OTORIO

Cybersecurity - Closing the Gap Between IT and OT

June 2022

Definitions

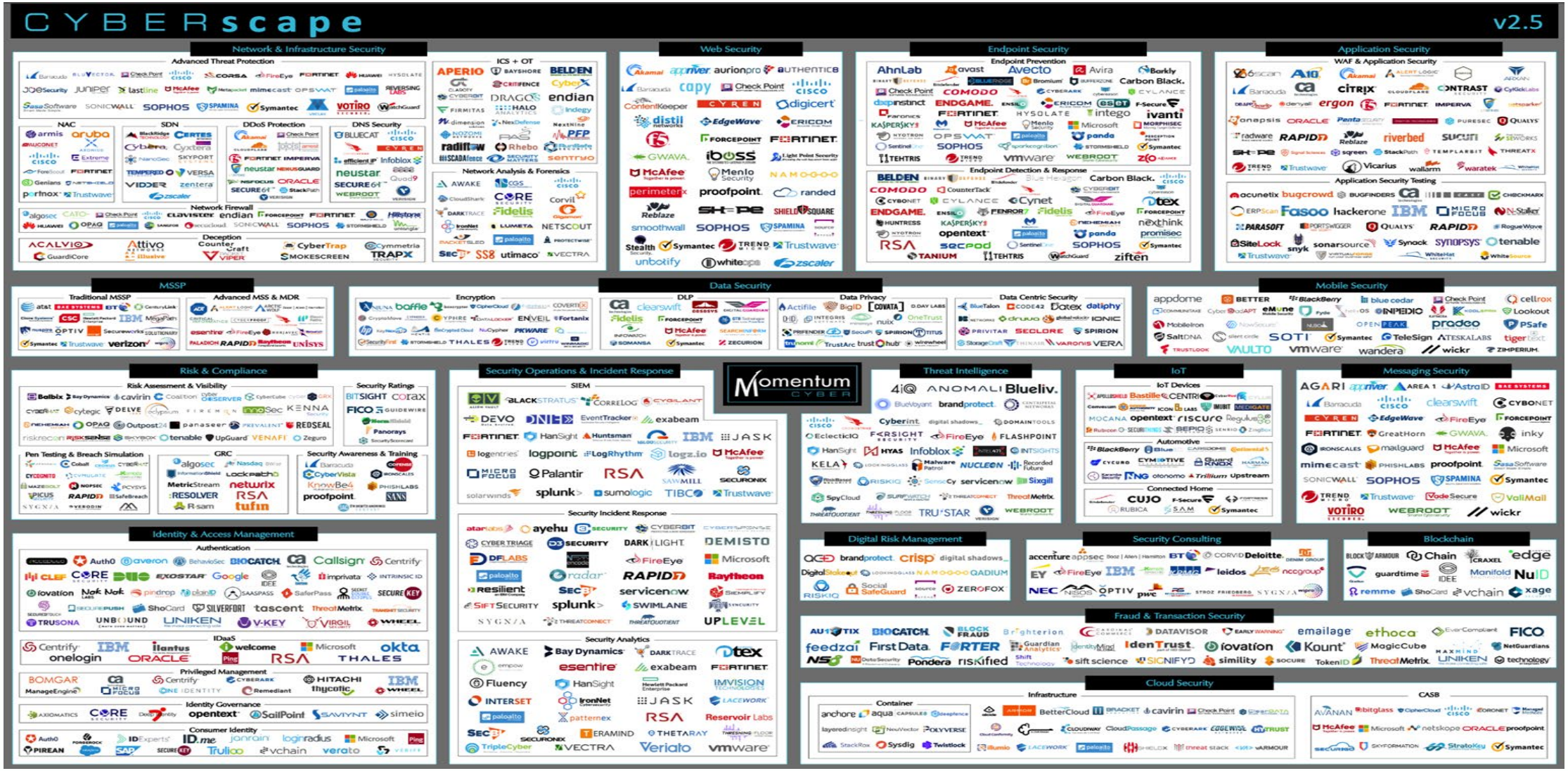
Information Technology (IT) is defined as hardware, software and communications technologies that focus on the storage, recovery, transmission, manipulation, and protection of data.

Operational Technology (OT) is defined as hardware and software that detects or causes a change through the direct monitoring and control of physical devices, processes, and events

Questions to Ask

- Is the sector doing enough to address the security of critical infrastructure?
- Will digital transformation impact the grid and change the architecture of an LDC's network
- How do we drive awareness at the appropriate levels within our organization?

Some Say They Have the Answers

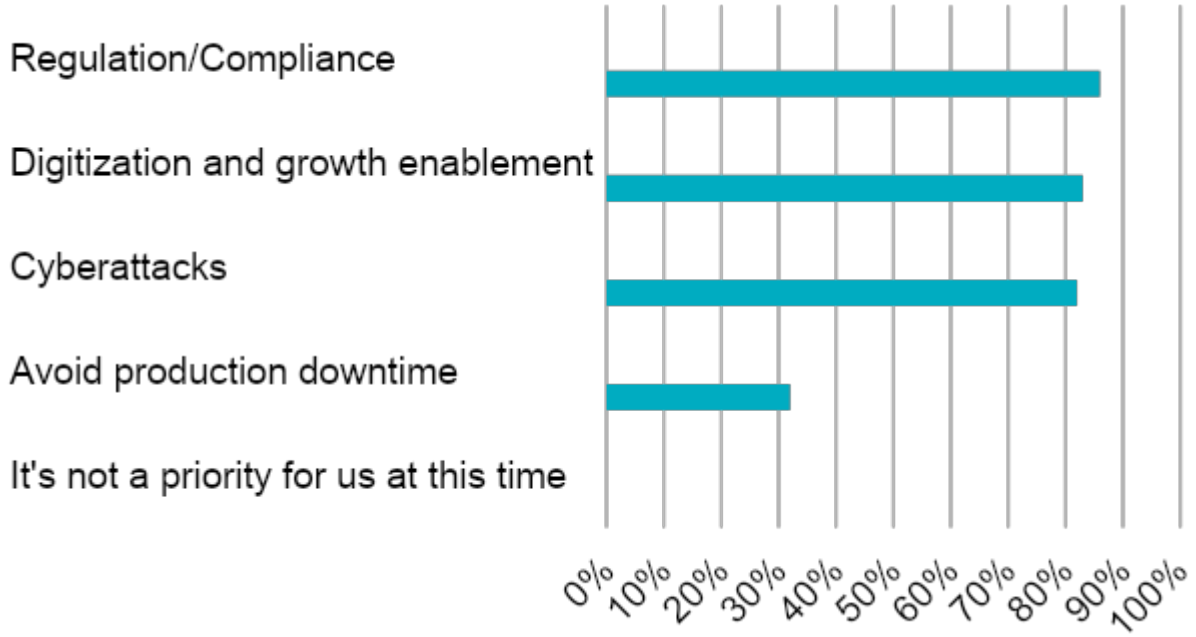


OEB Cybersecurity Framework - A Recap

- The framework has done well to drive awareness within the sector
- Significant, focused investment has been made
- Encouraging amounts of collaboration
- Gaps in coverage - will be dealt with in the next update
- The drive for true security maturation naturally lessens after compliance requirements have been met

Compliance is the Main Driver for OT Security

1. Compliance is number one driver at 86%
2. Digitization and Growth ranks higher than Cyber attacks
3. Cyberattacks still make up a large percentage

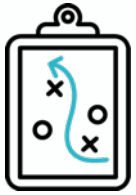


Digitization

Fundamental Impact on Operational Technology Security

Consumer Expectations

We continue to move to a cleaner energy economy



A New Playbook

We will see a push to not just “do” digital but “be” digital

Focus and Pace

Digital efforts will be consistently front of mind and drive an increased pace of change

Skills Gap

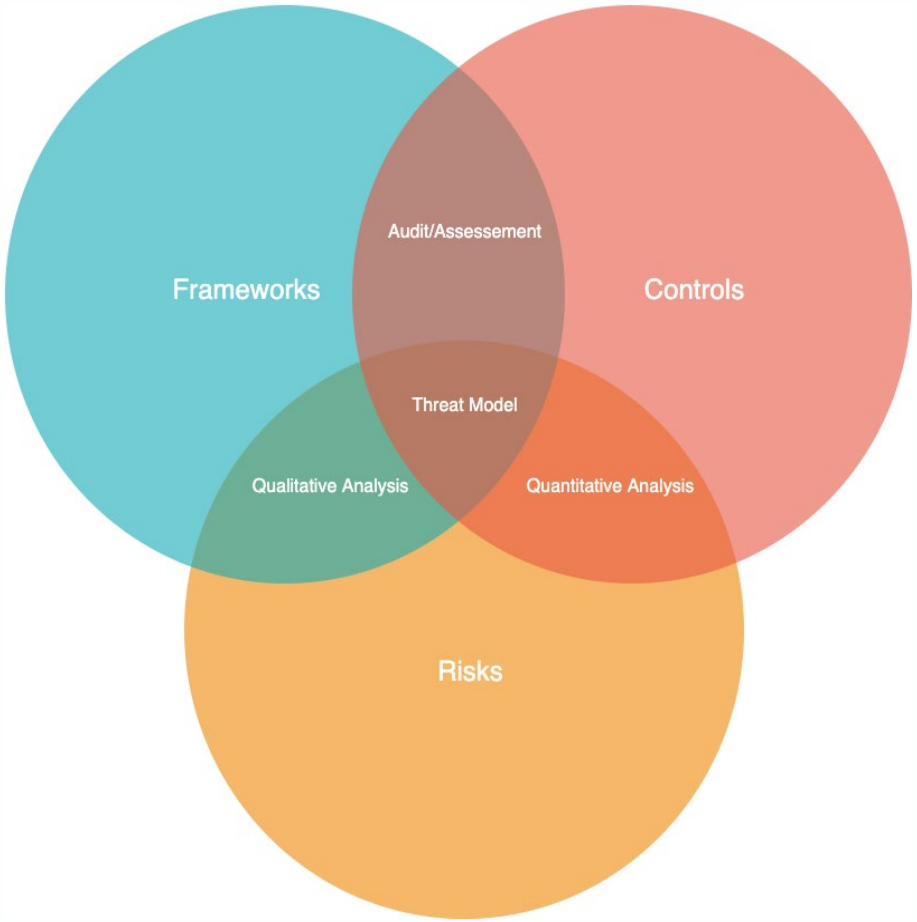
Distinct need to increase knowledge and capability - might drive the need to re-skill

Prediction

We are quickly moving towards a world where there will not a distinction between IT and OT for critical infrastructure organizations.

While the final state will be ideal. We need to securely manage this change.

Cybersecurity Operational Model



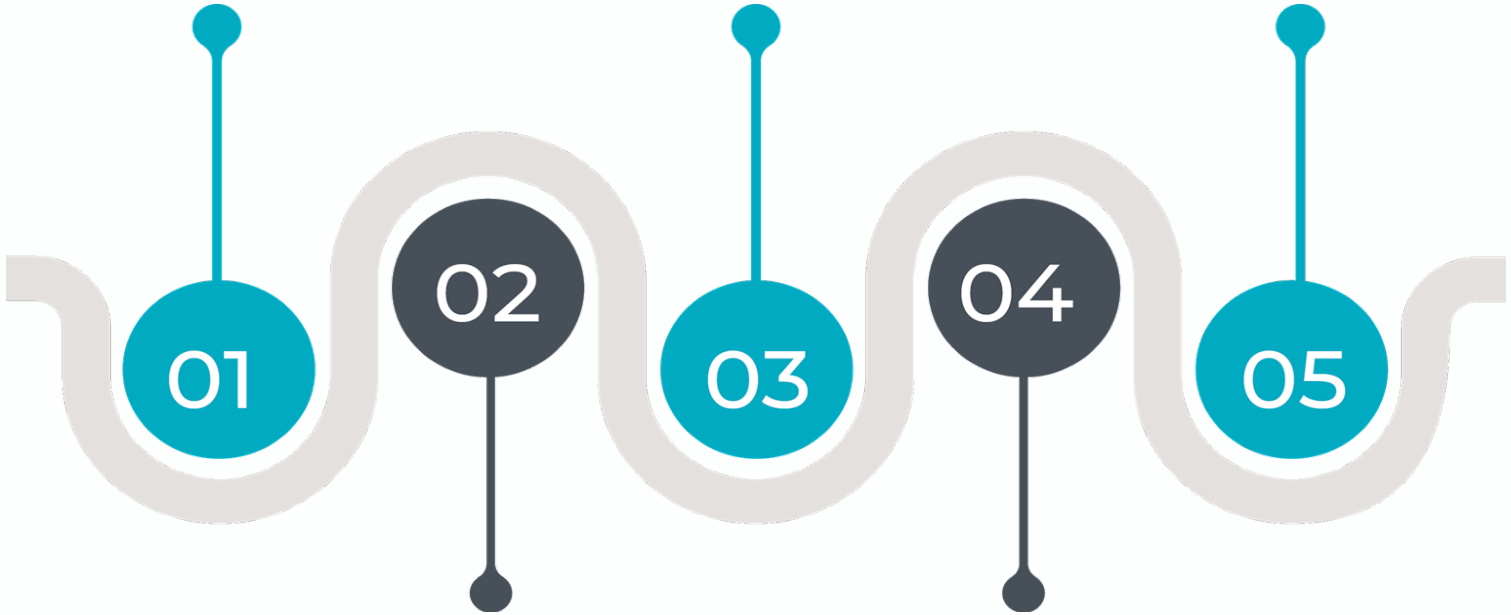
1. Audit/Assessment
2. Qualitative Analysis
3. Quantitative Analysis
4. Threat Model

Tackling the Changing Dynamics

Drive Awareness
Digitization creates opportunity across the oganization

Up-skill / Re-skill
Staffing dynamics will need to change

Change the “How”
Today’s organizational structure might not serve future



Collaborate
Foster an environment of knowledge sharing

Involve the Supply Chain
Strategic relationships are crucial

What Can you Do Today?

- Identify who owns risk - ensure they are involved
- Form cross-department/cross-function committees - give them a project
- Build margin for innovation
- Extend cybersecurity training

OTORIO

Stay safe