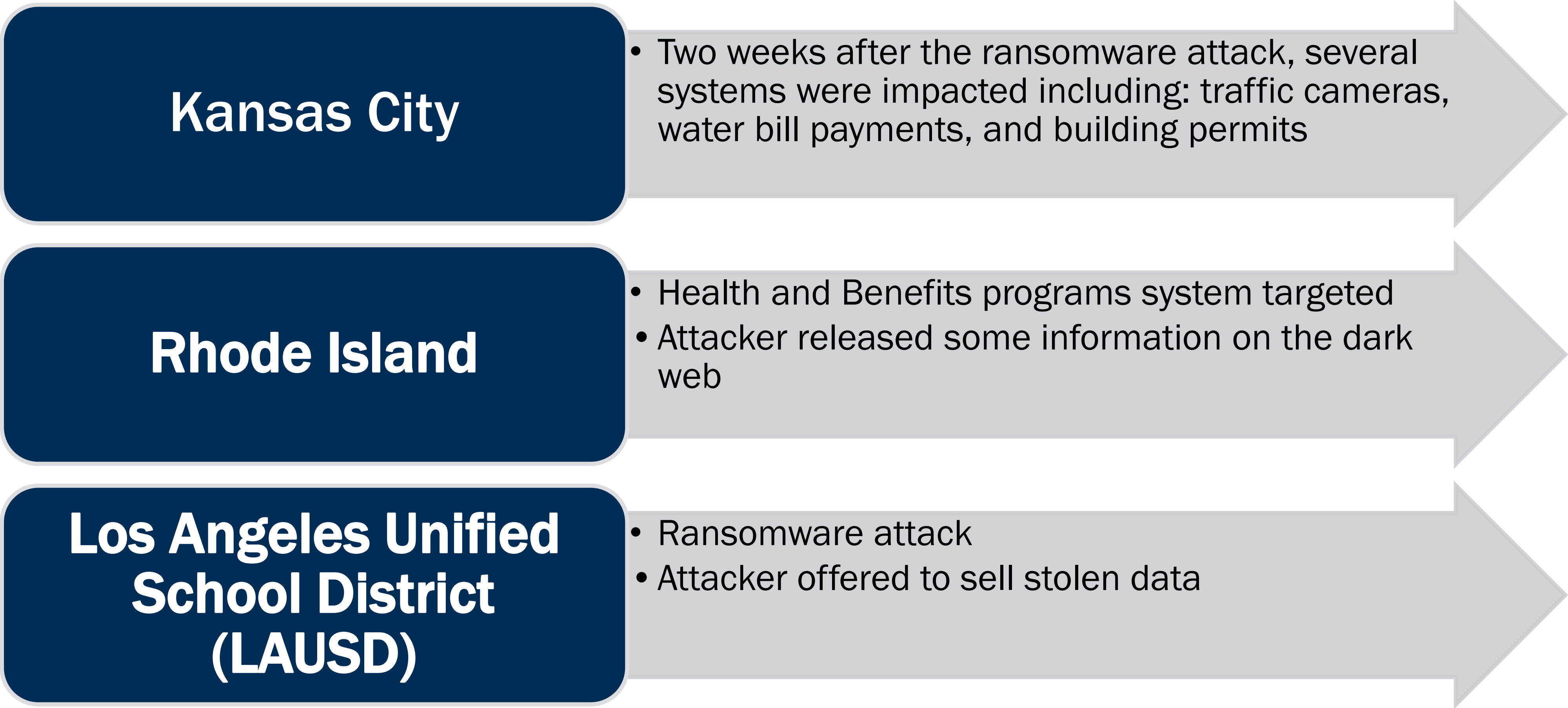
Defend Denver

Cybersecurity Strategy

Approach to Cybersecurity

- Change approach as adversaries change
- Security must be integral
- Effective cybersecurity program includes people, processes and technology
- Safety environment and other high value targets are first priority
- Reduce complexity
- Automate wherever possible, including using AI
- Compliance does not equal secure
- Efficiency in purchasing and maintaining security products
- Deliberate with intended results of initiatives
- Aim for security controls, solutions and processes with least amount of disruption

Cybersecurity Incidents



Kansas City

- Two weeks after the ransomware attack, several systems were impacted including: traffic cameras, water bill payments, and building permits

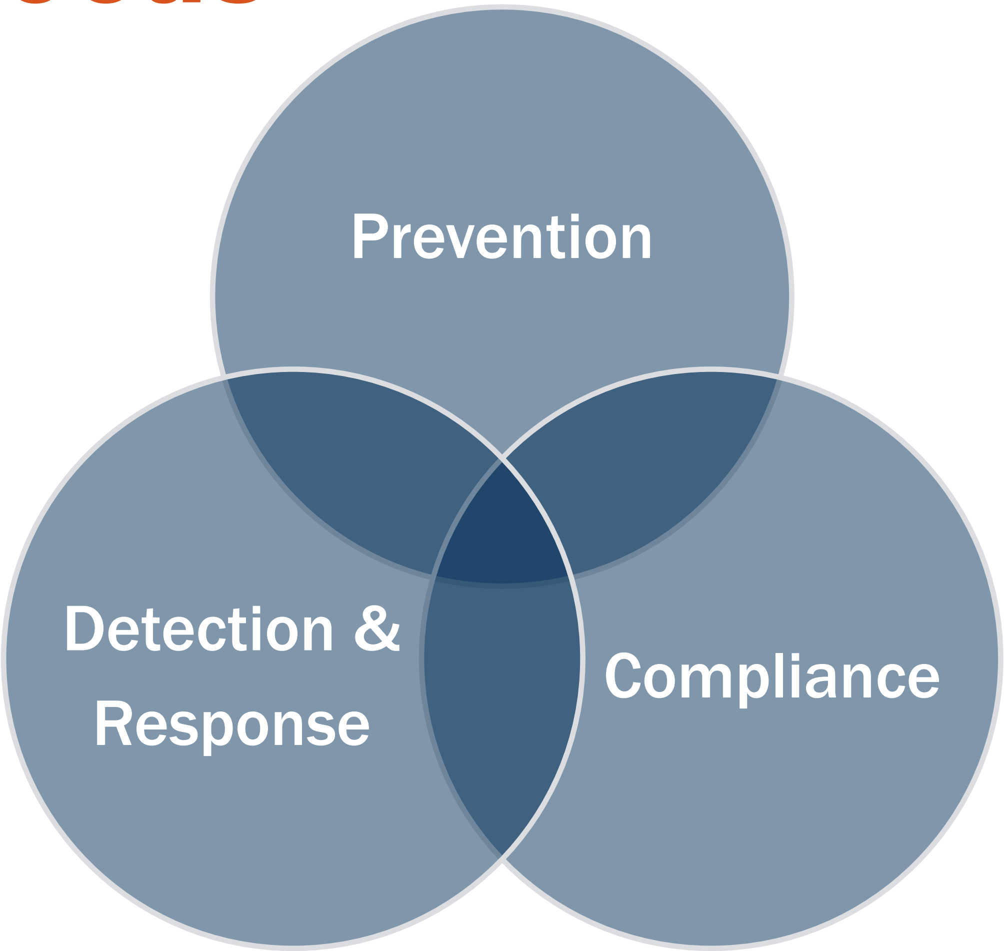
Rhode Island

- Health and Benefits programs system targeted
- Attacker released some information on the dark web

Los Angeles Unified School District (LAUSD)

- Ransomware attack
- Attacker offered to sell stolen data

Strategic Focus



Prevention

Detection & Response

Compliance

Strategic Focus – Prevention

- Systems, networks, and applications resistant to current and emerging cybersecurity threats
- Recruit, retain, and train staff
- Security policies, standards, and guidelines
- Promote the need for cybersecurity across CCD
- Partner with technology teams
- Implement NIST CSF as the risk management framework
- Lifecycle management

Strategic Focus – Detection & Response

- Sustain necessary tools and processes to preserve 24/7/365 monitoring for threats and incidents
- Maintain incident response and digital forensic capability
- Partner with outside agencies for collaboration and support

Strategic Focus – Compliance

- Continuous compliance assessments
- When gaps and deficiencies are discovered, work together with necessary groups to resolve as quickly as is feasible

Current State – Prevention

- EDR
- Vulnerability scanning
- Identity and Access
- DNS protection
- Email filtering
- Data Loss Prevention (DLP)
- Awareness training
- Configuration Management Database (CMDB)
- Privilege Access Management (PAM)

Future State – Prevention

- Network modernization
- Improve vulnerability remediation timeframe
- Increase awareness
- Expand CMDB
- Reduce number of administrative accounts and restrict access
- Increase visibility and controls in IoT/ICS environments
- Full implementation of existing security tools
- Frequent penetrating testing
- Annual incident response tabletop exercises
- Mature secure coding practices
- Increase encryption strength to prepare for quantum computing

Current State – Detection & Response

- In-house monitoring 6am – 6pm
- 3rd party monitoring 24/7/365
- Automations
- Incident Response Plan (IRP)

Future State – Detection & Response

- Increase partnership with 3rd party incident response firm and external legal counsel
- Improve incident response plan
- Establish breach communication plan
- Add more useful external threat feeds

Current State – Compliance

- Non-compliant with PCI
- Compliance with CJIS

Future State – Compliance

- Achieve and maintain PCI compliance
- Build robust GRC program that includes continuous monitoring
- Grow Risk Management program
- Establish useful metrics
- Report on cybersecurity program to Mayor’s office every quarter
- Establish Cybersecurity Risk Committee
- Perform CIS-18 IG1 assessment