

2021 State of Industrial Cybersecurity

December 8, 2021 | Moderated by Sam Wilson | Dragos





Shon Gerber Chief Information Security Officer, INVISTA **Doug Short** Chief Information Officer, Trinity River Authority of Texas



Steve Applegate Chief Information Security Officer, Dragos **Paul Reyes** Chief Information Security Officer, Vistra

Before we get started...

- Webinar is being recorded
- Recording will be shared this week
- Phones are muted
- Please submit questions using Q&A below



Study Background

• Sponsored by Dragos, conducted by Ponemon Institute

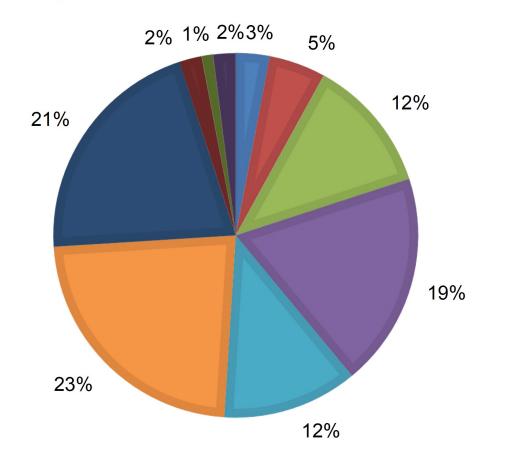


- 603 IT and OT security practitioners from managerial to C-level in the United States
- All familiar with cybersecurity initiatives and ICS/OT security practices within their organizations



Survey Demographics

Figure 16. Current position within the organization

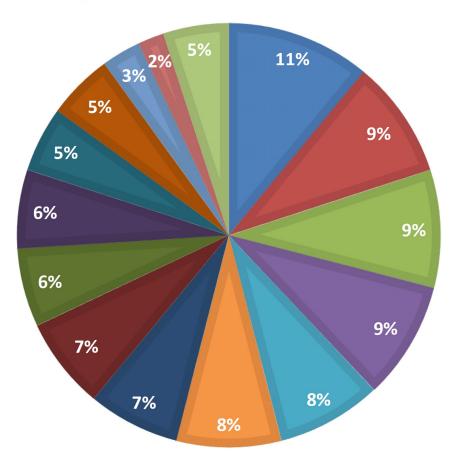


- Senior Executive
- Vice President
- Director
- Manager
- Supervisor
- Engineer
- Technician
- Staff/Analyst
- Consultant
- Contractor



Survey Demographics

Figure 17. Primary industry focus

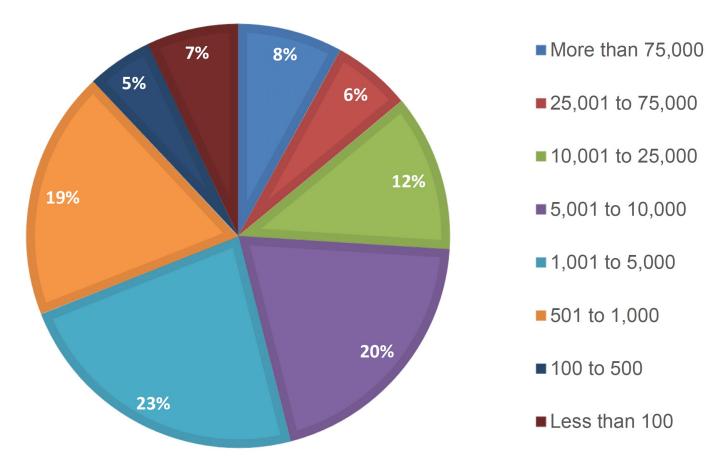


Technology & Software Industrial & Manufacturing Electric Power & Equipment Transportation & Logistics Data Centers Engineering & Construction Consumer Products Heavy Machinery Chemicals ■ Oil & Gas Metals & Mining Pharmaceutical Food & Beverage Water Other



Survey Demographics

Figure 18. Global full-time headcount





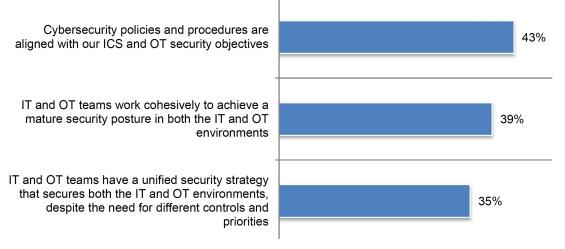
AUDIENCE POLL: OT MATURITY

IT and OT Alignment

Key Findings

- 50% of respondents are optimistic about the future of their ICS/OT cybersecurity program
- However, only 21% say their ICS/OT program activities have achieved full maturity and emerging threats drive priority actions

Figure 1. Perceptions about IT and OT alignment Strongly agree and Agree responses combined





Key Findings

- **Cultural** and **technical** differences between IT and OT cause conflicts between the two functions, e.g.:
 - patch management (50%),
 - unique requirements of ICS vendors (44%)
- Organizations effective in discovering and maintaining an inventory of all devices attached on the OT network: 45%
- Organizations effective in gathering intelligence about threats to the ICS/OT environment: 46%



Key Findings

- Respondent organizations who had an ICS/OT cybersecurity incident in the past two years: 63%
- Average cost per cybersecurity incident: \$2,989,550
- By far the VP of Engineering is most accountable for the security of the ICS/OT program (25%), vs CISOs (12%)
- Those reporting a lack of clear "ownership" on industrial cyber risk: 43%



Our guest panelists





Shon Gerber Chief Information Security Officer, INVISTA **Paul Reyes** Chief Information Security Officer, Vistra



Doug Short Chief Information Officer, Trinity River Authority of Texas



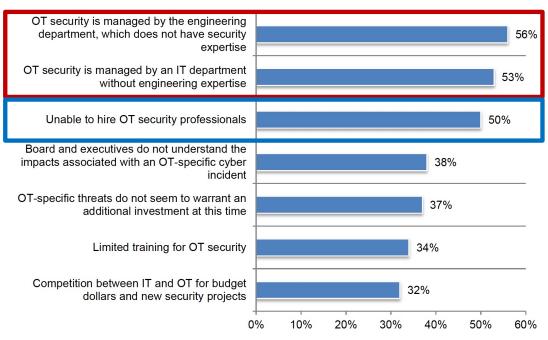
Steve Applegate Chief Information Security Officer, Dragos



ICS/OT Investment Blockers

- Do Engineering/Operations departments have cyber expertise?
- Does IT have enough understanding of operations?
- Are both departments working together?

Figure 13. What are the primary blockers for investing in ICS and OT cybersecurity? Three responses permitted





The Talent Crunch

- Finding, attracting and retaining ICS/OT cyber talent
- Training existing personnel to expand or move into cybersecurity responsibilities

Figure 14. What are your organization's top three investment priorities for ICS and OT cybersecurity in 2021? More than one response permitted

OT/ICS specific gap, risk, or vulnerability assessment to understand any weaknesses in 60% our security posture Threat intelligence specific to our industrial 56% sector, ICS and OT devices, and geography Hiring experts in OT and ICS cybersecurity 49% Strong network segmentation between corporate 47% IT and OT environments Vulnerability management solutions for ICS and 44% OT devices Asset management solutions for ICS and OT 41% devices Training for OT and ICS cybersecurity skills 40% OT-specific network detection sensors/platforms 38% 32% MSSPs with ICS cybersecurity experience System hardening for OT devices, where 29% possible Physical security controls to augment 24% cvbersecurity Passive safety controls and/or separating safety 23% systems from the OT network No investment priorities in 2021 15% 20% 30% 40% 50% 60% 70%

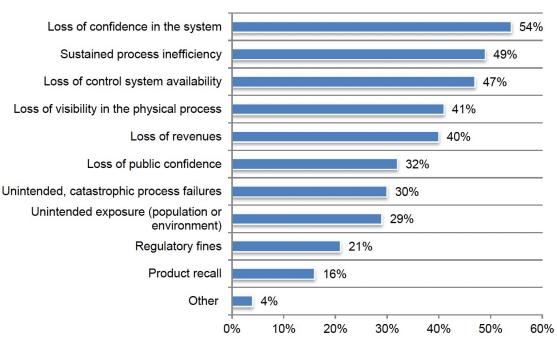


DRAGOS

Cyber Incidents and Ransomware

- 63% respondents whose organizations had an ICS/OT cyber incident in the past 2 yrs
- 29% say their organization experienced a ransomware attack in the past two years
- 51% of these say their organizations paid an average ransom of more than \$500k

Figure 16. What were the consequences of the cybersecurity incident? More than one response permitted



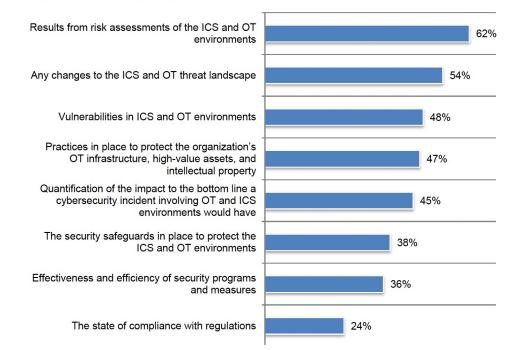
How much does the Board know?

- 25% of organizations do not report ICS/OT initiatives to their Board
- Of the 75% that do, popular topics include:
 - Risk assessment results
 - Changes in threat landscape
 - IT/OT vulnerabilities

Only IT initiatives reported IT and OT initiatives are not reported to the Board IT and OT initiatives reported together Only OT initiatives reported 0% 5% 10% 15% 20% 25% 30% 35%

Figure 5. How are IT and OT cybersecurity initiatives reported to the board of directors?

Figure 6. What topics are covered during the board meetings? More than one response permitted





Conclusions and Recommendations

- Create cross-functional teams of IT and OT SMEs to bridge the cultural divide
- 2. Regular board meetings to discuss security safeguards, and bottom line impact
- 3. Ensure enough budget and personnel to improve visibility and detection of threats and vulnerabilities across all environments
- 4. Map out threat-driven and consequence-driven scenarios most likely to impact high-priority assets.
- 5. Leverage partners and 3rd parties to bridge internal gaps (e.g. with rapid incident response retainer) and tie it to the business problem.



dragos.com/contact/

dragos.com/careers

