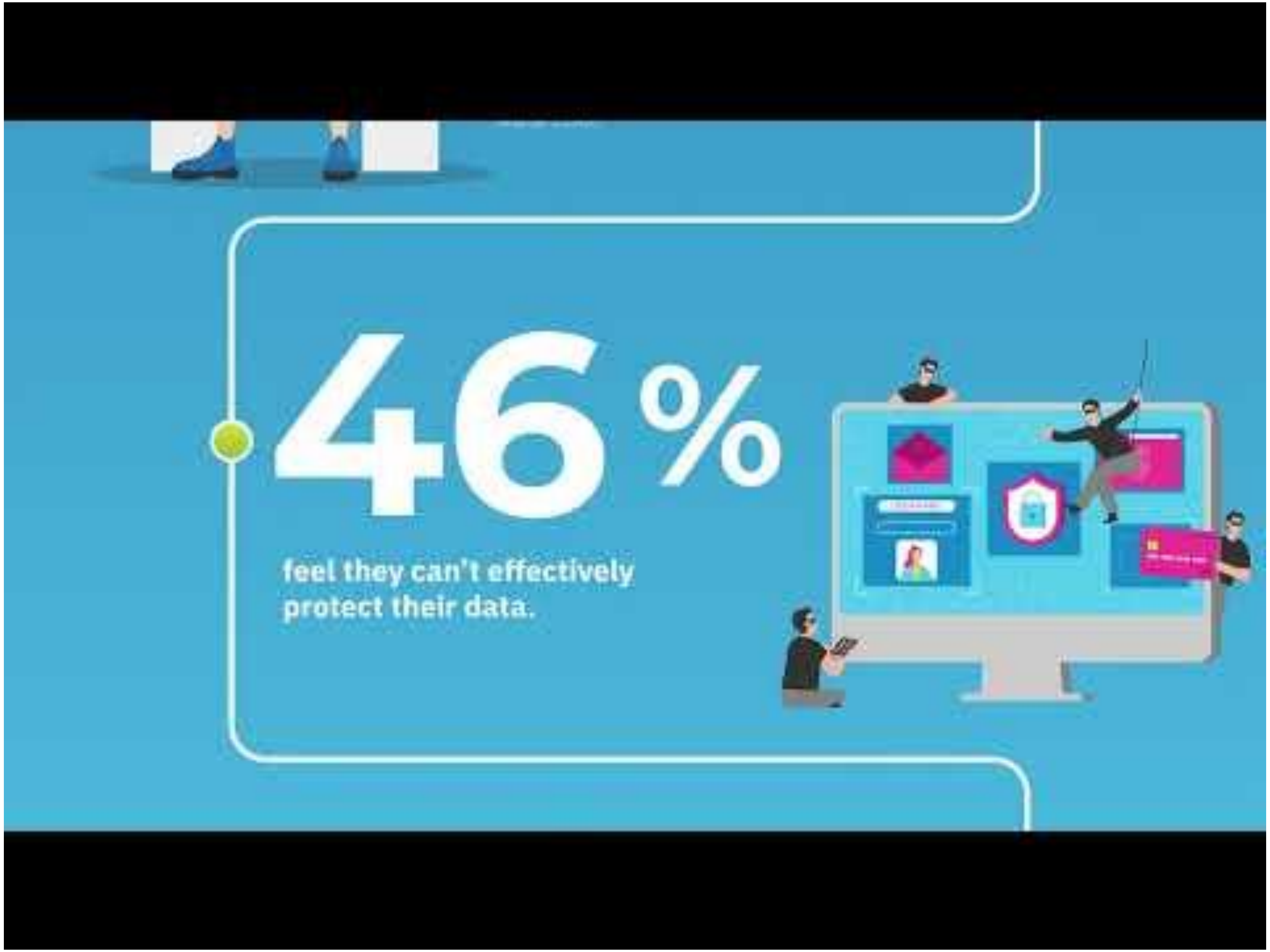
33% of people report that they rarely or NEVER install software updates on their devices

Cybersecurity: Patching

Patches are software and operating system updates that address security vulnerabilities within a program or product

- Enable automatic software updates
- Do not use unsupported end of life software
- Always visit vendor sites for software updates
- Avoid software updates while using untrusted networks

New vulnerabilities are continually emerging but the best defense against attackers is simple: Keep software up to date



46%

feel they can't effectively protect their data.

Cybersecurity: Data Backups

50% of backups fail because they aren’t tested

Cybersecurity: Data Backups

Leverage protections for backups including physical security, encryption, and offline copies

- Establish regular automated backups and redundancies of key systems
- Use on-site and remote backup methods
- Prioritize backups
- Regularly test backups

Ransomware
CYBERSECURITY AWARENESS MONTH
265

Cybersecurity: Endpoint Detection & Response

US ransomware attacks cost an estimated $623.7 million in 2021

Cybersecurity: Endpoint Detection & Response

Endpoint Detection & Response (EDR) is a security tool that detects & prevents a wide range of known & unknown cyber attacks on devices

- Real time response
- Telemetry data to monitor live events
- Sends alerts of suspicious activity
- State of Iowa uses CrowdStrike Falcon

EDR tools are most effective when combined with 24x7 monitoring and alerting

Cybersecurity: Monitoring and Alerting

Security Operations Centers monitor, prevent, detect, investigate, and respond to cyber threats

Cybersecurity: Monitoring & Alerting

What does a Security Operations Center (SOC) do for me?

- Provides 24x7x365 monitoring and heightened cyber support
- Improves response time and visibility in cyber threat responses
- Shares real-time cyber threat intelligence of observed vulnerabilities

EDR & SOC Services for Local Governments:

Endpoint Detection & Response + Security Operations Center Monitoring services are currently available to local governments at no charge through federal grant funds

Email OCIO at: government.services@iowa.gov to get started!

Cybersecurity Best Practices

People

Passwords

Patching

Data Backups

Endpoint Detection & Response

Monitoring & Alerting

Strategic Partnerships

MS-ISAC:
www.cisecurity.org/ms-isac

CISA: cisa.gov

HSEMD:
homelandsecurity.iowa.gov

ICIT:
iowacountiesit.org

ICIT & ISAC Tech Service Bureau

- **Iowa County Information Technology (ICIT)**
  - Technology/GIS resource for counties and affiliate of ISAC
  - Provide members with education & collaboration opportunities
  - Contact: **Andrew DeHaan** at adehaan@marioncountyiowa.gov

- **ISAC Tech Service Bureau**
  - Enhance technology resources to Iowa counties
  - Point of Contact for State and Federal partners
  - Contact: **Joel Rohne** at jrohne@iowacounties.org

OCIO Contacts

Looking for proactive cyber support?

Jess Flaherty, Local Government Program Manager

515.380.3765 | government.services@iowa.gov

Need to report cyber incident?

State of Iowa's Security Operations Center

1.855.442.4357 | 515.725.1296 | soc@iowa.gov

CONNECT WITH US

Follow us

@IowaOCIO

Visit us

@StateofIowaOCIO

**OCIO.iowa.go
v**