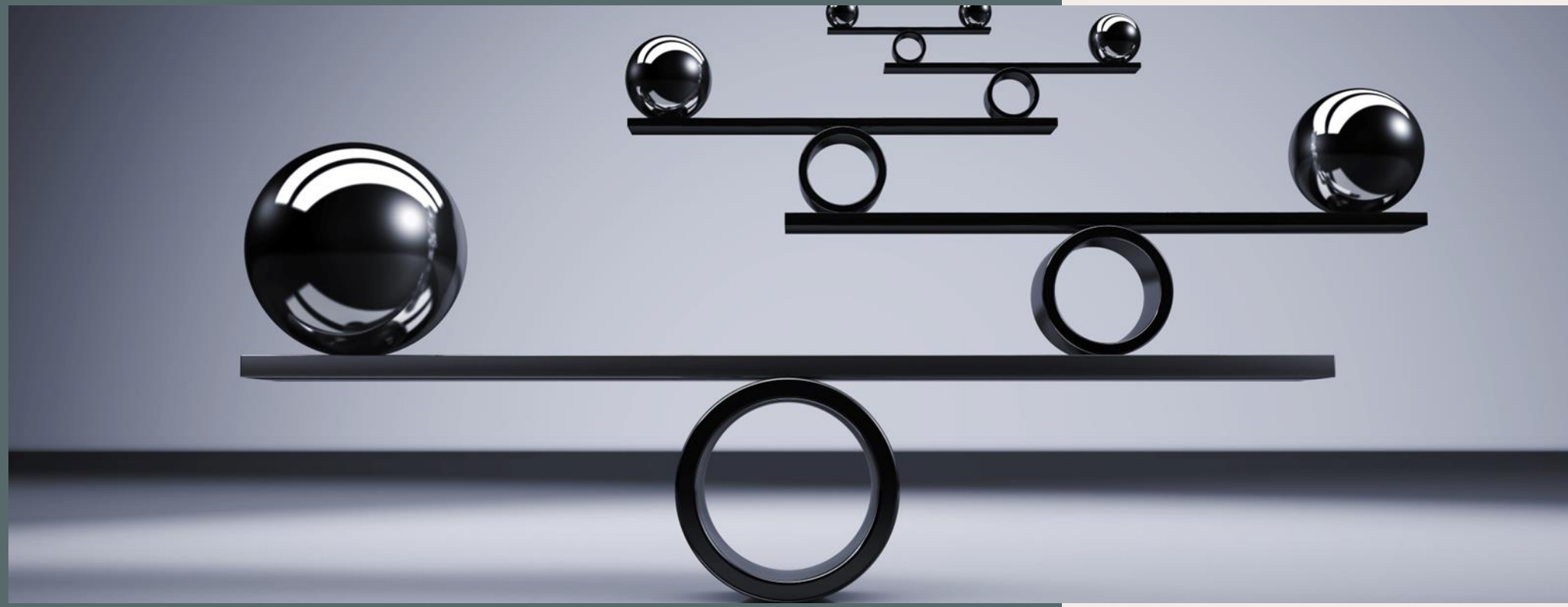


Security for the C-Suite:
How to build a good Security Team

Workshop Part III

Tobin Joseph

01/12/2023

Agenda

Strategic Planning to build a good security team: Strategy Design

Define objectives for your strategies

Define actions and goals

Identify and assign actors

Areas of expertise (review)

What to look for in the people for the team

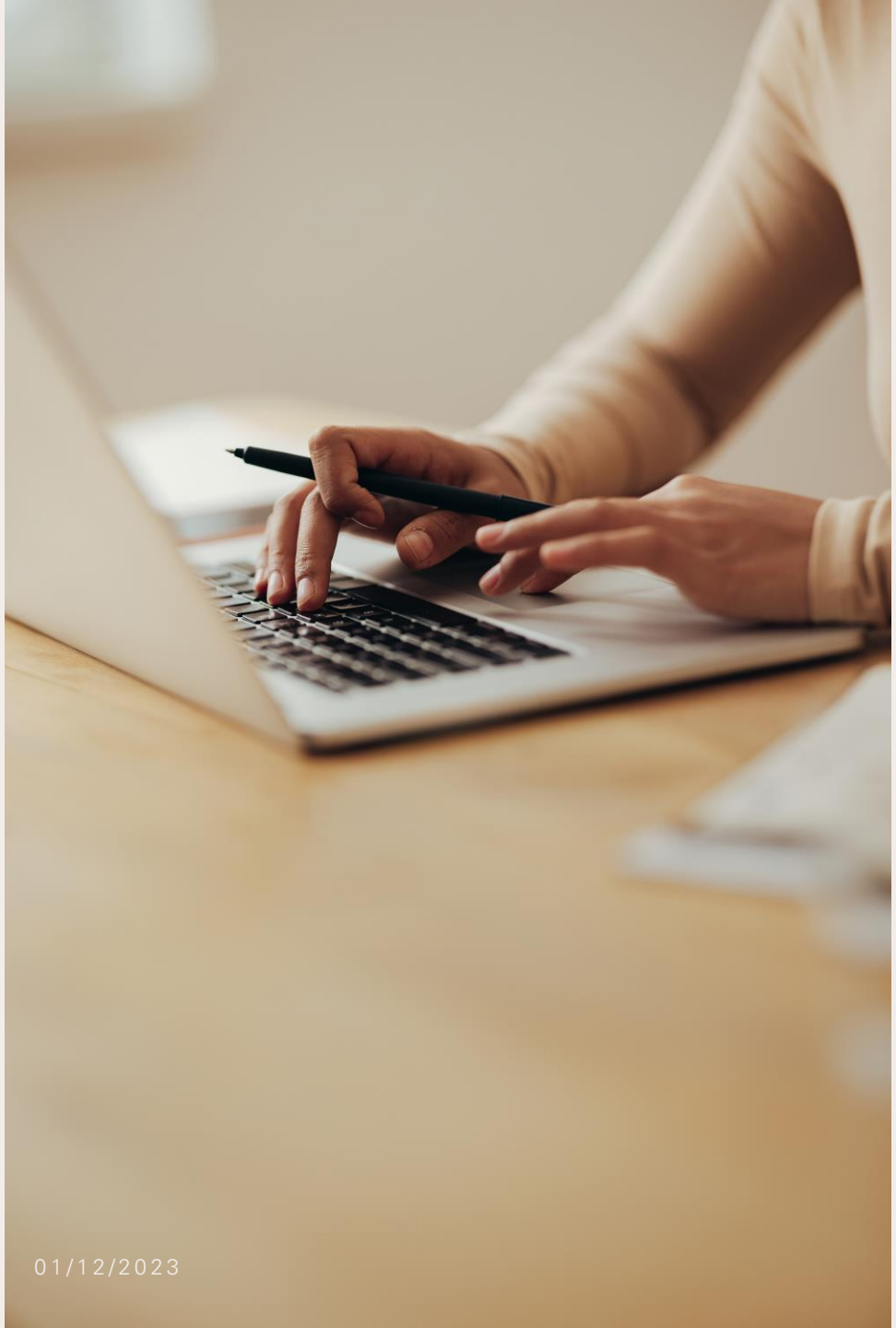
Defining metrics

Group Exercise

Strategic Planning to build a good security team

From your SWOT Analysis, you can take your strengths and opportunities to create strategies to counter your weaknesses and manage your threats.

Strategic Planning: Objectives



Objectives

The strategies should define an objective to be achieved and a general way to achieve those objectives. You must take your strategies to build your team starting from the current needs and means of your organization and then plan on a build-up as your organization changes. When building your cyber team, seeking outside talent is always going to be part of the process, though often overlooked is the importance of first focusing on how an existing team can be improved and further trained.

Actions to fulfill your strategy objectives

Drill down on the objectives to define specific actions in your strategies. Define goals for these specific actions. Your goals are the specific outcomes you are trying to achieve.

Your goals need to be made SMART--Specific, Measurable, Achievable, Results-Focused, and Timebound. Define metrics to measure your current position and progress toward achieving your goals. Where you are now, where do you want to be and how much is your pace of progress toward that goal? You will need to use KRIs and KPIs in this specific situation of security for operational measures as you build the team. Also, you could measure how many skills you have filled, redundancy of skills and desired skills, whether in-house or outsourced.

Identify and assign actors

Identify and assign actors to the defined actions. Some actions make require a team effort between different departments. Maybe the administration department handles physical security and the CISO manages the technological side of it. The CISO might create and/or evaluate suppliers for employee training in security/cybersecurity awareness but HR might run the scheduling and monitoring of attendance and successful completion of the training.

Areas of Expertise to Cover

- ❑ Physical access to client/business partner areas.
- ❑ Handling of physical items.
- ❑ Governance, Risk, and Compliance.
- ❑ Architecture.
- ❑ Data Loss Prevention.
- ❑ Identity and Access Management.
- ❑ Secure Devops / DevSecOps.
- ❑ Secure Software Development.
- ❑ Supply Chain/Client Interconnections.
- ❑ Employee Training / Testing and the Organization’s Security Culture.
- ❑ Skill Background and Representation Diversity.
- ❑ Attack Identification Capabilities.
- ❑ Forensic Analysis.
- ❑ Incident Response and Recovery.
- ❑ Penetration Testing.
- ❑ Disaster Recovery Plan Execution Testing.

What to look for in the people for the team

Secure software development skills.

Ability to analyze, diagnose, and detect security risks.

Interest and understanding of the latest news and developments in security/cybersecurity.

Understanding of network architecture.

Understanding of process architecture.

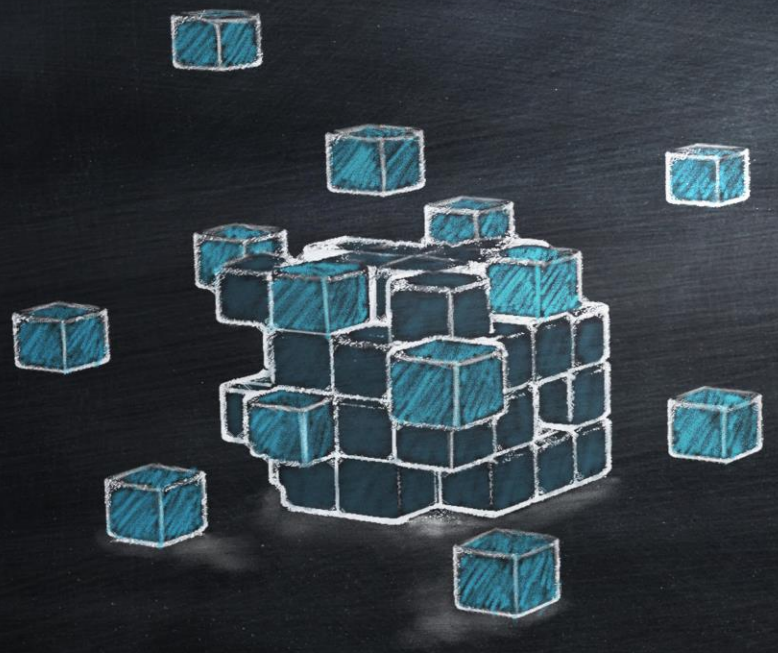
Strong communication and collaboration skills.

Cultural fit into the organization.

Defining Metrics

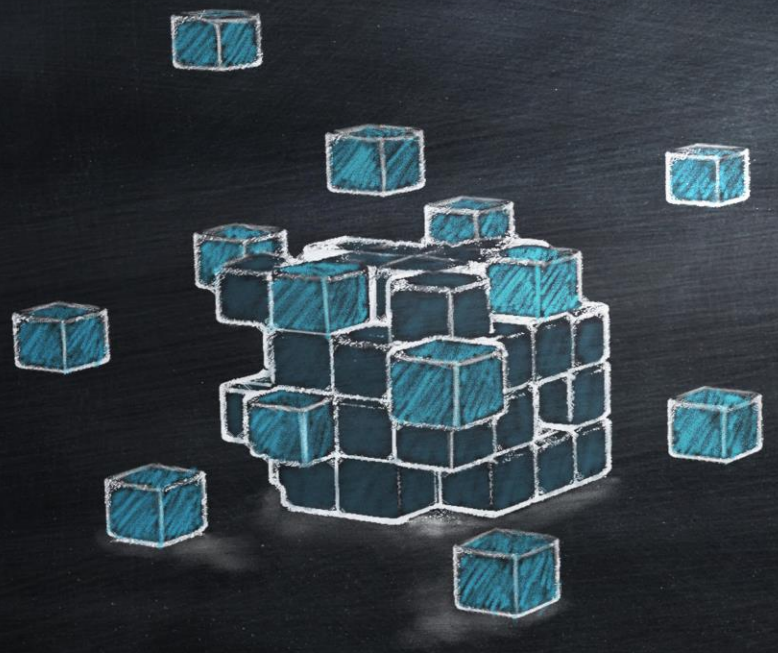
Company-wide objectives and goals will need to be subdivided into Departmental Strategies with their defined internal objectives and goals aligned with the company-wide strategies. Company-wide metrics are more business focused than technical focused, and sometimes in the cybersecurity space people fail to make this differentiation. One key skill of the CISO is to be able to translate technical terms and measures into business terms and measures that accurately reflect the reality of the security posture and response strategies in the organization.

Example KRIs & KPIs



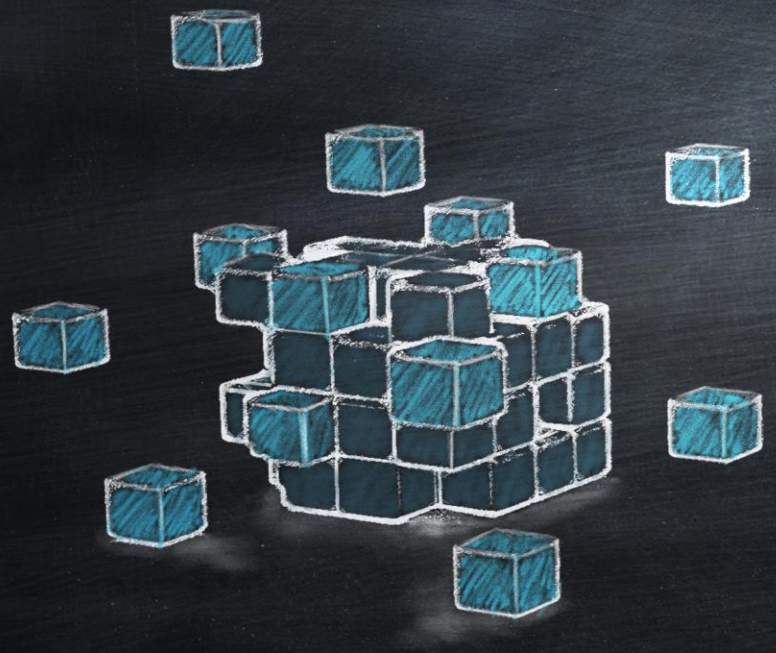
- Intrusion attempts vs. actual security incidents. This metric offers general insight into existing vulnerabilities, the state of preparedness, and how the organization responds to attacks.
- Mean time to detect (MTTD). This is a crucial element because the faster an organization identifies an attack, the greater the odds it can contain it with minimal damage.
- Mean time to respond (MTTR). The ability to neutralize a threat and get systems back online is critical because as events drag out, risks and costs increase.
- Mean time to contain (MTTC). This metric refers to the average time required to shut down all attack vectors across all endpoints and minimize the probability of any further damage.

Example KRIs & KPIs (continued)



- Unidentified devices on the network. An ability to discover and tag unidentified devices greatly reduces the odds that someone has unauthorized access to the network.
- Patching cadence and effectiveness. It's vital to ensure that software patches are applied quickly and effectively. However, it's also important to know which patches should be prioritized.
- Training effectiveness. Ensuring that employees understand how to respond to attacks is essential. Human error is a leading cause of intrusions and breakdowns. For instance, phishing test success rates and dynamic risk scoring offer insights into how a training program is performing.

Example KRIs & KPIs (continued)



- Peer and industry benchmark data. With independent data, it's possible to know how an enterprise is performing compared to others in the industry. However, it's also important to understand whether industry benchmarks are adequate so that an organization doesn't regress to the mean.
- Security audit compliance. This metric delivers actionable information about whether tools, technologies, and procedures are working — and where they're falling down.
- Third-party risk and compliance. Extended supply chains, third-party vendor apps, and APIs all represent risk. As a result, it's vital to understand risks in the context of third-party privileges and relationships.

Exercise

Create preliminary strategies from your previous SWOT analysis defining objectives taking into consideration the areas of expertise. Drill down to actions with SMART goals, identify and assign actors, if possible, using the things to look for in people to help define the actors in addition to the areas of expertise. Define your metrics for the goals.