

Cybersecurity

Is Your Utility Cyber Resilient?

Kevin Morley, PhD
American Water Works Association



American Water Works
Association

IS YOUR UTILITY CYBER RESILIENT?



Awareness



Analysis



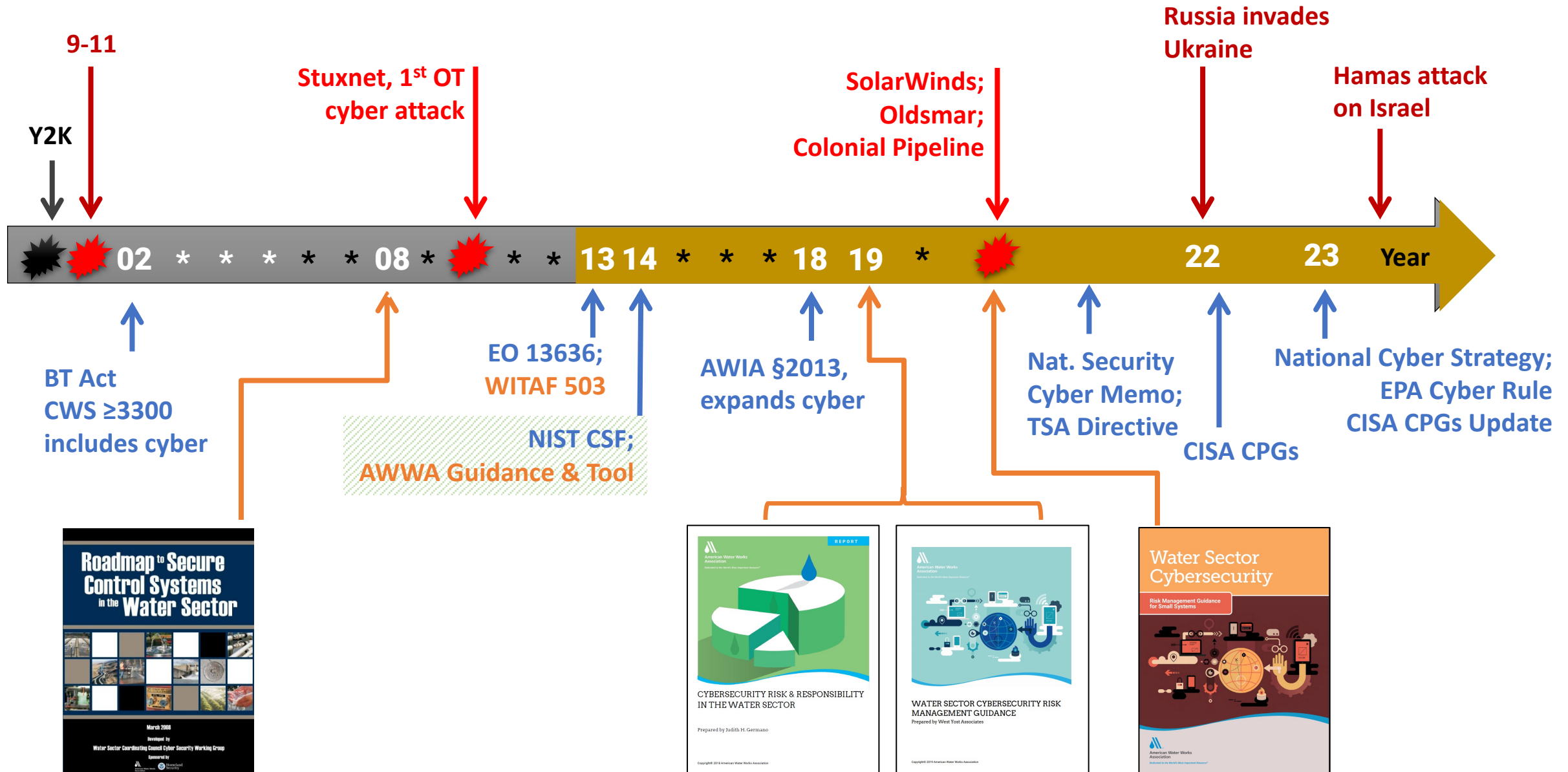
Action



Cybersecurity Reconsidered

Threat Actor	=	someone who wants to punch you in the face
Threat	=	the punch being thrown
Vulnerability	=	your inability to defend against the punch
Risk	=	the likelihood of getting punched in the face
Acceptable Risk	=	your willingness to be punched in the face

Where Have We Been? Where Are We Now?





AWARENESS

Cybersecurity Policy Matters

💧 ***EPA Sanitary Survey Cyber Rule***

- 💧 *Legal challenge filed by MO, AR, IO, joined by AWWA, NRWA*
- 💧 *Nationwide injunction July 12, 2023*
- 💧 *Rule withdrawn October 12, 2023*

💧 ***Congressional Activity***

- 💧 *Two hearings (Jan 31 and Feb 6)*
- 💧 *Legislation pending on coregulatory approach*

💧 ***AWIA §2013***

- 💧 *Round 2 begins March 2025*
- 💧 *Targeted enforcement activity anticipated*



Cybersecurity Incident Reporting

Proposed rule: Mar. 2024

Final rule: Aug. 2025

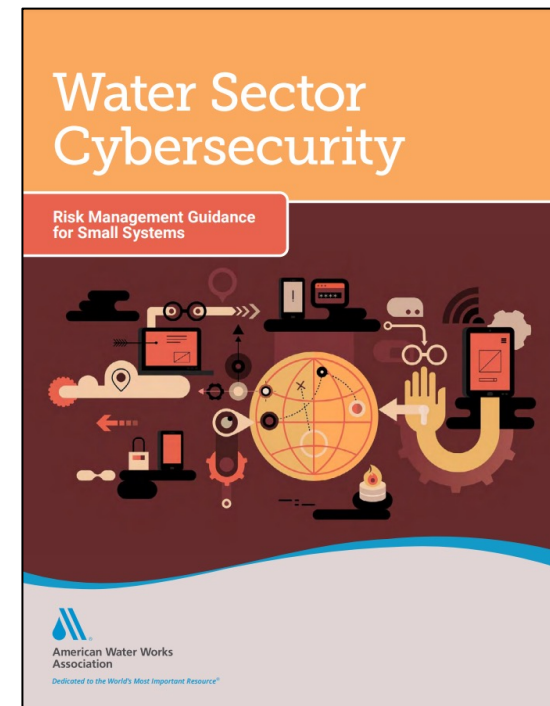
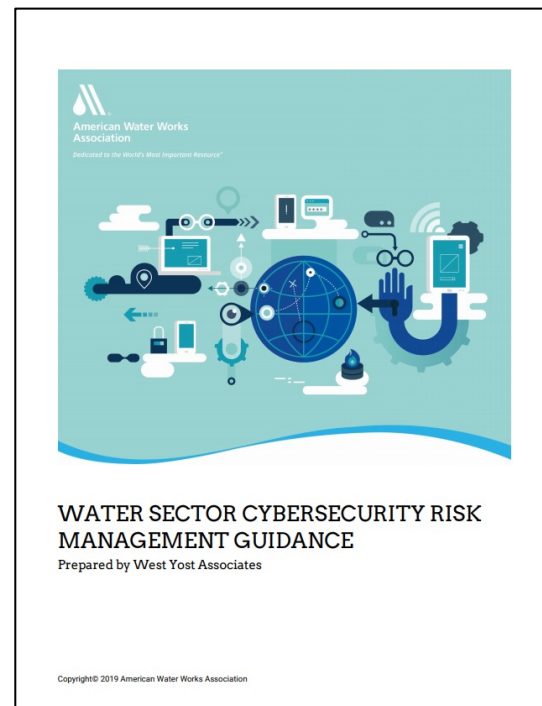




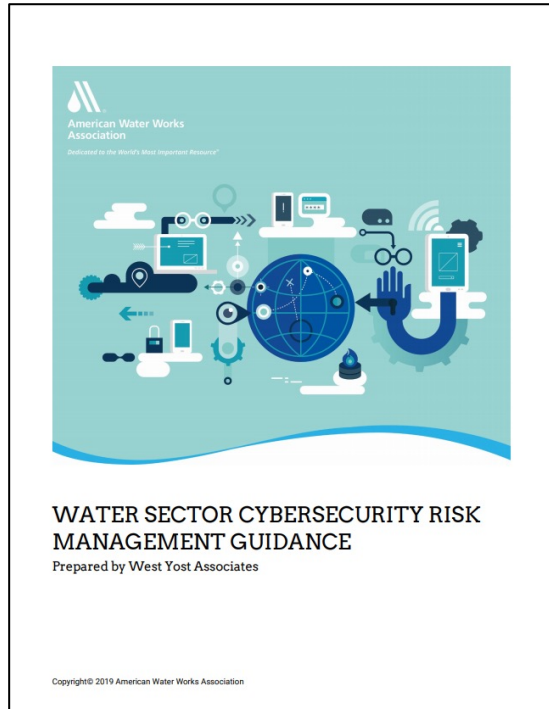
ANALYSIS

Key Steps

- 💧 ***Leadership commitment & culture***
- 💧 ***Build team to manage risk & resilience***
- 💧 ***Leverage resources for due diligence***
- 💧 ***Update Risk & Resilience Assessment***
- 💧 ***Integrate into Emergency Response Plan***
 - 💧 ***There is a clear obligation to take action to address cyber risks***



CYBERSECURITY DUE DILIGENCE



Control Status Summary:

The second table summarizes the user defined implementation status of the recommended controls from the RRA- Control Output tab. The colors provide a visual indication of the recommended controls with the associated status.

	Total Controls Not Fully Implemented	Not Planned and/or Not Implemented - Risk Accepted	Controls Planned and Not Implemented	Controls Partially Implemented	Controls Fully Implemented and Maintained
Priority 1 Controls	22	0	15	7	13
Priority 2 Controls	6	7	6	0	18
Priority 3 Controls	17	0	0	17	3
Priority 4 Controls	2	7	0	2	0

% of Recommended Controls Currently "Fully Implemented and Maintained":				36%
% Recommended Controls that are "Partially Implemented" or "Planned and not Implemented":				49%
% Recommended Controls that are "Not Planned and/or Not Implemented - Risk Accepted":				15%
Controls Missing Implementation Status:				0

Not Planned and/or Not Implemented – Risk Accepted

The controls are not currently implemented or planned for implementation. The organization accepts risks associated with the controls not being implemented.

Planned and Not Implemented

Priority 1 or Priority 2 controls that have not been implemented; however, implementation of the controls are planned.

Planned and Not Implemented/Partially Implemented –

Priority 1 or Priority 2 controls that are partially implemented by internal or external resources. Priority 3 or Priority 4 controls that are neither planned nor implemented.

Partially Implemented –

Priority 3 or Priority 4 controls that are partially implemented by internal or external resources.

Partially Implemented –

Priority 3 or Priority 4 controls that are partially implemented by internal or external resources.

Fully Implemented and Maintained –

The controls are fully implemented and actively maintained by internal or external resources.

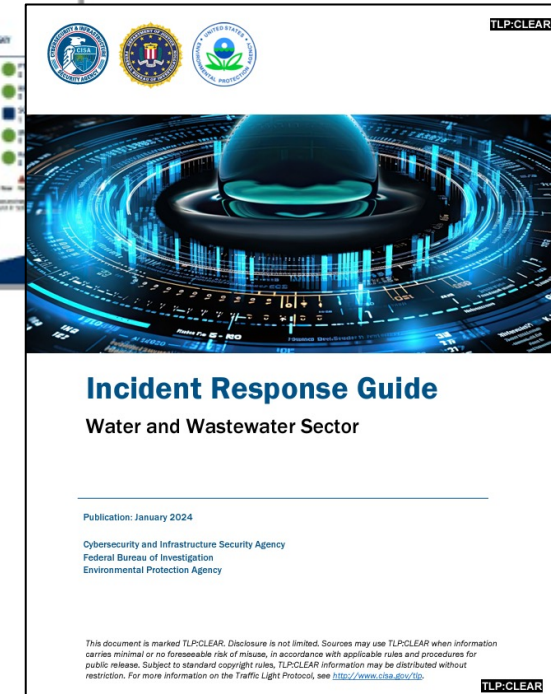
www.awwa.org/cybersecurity



Action

“No Action” is Unacceptable

- 💧 *Assess Utility Cyber Vulnerabilities ASAP*
- 💧 *Enroll in CISA’s Vulnerability Scanning Service*
 - 💧 *Email vulnerability@cisa.dhs.gov*
- 💧 *Use AWIA RRA & ERP as funding business case*
- 💧 *Develop an Incident Response Plan*



?? QUESTIONS ??

Kevin M. Morley, PhD

Manager, Federal Relations

AWWA – Government Affairs

202-326-6124 or kmorley@awwa.org

www.awwa.org/cybersecurity

www.awwa.org/risk

