Developing a Strategic ICS/OT Cybersecurity Roadmap Using Intelligence and Consequence Driven Analysis

As Easy as A, B, C

Robert M. Lee,
CEO & Founder,
Dragos

Ramsey Hajj,
ICS Leader
Deloitte & Touche LLP

May 20, 2020

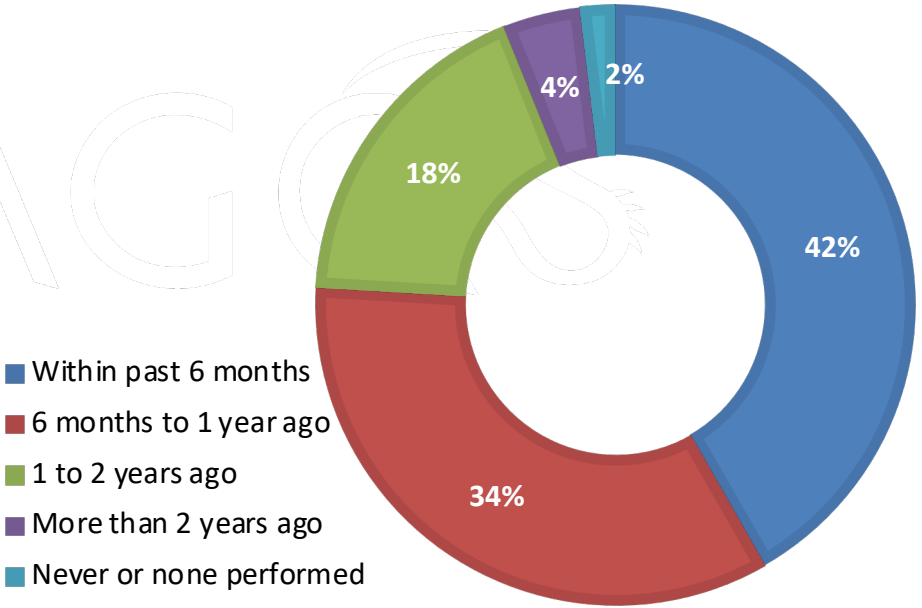
DRAGOS

Securing OT – MAPI survey results

Ensure leaders within the company aware of the existing OT security program and risks

Are you aware of your organization's OT (operational technology) security program?

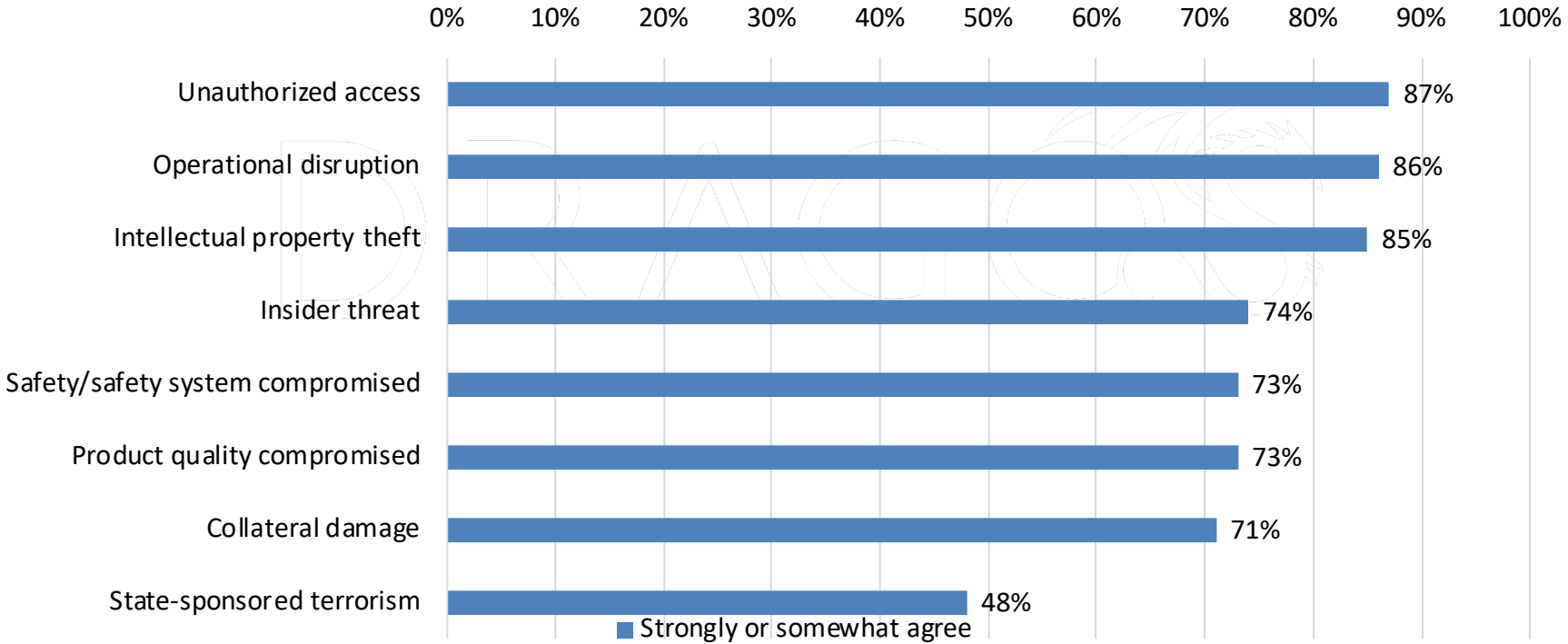
Only 4 in 10 companies performed cyber risk assessments in the last six months



…and these numbers may be significantly overstated when considering OT risk…

Respondents indicated unauthorized access and disruption among the major concerns

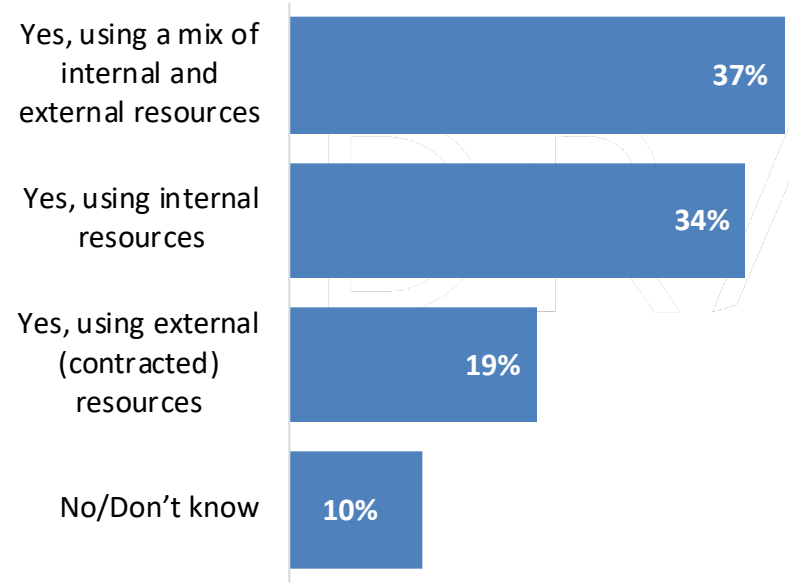
Cyber risks in OT environments



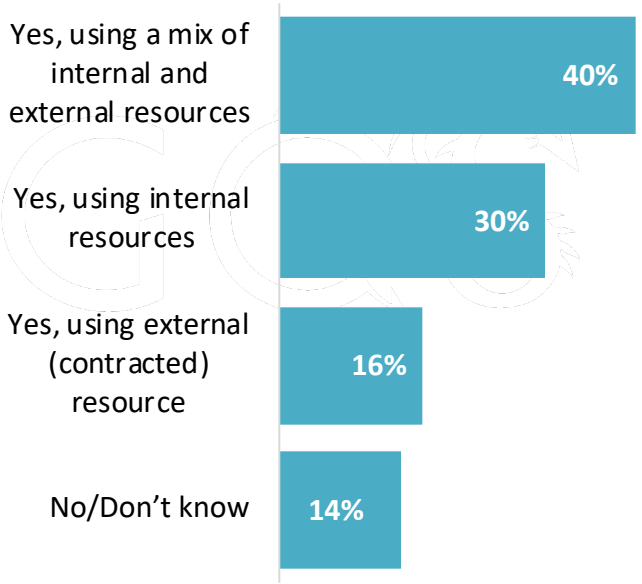
Ability to detect/respond to events in OT environments continue to lag enterprise networks

Cyber event detection and response

*Capabilities to **detect** cyber events*



*Capabilities to **respond** to cyber events*



Source: 2019 Deloitte and MAPI Smart Factory Study

Top 6 initiatives to secure OT environments

During our previous discussion, the following categories were shard as having the highest returns to an organization's OT cyber risk profile. Let's consider the application of smart factory initiatives and the importance of enhancing capabilities

1. Alignment between business, OT, and IT
2. Improved OT visibility
3. Extended network segmentation
4. Improved management of powerful IDs and vendors
5. Integrated IT and OT security and threat management programs and platforms
6. Enhanced response and recovery capabilities

Source: 2019 Deloitte and MAPI Smart Factory Study

THE PROBLEM

Cybersecurity requires a solution that encompasses People, Process, and Technology

Sometimes these efforts can be done in parallel, sometimes they cannot be

The requirements you have at your industrial organization are driven by the business goals, the threat landscape, and consequences you wish to avoid regardless; this means your journey is going to be at least somewhat different from others even in the same industry

The reality is having a single over arching roadmap (IT and OT) would be a nice goal but OT must be treated differently (different challenges, mission, threats, etc.)

DRAGOS

Common Mistakes

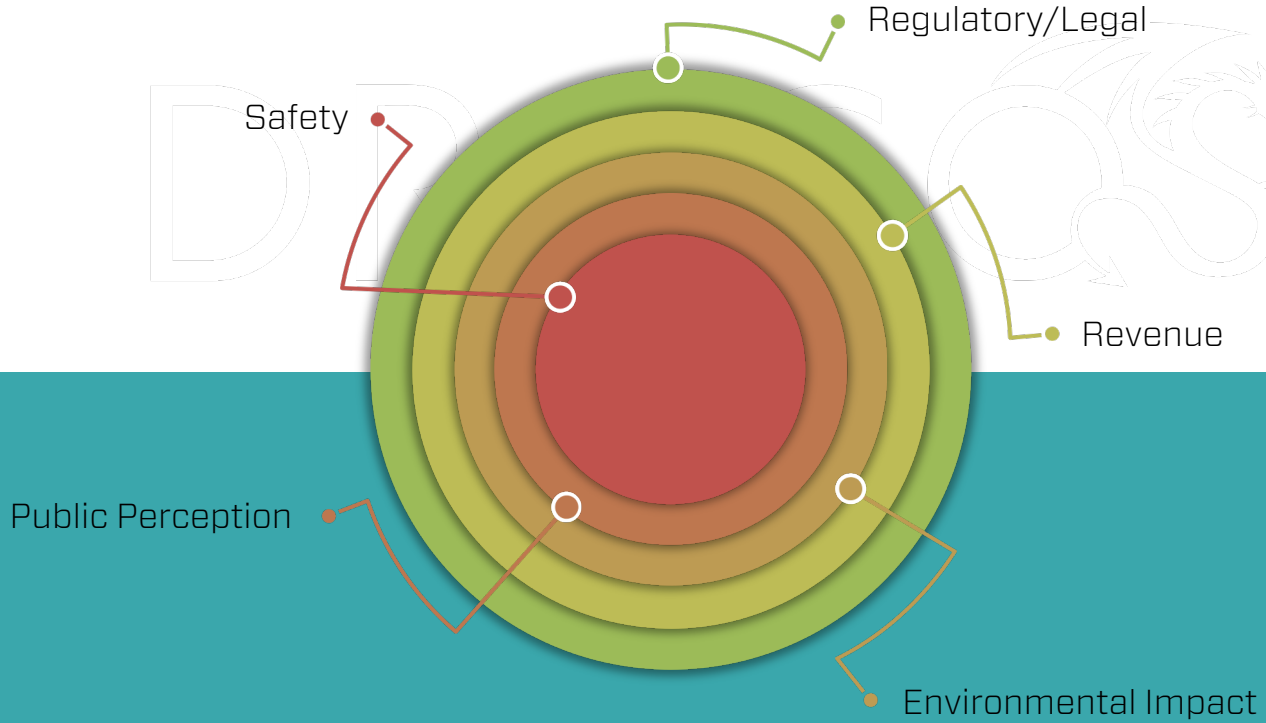
1. The org builds a single IT/OT cybersecurity roadmap or has “OT Security” as a single item in your Enterprise security roadmap
2. The org treats your organization as a single type of infrastructure (rolling out a solution at a Transmission Substation is different than a Generation facility is different than a Pipeline from a Refinery)
3. The org has vague criteria and surveys that drives metrics instead of easily understandable goals for the entire team to process and work towards
4. The security roadmap is generated from standards/regulations instead of mapped to it after the fact once the requirements are understood
5. The efforts in the security roadmap are executed one after another or parallel where it is in year 2, 3, 4, or 5 before your most critical facilities have all the required security controls (i.e. peanut butter spread)

Six Steps to ICS Security Roadmap

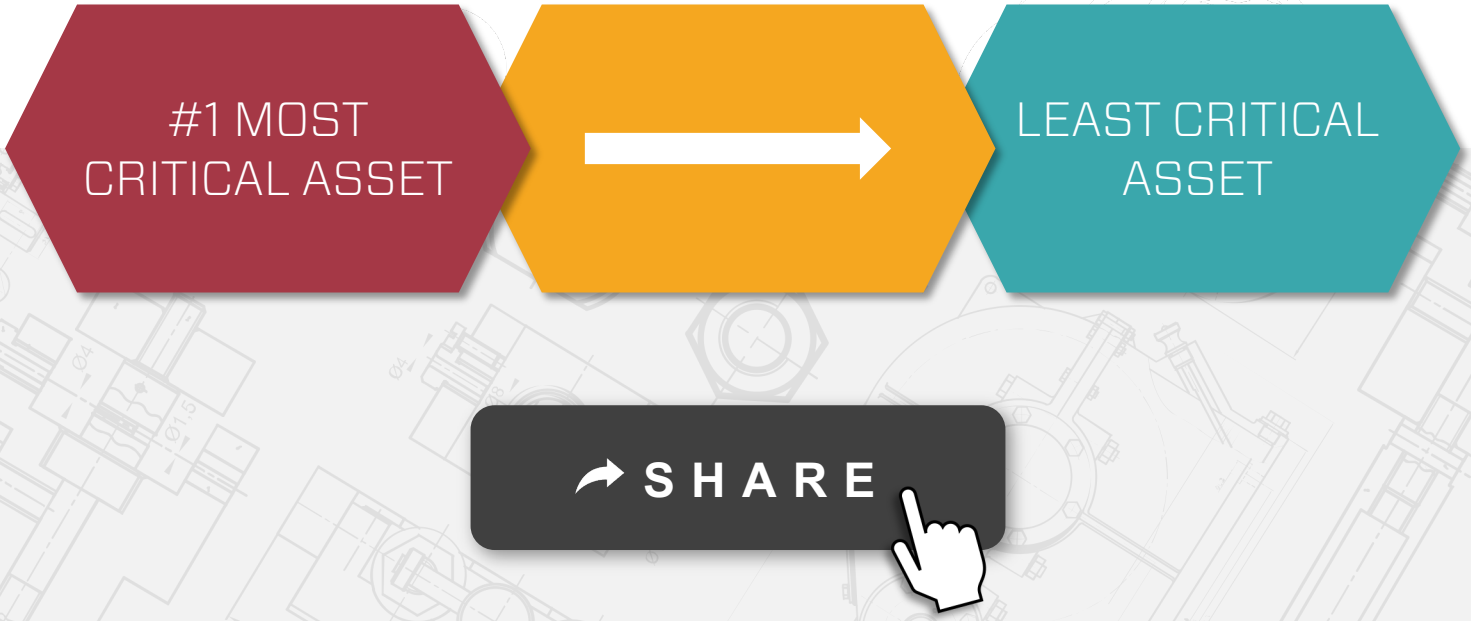
1. Determine your business priorities
2. Prioritize your assets
3. Determine your threat and consequence driven scenarios
4. Determine your controls
5. Determine your A – B – C class assets
6. Execute and measure

DRAGOS

STEP 1: Determine Your Organizational Priorities

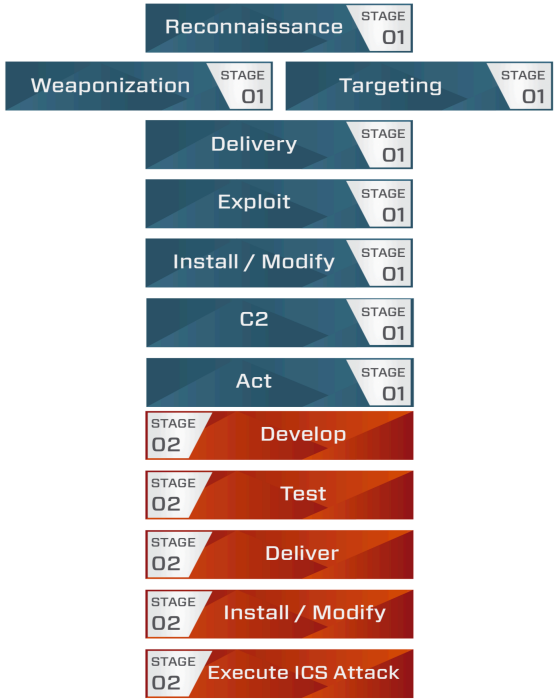


STEP 2: Prioritize Your Assets



STEP 3: Determine Your Threat and Consequence-Driven Scenario

- **Don't protect against every exploit, vulnerability, malware, etc.**
- **Think about threat scenarios.**
- **Prioritize the threat scenarios, then pick consequence scenarios.**
- **Use models such as the ICS Cyber Kill Chain to think of each step in the scenario.**



DRAGOS

STEP 4: Determine Your Controls

ARCHITECTURE → PASSIVE DEFENCE → ACTIVE DEFENCE

- For every observable step, note what would have been most effective
- Each will have people, process, and technology implications
- Think of these as: Preventive, Detection, and Responsive Controls
- Map these to your framework/regulation of choice afterwards

DRAGOS

STEP 5: Determine Your A – B – C Class Assets

1. **Take your ranked list, your security controls list for the end-to-end scenarios you developed and validate that you could roll these out at your top 10% of your Assets**
2. **If your work is validated, break your ranked list into an A, B, and C list**
3. **A class assets will have full coverage on your 3-5 scenarios**
4. **B class assets will have full coverage on your 1-2 top scenarios or partial coverage**
5. **C class assets will have at least a couple of the most important controls**

   E.g. Incident Response plan and Segmentation

How many assets are in A, B, or C classes will depend on how many assets you have, what budget and resources you have, and how much time you need. Generally A class is 10-15% of the environment, B class are 16-50%, and C class is all else

DRAGOS

STEP 6: Execute and Measure

- **Roll out the efforts to your A class assets, whatever you learn adapt early on (instead of Year 5 in a 5-year roadmap realizing your controls don't work together)**
- **You should measure (KPIs) your coverage against scenarios across A/B/C class**
- **You should measure how many C class assets you move into B class assets and how many B class assets move into A class assets**
- **When new threats/scenarios come up you should be able to communicate to executives on the coverage you already have based on the investments and if anything new is needed (e.g. "if you want to be covered against this scenario at A class assets here's the trade off or cost")**
- **You and your executives get the visibility to understand your coverage**

DRAGOS

Dragos Platform Roll Out Example

1. **Month 1: Dragos Platform (asset identification and ICS threat monitoring/response control) roll out at 5-15 plants/substations/sites**
    a. **Ensure the value is there as expected**
2. **Month 6-12: Achieve 10-15% coverage by deploying to your A class assets**
3. **Month 12-36: Achieve coverage in your B class assets**
4. **Month 36+: If its a top 2-3 control for your C class assets roll it out there; if not roll it out to any C class assets that get moved into a B class asset over time**
    a. **The goal is to constantly be bringing up the coverage of your environment based on your budget and resources**