

DRAGO 

pillsbury

WEBINAR

# Navigating the SEC Rules for Enhanced Cybersecurity in IT and OT Environments

Thursday, February 1st @ 2 PM ET



**Betsy Guarnieri**  
General Counsel  
Dragos



**Mark Stacey**  
Director of Strategy  
Dragos



**Brian E. Finch**  
Partner, Co-Leader,  
Cybersecurity, Data  
Protection & Privacy  
Practice  
Pillsbury



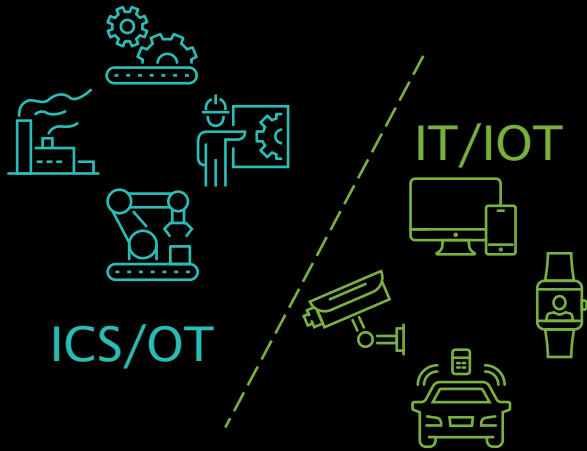
**David Oliwenstein**  
Partner  
Pillsbury

## Discussion Topics

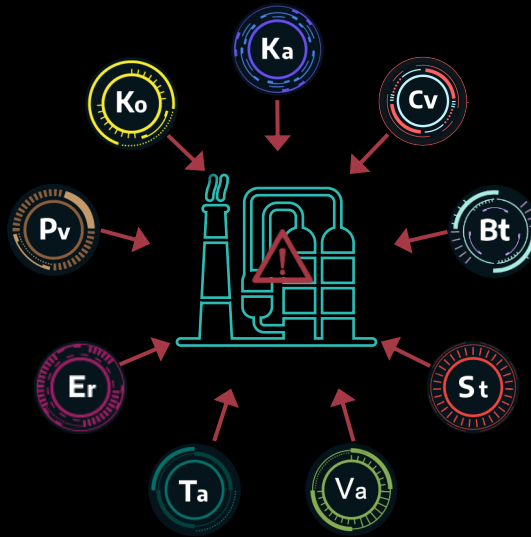
- OT Threat Evolution
- Overview of the New Cyber Disclosure Regime
- Complying with Disclosure Requirements
- Complying with Disclosure Controls and Procedures Requirements
  - Invoking the National Security and Public Safety Exception
- Concluding Remarks and Questions

# OT Threat Evolution

# ICS/OT CYBER SECURITY ISSUES



ICS/OT Systems, Networks, & Vulnerabilities are Very Different from IT/IOT



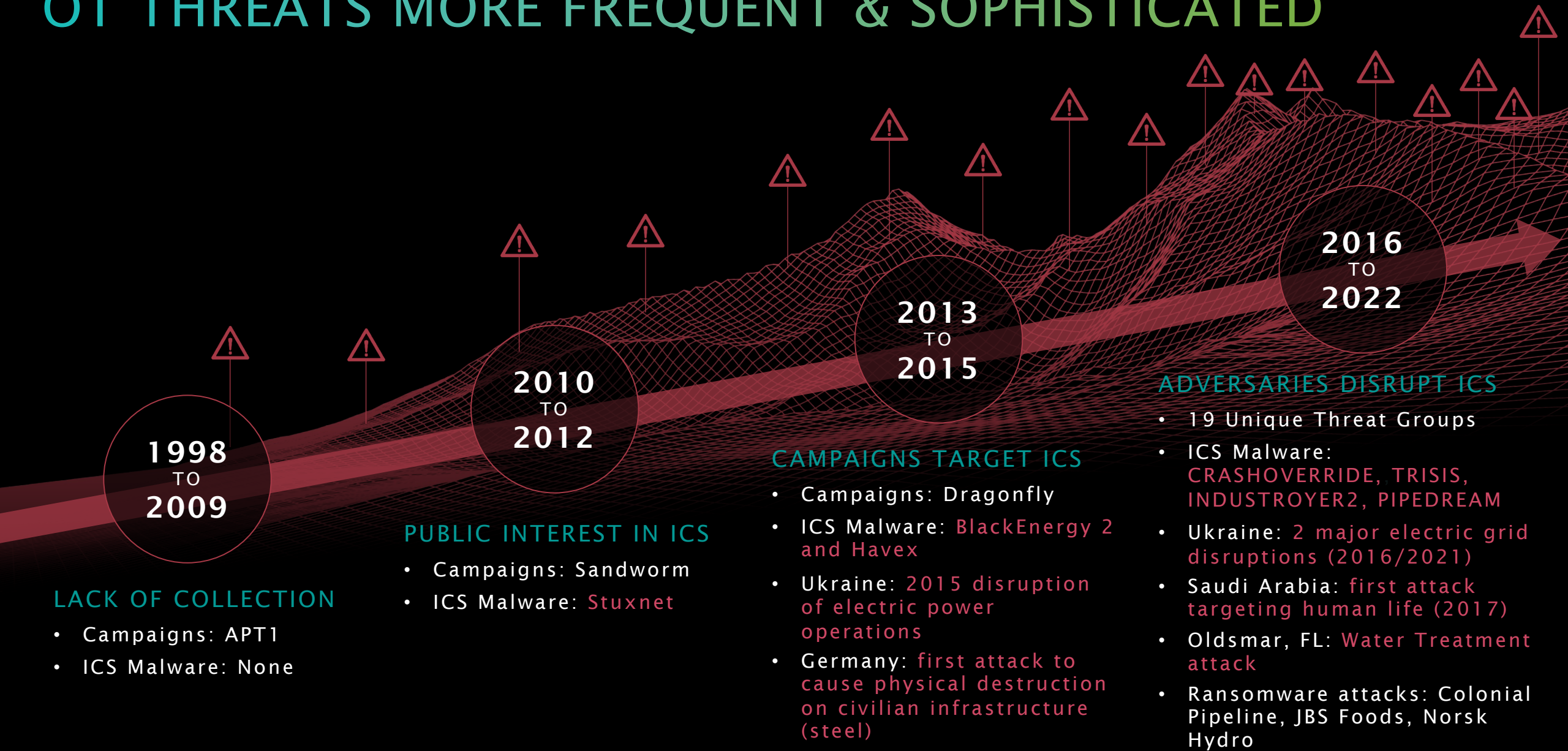
Specialized Threat Groups Target ICS/OT Systems With TTPs Specific to the Environments



There Can Be Significant Impacts to Public Safety, Environment, & Revenue

ICS/OT SECURITY INVESTMENTS SIGNIFICANTLY LAG IT SECURITY

# OT THREATS MORE FREQUENT & SOPHISTICATED



**1998  
TO  
2009**

## LACK OF COLLECTION

- Campaigns: APT1
- ICS Malware: None

**2010  
TO  
2012**

## PUBLIC INTEREST IN ICS

- Campaigns: Sandworm
- ICS Malware: Stuxnet

**2013  
TO  
2015**

## CAMPAIGNS TARGET ICS

- Campaigns: Dragonfly
- ICS Malware: BlackEnergy 2 and Havex
- Ukraine: 2015 disruption of electric power operations
- Germany: first attack to cause physical destruction on civilian infrastructure (steel)

**2016  
TO  
2022**

## ADVERSARIES DISRUPT ICS

- 19 Unique Threat Groups
- ICS Malware: CRASHOVERRIDE, TRISIS, INDUSTROYER2, PIPEDREAM
- Ukraine: 2 major electric grid disruptions (2016/2021)
- Saudi Arabia: first attack targeting human life (2017)
- Oldsmar, FL: Water Treatment attack
- Ransomware attacks: Colonial Pipeline, JBS Foods, Norsk Hydro

# Overview of the New Cyber Disclosure Regime

# Material Cybersecurity Incidents

**In Brief:** Disclose any cybersecurity incident that you conclude is material

**What:**

- Material aspects of nature, scope, and timing
- Impact, or reasonably likely impact, on the company, including financial condition and operations

**When:** Within four business days of materiality determination, unless Attorney General invokes national security or public safety exemption

- Up to 120 days
- Further extensions only granted by order of the Commission

**Also Note:** If certain information is not available at time of filing, companies must note that and file an amendment

# Materiality Assessment Applies to Related Occurrences

**In Brief**: Disclose “a series of *related* unauthorized occurrences” if they are material in the aggregate

- Triggered “even if the material impact or reasonably likely material impact could be parceled among the multiple intrusions to render each by itself immaterial”

**When**: Subject to the same four-day 8-K window

**Also Note**: Replaces the SEC’s original proposal that would have broadly required disclosure (in 10-K and/or 10-Q) when any series of individually immaterial incidents becomes material in the aggregate

**Also Note**: Final rule includes accidental occurrences in definition of “unauthorized occurrences”



# Risk Management and Strategy

**In Brief**: Disclose risk management and strategy to address cybersecurity and material cyber risks

**What**:

- Processes (if any) to assess, identify, and manage material cybersecurity risks, including (non-exhaustive):
  - Integration into overall risk management
  - Use of third parties
  - Processes to address third-party risk
- Describe whether any risks have (or are reasonably likely to have) materially affected strategy, operations, or financial condition

**When**: Annual report on Form 10-K

# Corporate Governance

**In Brief**: Disclose information about the board and management's oversight

**What**:

- The board's oversight of cyber risk, responsible board committees, and processes to elevate cyber risks to the board
- Management's role in assessing and managing risk, including:
  - Which management positions are responsible and relevant expertise
  - Processes to elevate risk to management
  - Whether management elevates cyber risk to the board

**When**: Annual report on Form 10-K







# SEC's Cyber Enforcement Toolkit

**Key Question:**  
**Where Does the New Rule Leave the Division of Enforcement?**

Public Companies
Anti-fraud provisions
Disclosure violations
Disclosure controls and procedures
Internal accounting controls
Insider trading
Regulation FD

# Where Cyber Disclosures Fit in the OT Incident Response Process

# INCIDENT RESPONSE PROCESS IN OT

 <b>PREPARATION</b>	INCIDENT RESPONSE TEAM
 <b>IDENTIFICATION</b>	INCIDENT RESPONSE TEAM
 <b>CONTAINMENT</b>	OT OPERATORS
 <b>ERADICATION</b>	OT OPERATORS
 <b>RECOVERY</b>	OT OPERATORS
 <b>LESSONS LEARNED</b>	JOINT ACTIVITY

You will need to have established, documented, and practiced incident response protocols

Your board or leadership will need to communicate with IR teams to evaluate materiality

Materiality can come into play at any stage of this process

# Complying with Disclosure Requirements, Controls, and Procedures

# Assessing Materiality – General Principles

- Apply traditional principles of materiality
  - *Basic Inc. v. Levinson*, 485 U.S. 224 (1988): Substantial likelihood that a reasonable shareholder would consider information important *or* significantly alters the “total mix” of information
  - **Doubts should be resolved in favor of disclosure**
- Consider longstanding materiality guidance
  - Staff Accounting Bulletin No. 99
  - Evolving case law
  - Quantitative and qualitative factors

# Assessing Materiality of Cyber Incidents

## Materiality Analysis Must Consider

- 1) Incident Specific Factors
- &
- 2) Company Specific Factors

***Analysis Must Not Be Overly Formulaic or “One-Size-Fits-All”***



# “Red Flags” of a *Potential* Material Incident



- Attack involves a high volume of data
- Attack involves important data
- High probability of future event(s)
- Attacks from persistent threat actor
- Significant system downtime
- Attack that may impact a company’s financial position
- Incidents that may impact a company’s relationship with suppliers or customers
- Risk to intellectual property
- Reputational harm

# Materiality – Additional Important Factors

- Materiality doesn't just mean “financial condition or results of operations”
- Qualitative factors should also be considered, including:
  - Reputational harm
  - Customer or vendor relationships
  - Harm to competitiveness
- No exemption for incidents on third-party systems
- Possibility of litigation, regulatory investigations or actions, including state regulatory action, should be considered
- SEC: actions by “non-U.S. authorities” may be considered material

# The Role of Security Experts

## **Key Question:** **What Is the Role of Security Experts in Materiality Assessments?**

- Must involve security team in materiality assessments, but ultimate responsibility rests with those with authority over disclosures
- CISO can help other executives understand:
  - Incident severity
  - The nature of any ongoing threat
  - Remediation
- SEC: “Predominant view is that materiality judgments can only be properly made by those who have all the facts” (Staff Accounting Bulletin 99)
- Disclosure decision should leverage all available expertise

# The Role of Policies and Procedures

**\*\* Consider a standalone policy for cyber-related materiality and disclosure determinations \*\***

## Policy Considerations

- Must be specific to your business and risk profile
- Should not be overly formulaic
- Should consider any “unknowns” that linger after incident response investigation
- Who is making the final decision (i.e., board or management)?

**SEC recognizes that many materiality determinations require management judgment**

# Overview of Disclosure Controls and Procedures

“[C]ontrols and other procedures of an issuer that are designed to ensure that information required to be disclosed by the issuer in the reports that it files or submits under the [Exchange] Act . . . is recorded, processed, summarized and reported, within the time periods specified in the Commission’s rules and forms.”

(Exchange Act Rule 13a-15(e))

**In the event of an incident, SEC will assess whether, how, and when information flowed up the corporate ladder**

# Overview of Disclosure Controls and Procedures (*Cont.*)

Every cyber issuer enforcement action to date has had a DC&P component:

- *SEC v. SolarWinds* (Oct. 2023)
- *In the Matter of Blackbaud, Inc.* (Mar. 2023)
- *In the Matter of Pearson plc* (Aug. 2021)
- *In the Matter of First American Financial Corp.* (June 2021)
- *Altaba Inc., f/d/b/a Yahoo! Inc.* (April 2018)

**Public companies should assess any gaps in incident response or policies and procedures that may hinder assessment of materiality**

# The Timing Requirements Imposed By New Rule

## Materiality Determination

*“Without unreasonable delay”*

SEC will consider:

- How quickly were internal decisionmakers convened
- Compliance with internal policies
- Pace of internal investigation
- Resources invested
- The nature of the incident

## Incident Disclosure

*Four business days from materiality determination*



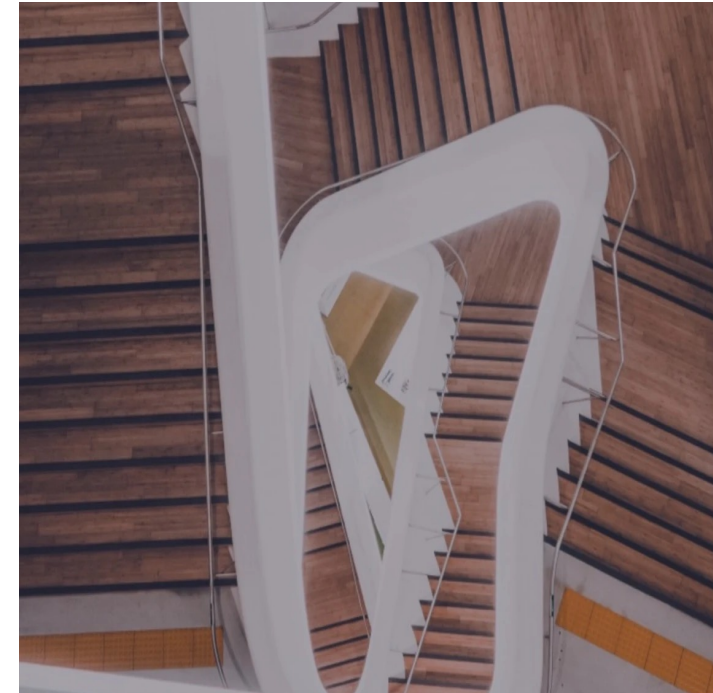
# Identifying and Tracking Cyber Incidents

- Prerequisite to disclosure is to monitor and track cyber incidents
- Develop internal infrastructure
- Companies will need to monitor and assess *immaterial* cyber breaches
  - Assess cumulative impact of all related incidents
  - Policies should address often companies update, assess, and retain information regarding immaterial incidents
- Companies must balance recordkeeping obligations with practical considerations
- Controls must cover third-party risk



# Elevating Cyber Incidents

- Policies, procedures, and training must address escalation of cyber incidents up the corporate ladder – who, how, when
- Disclosure Committee Considerations
- Inform Auditors and External Counsel
- Do not downplay the seriousness of an event - beware of “may” disclosures, consider duty to update
- Review existing disclosures for accuracy
- Disclosure obligations can arise even absent a breach



# Invoking the National Security and Public Safety Exception

# Overview of the Exception

- Final rule includes a delay provision where disclosure poses a substantial risk to national security or public safety
- Requires approval from the Attorney General
- Length of delay
  - Two successive 30-day periods
  - An additional 60 days in “extraordinary circumstances” (national security concerns only—public safety insufficient)
  - Further extensions by Commission order only
- SEC working with Justice (FBI) and other agencies when considering an exception

# Invoking the Exception

- Justice and SEC have made it very clear: **EXCEPTIONS RARELY GRANTED**
- SEC has developed an interagency communication process with DOJ
  - DOJ will notify the company about communications with SEC
- Key takeaways from Justice Dept. guidance when extensions might be considered if the filing:
  - Would undermine remediation efforts for critical infrastructure.
  - The attack method used a tactic/technique for which this no widely known fix.
  - Attack hit sensitive government information and disclosing that would cause wider national security harm.
- Justice says there IS **NO** presumption of approval or denial, but denial should be the expectation.
- SO – don't expect an exception/delay and PREPARE NOW to file an 8-K

# Policy Considerations

- Companies for which incidents are likely to have national security or public safety implications should consider developing policies and procedures
- Policies and Procedures should address:
  - Determining whether disclosure presents national security or public safety concerns
  - Individuals responsible for seeking delay
  - Communication procedures with DOJ (e.g., whether to involve other law enforcement officials)

# In Practice: Collaboration Across the Enterprise

# Case Study: IT Incident in Manufacturing




IT incident with operational impacts

Resulted in significant business challenges

Materiality evolved in real time

# 5 CRITICAL CONTROLS FOR WORLD-CLASS OT CYBERSECURITY



ICS Incident Response Plan

1



Defensible Architecture

2



ICS Network Visibility & Monitoring

3



Secure Remote Access

4



Risk-Based Vulnerability Management

5



Submit Your Questions!

THANK YOU

To reserve your copy of the  
2023 Year In Review Report, visit:

[dragos.com/year-in-review-preregister](https://dragos.com/year-in-review-preregister)

