Dominic Saebeler - J.D.
Director of Cybersecurity and Risk Management
Illinois Commerce Commission

Business, People & Regulatory Considerations in Cybersecurity and Risk Management:
Predicting Viability of Innovative Solutions
Today’s Agenda

Why are we here today?

The Evolving PUC Role

Solving Complex Problems

5 Business & Regulatory Areas of Consideration

Deeper Dive Into Areas of Consideration

Now What?

Wrap Up
The views and opinions expressed herein strictly represent those of the presenters at this moment, and may not necessarily agree with positions of ICC Commissioners or Commission Staff. The presenters reserve the right to change those views and opinions as new information becomes available.

Nothing in this presentation should be interpreted as legal advice. You should accept legal advice only from a licensed legal professional with whom you have an attorney-client relationship. You should contact such a lawyer who may assist you in any matters to which you desire legal advice.
Business and Regulatory Considerations while Solving Complex Cyber Risk Challenges

CREDC, students and industry partners are all working together to solve complex problems through identifying, creating, testing and delivering innovative solutions to address evolving cybersecurity challenges.

Innovative solutions are sometimes tempered by the reality of Marketplace Dynamics, Financial Issues, Consumer and Business Interests, Personnel Challenges, Operational Context and the backdrop of Policies, Standards and Regulations.
Asking Good Questions

Is the human element being addressed?

Ultimately people will make thing work or they won’t

Will utilities embrace regular partnership with research universities and provide access to OT environments & share anonymized data in support of your solving security challenges?

Does this solution address and or consider cybersecurity supply chain risk? This is become a fundamental consideration of new product design whether your solution targets supply chain or just exists within it.

Will federal and/or state laws have a direct impact on utility decision making – as utilities select cyber threat prevention software and hardware?

Will federal and/or state utility regulators incentivize or support economically sound investment decisions to integrate new solutions that address evolving cyber risk challenges?
Delivering Value in a Kitchen with Many Chefs

Multiple market participants will have a say in how, when and if solutions are reviewed and whether they are eventually adopted by the marketplace.

Governments Entities
- FERC, NERC, DHS,
- Federal Agencies – FERC, FEMA, DHS, FBI, etc.
- NSF, NSA, DOE
- State Regulators, Emergency Management,
- State Police & Army National Guard

Utility Industry & Organizations
- IOUs, COOPs, Municipal Utilities, RTOs ...
- Standards Associations
- Information Sharing Centers
- Manufacturers
- Consultants

Research Institutions, National Labs & Trade Organizations
- Higher Education – UIUC, NCSA, University of Arkansas, WSU, Dartmouth, MIT, more
- National Labs: NREL, Argonne, PNL, ...
- EEI, NRECA, APPA, NGA, AGA ...

What Solutions Will Find their Way into the Marketplace?
Today's Agenda

The Evolving PUC Role

Solving Complex Problems

5 Business & Regulatory Areas of Consideration

Deeper Dive Into Areas of Consideration

Now What?

Wrap Up
U.S. state utilities commissions [URC, PUC or PSC] are typically governing bodies created to regulate the rates and services of public utilities operating in their respective jurisdictions (typically a state). They balance many factors including setting manageable rates, attracting investment and upgrade potential, reliability, resiliency and security of utilities.

In 2017, The Illinois Commerce Commission Created the Office of Cybersecurity and Risk Management to focus additional attention on the emerging risks posed by cyber threats to critical infrastructure in the electric, gas, water and telecommunications industries that operate and provide essential services to consumers and businesses within Illinois.

PUCs from states across the country are in various stages of actively assessing, directing, supporting and promoting economically appropriate measures be taken by utilities to ensure the reliability, resiliency and security of critical infrastructure in the electric, gas, water and telecommunications industries. These efforts should be consistent, adaptive and directed toward addressing the persistent and ongoing cyber threats to their operations and secure information.
Why Regulation?

Economist Alfred E. Kahn, who chaired the New York Public Service Commission during the 1970s, famously observed, “All regulation is incentive regulation.”
ICC – Cybersecurity & Risk Management (C&RM) Progress

Review legislation related to cybersecurity focused initiatives or potential requirements to assist in determining potential impacts.

Facilitate ongoing awareness and open dialogue about the role of the PUC in cybersecurity related strategy in the utility industry.

Model this type of PUC role for other states and exchange strategies between states.

Drive Discussion around Cybersecurity Supply Chain Management and associated best practices.

Participate in the analysis of and around best practice adoption and the role of third party audits in testing the practical applications and how those audits could best be facilitated.

Secure Integration of New Technologies

Role of the ICC/PUC

Collaboration and Knowledge Sharing

Cyber Defense Activity and Oversight

Legislation and Policy Review and Recommendations

Drive further collaboration and knowledge sharing between the various utilities in order the move toward consistent best practice adoption.

Explore new opportunities for a PUC to assist in optimizing communication channels between utilities and the federal and state government(s) to prepare for and address fallout and recovery from an actual cyber event.

Facilitate the hosting of table top exercises and strategy workshops within utility industry.

Participate in and drive the ongoing exchange of information related to the benefits and risks associated with the emergence of new technologies and their integration into utility operations.
Today’s Agenda

- Solving Complex Problems
- 5 Business & Regulatory Areas of Consideration
- Deeper Dive Into Areas of Consideration
- Now What?
- Wrap Up
Problem Solving
Unforeseen Issues
Ongoing Challenges

Reality Pushes Back
- Research and design of new solutions must be tied to solutions that consider realistic context and the potential for unplanned factors and inputs.

Chicken and the Egg Concept
- Are we first asking what problem needs to be solved or are we searching for a problem our solution might address?

The Best Solution Doesn’t Always Win
- Someone else may not want your solution to work – even if it’s better.
Many Issues to Address

https://www.einfochips.com/blog/shaping-up-analytics-for-the-smarter-grid/
https://www.allot.com/blog/iot_cybersecurity_challenges_and_solutions/
https://smartgridawareness.org/2017/01/07/cyber-attack-surface-of-unprecedented-scale/

https://automation.isa.org/integrated-security-strategy-protect-industrial-assets/

AMI Network with Potential Attack Vectors

Figure 3: AMI Information Network

Utility Cyber Challenges

- Secure Data Collection & Transfer from IoT Devices
- IT/OT Integration
- Patch Management
- Remote Device Management
- Application Whitelisting
- Data Access and Protection
- Access to Timely Relevant Threat Intelligence

- Supply Chain Risk Management
- Recruiting & Retaining Skilled Cyber Talent
- Access To Useful Metrics
- Cyber Insurance
- Managing Regulatory Interactions
- Employee Behavior
- Physical Security Concerns
- Managing Employee Behavior
Today’s Agenda

5 Business & Regulatory Areas of Consideration

Deeper Dive Into Areas of Consideration

Now What?

Wrap Up
Today’s Agenda

- Deeper Dive Into Areas of Consideration
- Now What?
- Wrap Up
Considerations

MARKETPLACE DYNAMICS

- The Interplay of Consumer and Business Interests
- Tariffs – Trade Agreements and Macro Economic Factors
- Government Contracting, Bidding Process, Specifications, & Influence of Consultants on Marketplace
- International Logistics, Support & Supply Chain Security Risk Issues
- Dominant Market Player Resistance & Competitive Advantage v. New Products

Will the Market Support this new Product? & Who Will Pay For IT?

Advocacy and special interest groups may interfere with marketplace product adoption?

Are Consumers Willing to Pay More For the Additional Benefit / Security of the proposed solution?

Industry Adoption Challenges Exist including navigating co-dependencies – Stakeholders are Still Figuring Out How to Balance Risk and Information Sharing

Are Consumers Willing to Pay More For the Additional Benefit / Security of the proposed solution?

Is there a Potential Environmental Consideration Preventing Adoption?

Deciding Who is responsible for Solving the Problem

Advocacy and special interest groups may interfere with marketplace product adoption?
Balancing Interests

Fundamental Expectations: Reliability, Privacy & Low Rates

Enhance Grid Operations and Efficiency + Ensure Access to Capital & Return on Investment for IOUs


Utility & RTOs Must Balance Load/Demand/Capacity Availability & Cost

Consumer & Business Interests

Utility Interests
Supply Chain Security

The Increasingly International Supply Chain is full of Security Risk Issues

Huawei phones, Kaspersky software banned by some State Governments and Federal Agencies

Supply Chains are extremely complicated and involve multiple players – utilities are trying to enforce compliance with best practices but can only reach so far into the vendor business models

http://archive.cotsjournalonline.com/articles/view/103197
Environmental Policy Issues

DIRTY ENERGY
FINITE SOURCES

CLEAN ENERGY
RENEWABLE SOURCES


SUBSIDIZE THIS

The panel shows the environmental impact of subsidizing different energy sources. The graph illustrates the cost savings associated with clean energy compared to dirty energy. The following facts are highlighted:

- Clean Energy: $2.3 billion savings
- Solar Power: $1.6 billion savings
- Wind Energy: $16.8 billion savings
- Coal Power: $70.2 billion savings

The data is based on the annual energy consumption of the United States. Clean energy sources are projected to save the country significant amounts of money, reducing the overall cost of energy. 

https://alternativeenergy1.weebly.com/blog/archives/03-2015
Dominant Market Players


### Dominant Market Players

#### 100 Years Ago

<table>
<thead>
<tr>
<th>Industry</th>
<th>Company</th>
<th>Share</th>
</tr>
</thead>
<tbody>
<tr>
<td>Steel</td>
<td>US Steel Corporation</td>
<td>67%</td>
</tr>
<tr>
<td>Refined Oil</td>
<td>Standard Oil</td>
<td>87%</td>
</tr>
<tr>
<td>Sugar</td>
<td>American Sugar Refining Company</td>
<td>98%</td>
</tr>
</tbody>
</table>

#### Today

<table>
<thead>
<tr>
<th>Industry</th>
<th>Company</th>
<th>Share</th>
</tr>
</thead>
<tbody>
<tr>
<td>Health Insurance</td>
<td>Blue Cross Blue Shield, United Health, Aetna, Cigna</td>
<td>80%</td>
</tr>
<tr>
<td>Beef</td>
<td>Tyson Foods, National Beef, JBS USA, Cargill</td>
<td>85%</td>
</tr>
<tr>
<td>Beer</td>
<td>AB InBev, Molson Coors</td>
<td>70%</td>
</tr>
</tbody>
</table>
Complex - Connected Utility Footprint

Purchasing - The Bidding Process

**RFI**
Request For Information
- Purchaser does not have sufficient information to write a detailed request
- Purchaser is not necessarily committed to buying
- Likely to involve a further request before a final decision.

**RFP / RFO**
Request For Proposal or Request For Offer
- Purchaser seeks solutions-based submissions to meet their needs
- Possibly no clear specification
- Greater flexibility than an RFT
- Suited to professional services.

**RFQ**
Request For Quotation
- Purchaser has clearly defined criteria or specification
- Judged primarily or solely on price
- Purchaser is committed to buying.

Image created by www.writehouse.com.au

Considerations

Will Utilities Decide to Buy this New Product?

Timing – Utility is Already Invested in Alternate Solution(s) – Long term Investments in existing Equipment with Multiple Decade Depreciation Plans (Sunk Cost)

Budget for Security is Already Maxed out or Committed to Other Solutions or Internal R&D Expenditures

Capital v. Operational Expense Dynamics
Decision Making & Rate Making

It is all about Metrics

Complexity of Determining the Payback on New Product Investments

Procurement Issues – Bidding, Specifications & Existing Contractual Commitments

Will the Industry Pay more for an Innovating Solution? Are there Metrics Available to Support the Investment Thesis?
Utility Rate Setting

Utilities Recovery their Costs through Rates – Approved by a PUC

PUC Balances the interests of all stakeholders

Illinois PUC Mission:
Ensure - adequate, efficient, reliable, environmentally safe, least-cost public utility services . . . equitable to all” “affordable”
And “prices that accurately reflect long-term cost of such services” – plus “a sufficient return on investment . . . to attract capital”

Utilities must decide how to balance the allocation of its resources – Capital Expenses or Operational Expenses

http://archive.cotsjournalonline.com/articles/view/103197
CAPEX or OPEX

CAPEX

- Buy or Build Asset
- Long-Term Focus

Utilities are permitted a Rate of Return on these Investments

OPEX

- Run the Business Today
- Near-Term Focus

Utilities are typically not permitted a Rate of Return on these Investments
Revenue Requirement Formula

Rate Base \times \text{Rate of Return} = \text{Required Operating Income} + \text{Expenses} = \text{Revenue Requirement} → \text{Customer Rates}

- **Rate Base**: $\$\$\$ invested in plant assets and working capital to provide utility services < accumulated depreciation
- **Rate of Return**: Sum of weighted costs of debt, preferred stock and common equity
- **Required Operating Income**: $\$ needed by utility to earn a fair return for utility’s investors
- **Expenses**: Income taxes, other taxes, depreciation, amortization, and operating & maintenance expense
- **Revenue Requirement**: Total Cost required for utility to operate each year – collective amount received from rate payers
- **Customer Rates**: Access to market capital is critical to sustain long term investment and upgrades cycles – Investors will avoid uncertainty
Types of Rate Case in Illinois

Traditional Rate Case
- Utility Decides It isn’t making enough Money
- 11 Month Process – Rates In Effect Next Year
- No Reconciliation – Over or Under Recovery Could Occur
- Rates Remain in Place until another Traditional Rate Case – Initiated by Utility – Rates Heavily Contested

Formula Rate Case
- Parties Agree to Revisit Each Year
- 8 Month Process
- Reconciliation in the Year After Rates are Effective
- Rolling Rate Adjustments Annually (T-Bill)
In **2016**, the ICC formula rate Order had three main parts:
- A “formula rate update” that sets new distribution rates for 2017 based on 2015 data;
- A reconciliation of costs utility charged in 2015 to ICC-approved 2015 actual costs, the difference of which will be charged or refunded to ratepayers in 2017; and
- A calculation of the ROE collar, with the result charged or refunded to ratepayers in 2017.

In **2016**, the 2015 FERC Form 1 was used for two different purposes:
- To estimate rates for 2017; and
- To reconcile rates charged in 2015 (determined in 2014 rate case) to approved 2015 actual costs.
The Illinois ICC is Currently Considering Cloud Computing Financial Treatment for Transmission systems

Performance Based Regulation

Cost of Service Base Revenues

Basic PBR (Limited PIMs, Limited Formula) – Where the majority of utility revenues are subject to Cost-of-service-regulation (COSR), but modified with multi-year rate plans and/or decoupling. Performance Incentive Mechanism (PIM)s are used to improve core services; some states may include energy efficiency incentives. California’s present regulatory system could be considered a form of Basic PBR.

Revenue Cap (Limited PIMs, Formula w/ exogenous ‘x-factors’) – Where a revenue (or price) cap is established with adjustments based on desired productivity improvements. In this model PIMs are used sparingly, typically to prevent degradation of core services. The UK (prior to RIIO), Australia and several European and Latin American countries have used Revenue Cap regulation and its antecedent price-cap regulation.

Hybrid PBR (PIMs, Limited Formula) – Similar to Basic PBR in that COSR regulation is retained. The approach diverges in that it envisions broad use of performance incentives to accomplish social goals and to meet utilities’ revenue requirement. New York’s regulatory system may resemble a form of Hybrid PBR once the Reforming Energy Vision (REV) process is completed.

Integrated PBR (PIMs, Formula w/ exogenous ‘x-factors’) – An Integrated PBR model would include both a revenue cap and broad use of targeted incentives. The best examples of initial attempts at such an approach are the UK RIIO and to a lesser degree the Ontario Renewed Regulatory Framework for Electricity Distributers models.

BENCHMARKED BASE REVENUES

Narrow Incentives

Basic PBR

Hybrid PBR

Revenue Cap

Integrated PBR

Broad Incentives

BENCHMARKED BASE REVENUES

California Public Utilities Commission Report on PBR – Theory and Application to California:
Considerations

Am I considering the human aspects of adoption?

Someone has to implement your solution & make decisions – is it too complex? Will employees fight it? Is it intuitive?

Does it require a different skill set? Specialization? Training?

Adoption Resistance – I like the tool that I have now

Will this solution create a greater risk of human error and introduce new elements of risk by failure to execute properly? Will additional complexity lead to confusion, especially during times of stress? Training Considerations

Availability Gap - Negative Employment Projections – will the business have employees with the skill sets needed for your solution?

Is there a collective bargaining agreement in place – does the union have a say in training?

Does Automation replace human based roles – is it complementary – does it free up resources to do other tasks?
Human(s) Error(s)

Potential Points of Attack

Require Security Training for All Employees

Human error plays one of the biggest roles in security breaches today. Nine in 10 companies now require this training to assess or improve security knowledge among their employees.

ARE YOUR EMPLOYEES EDUCATED ABOUT CYBER-RISKS?


Cyber Talent Gap

https://medium.com/@jayeshbhire/resolving-the-cyber-skills-gap-shortage-d67c2ede7db1

MIND THE GAP

By 2022, there will be a shortage of 1.8 million information security workers.

1,800,000

NUMBER OF WORKERS

NUMBER NEEDED

Surpassing Baby Boomers as the largest living generation, Millennials will be critical for filling the employment gap. To secure the best talent, it’s important to understand who Millennials are and what motivates them.

https://www.boston.gov/news/demand-high-cybersecurity-workers

Cyber Security Resources (cont.)

Biggest SKILLS GAP in today’s security professionals:

![SKILLS]

- **Ability to understand business**: 52%
- **Technical skills**: 25%
- **Communication skills**: 17%

FEWER THAN HALF are CONFIDENT in their team’s ability to handle anything beyond simply cyber incidents

![ONLY 46%]


https://medium.com/@drpolonski/can-we-teach-morality-to-machines-three-perspectives-on-ethics-for-artificial-intelligence-64fe479e25d3
## Personnel Challenge Implications

<table>
<thead>
<tr>
<th>Utility Existing Challenges</th>
<th>Impact on Product Adoption</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Access To Talent</strong></td>
<td></td>
</tr>
<tr>
<td>› Need to Recruit and Retain top level talent</td>
<td>› Are external resources available to implement new solutions?</td>
</tr>
<tr>
<td>› Competing with High Tech Industry for Cyber Skills</td>
<td>› Does the need for 3rd party installation increase cost?</td>
</tr>
<tr>
<td><strong>Competing Priorities</strong></td>
<td></td>
</tr>
<tr>
<td>› Limited Existing Staff has a full plate with current assets</td>
<td>› New Product Adoption may be stalled behind existing projects and taxed resources</td>
</tr>
<tr>
<td><strong>Skill Gap</strong></td>
<td></td>
</tr>
<tr>
<td>› Time is needed for training and system testing</td>
<td>› Product Adoption may be impacted by steep learning curve</td>
</tr>
<tr>
<td>› Existing Staff may need to learn additional skill sets to maximize value of new product(s)</td>
<td>› Does new product require advanced skill set?</td>
</tr>
<tr>
<td><strong>Human Error</strong></td>
<td></td>
</tr>
<tr>
<td>› Do new solutions create potential for additional risk to overworked teams</td>
<td>› Must consider – difficulty factor of product use and whether new risk is acceptable</td>
</tr>
</tbody>
</table>
Considerations

Will this product solve more problems than it might create when in production?

Existing Security Products, Dynamics, Frameworks and Investments and integration issues

Risk Management Strategies, Measurements & Implementations

Risk Based & Compliance Based Approaches

Does this new product create a new and different kind of risk along with the value proposition?

Operational Technology and Information Technology Integration Issues and Ownership

Does this product add some new value / efficiency / automation / that overcomes opposition to one for one trade off?

Are there interoperability consideration for adoption – legacy software, hardware and equipment needs to work with the new solution – but can’t

Are operators willing to trust equipment from new company, with potentially unknown suppliers that does not have a track record / perceived staying power?
OPERATIONAL RISKS ARE DYNAMIC
Risk Management

Defining Risk & Risk Management

**Risk:** A probability or threat of damage, injury, liability, loss, or any other negative occurrence that is caused by external or internal vulnerabilities, and may be avoided through preemptive action.

http://www.businessdictionary.com/definition/risk.html

**Risk Management:** Identification, analysis, assessment, control, and avoidance, minimization, or elimination of unacceptable risks.

An organization may use risk assumption, risk avoidance, risk retention, risk transfer, or any other strategy (or combination of strategies) in proper management of future events.

http://www.businessdictionary.com/definition/risk-management.html
Business Elements of Utility Risk Formula

1. Threat
   - Lack of Funding
   - Failure of Imagination
   - Malicious Actors
   - Natural Hazards
   - Software Virus
   - Lack of Information

2. Vulnerability
   - Human Error
   - Equipment Failure
   - Unprotected Devices
   - Unsecured 3rd Parties
   - Shadow IT
   - IT/OT Convergence

3. Consequence
   - Economic Loss
   - Injury or Death
   - Loss of Trust
   - Cascading Impacts
   - Social Unrest
   - Political Conflict
IT/OT Convergence

Industrial IT and OT Systems and Devices

https://www.arcweb.com/blog/it-ot-cybersecurity-convergence

Figure 1: IT and OT collaborating on cybersecurity?

Source: PMMI Business Intelligence: The Evolution of Automation 2017

https://www.oemmagazine.org/technology-topics/information-security/note-corporate-operations-management-cybersecurity-your
Risk Mitigation


http://tierrasalto.com/risk-management-degree/
Event Response Planning

Response Coordination – who is in charge?

- Governmental entities
- Utilities
- First Responders (police, fire, national guard, etc.)
- Humanitarian Groups
- Businesses
- Military
- Medical
- Press, Social Media, etc.
Considerations

POLICIES, STANDARDS & REGULATIONS

Will this solution work with existing and emerging standards, best practices and frameworks?

Are legislatures considering new laws that might interfere with adoption?

Are there Regulations that might prohibit or minimize the ability for the solution to work?

Litigation Risk – Is there an Assumption of New Risk or Exposure through Adoption use of new products and components etc.

Data Privacy Laws and Considerations

Intellectual Property Considerations: Has someone else already designed something similar? Are there IP obstacles and risk to adoption of this solution?

Compliance Challenges – does this solution support or conflict with obligations to meet certain requirements?
Formal Oversight

Federal Government
- Congress
- Federal Enforcement Agencies
  - FERC/NERC
- National Security Agencies
  - IRS

State & Local Governments
- State Legislatures
- Public Utility Commissions
- State EPA's
- Departments of Revenue

International Governments, Treaties & Regional Organizations
European Union, Germany, China, Russia, North Korea, South American, Africa – NAFTA, OPEC, WTO, etc.

Technical and International Standards Organizations
- NIST, ASTM, IEEE, URS, ISO, ANSI, CEN, ITU, IEC, NISO, W3C, OSHA, SSDA, UL, SDA, UTSI, TIA, etc.

Judicial & Administrative and Intellectual Property Courts
- Federal Courts
- State Courts
- Subject Matter Courts
- Administrative Law Judges
Legal Considerations

• Data Privacy Regulation
• Breach Disclosure Requirements
• Indemnification for Loss
• Cyber Insurance – Does it lower premium cost
• M&A Due Diligence – what are we buying?
• Addressing Intellectual Property
• Contractual Relationships
  • Existing contractual relationships may prevent new solution adoption
• Product Liability Concerns – Is the risk increased?
General Data Protection Regulation (GDPR)

- Effective May 25, 2018; Stakeholders: Data Controllers, Processors and Subjects;

- A presence in any EU Country or Processes personal data of EU citizens & (250+ employees or < but impact the rights and freedoms of EU citizens or include certain sensitive personal data);

- New rights for people to access the information that companies hold about them + obligations for better data management for businesses & a new regime of fines;

- Companies covered by the GDPR are accountable for their handling of people's personal information. This can include having data protection policies, data protection impact assessments and having relevant documents on how data is processed;

- Seven Principles: Lawfulness, fairness & transparency, data minimization, scope limitation, accuracy, storage limitation, integrity and confidentiality and accountability (fines);

https://eugdpr.org/
California Consumer Privacy Act (CCPA)

• Effective on January 1, 2020 but note 12-month “lookback”

• The Act applies to all business (equivalent to “data controllers”) that collect or use this personal information, not just those companies in California

• Applies to “consumers,” i.e., California residents. Rough equivalent to “data subjects.” Includes employees and in some cases patients and students.

• Rights include: (1) to be informed about personal data collected by a business and rights to access and delete that information; (2) a right to prevent personal information from being sold to third parties, and (3) a right to direct third parties that already have personal data to not use it.

• The California Attorney General may bring actions for civil penalties of up to $7,500 per violation and there is a limited private right of action for individual victims of data breaches for penalties ranging between $100–750 per violation.

While the GDPR is longer, the CCPA is much more complex.

The right to prevent sale of data to third parties is a primary difference between the two and will likely wreck the business models of many companies.

Creation/update of a data inventory is the most important element of complying with both regulation.
Privacy Legislation

GDPR
EU 2016/679
General Data Protection Regulation 4.16.2016

AB375, Title 1.81.5
The California Consumer Protection Privacy Act of 2018 - CCPA

State Bills Modeled on the CCPA
- HI - S.B. 418
- MD - S.B.613/H.B. 901
- MA - S.D. 341
- NM - S.B. 176
- RI - S.B. 234

State Bills Not Modelled on CCPA
- IL - S.B. 2149/H.B.2736
- NJ - A.B.4640/S.B. 3153
- NY - S.B. 2323/A.B. 3818 & NY - S.B. 1177
- NY - S.B.224/A.B.3739
- OR – H.B. 2866
- VA – H.B. 2535
- WA - S.B. 5376/H.B. 1854
- WA - H.B. 2046

Other State Bills
- AZ - H.B. 2259
- CA - A.B. 288
- CT - H.B. 6601
- MT – H.B. 457
- NJ – S.B.2634/A.B. 3923

Intellectual Property
Challenges and Protections

Summary of Intellectual Property

**Trade Secrets**
- Best example is "secret formula for Coca-Cola."
- Most technology companies rely on trade secrets as primary means of protecting IP.
- Most fragile form of intellectual property.

**Copyrights**
- Work must be novel, but must be "original" (not copied).
- Suggestive or "distinctive" marks are stronger than "descriptive" or "generic" marks (no protection).

**Trademarks**
- Trademark generally must be distinctive of product and not the generic name for that type of product.
- Protects sayings and other forms of expression from unauthorized duplication, modification, and distribution.
- Protects expression of an idea, not the idea itself.

**Patents**
- Issued US patent gives owner right to exclude others from making, using, selling, offering to sell or importing the claimed invention in the US without a license.

**Overview**
- Government
  - Trade Secrets: Nothing
  - Copyrights: Registration (Copyright Office)
  - Trademarks: Prosecution (US PTO)
  - Patents: Prosecution (US PTO)

**Implementation Plan**
- **Objectives**
  - 1) intangible
  - 2) a “right to exclude”
  - 3) protect personal property.

**Intellectual Property vs**
- Trademark vs Copyright
- Trademark vs Copyright
- Patent vs this logo
- Trademark vs this invention/

http://www.creditlenders.info/trademark-vs-copyright/trademark-vs-copyright-patent-this-logo-trademark-this-invention/
Considerations

- Marketplace Dynamics
- Financial Decision Making
- Personnel Challenges
- Operational Context
- Policies, Standards & Regulations
Today’s Agenda

Now What?
"We TOLD you it was hard." "Yeah, but now that I'VE tried, we KNOW it's hard."

https://xkcd.com/1831/
Review & Takeaways

 Dirty But Cheap often beats Clean but Expensive – *absent outside factors forcing adoption

 How does my product impact Cybersecurity Insurance?

 People have to make your Solution work in the Field - without you – will they understand it?

 Figure out Who is going to Pay for this Product or solution and Why?

 Articulate the new value 1-4-1 replacements are < appealing as they miss the why

 History Is Very Powerful – You will likely fight change resistance & intrenchment

 It’s All About Metrics – Can I Measure it Impact?
Wow Me Please

Another Sensor?

Another Threat Intel Discovery Tool?

Another Type of Firewall?

Another Application to Manage?

With Limited Time, Money, Resources, and Many Competing Projects and Priorities for Employee Activities – Utilities Are Busy

New Solutions Need to Really Deliver Some New Value to Warranty Another Moving Part
Find New Ways to Measure the Impact of Cybersecurity Investment

Address IT/OT integration Challenges

Find New Ways to Minimize Human Risk Factors

Automating Data Anonymization

Help Insurance Companies Quantify Cyber Risk to Write better Policies

Increase Security platforms on IoT Devices

Figure out how to secure more or all of the Supply Chain

Help Utilities Communicate Risk Measures with Regulators
Planning Checklist

**Plan to Understand**
- How does this fit into the “as-is-state”?
- Determine & explain design assumptions
- Know where opposition might come from
- Know where the value comes from
- Will this product work in a legacy environment?
- Check legal and IP landscape
- Understand procurement dynamics
- Anticipate human behavior factors - pro/con
- Is there a transition period?
- Who will be selling your product?
- Will businesses and consumers pay for this solution?

**Plan to Address**
- Supply chain risk
- Interrogability issues
- Complexity of Use
- Anticipated training needs
- Long term support
- Compliance requirements
- Remote access issues
- Patches and upgrades
- Warranty issues
- Connected elements
- Interdependencies
- Ripple effect of required changes to existing tools
- On Prem Off Prem?

**Anticipating Viscosity**
- Get ahead of your challenges
- Find partners and support
- Get on the shop floor
- Learn what doesn’t work - pivot away
- Vet IP issues
- Ask tons of questions
- Listen and adjust
- Avoid biases
- Why this product – now
Read Books
Not Assigned to You

- If I Understood you, Would I Have this Look on My Face – Alan Alda
- Tipping Point – Malcom Gladwell
- The Laws of Simplicity – John Maeda
- HBRs the 10 Must Reads on Innovation – Harvard Business Review
Charles H. Duell was the Commissioner of the US patent office in 1899 when he was famously attributed to have uttered:

"everything that can be invented has been invented."
Thank You