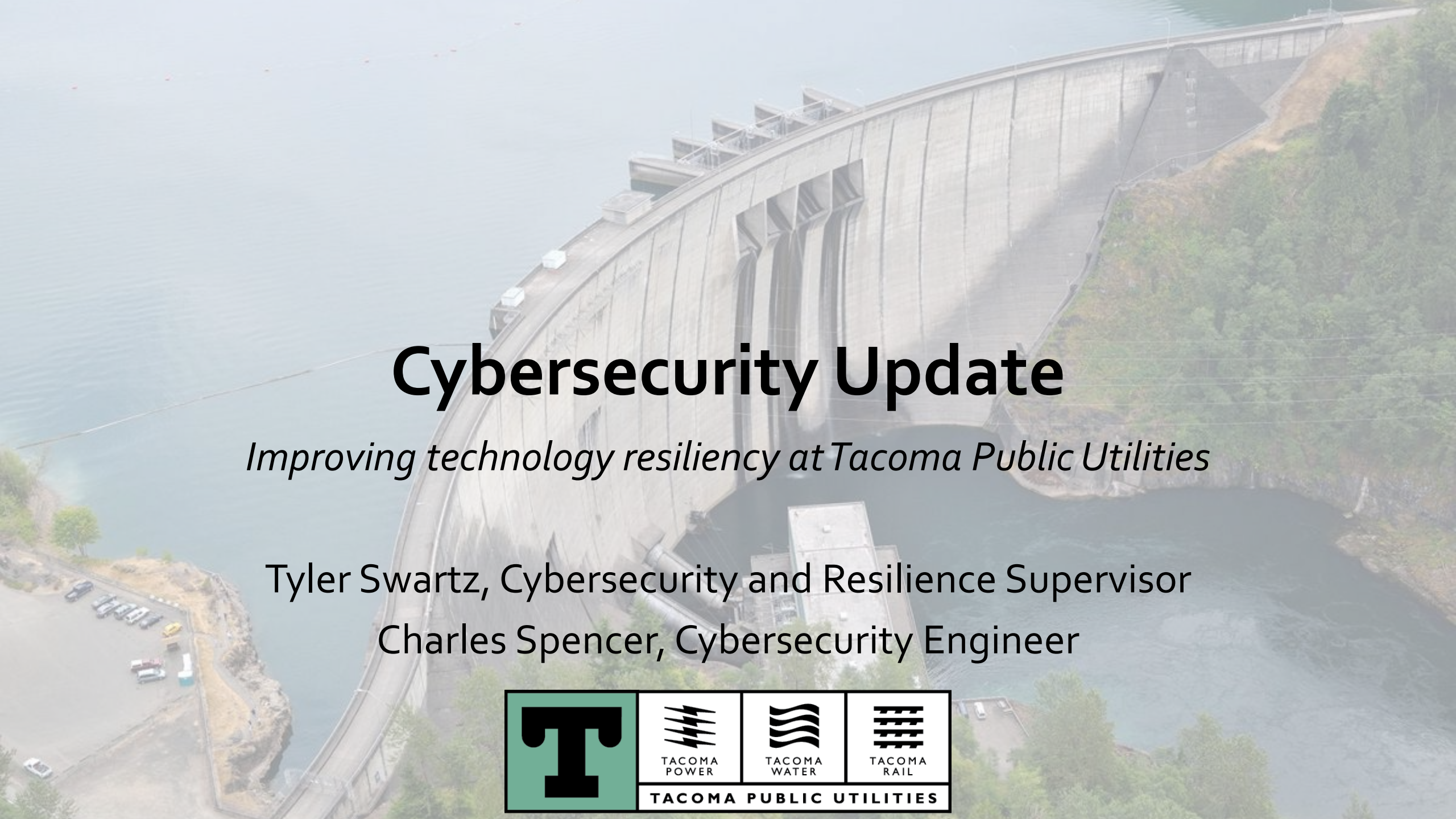


Cybersecurity Update

Improving technology resiliency at Tacoma Public Utilities

Tyler Swartz, Cybersecurity and Resilience Supervisor
Charles Spencer, Cybersecurity Engineer

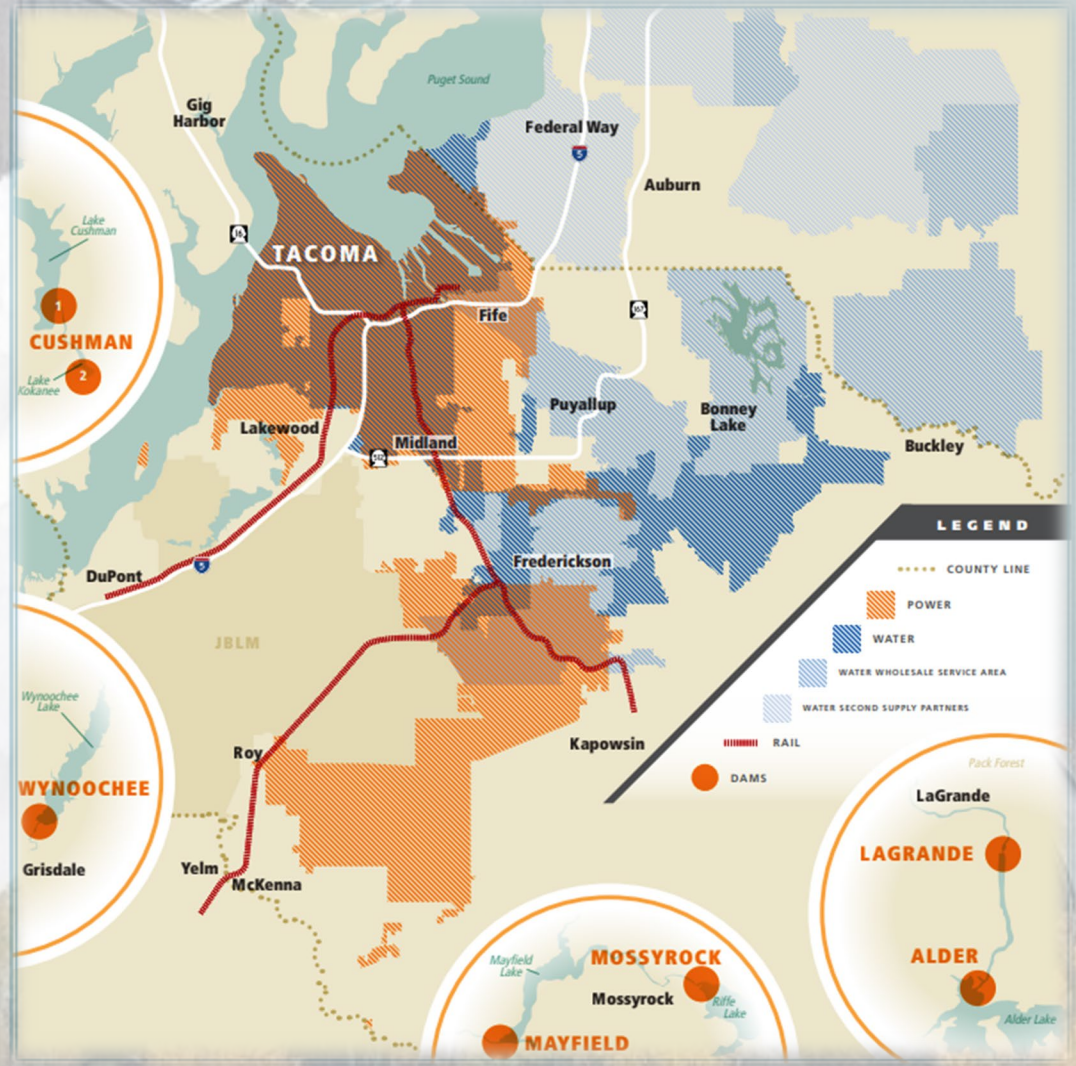
TACOMA POWER | TACOMA WATER | TACOMA RAIL
TACOMA PUBLIC UTILITIES

TACOMA POWER | TACOMA WATER | TACOMA RAIL

TACOMA PUBLIC UTILITIES

Agenda

- LPPC Maturity Assessment
- Solarwinds (Sunburst) Compromise
- Industry Engagements & Knowledge Sharing
- GridEx VI
- Key Accomplishments
- Questions



2019

LPPC Cyber Security Principle Metrics

Effectiveness of LPPC Principles

Legend

Greater than 3	Higher Risk
Greater Than 1	Moderate Risk
Less than or equal to 1.0	Lower Risk

Results

Overall Average Risk

(Risk Levels will automatically populate once LPPC Metrics Tab Tool is completed)

1.0 - Executive Management Must Champion Cyber Security Efforts	Moderate Risk
2.0 - Cyber security programs and policies need to be documented and maintained	Moderate Risk
3.0 - Enterprise, not departmental, cyber security programs are essential	Moderate Risk
4.0 - Develop and maintain a plan to respond to cyber security incidents before they hap	Moderate Risk
5.0 - Communicate Policies and Risks to Boards and Executive Management.	Higher Risk
6.0 - Develop and maintain an effective cyber security staff	Moderate Risk
7.0 - Build Public-Private partnerships for Information Sharing.	Moderate Risk
8.0 - Implement a Cyber Security Awareness, Communication and Education Strategy.	Moderate Risk
9.0 - Use external resources to periodically assess the cybersecurity program and risk.	Lower Risk
10.0 - Develop and maintain secure system design processes	Higher Risk

2020

LPPC Cyber Security Principle Metrics

Effectiveness of LPPC Principles

Legend

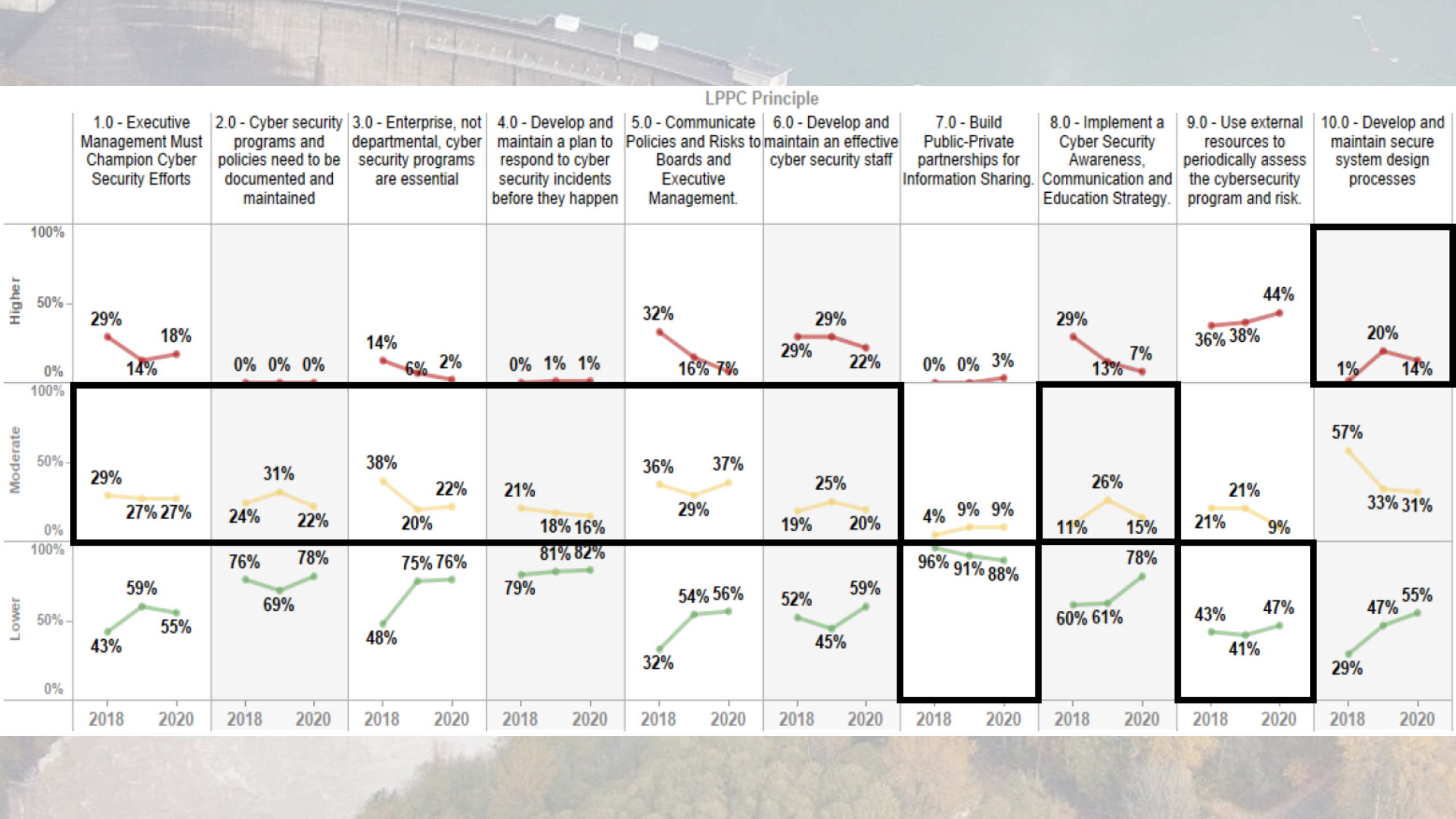
Greater than 3	Higher Risk
Greater Than 1	Moderate Risk
Less than or equal to 1.0	Lower Risk

Results

Overall Average Risk

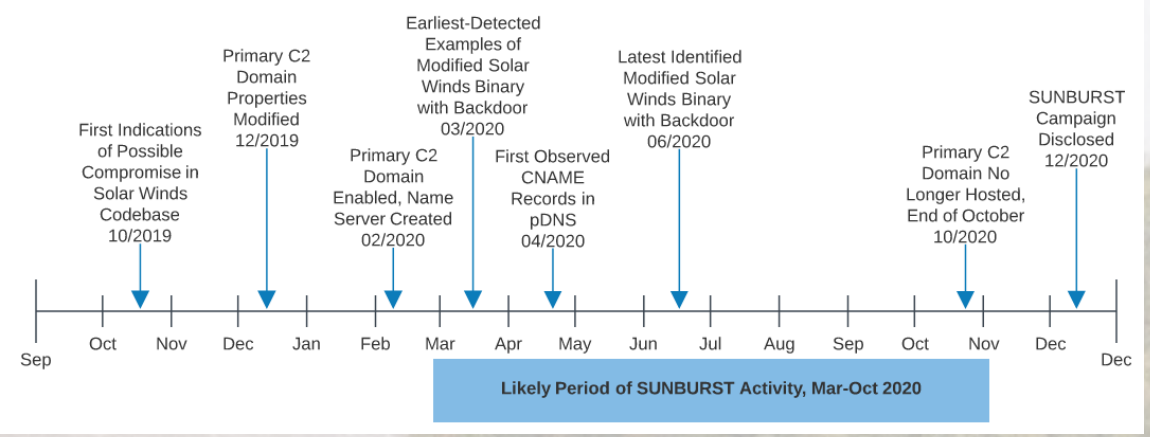
(Risk Levels will automatically populate once LPPC Metrics Tab Tool is completed)

1.0 - Executive Management Must Champion Cyber Security Efforts	Moderate Risk
2.0 - Cyber security programs and policies need to be documented and maintained	Moderate Risk
3.0 - Enterprise, not departmental, cyber security programs are essential	Moderate Risk
4.0 - Develop and maintain a plan to respond to cyber security incidents before they hap	Moderate Risk
5.0 - Communicate Policies and Risks to Boards and Executive Management.	Moderate Risk
6.0 - Develop and maintain an effective cyber security staff	Moderate Risk
7.0 - Build Public-Private partnerships for Information Sharing.	Lower Risk
8.0 - Implement a Cyber Security Awareness, Communication and Education Strategy.	Moderate Risk
9.0 - Use external resources to periodically assess the cybersecurity program and risk.	Lower Risk
10.0 - Develop and maintain secure system design processes	Higher Risk


LPPC Principle
1.0 - Executive Management Must Champion Cyber Security Efforts
2.0 - Cyber security programs and policies need to be documented and maintained
3.0 - Enterprise, not departmental, cyber security programs are essential
4.0 - Develop and maintain a plan to respond to cyber security incidents before they happen
5.0 - Communicate Policies and Risks to Boards and Executive Management.
6.0 - Develop and maintain an effective cyber security staff
7.0 - Build Public-Private partnerships for Information Sharing.
8.0 - Implement a Cyber Security Awareness, Communication and Education Strategy.
9.0 - Use external resources to periodically assess the cybersecurity program and risk.
10.0 - Develop and maintain secure system design processes
Higher
Moderate
Lower
100%
50%
0%
29% 14% 18%
0% 0% 0%
14% 6% 2%
0% 1% 1%
32% 16% 7%
29% 29% 22%
0% 0% 3%
29% 13% 7%
36% 38% 44%
1% 20% 14%
29% 27% 27%
24% 31% 22%
38% 20% 22%
21% 18% 16%
36% 29% 37%
19% 25% 20%
4% 9% 9%
11% 26% 15%
21% 21% 9%
57% 33% 31%
43% 59% 55%
76% 69% 78%
48% 75% 76%
79% 81% 82%
32% 54% 56%
52% 45% 59%
96% 91% 88%
60% 61% 78%
43% 41% 47%
29% 47% 55%
2018 2020

SolarWinds (Sunburst)

- **On 13 December 2020, DHS-CISA reported Active Exploitation of SolarWinds Orion Platform Software (Network Management Software)**
- **Supply chain attack compromise effecting Multiple Government Agencies and Public/Private Entities**
- **Identified by security company FireEye ranging back from Spring 2020 to current through Network Monitoring Software Known as SolarWinds Orion**
- **Likely APT29/Cozy Bear attributions which aligns with Russian SVR TTPs**



-262 Days from Initial Compromise to Detection

Impact

TPU Actions

- 14 December UTS Cybersecurity Declared Incident and performed full litany of incident response activities.
- 2 known affected severs in our environment but C2 establishment contained due to network segmentation.
- Affected servers archived for potential forensics, but decommissioned.
- Continue to monitor for known indicators of compromise.

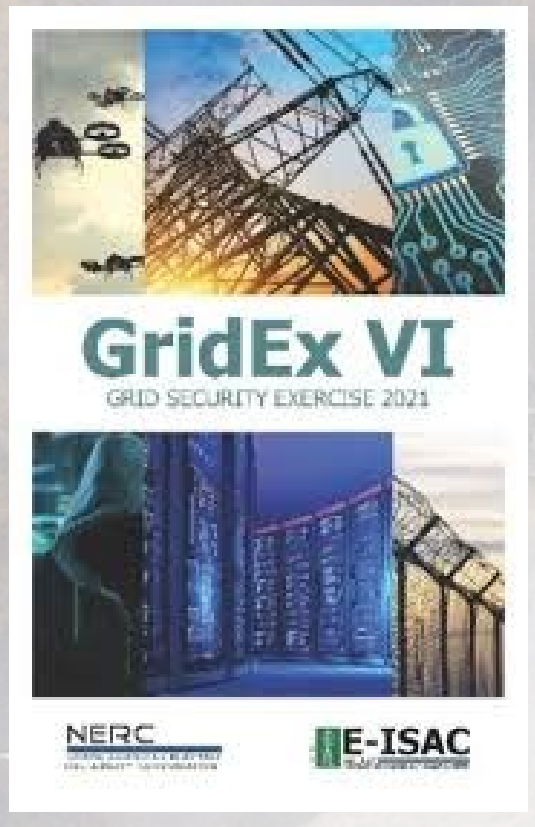
Moving Forward

- Agencies and Security Companies continue threat hunting and research. Secondary and Tertiary effects due to initial compromise
- CISA has published Emergency Directive 21-20 which sets forth required set of actions for government agencies. TPU is using it as a guide for mitigation and potential re-establishment of SolarWinds services.
- Once Risk is deemed appropriately mitigated SolarWinds Service will be fully restored and appropriate Security Guidelines via 21-20 will be implemented.
- Continue to monitor for known indicators of compromise.

CMAT Ongoing Engagements

National Guard Cyber Mission Assurance Team

Expanded Incident Response



Exercising our Partnerships sd7

Information Sharing

E-ISAC — A DIVISION OF NERC — ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER

MS-ISAC — MULTI-STATE Information Sharing & Analysis Center™

Utility Agencies

AMERICAN PUBLIC POWER ASSOCIATION

ESCC — Electricity Subsector Coordinating Council

LPPC — LARGE PUBLIC POWER COUNCIL

Public Relations & Media

komo 4 — Q13 FOX — KIRO 7

State & Local Government Emergency Management

EMERGENCY MANAGEMENT DIVISION — WASHINGTON

Tacoma

Pierce County — EMERGENCY MANAGEMENT

Law Enforcement

WASHINGTON STATE FUSION CENTER — WSFC

U.S. DEPARTMENT OF HOMELAND SECURITY

DEPARTMENT OF JUSTICE — FEDERAL BUREAU OF INVESTIGATION

TACOMA POWER | TACOMA WATER | TACOMA RAIL

TACOMA PUBLIC UTILITIES

Key Accomplishments

Integrate technology & foster innovation to deliver affordable, flexible, secure, resilient, and sustainable power & water services for our customers

Consolidated Incident Response Plan

Water SCADA Modernization

Modern Security Policy and Program

NSOC Commissioning

Endpoint Detection and Response

TPU's Cyber Security Program – Key Tenets

Effective utilization of cyber talent

Stronger customer trust

Greater reliability

Enhanced resiliency