Inland Empire Utilities Agency
A MUNICIPAL WATER DISTRICT

AGENDA

WORKSHOP
OF THE
BOARD OF DIRECTORS

WEDNESDAY, APRIL 5, 2017
10:00 A.M.

INLAND EMPIRE UTILITIES AGENCY*
AGENCY HEADQUARTERS
EVENT ROOM – BUILDING B
6075 KIMBALL AVENUE
CHINO, CALIFORNIA 91708

CALL TO ORDER OF THE INLAND EMPIRE UTILITIES AGENCY BOARD OF DIRECTORS WORKSHOP MEETING

FLAG SALUTE

PUBLIC COMMENT

Members of the public may address the Board on any item that is within the jurisdiction of the Board; however, no action may be taken on any item not appearing on the agenda unless the action is otherwise authorized by Subdivision (b) of Section 54954.2 of the Government Code. Those persons wishing to address the Board on any matter, whether or not it appears on the agenda, are requested to complete and submit to the Board Secretary a "Request to Speak" form which are available on the table in the Board Room. Comments will be limited to five minutes per speaker. Thank you.

ADDITIONS TO THE AGENDA

In accordance with Section 54954.2 of the Government Code (Brown Act), additions to the agenda require two-thirds vote of the legislative body, or, if less than two-thirds of the members are present, a unanimous vote of those members present, that there is a need to take immediate action and that the need for action came to the attention of the local agency subsequent to the agenda being posted.

1. WORKSHOPS

A. CYBER SECURITY TRAINING

B. ENERGY MANAGEMENT WORKSHOP #1

2. **CLOSED SESSION**

A. **PURSUANT TO GOVERNMENT CODE SECTION 54957 – PERSONNEL MATTERS**

General Manager

3. **ADJOURN**

*A Municipal Water District

In compliance with the Americans with Disabilities Act, if you need special assistance to participate in this meeting, please contact the Board Secretary (909) 993-1736, 48 hours prior to the scheduled meeting so that the Agency can make reasonable arrangements.

Proofed by: ______

Declaration of Posting

I, April Woodruff, Board Secretary of the Inland Empire Utilities Agency*, A Municipal Water District, hereby certify that a copy of this agenda has been posted by 5:30 p.m. at the Agency's main office, 6075 Kimball Avenue, Building A, Chino, CA on Thursday, March 30, 2017.

____

April Woodruff

WORKSHOP

1A

Cyber Security for Management and the Boardroom One Hour Version

Prepared for Inland Empire Utilities Agency

445G

Learning Tree® International

Training You Can Trust®

Course Objectives

- **For many organizations (private sector and government), the threat of a major cyber security breach is one of its largest risks**
  - Financial, reputational, and even physical harm can result
  - Career-threatening liability issues for executives and board members

- **In this course, the objectives are to:**
  - Provide baseline knowledge of cyber security issues
    - With a focus on its difficulty and scope
  - Highlight that cyber security is a risk management problem
    - And recognize the need for a robust risk management process
  - Explain board and C-suite responsibilities in regards to cyber security
  - Outline tools to help implement an effective governance structure
    - Without which your organization, and you, might be at risk

Course Contents

	Introduction and Overview
Chapter 1	Major Issues in Cyber Security
Chapter 2	Cyber Security Risk Management Process
Chapter 3	Guidance for Managers and Board Members
Chapter 4	Course Summary

- **The course is 1 hour**
- **Course materials include**
  - *Navigating the Digital Age: The Definitive Cybersecurity Guide for Directors and Officers*. Caxton Publishing, 2015. Download your free PDF, Kindle, or Epub copy at https://www.securityroundtable.org/the-book/.
  - Tools to support efforts in your organization to implement an effective Cyber Security Risk Management Process

Chapter 1

Major Issues in Cyber Security

Learning Tree International

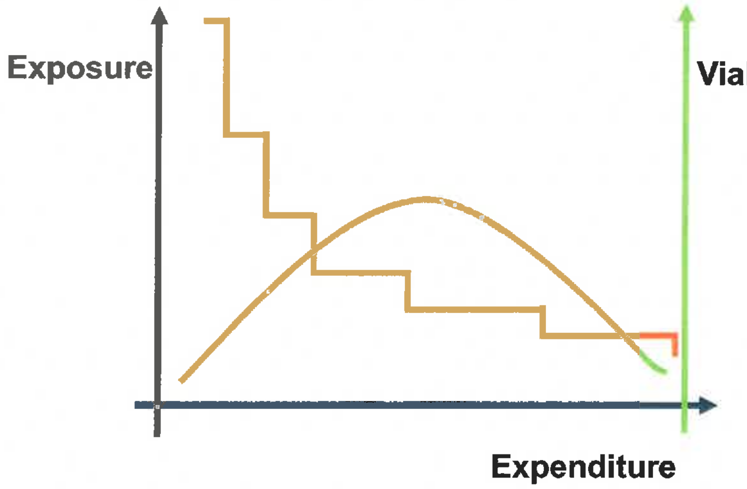
Training You Can Trust

Chapter 1 Contents

- ➢ **Why Cyber Security Is So Difficult!**
- **Related Privacy Issues**
- **How High Are the Stakes?**

Why Is Cyber Security So Difficult?

- **Total protection cannot be achieved**
  - Nothing is unbreakable no matter how much you spend
- **If you spend nothing, your vulnerability is essentially infinite**
- **A viability plot shows competing factors**
  - Confidence in the organization
  - Cost of providing that confidence
- **Collecting data to make quantitative decisions is very difficult**



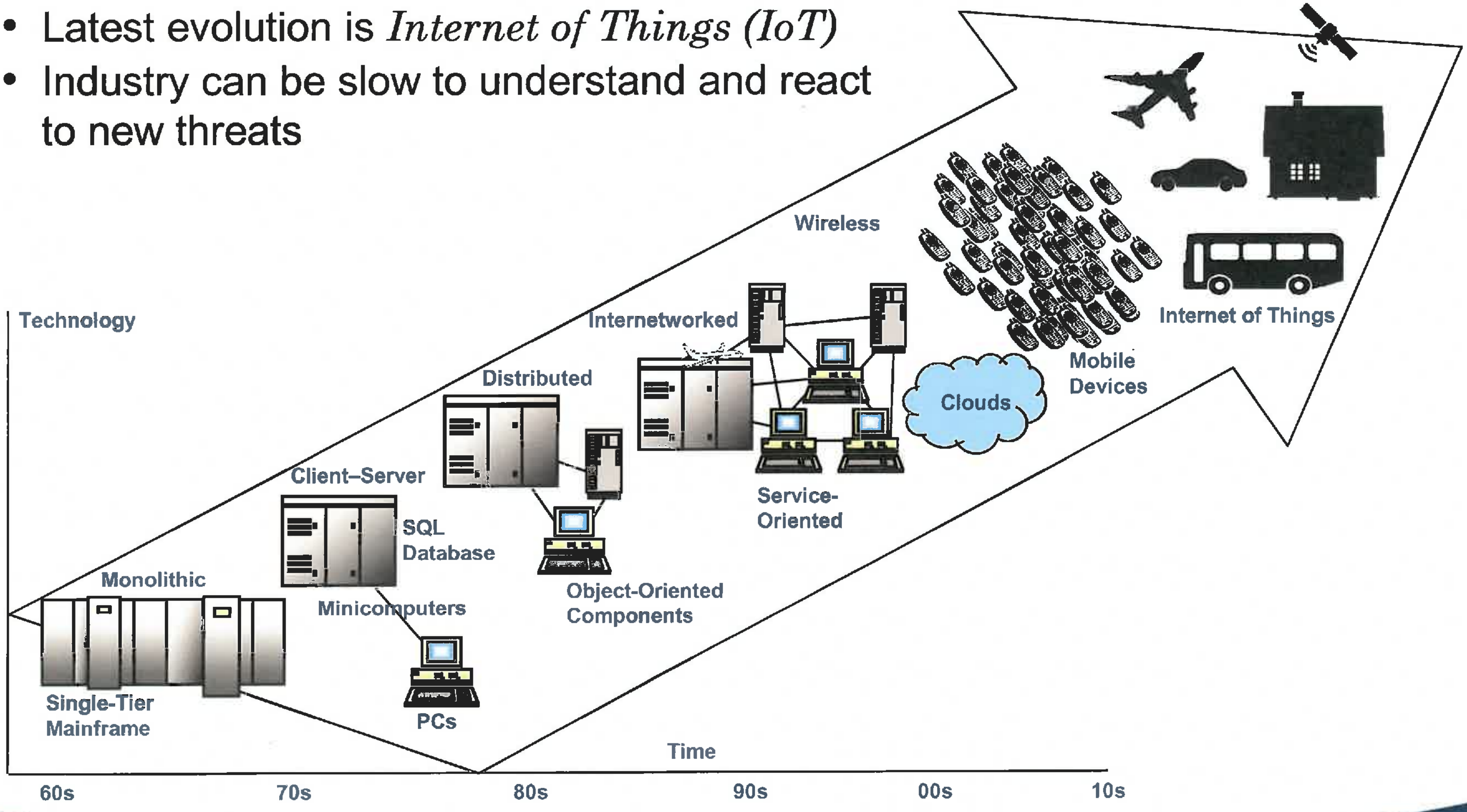
- **As a result, assessing quantitative risk and ROI is very difficult**

ROI = return on investment

Why Is It So Difficult: System Complexity

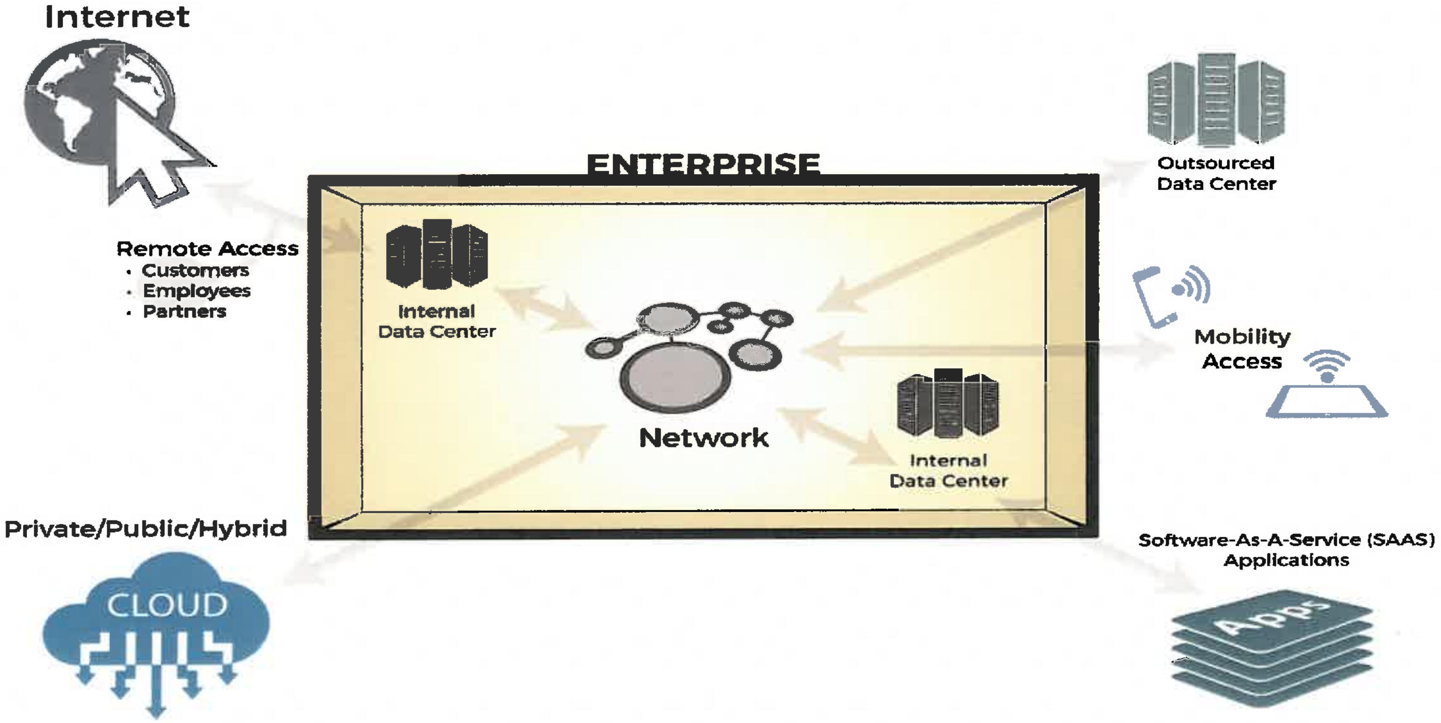
The Network Is the System

- **Systems are complex and getting more complex all the time**
  - Latest evolution is *Internet of Things (IoT)*
  - Industry can be slow to understand and react to new threats



Why Is It So Difficult: No Perimeter To Defend

- **This repeats—enterprise to enterprise to enterprise**
  - You won't know where they have been



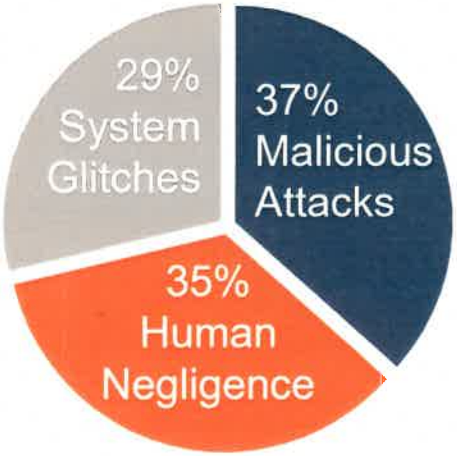
Why Is It So Difficult: Technology Choices

- **There are literally thousands of different cyber security hardware and software tools**
  - Almost impossible to evaluate effectiveness or suitability

It gets worse…

- **No tool does it all—need to integrate multiple tools**
- **Many breaches are caused by social engineering compromise of legitimate access credentials**
  - Difficult to detect
- **Once an organization is breached, sophisticated adversaries move laterally and infect other systems**
  - Can be difficult to eradicate, especially an APT actor

Major Causes of Data Breach



Why Is It So Difficult: Workforce Skills

- **Whatever your cyber security goals are, the people in your organization will need to implement it**
  - A competent, well-trained workforce is paramount for success
  - Yet those competent individuals are in high demand

It gets worse…

- **By 2017, we will have a shortage of 2 million cyber security professionals worldwide, according to the UK House of Lords Digital Skills Committee***

- **Between 2007 and 2013, postings for cyber security jobs rose 74 percent, more than twice the rate of IT jobs as a whole****

- **64 percent of high school students in the U.S. do not have access to computer science classes or other classes that would help prepare them for a career in cyber security†**

*Morgan, Lewis. "Global Shortage of Two Million Cyber Security Professionals by 2017." IT Governance. October 30, 2014.
**Burning Glass. *Job Market Intelligence: Report on the Growth of Cybersecurity Jobs.* March 2014.
†Source: Raytheon and the National Cyber Security Alliance. *Preparing Millennials to Lead in Cyberspace.*

Chapter 1 Contents

- Why Cyber Security Is So Difficult!

➢ **Related Privacy Issues**

- How High Are the Stakes?

Privacy Concerns

- ***Personally identifiable information (PII)*** **and** ***Sensitive Personal Information (SPI)*** **are part of privacy laws worldwide**
  - Information that can be used to "identify, contact, or locate a single person, or to identify an individual in context"*

- ***Privacy*** **is different than cyber security but…**
  - They "intersect through breaches"*
- **Privacy laws vary but are heading toward holding company personnel individually responsible in some cases**
  - Including the board and C-suite

❓ **Attack, glitch, negligence, other—what caused each of the following?**

- 56 million Home Depot records (2015) ______________________________
- 40 million Target records (2013) ___________________________________
- Office of Personnel Management (OPM) (most sensitive of PII) __________

____

* Rosenquist, Matt, ed. *Navigating the Digital Age: The Definitive Cybersecurity Guide for Directors and Officers*. Caxton Publishing, 2015. Download your free PDF, Kindle, or Epub copy at `https://www.securityroundtable.org/the-book/`.

Chapter 1 Contents

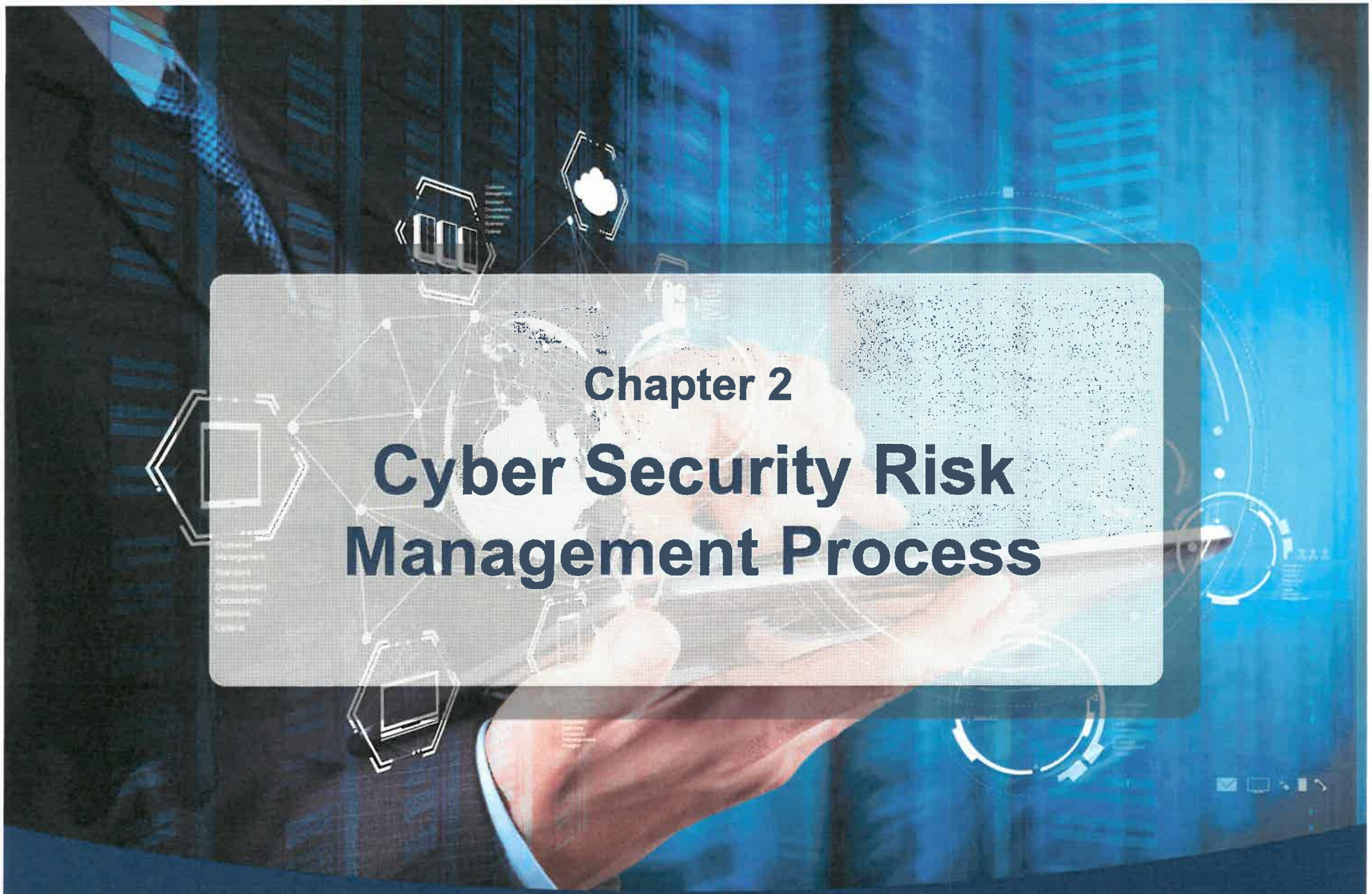
- Why Cyber Security Is So Difficult!
- Related Privacy Issues

➢ **How High Are the Stakes?**

Impact of a Breach

- **Breaches may result in**
  - Nothing at all
  - Organizational embarrassment
  - Loss of customer confidence
  - Denial of service availability
  - Theft of intellectual property (IP)
  - Release of proprietary content
  - Physical damage
  - Business termination
  - National security crisis
  - Litigation and lawsuits
  - Loss of life or limb

- **All are potentially time-consuming and can have a huge impact on reputation and financial security**



Chapter 2

Cyber Security Risk Management Process

Learning Tree International

Training You Can Trust

Chapter 2 Contents

- ➢ **Cyber Security Tools and Frameworks**
- **Cyber Security Risk Management Process**

Cyber Security Risk

- **Cyber security is ultimately a risk-management problem**
  - Similar to those we have handled before with many similar solutions
- **Risk is the likelihood of loss (inherent to any enterprise)**
  - Often expressed as: **Risk = Vulnerability x Threat x Asset Value**

- **More on cyber security risk to come…**

Cyber Security Risk Management: Frameworks

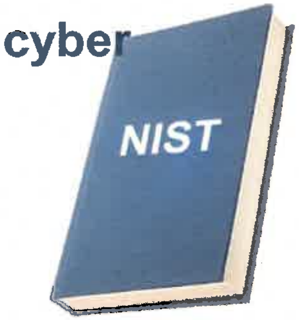
- **How-to guides for security policies and practices**
  - Vary greatly in
    - Focus
    - Completeness
    - Flexibility

- **All frameworks describe behavior in terms of security controls**

- **Many widely used security frameworks are available**
  - May be mandatory for certain organizations
  - Some are industry-specific
  - Some publish auditing guidance
  - Some provide certification for external auditors

Cyber Security Frameworks: NIST

- **We recommend use of the NIST Cyber Security Framework**
  - Also recommended by the American Water Works Association (AWWA)
- **Developed in response to Presidential Directive 13636, *Improving Critical Infrastructure Cyber Security***
  - More than 3,000 people from diverse parts of industry, academia, and government participated in workshops and webinars
- **The NIST Framework is becoming recognized as guidance to develop an appropriate *risk-based approach* to addressing cyber security threats**
  - For organizations of all types beyond critical infrastructure



- **Other Advantages**
  - Appropriate for both government or private-sector
  - Developed as high-level guidance and approach
  - Scalable, flexible, comprehensive, and explicit
  - Suitable for incorporating industry-specific requirements
  - References elements of NIST SP 800, ISO/IEC 27001, and COBIT

Elements

The NIST Framework is composed of three elements:

- **The *Framework Core* (“Core”)**
  - A set of cyber security activities, desired outcomes, and applicable references that are common across critical infrastructure sectors
  - The Core consists of five concurrent and continuous Functions
    - Identify, Protect, Detect, Respond, Recover
- ***Framework Implementation Tiers* (“Tiers”)**
  - Provide context on how an organization views cyber security risk and the processes in place to manage that risk
- **A *Framework Profile* (“Profile”)**
  - Represents the outcomes based on business needs that an organization has
    - Selected from the Framework Categories and Subcategories
  - Characterized as the alignment of standards, guidelines, and practices to the Framework Core in a particular implementation scenario
- **See `http://www.nist.gov/cyberframework/`**

Other Management Tools: CIS 20 Critical Security Controls

Center for Internet Security (CIS) Critical Security Controls – Version 6.0

- **20 recommended actions that provide specific and actionable ways to stop today's most pervasive and dangerous cyber attacks**
  - Organizations will typically use these controls as guideposts in developing a comprehensive plan
- **Judgment is needed!**
  - Not all 20 controls should be uniformly applied in every enterprise
  - CISOs and their teams should apply risk-based criteria to determine the appropriate prioritization and use
- **A key best practice for senior management is reporting on CIS 20 status**
  - Insist on regular understanding and updates on the actions (at least annually)
  - Include which ones are being used
    - How comprehensively are they deployed across the enterprise?
    - If not fully deployed, what are the barriers and what are the mitigations?
  - Include the rationale for those not being used

CIS 20 Critical Security Controls

CSC	Control Title
1	Inventory of Authorized and Unauthorized Devices
2	Inventory of Authorized and Unauthorized Software
3	Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
4	Continuous Vulnerability Assessment and Remediation
5	Controlled Use of Administrative Privileges
6	Maintenance, Monitoring, and Analysis of Audit Logs
7	Email and Web Browser Protections
8	Malware Defenses
9	Limitation and Control of Network Ports, Protocols, and Services
10	Data Recovery Capability
11	Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
12	Boundary Defense
13	Data Protection
14	Controlled Access Based on the Need to Know
15	Wireless Access Control
16	Account Monitoring and Control
17	Security Skills Assessment and Appropriate Training to Fill Gaps
18	Application Software Security
19	Incident Response and Management
20	Penetration Tests and Red Team Exercises

- **CIS 20 Critical Security Controls – Version 6.0**

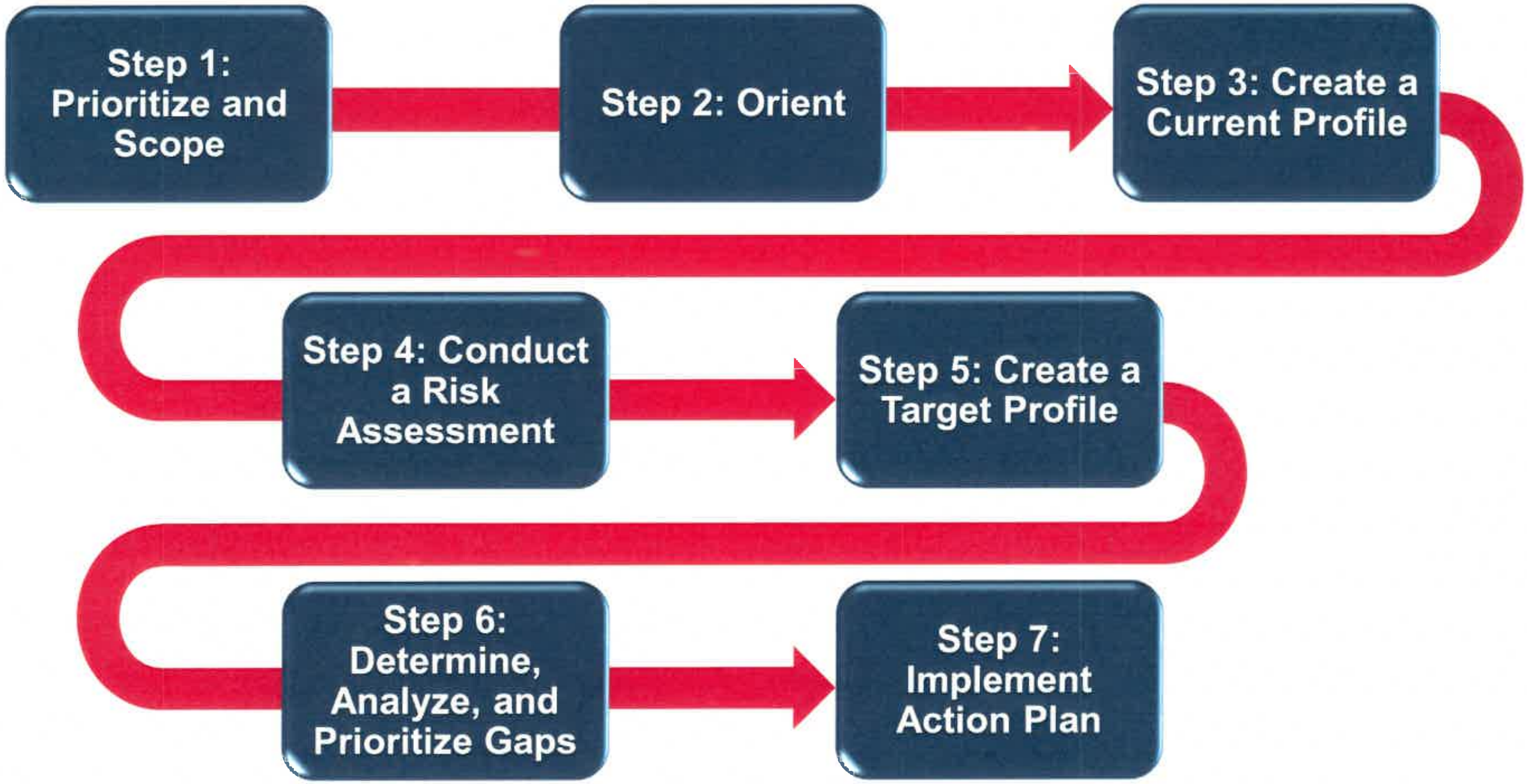
Chapter 2 Contents

- Cyber Security Tools and Frameworks

➢ **Cyber Security Risk Management Process**

NIST Cyber Security Framework: Process

Recommendations on Creating or Improving a Cyber Security Program



Step 1: Prioritize and Scope

Step 2: Orient

Step 3: Create a Current Profile

Step 4: Conduct a Risk Assessment

Step 5: Create a Target Profile

Step 6: Determine, Analyze, and Prioritize Gaps

Step 7: Implement Action Plan

Cyber Security Risk Management Process: Leveraging NIST

Step 1: Prioritize and Scope

- Identify business/mission objectives and high-level organizational priorities
- Make strategic decisions regarding cyber security implementations and determine the scope of systems and assets

Step 2: Orient

- Identify related systems and assets, regulatory requirements, and overall risk approach
- Identify threats to, and vulnerabilities of, systems and assets

Step 3: Create a Current Profile

- Indicate which Category and Subcategory outcomes from the Framework Core are currently being achieved
- Cross-check against the CIS 20 Critical Security Controls and the 82 controls contained in the AWWA document “Process Control System Security Guidance for the Water Sector”

Step 4: Conduct a Risk Assessment

- Analyze the operational environment in order to discern the likelihood of a cyber security event and the impact that the event could have on the organization
- Incorporate emerging risks and threat and vulnerability data to assess the likelihood and impact of cyber security events

Cyber Security Risk Management Process: Leveraging NIST

Step 5: Create a Target Profile

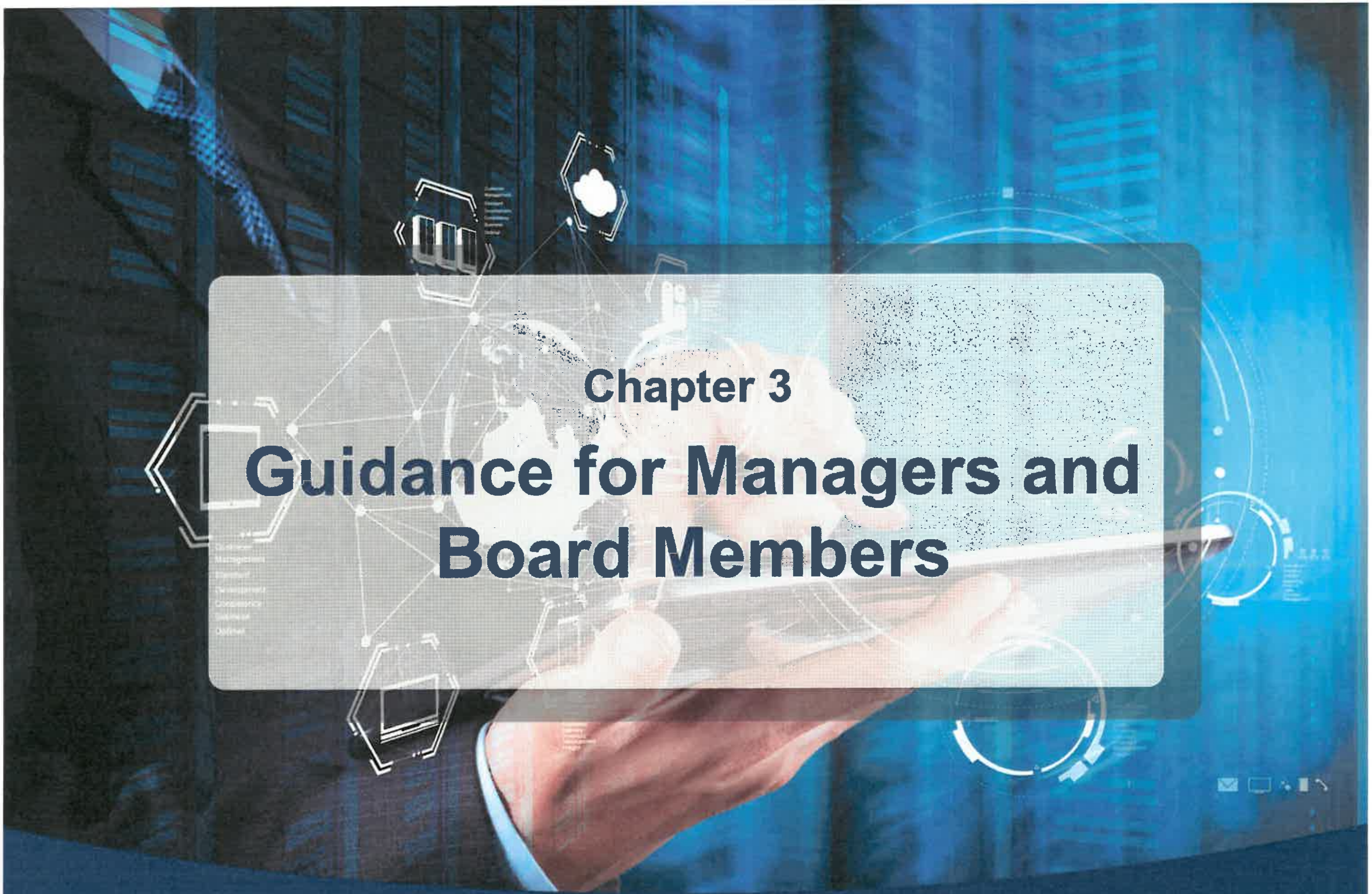
- Focus on the assessment of the Framework Categories and Subcategories describing the organization's desired cyber security outcomes
- Leverage the CIS 20 Critical Security Controls/AWWA 82 controls as well in the assessment

Step 6: Determine, Analyze, and Prioritize Gaps

- Compare the Current Profile and the Target Profile to determine gaps
- Create a prioritized Action Plan to address those gaps that draws upon mission drivers, a cost/benefit analysis, and an understanding of risk to achieve the outcomes in the Target Profile
- Determine resources necessary to address the gaps

Step 7: Implement Action Plan

- Determine which actions to take in regards to the gaps
- Monitor the current cyber security practices against the Target Profile
- Revisit the process on a regular (at least annual) basis



Chapter 3

Guidance for Managers and Board Members

Learning Tree International

Training You Can Trust

Chapter 3 Contents

- ➢ **Cyber Security Governance and Oversight**
- **Board Member Duties**
- **Cyber Security Breaches and Response**
- **Cyber Security Insurance**

Cyber Security Governance and Oversight

- **Establish a formal Cyber Security Risk Management Process**
  - The NIST Framework is not mandatory but…
  - It provides credibility in offering a robust model
- **Senior managers and board members must be engaged on a regular basis**
  - Stay informed
  - Direct the application of the risk management process
- **Think about appointing a Chief Information Security Officer (CISO)**
  - While not required, having an executive dedicated to cyber security has shown to improve overall cyber security posture

Cyber Security Risk Management Responsibilities

Process Step	CIO/CISO	Other Executives	CEO/CRO	Board of Directors
Cyber Security Risk Management Process	Responsible	Responsible	Accountable	Accountable
1. Prioritize and Scope	Responsible	Responsible	Accountable	Consulted
2. Orient	Responsible Accountable	Responsible	Consulted	Consulted
3. Create a Current Profile	Responsible Accountable	Responsible	Informed	Informed
4. Conduct a Risk Assessment	Responsible Accountable	Responsible	Informed	Informed
5. Create a Target Profile	Responsible Accountable	Responsible	Responsible	Informed
6. Determine, Analyze, and Prioritize Gaps	Responsible	Responsible	Accountable	Accountable
7. Implement Action Plan	Responsible Accountable	Informed	Informed	Informed

In the NIST Framework, what is your role? Responsible, Accountable, Consulted, Informed (RACI)?

Cyber Security Governance and Oversight

Plan for Enforcement…

1. Align management incentives to ensure cyber security risk management is taken seriously
2. Address need to fill talent gaps and conduct proper training for all employees and in particular those focused on cyber security
3. Develop an Incident Response Plan, and practice that plan through simulations or tabletop exercises
4. Ensure the board is effectively monitoring the cyber security risk management plan
5. Direct your organization to progressively reach the Adaptive tier

Chapter 3 Contents

- Cyber Security Governance and Oversight

➢ **Board Member Duties**

- Cyber Security Breaches and Response
- Cyber Security Insurance

Board of Directors Duties: Related to Cyber Security

➢ **Risk oversight responsibility**
- Need to ensure management is effectively handling cyber security risk through proper oversight and board action when warranted

➢ **Boards get into trouble when**
- Not engaged in any oversight of cyber security issues
- They make an uninformed or reckless decision that renders the corporation more vulnerable to cyber security attacks

➢ **Lawsuits brought against directors related to cyber security breaches have mainly focused on two allegations**
- Breached fiduciary duties by making ill-advised or negligent decisions
- Failure to act in the face of a reasonably known cyber security threat

➢ **Have a solid Cyber Security Risk Management Process and a clear governance model**
- Mitigates issues for Directors
- Benefiting the corporation as a whole

Board of Directors: Asking the Right Questions

➢ Cyber Security Risk Management Process

1. Has the organization developed a formal Cyber Security Risk Management Process?
2. What frameworks were used to build that process?
3. Is it clear who is responsible and who is accountable for each step of that process?
4. Does the board have visibility into each step of that process?

➢ Risk Assessment

5. Has the organization appropriately assessed its cyber security risks based on its business objectives?
6. How was that assessment conducted?

➢ Inventory

7. Does the organization have a comprehensive inventory of systems, hardware, and software assets?

➢ Security Controls

8. Does the organization understand what cyber security controls it currently has?
9. Is the organization using a standard control suite from which to choose and assess cyber security controls?

Board of Directors: Asking the Right Questions

➢ **Prioritization**

10. Has the organization properly prioritized its cyber security risks?
11. Are these priorities informed by corporate strategy and other business requirements?

➢ **Target State**

12. Has the organization developed a target set of controls to address cyber risk?
13. Does the organization have a prioritized set of actions to implement those controls?
14. Is there a documented rationale as to why the set of security controls was chosen?
15. Is the cost of having these controls understood?

➢ **Governance**

16. How frequent is the cyber security risk management plan updated?
17. What role does senior management (CEO, CRO) play in developing and approval of that plan? What role does the board have in developing and approval of that plan?

➢ **Incident Response**

18. Does the organization maintain a tested Incident Response Plan to be used in the event of a cyber incident?

Chapter 3 Contents

- Cyber Security Governance and Oversight
- Board Member Duties

➢ **Cyber Security Breaches and Response**

- Cyber Security Insurance

Incident Response Plan

The Incident Response Plan should include:

- ➢ **Key members of the team**
  - Specify their responsibilities and authorities
  - Identify who is leading the team
- ➢ **A structure for classifying events**
  - Severity and approaches to handling
- ➢ **A response protocol**
  - Key messages, Q&A documents, contact lists, etc.
- ➢ **Online communications such as dedicated website, blogs, etc.**
  - Ready to be used as necessary
- ➢ **Third parties that may be required for support roles**
  - E.g., forensics, crisis communications
- ➢ **Instructions on contacting authorities or law enforcement agencies**
  - Including criteria for deciding whether to contact them

Source: Rosenquist, Matt, ed. *Navigating the Digital Age: The Definitive Cybersecurity Guide for Directors and Officers*. Caxton Publishing, 2015, p. 268. Download your free PDF, Kindle, or Epub copy at https://www.securityroundtable.org/the-book/.

Chapter 3 Contents

- Cyber Security Governance and Oversight
- Board Member Duties
- Cyber Security Breaches and Response

➢ **Cyber Security Insurance**

Cyber Insurance

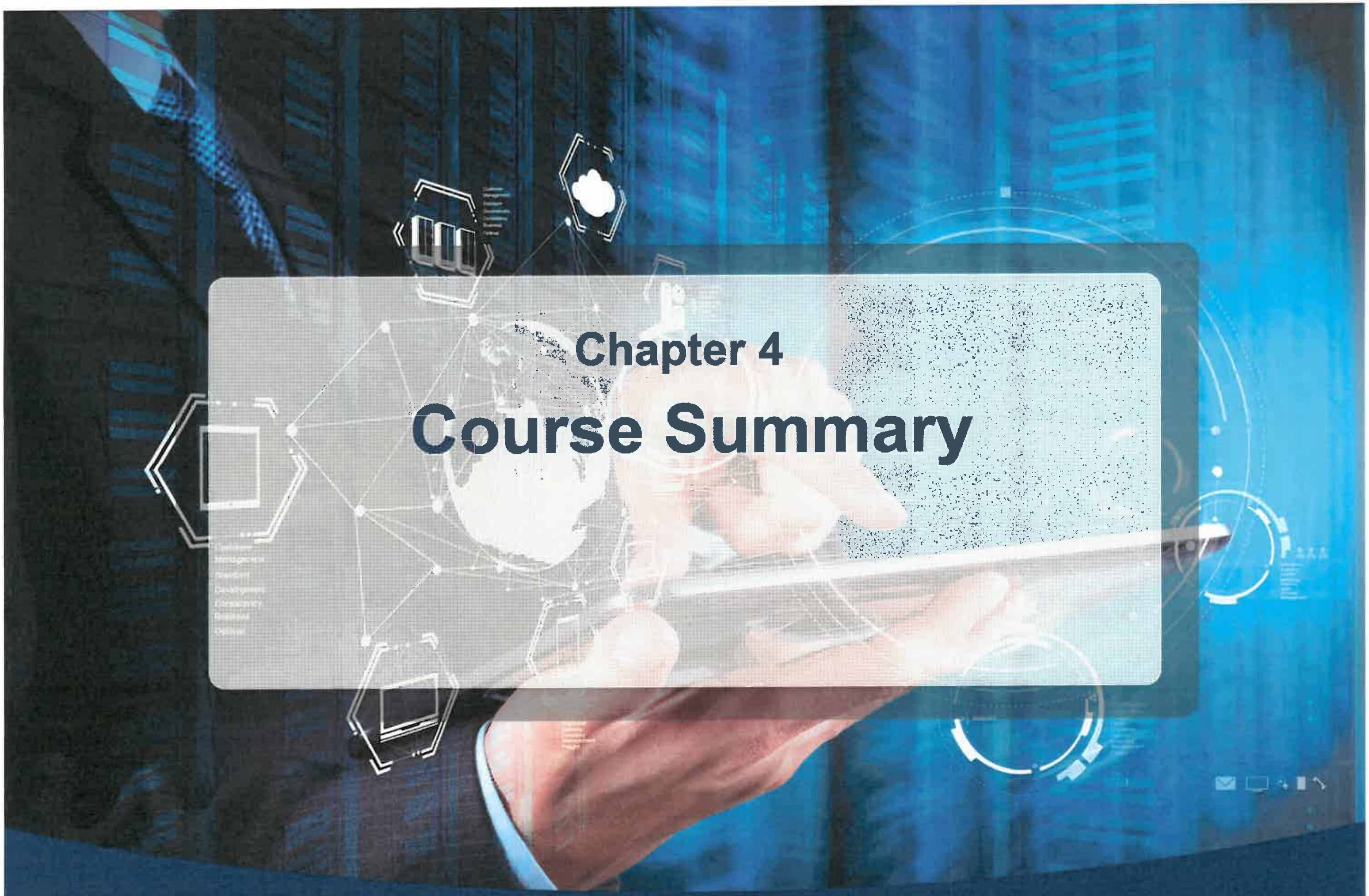
- **Cyber security insurance is an emerging tool for organizations to use as a cyber security risk mitigation approach**
- **Market is still relatively immature and evolving quickly**
  - Have corporate or outside counsel with expertise in this area advise management and the board

First-Party Coverage	Third-Party Coverage
Crisis Management (expenses following the wake of a breach, e.g., credit monitoring)	**Privacy Liability** (failure to protect privacy information)
Network Interruption (income loss associated with failure of computer systems/networks)	**Network Security Liability** (inability to access insured's network because of attack)
Contingent Network Interruption (third-party network failure affecting the organization)	**Regulatory Liability** (payments in connection with regulatory investigations, fines, etc.)
Digital Assets (expenses associated with replacing, recreating, etc., computer programs and data)	**PCI Data Security Standards Liability** (payment card industry demands for assessments, penalties, etc. in connection with PCI DSS noncompliance)
Extortion (payment to meet extortionist's demand to prevent a cyber security incident)	**Media Liability** (infringement of copyright or IP rights arising from media-related activities)

Source: Rosenquist, Matt, ed. *Navigating the Digital Age: The Definitive Cybersecurity Guide for Directors and Officers*. Caxton Publishing, 2015, p. 103. Download your free PDF, Kindle, or Epub copy at `https://www.securityroundtable.org/the-book/`.

Chapter 4

Course Summary



Course Summary

In this course, we have

- **Provided baseline knowledge of cyber security issues**
  - With a focus on its difficulty and scope
- **Highighted that cyber security is a risk management problem**
  - And recognized the need for a robust risk management process
- **Explained board and C-suite responsibilities in regards to cyber security**
- **Outlined tools to help implement an effective governance structure**
  - Without which your organization, and you, might be at risk

Reference Material

- NIST Cyber Security Framework
  - http://www.nist.gov/cyberframework
- NICE National Cyber Security Workforce Framework
  - http://csrc.nist.gov/nice/framework/
- Center for Internet Security (CIS)
  - https://www.cisecurity.org
- Technical vulnerabilities are tracked and explained in the U.S. National Vulnerability Database
  - https://nvd.nist.gov/cwe.cfm
- Web vulnerabilities are available at the OWASP Top 10
  - http://owasp.org
- Textbook provided with this course
  - Rosenquist, Matt, ed. *Navigating the Digital Age: The Definitive Cybersecurity Guide for Directors and Officers*. Caxton Publishing, 2015. Download your free PDF, Kindle, or Epub copy at https://www.securityroundtable.org/the-book/.

Reference Material

- **AWWA G430-14 Security Practices for Operation and Management**
  - **https://www.awwa.org/store/productdetail.aspx?productid=45320372**
- **AWWA Process Control System Security for the Water Sector**
  - https://www.awwa.org/Portals/0/files/legreg/documents/AWWACybersecurityguide.pdf

Additional Course Tools

Additional tools have been provided as separate handouts for the following:

- An outline for a Cyber Security Action Plan based on the NIST Cyber Security Framework and incorporating the CIS 20
- A glossary of standard cyber security terms for quick reference
- The list of key questions any board member should ask of management about the organization's cyber security posture

WORKSHOP

1B

Energy Management Workshop #1

Long Term Planning: RP-5

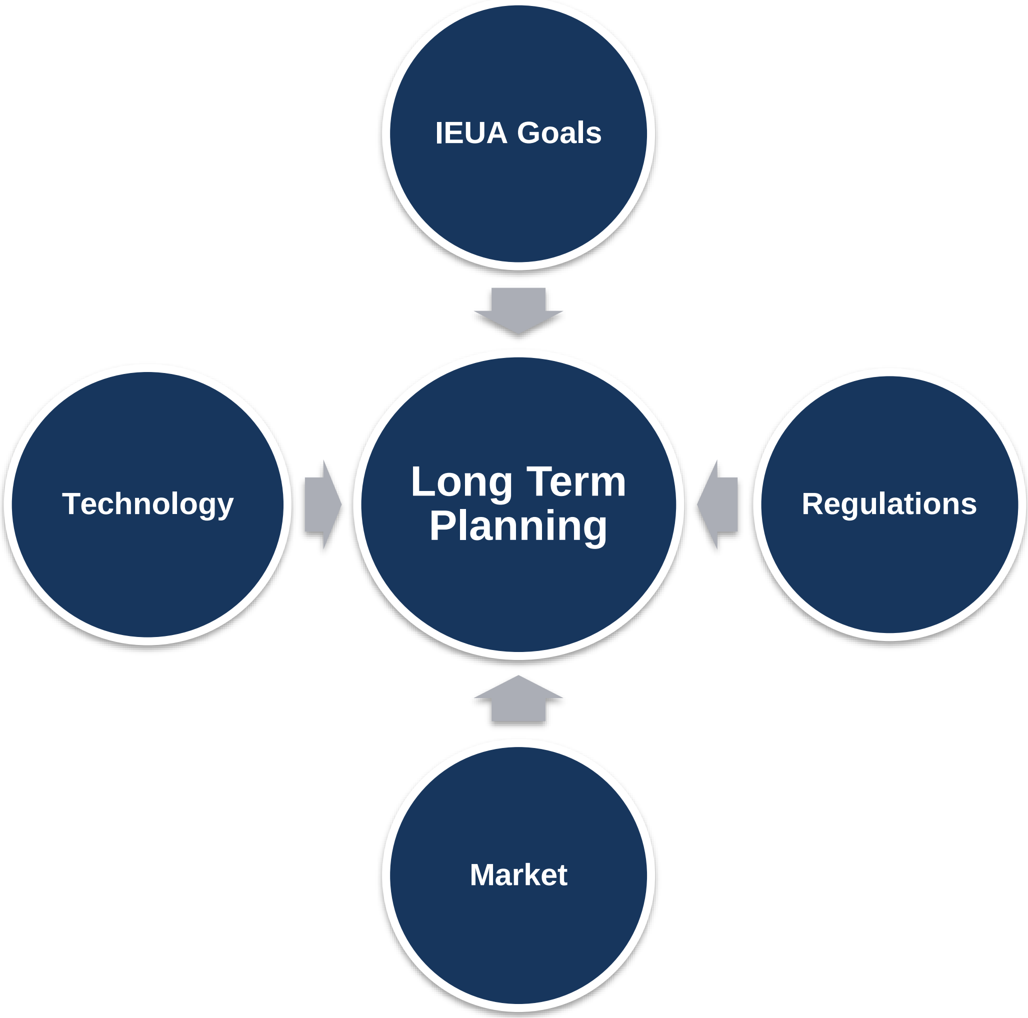
April 2017

Inland Empire Utilities Agency
A MUNICIPAL WATER DISTRICT

Energy Management Drivers

- Fiscal responsibility
  - Cost containment
  - Budgeting
  - Future grant eligibility
- Operational reliability
  - Minimize dependence on utility
- Environmental Stewardship
  - Enhance air quality
  - Support state goals

Considerations



Energy Management

IEUA Mission Statement:

"… providing essential services in a regionally planned and cost effective manner…producing high-quality renewable products such as recycled water, compost and energy."

IEUA Business Goal, adopted December 2016:

"To **effectively manage energy resources** including renewable energy initiatives and programs to achieve statewide environmental and renewable energy goals, and stabilize future costs."

Energy Management Initiatives

2015 Energy Management Plan

- Peak power independence
- Grid interdependence
- Organics diversion
- Carbon neutrality
- Energy efficiency

Peak Power Independence

2015 ENERGY MANAGEMENT PLAN

Onsite electricity generation during peak energy use/pricing period by 2020 through

- Increased energy efficiency
- Increased on-site energy generation
- Diversified energy portfolio
- Energy demand response
- Grid Interdependence

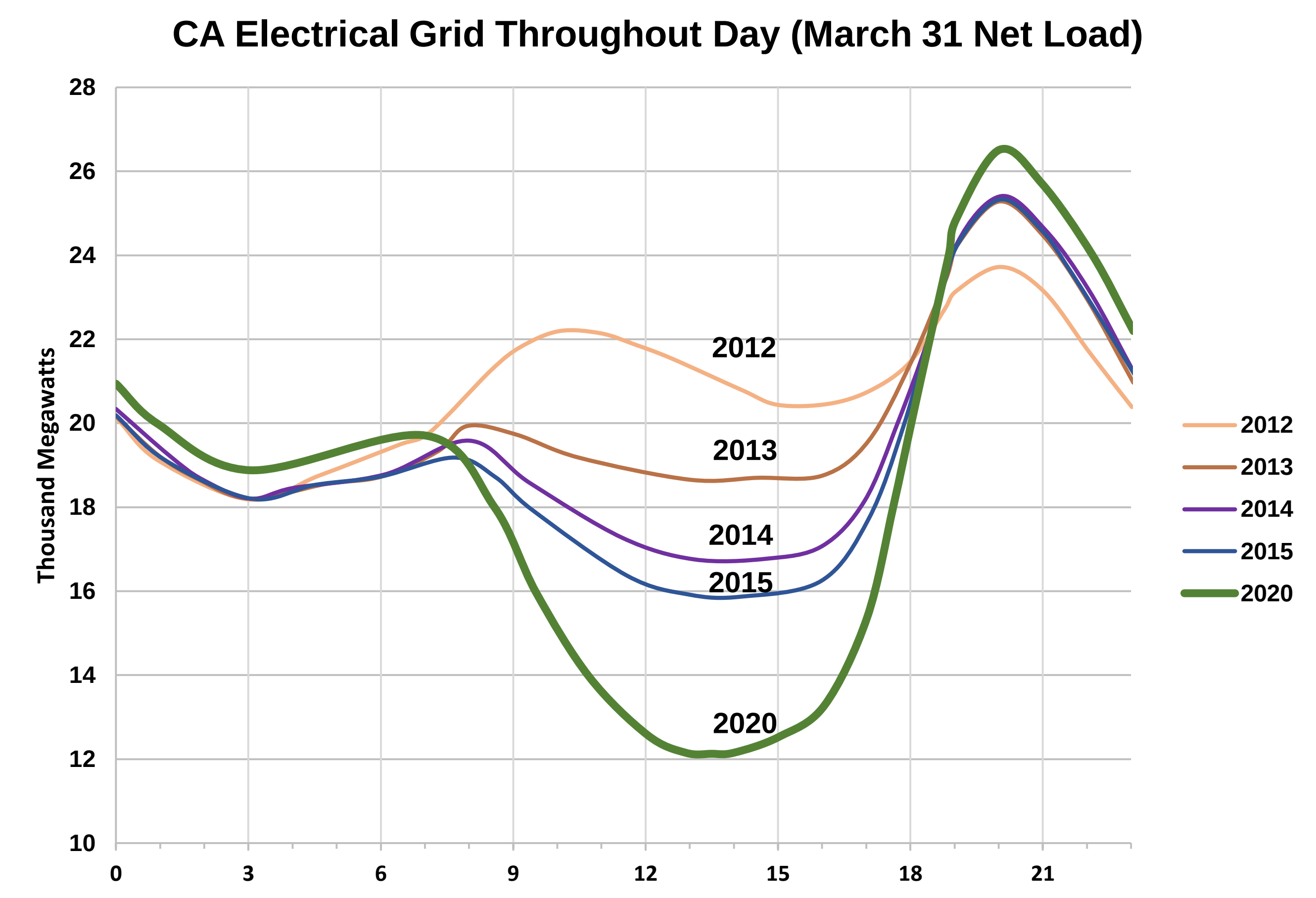
Inland Empire Utilities Agency
A MUNICIPAL WATER DISTRICT

Grid Interdependence

Between grid system operator, utilities, customers

- Effective use of existing resources
- Match generation with demand cost effectively
- Reduced dependence on expensive peak demand power plants
- Battery storage

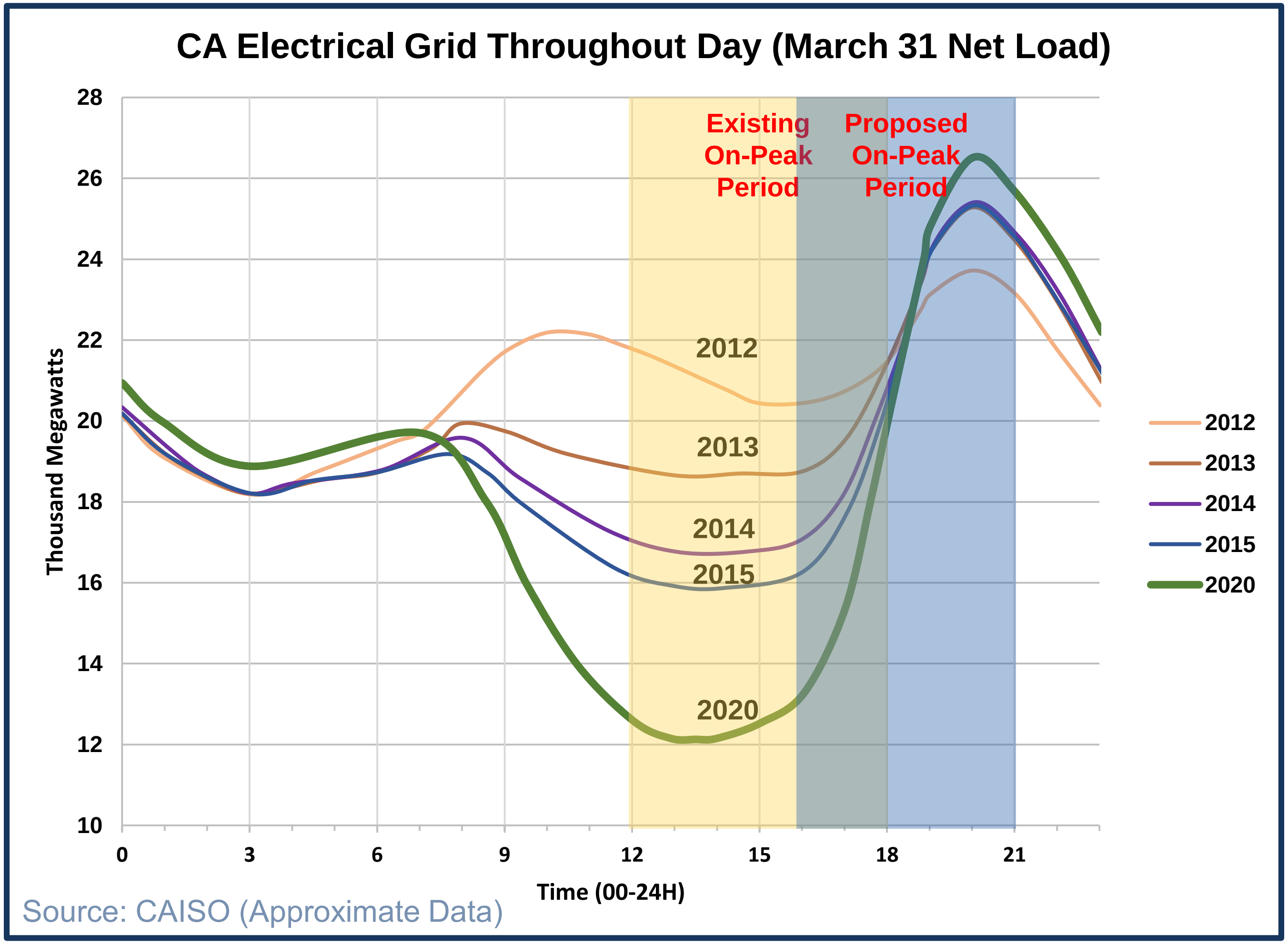
Grid Interdependence
Duck Curve



Source: CAISO (Approximate Data)

Inland Empire Utilities Agency
A MUNICIPAL WATER DISTRICT

Grid Interdependence
Duck Curve



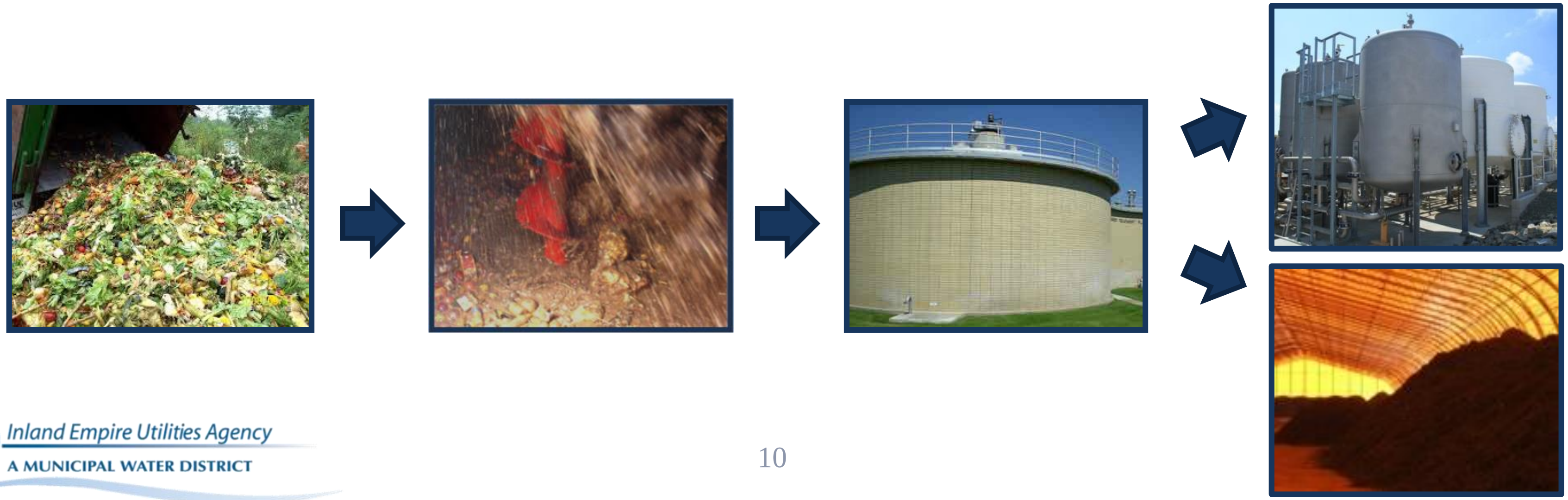
Source: CAISO (Approximate Data)

Inland Empire Utilities Agency
A MUNICIPAL WATER DISTRICT

Organics Diversion

Divert food waste from landfills to IEUA’s solids facilities

- Assist IEUA in meeting its long term energy needs
- Reduce critical short-lived climate pollutants
- Allow IEUA to assist Member Agencies to comply with the State’s organics diversion requirements



Carbon Neutrality

2015 ENERGY MANAGEMENT PLAN

IEUA to maximize opportunities to meet power needs with carbon neutral sources

- Biogas optimization
- Increased plant efficiencies
- Renewable projects
- Goal is to reach 100% by 2030

Energy Efficiency

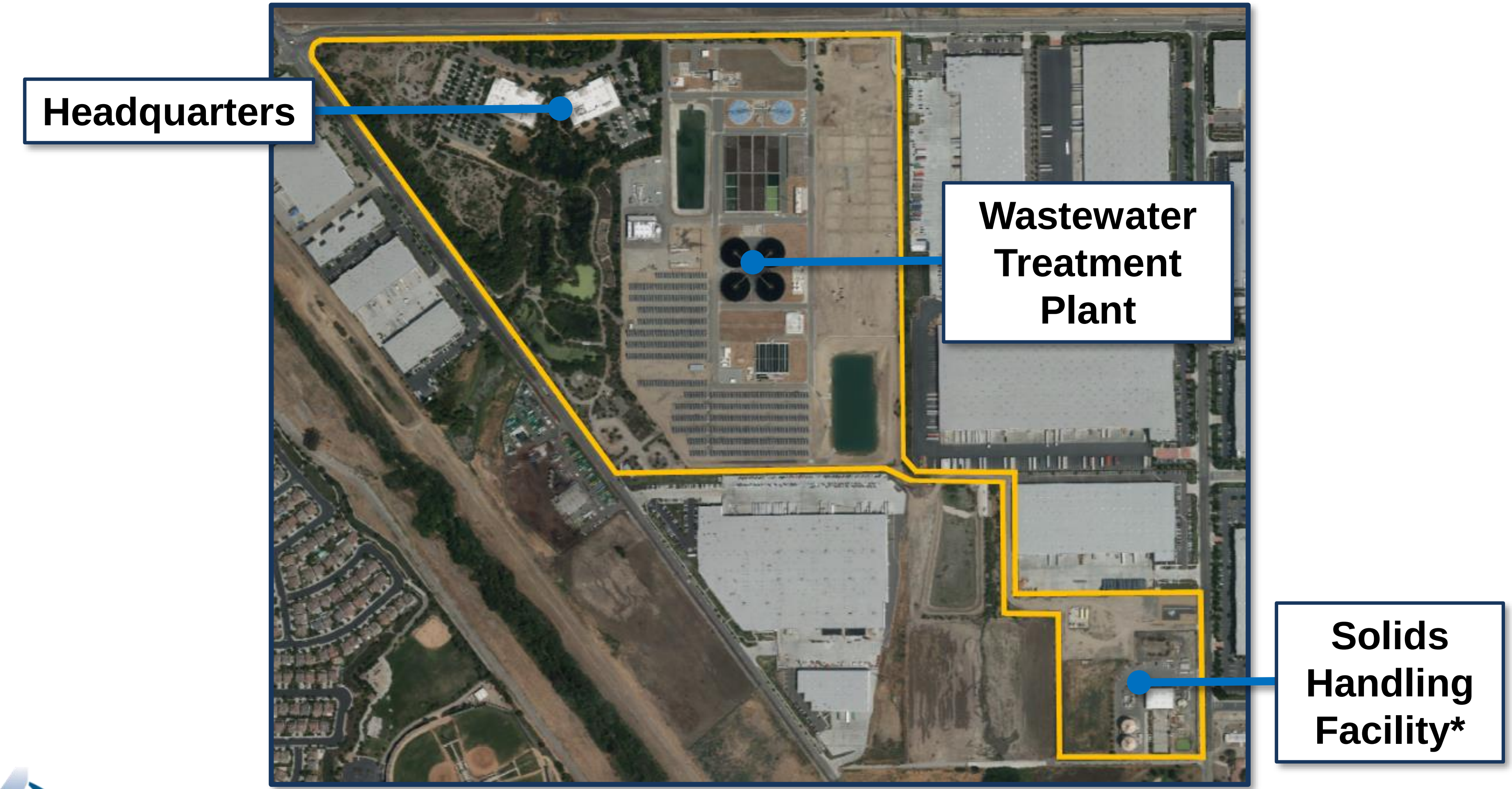
2015 ENERGY MANAGEMENT PLAN

Effectively manage and reduce energy consumption

- Facility audits
- Energy monitoring and benchmarking
- Energy retrofits
- Treatment process optimization
- Sustainable design and procurement

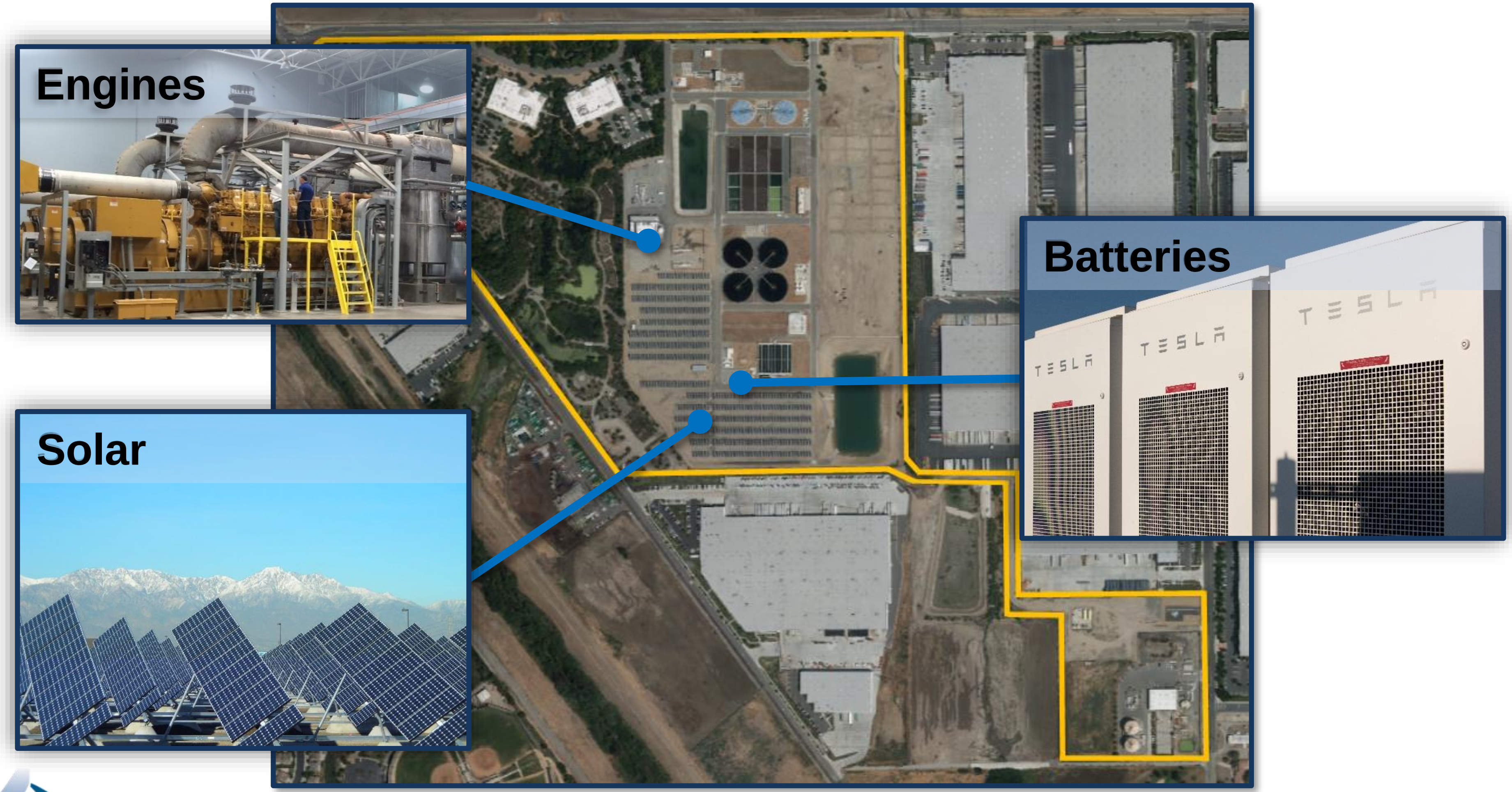
Inland Empire Utilities Agency
A MUNICIPAL WATER DISTRICT

Case Study – Regional Plant No. 5



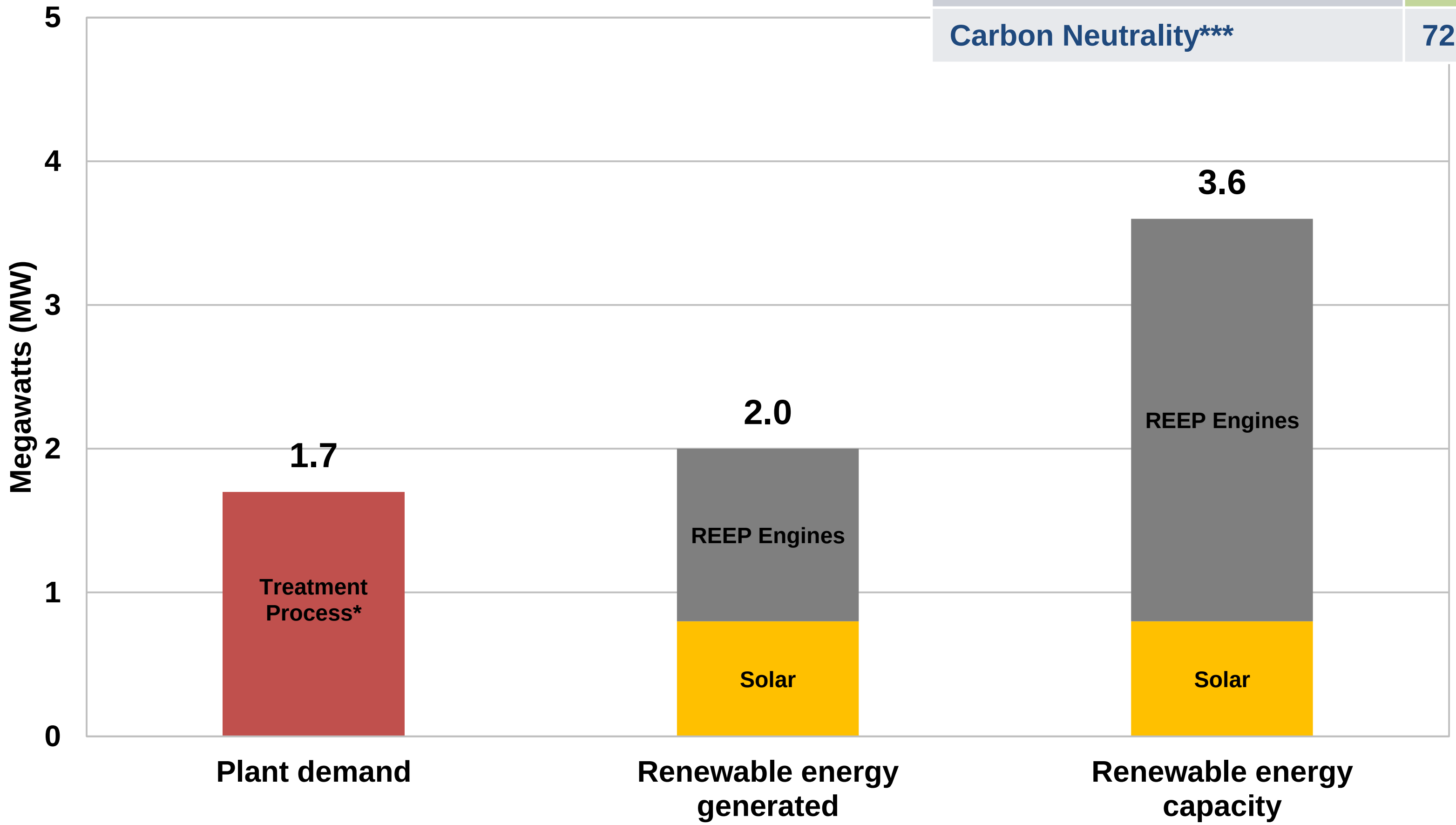
*Operated by Inland BioEnergy (IBE)

Existing Renewables & Resource Management @ RP-5



Regional Plant No. 5 (Current, 10 MGD)

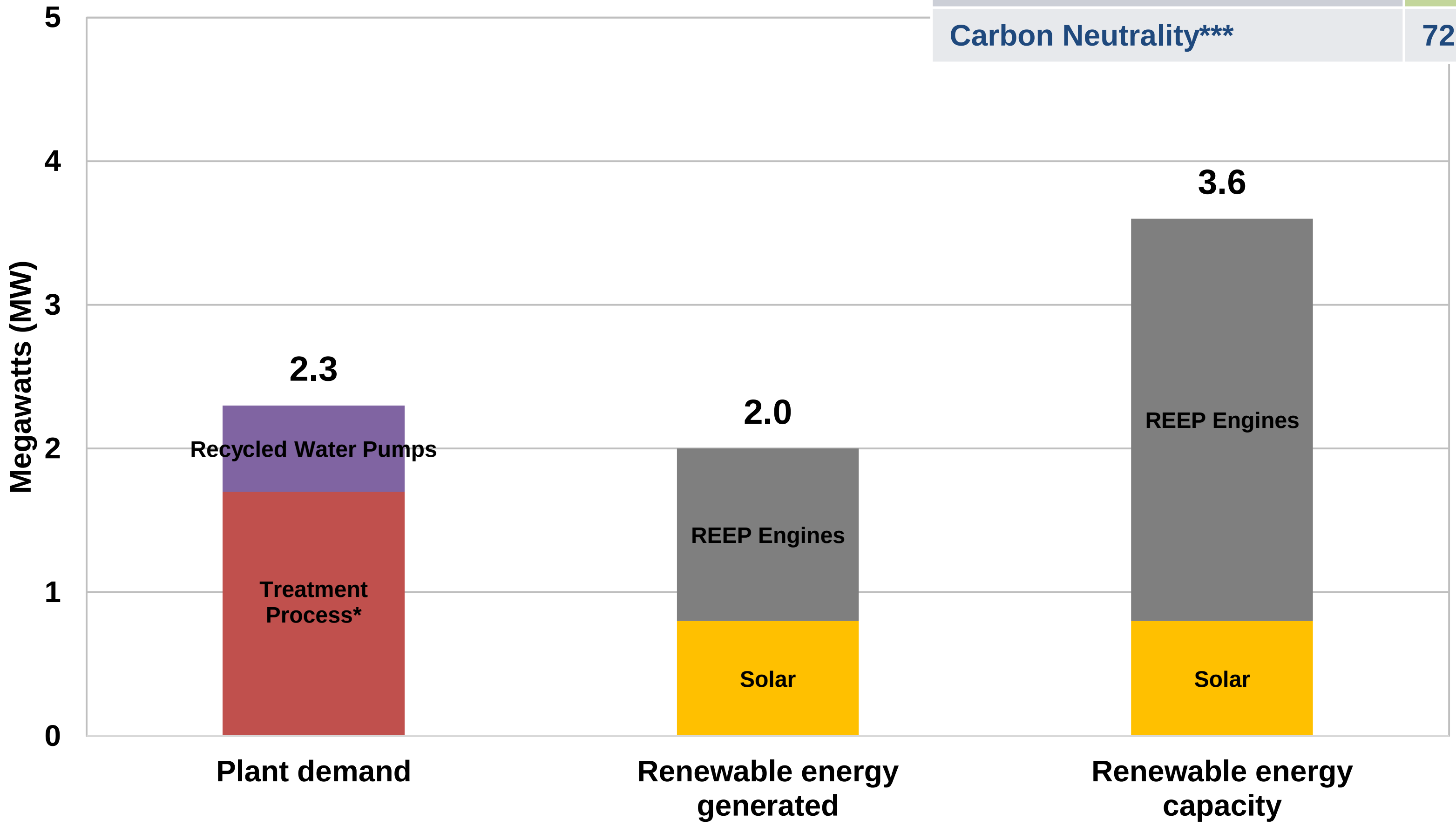
Goals	
Peak Power Independence	Yes
Grid Interdependence	Yes
Organics Diversion**	Yes
Carbon Neutrality***	72%



* Includes RP-2 and RP-5 Campus
**Organics diversion indirectly achieved through RP-5 SHF
*** 48% of the attributes assigned to IBE by contract for RP-5 SHF

Regional Plant No. 5 (Current, 10 MGD)

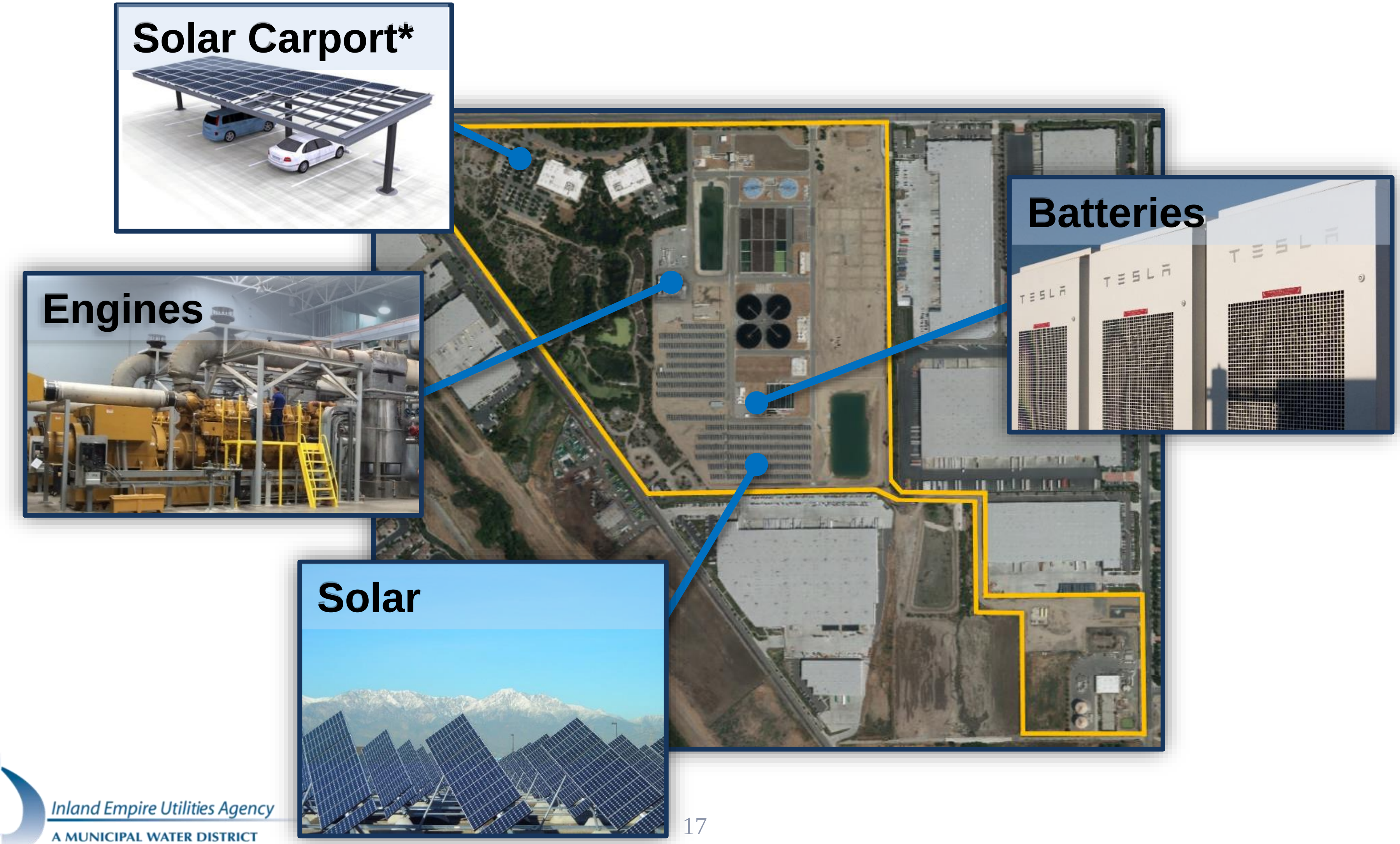
Goals	
Peak Power Independence	No
Grid Interdependence	Yes
Organics Diversion**	Yes
Carbon Neutrality***	72%



* Includes RP-2 and RP-5 Campus
**Organics diversion indirectly achieved through RP-5 SHF
*** 48% of the attributes assigned to IBE by contract for RP-5 SHF

Inland Empire Utilities Agency
A MUNICIPAL WATER DISTRICT

Potential Renewable* & Resource Management @ RP-5



Solar Carport*

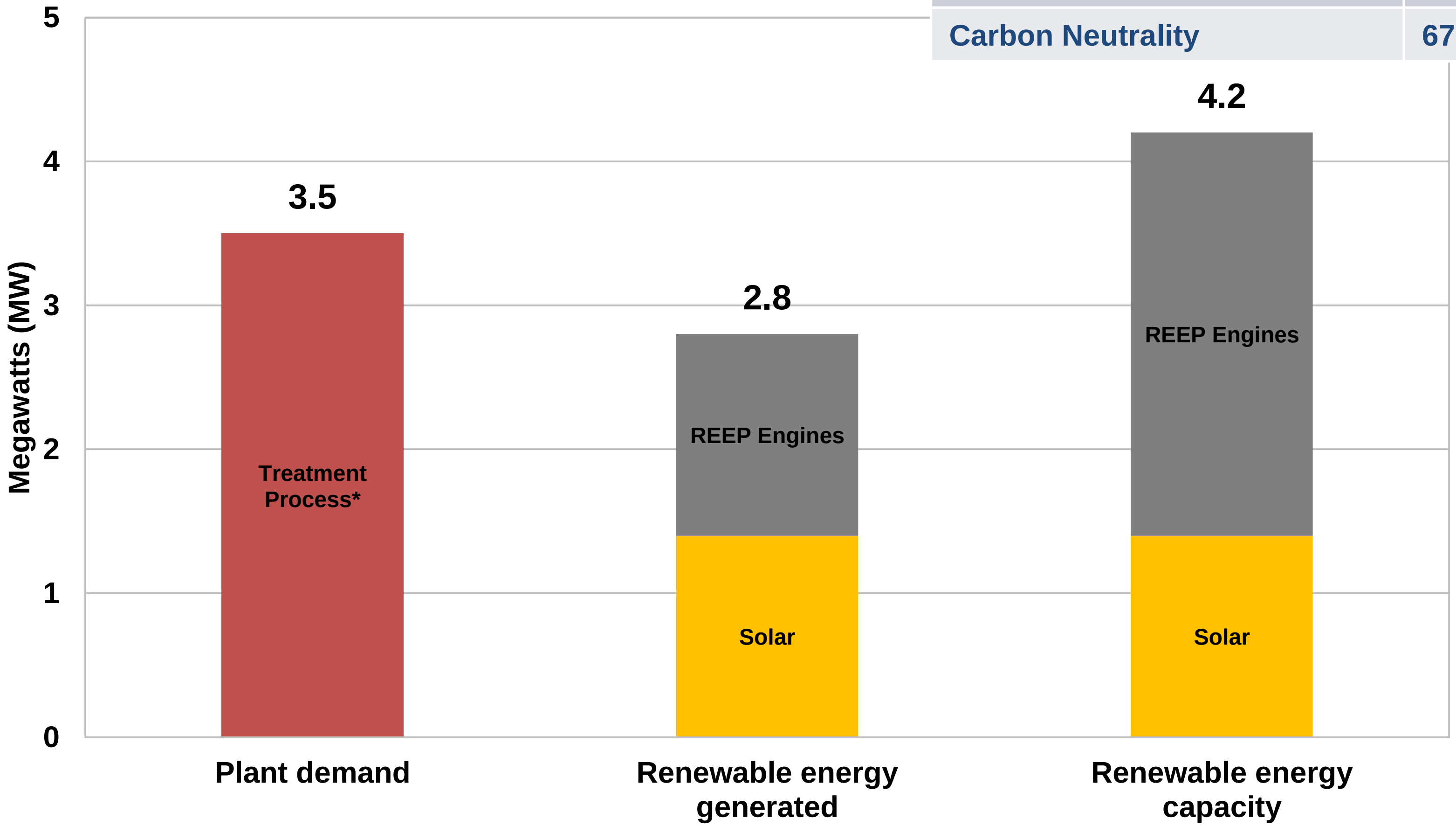
Engines

Batteries

Solar

RP-5 Biosolids Only (2025, 16 MGD)

Goals	
Peak Power Independence	No
Grid Interdependence	Yes
Organics Diversion	No
Carbon Neutrality	67%

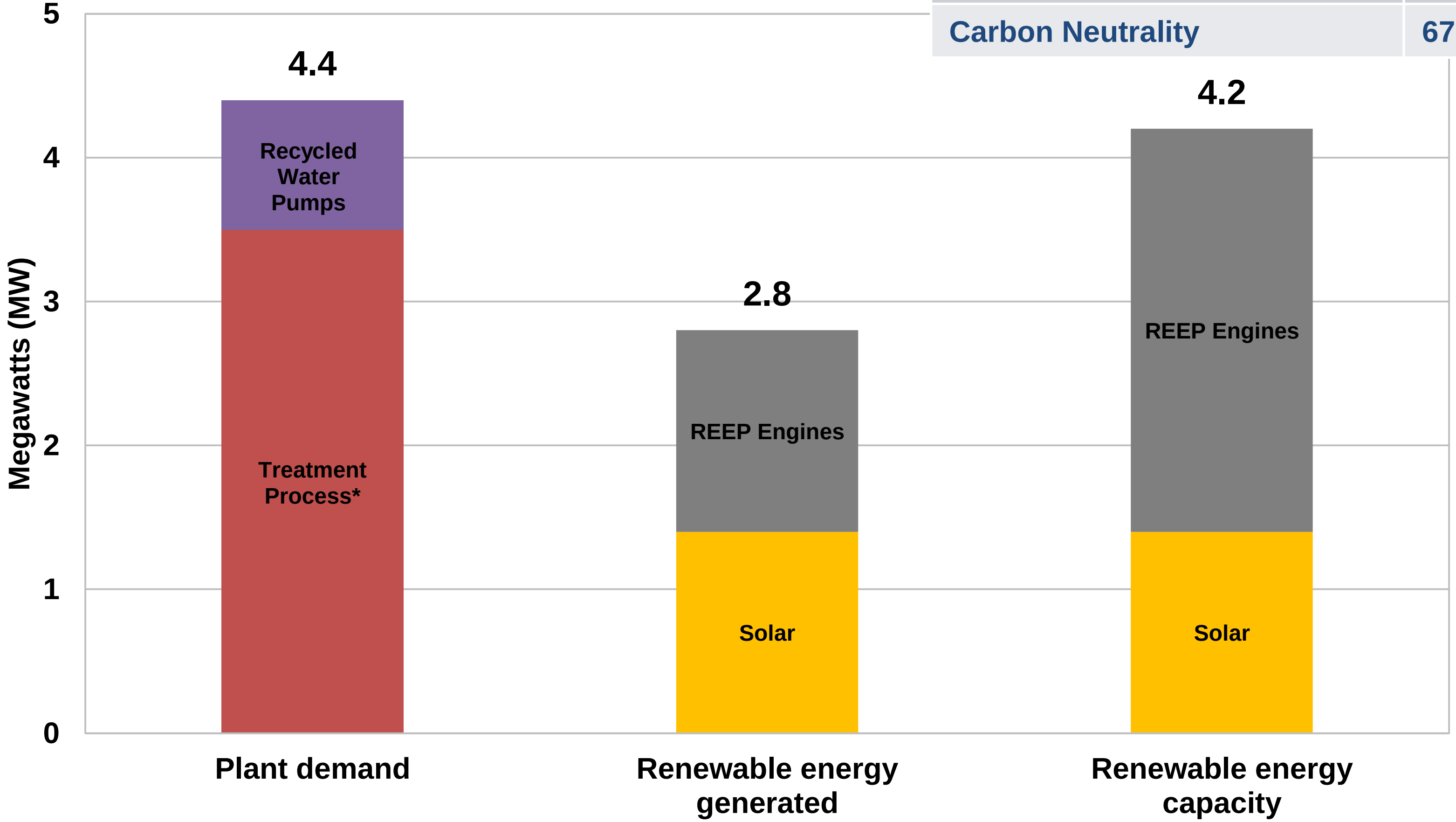


* RP-5 Campus (Liquid and Solid Treatment, Headquarters)

Inland Empire Utilities Agency
A MUNICIPAL WATER DISTRICT

RP-5 Biosolids Only (2025, 16 MGD)

Goals	
Peak Power Independence	No
Grid Interdependence	Yes
Organics Diversion	No
Carbon Neutrality	67%

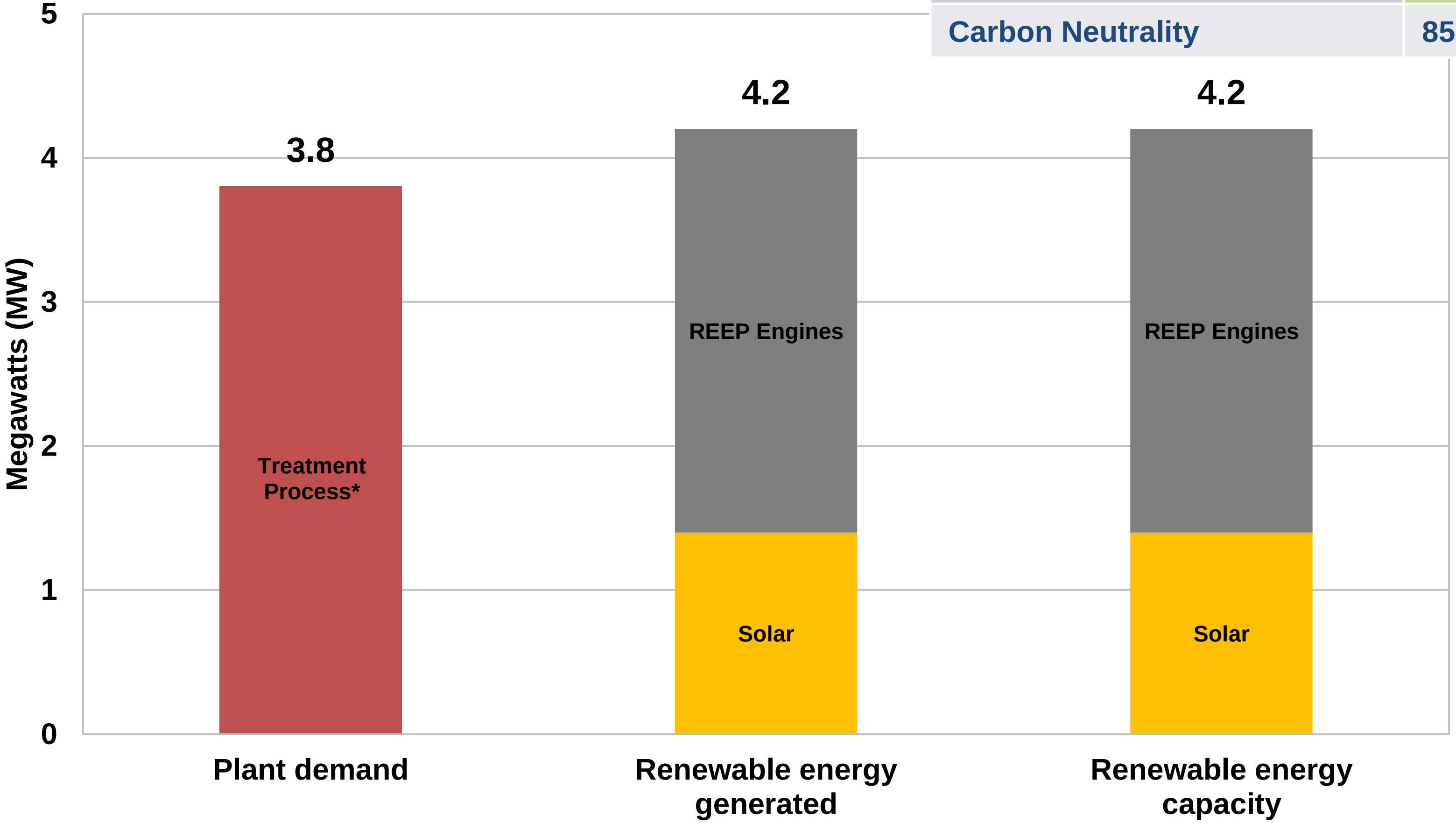


* RP-5 Campus (Liquid and Solid Treatment, Headquarters)

Inland Empire Utilities Agency
A MUNICIPAL WATER DISTRICT

RP-5 Biosolids and Food Waste (2025, 16 MGD)

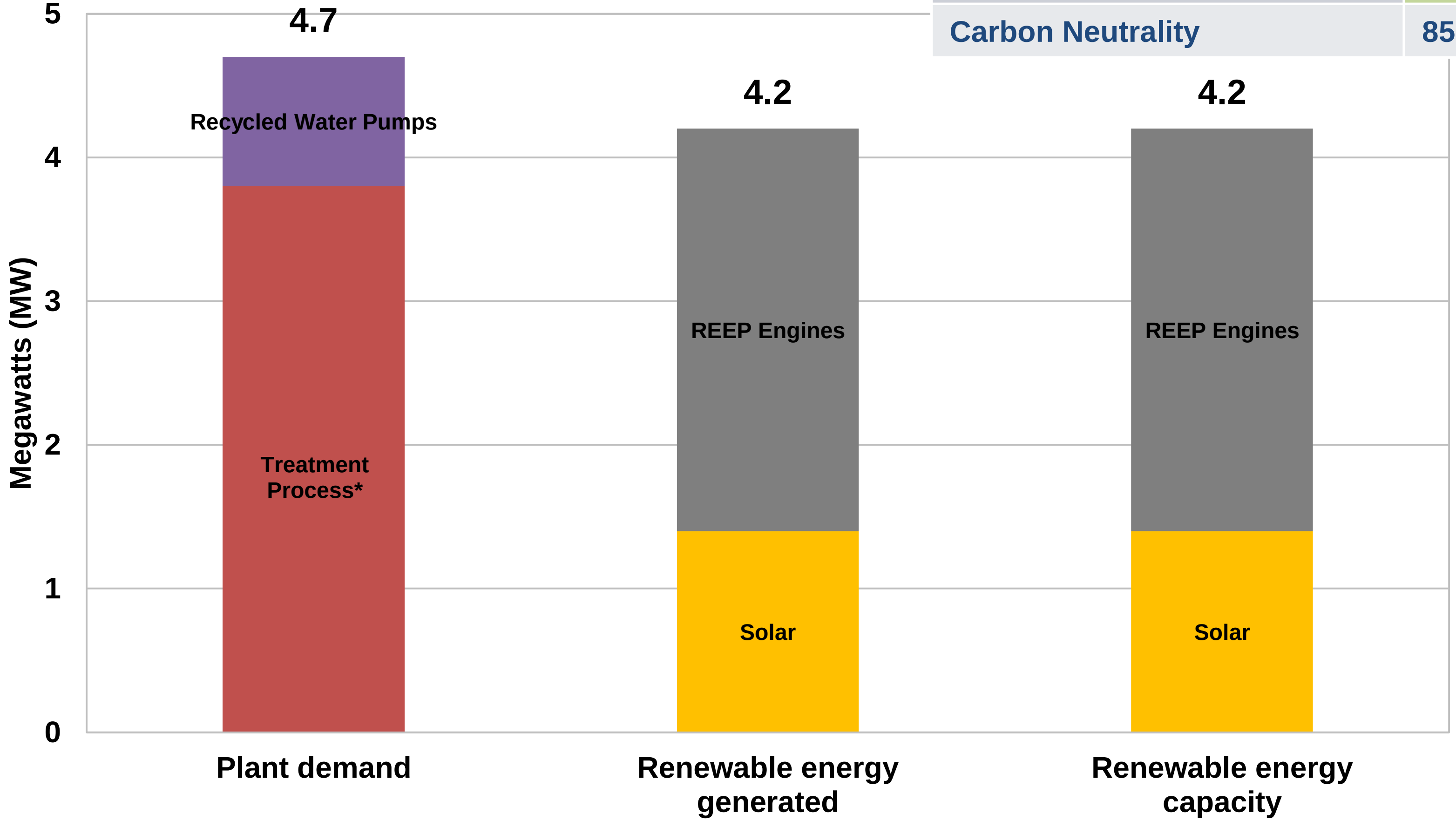
Goals	
Peak Power Independence	Yes
Grid Interdependence	Yes
Organics Diversion	Yes
Carbon Neutrality	85%



* RP-5 Campus (Liquid, Solid & Food Waste Treatment, Headquarters)

RP-5 Biosolids and Food Waste (2025, 16 MGD)

Goals	
Peak Power Independence	No
Grid Interdependence	Yes
Organics Diversion	Yes
Carbon Neutrality	85%

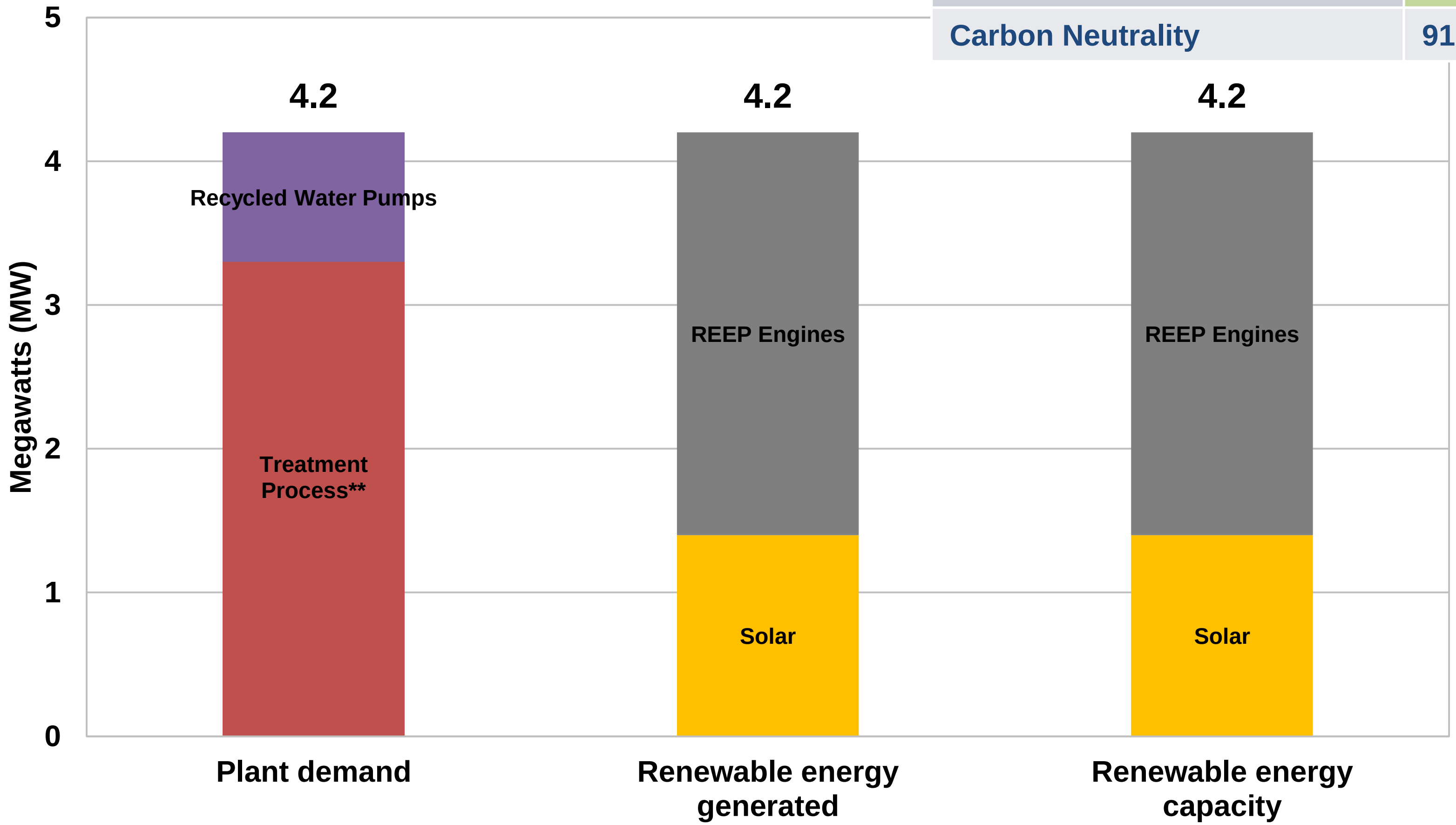


* RP-5 Campus (Liquid, Solid & Food Waste Treatment, Headquarters)

Inland Empire Utilities Agency
A MUNICIPAL WATER DISTRICT

RP-5 Biosolids, Food Waste, Energy Efficiency* (2025, 16 MGD)

Goals	
Peak Power Independence	Yes
Grid Interdependence	Yes
Organics Diversion	Yes
Carbon Neutrality	91%



*Energy efficiency potentially achieved through potential treatment process optimization

** RP-5 Campus (Liquid and Solid & Food Waste Treatment, Headquarters)

Next Step

- Energy Management Plan Workshop #2
  - May 2017