Creating a Results Oriented Culture – By Measuring What Matters

Execution is everything. How simple goal setting with clear objectives and key results that are measurable will propel your team to exceed expectations.

What kind of operational data demonstrates cybersecurity leaders’ long-term budgetary needs for their programs and at the same time shows the progress they’ve made over the years? Learn how a duo of cybersecurity professionals used thought leadership and a goals-based approach to build the case for past capital and future spend — a system that won them both dollars and trust with peers and their boards.

In this session we will provide real-world examples of what metrics were chosen to show progress, and how the speakers have gone about gathering them. We’ll discuss how to make a difference and influence change in your organization if you are an army of one or a few more. You will leave this session not with abstract ivory-tower ideas on measurement, but with actionable tactics you can put in place within your own program today.

• Telling your story – Using metrics and soft skills to change behavior
• Force Multiplier – Using Lean methodology borrowed from the manufacturing industry to improve operations and inject security as a measured component
• Be Indispensable – Control the technologies and processes that require you to be involved with delivering the cool stuff. Be a Business Enabler.
• Real world examples of metrics used in our organizations

TALK OUTLINE
CREATING A RESULTS ORIENTED CULTURE

By Measuring What Matters

Jack Nichelson (CISO, MRK Technologies)
JACK NICHELSON

- Chief Information Security Officer at MRK Technologies
- Previous Director of Infrastructure & Security for Medical Mutual of Ohio.
- Executive MBA from Baldwin-Wallace University
- Recognized as one of the “People Who Made a Difference in Security” by the SANS Institute and Received the CSO50 award for connecting security initiatives to business value.
- Adviser for Baldwin Wallace’s, State winner Collegiate Cyber Defense Competition (CCDC) team.

“Solving Problems, is my Passion”
If I just had a better team, I would do better. "Wrong"
If I am a better leader, my team will be better. That is what I had to learn as a leader and step up to make it happen.

- **Be Proactive** – Focus on what you can influence
- **Admit You Need Help** – Shine a light on the problem
- **Know Your Stakeholders** – Begin with the end in mind
- **Create a Problem Statement** – A goal without a plan is just a wish
- **Put first thing first** – Plan weekly, act daily

“There are no bad teams, only bad leaders.” - Jocko Willink
The most important person for you to manage effectively is yourself. To grow personally and professionally you need to know yourself before you can help others.

Recommendations:

- Take a step back and read “REWORK”
- Remove complexity – Start small
- Start at the epicenter, on what won’t change
- Focus on fewer problems that provide bigger returns
- Build an audience
- Keep score & publish it (Good or Bad)

“Think about how you can simplify security – make it easy – and focus on the basics.” - Dave Kennedy
To make stuff that matters, you have to know what matters. Work on solving the right problems.

“No one cares what you know until you show them how much you care”

- Security is about a lot more than just you
- You are taking actions to protect assets in the stewardship of others
- You are making choices which will impact the ways those around you conduct their business

“Effective managers take the time to identify stakeholders and know their pain points.”
We often focus on the problem and forget about the customer. They will forget the problem you solved before they forget how you made them feel.

- Security is a support role…your job is to help others safely do the things that make your organization productive
- You cannot do this job without help
- Your employees are not subject’s for you to dictate rules to…they are your customers
- If you treat them well, they will be your “army of human sensors”, bringing you all kinds of useful intel, and helping to enforce policies you’ve developed to protect them

“The day people stop bringing you their problems is the day you have stopped leading them” - Colin Powell
Change starts from within, so you have to make the decision to focus on the things you can influence rather than reacting to the things outside of your control.

Manage Yourself:
- Where and how are you spending your time & energy throughout the day?
- Make a list of the things that concern you and things you can influence.

Ask yourself these 3 questions every day:
- Did I do my best to spend my time on things I can influence?
- Did I do my best to set and communicate clear goals?
- Did I do my best to make progress toward goal achievement?

“The 1st metric you need to track is yourself”
CONCERN VS. INFLUENCE

Hackers
Organized Crime
State Sponsored

Higher Difficulty
~10% of incidents
- Nation States Threat Actor
- Advanced Persistent Threat
- Zero Day Attacks
- The Insider Threat
- Ransomware Attack
- The “Cloud”

Lower Difficulty
~90% of incidents
- Missing Patches
- Lost & Stolen Devices
- Local Admin Right’s
- Phishing
- Poor Passwords
- Legacy Hardware & Software

78% of initial intrusions rated as low difficulty

Focused 4 Results
1. Patching
2. Encryption
3. Privileged Access
4. Security Awareness
The Problem Statement significantly clarifies the current situation by specifically identifying the problem and its severity, likelihood, and impact. It also serves as a great communication tool, helping to get buy-in and support from others.

**Build & Execute plans to drive for results & share successes**

- Invest more time in project planning and due diligence; time spent defining the problem is NEVER time wasted.
- Write a Project Charter, clearly state the scope, objectives, participants, and success measurements.
- Create a Work Breakdown Structure to graphically represent the project scope, broken down in successive chunks with defined deliverables.

“**A problem well stated is a problem half-solved.**” – Charles Kettering
Focus on the important, not just the urgent. The urgent are not that important, and the important are never urgent.

Tips for taking back control of your time:
- Stop saying Yes, When you want to say No.
- Scheduled your own time with purpose & defend it!
- Don’t be afraid to close your email and turn off your phone

“Effectiveness requires the integrity to act on your priorities”
What Jack can get others to fix because they are **MEASURED**, have **OWNERSHIP** and are **ACCOUNTABLE**.

“Try Not to Become a Success. Rather Become a Person of Value.”
WHAT IS LEAN

• Eliminate waste…not people
• The process needs fixed…not the people
• Embrace the Red
• Measure what you want to make better don’t just measure to measure
• Understand the cause
• Came from the Manufacturing world but great for Cybersecurity

#InfoSecWorld
Gemba (現場) is a Japanese term referring to the place where value is created. The idea of Gemba is that the problems are visible, and the best improvement ideas will come from going to the Gemba.

“Good security is not something you have, it’s something you do” - Wendy Nather
THE POWER OF THE BOARD

• Each IT Team (e.g. development, infrastructure, database, etc.) has a board with a column on cybersecurity
• Shows pain points …embrace the Red
• 1-2 times a month each board is presented to everyone
• Once a week standup meeting (10 min) with CIO and Directors (including cybersecurity) to discuss the Red
# CYBERSECURITY DASHBOARD

<table>
<thead>
<tr>
<th>Framework Core Area</th>
<th>Description</th>
<th>Activities</th>
</tr>
</thead>
</table>
| **Identify** *(Maturity Level)* | Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities. | *(FY20-21) Conducted review of program maturity against NIST CSF  
*(FY20)* Added an Associate IT Risk Analyst FTE |
| **Protect** *(Maturity Level)* | Develop and implement appropriate safeguards to ensure delivery of critical services. Supports the ability to limit or contain the impact of a potential cybersecurity event. | *(FY20)* Established a part-time Cybersecurity Education and Awareness function - Cybersecurity Month, education content, employee engagement, etc.  
*(FY21)* Requesting a full-time Cybersecurity Education and Awareness position * |
| **Detect** *(Maturity Level)* | Develop and implement appropriate activities to identify the occurrence of a cybersecurity event. | *(FY20)* Deployed “Report Phishing Button” to email clients  
*(FY21)* Cloud Security and Compliance Orchestration |

Can self score or contract out

Map what you did and what you want to do against a framework

* Actions recommended to increase NIST CSF Maturity

Point out what you did/are proposing to increase maturity
PARETO CHARTS ARE YOUR FRIEND

• Highlights the cause of problems or your “problem children”
• Small bites of the elephant
• Results
  • Saw teams ask for access to our vulnerability scanner
  • Did their own reviews and prioritization
  • Allowed the teams to find the metrics that worked for them
  • Saw results

#InfoSecWorld
REPORT CARDS

- Services available to grade your security **daily**
- Everyone understands an “A” is good and a “F” is bad
- Managers, directors, and CIOs don’t like getting F’s
- Good for knowing what to focus on and developing/justifying policy/standards
- Warning…might not be good for Board (too much detail?)

#InfoSecWorld
REPORT CARDS FOR THE BOARD

• Same services provide reports for the Board

• Boards may not care as much about the grades but they do care how you compare to the industry

• Use the fact that this is reported to senior management to influence teams to improve security
THE JOURNEY

• Visit someone doing it…with your boss
• Partner with your Continuous Improvement Team…don’t have one…check with your local college and see if they can help with Lean
• Lean Training for Everyone…not only to learn but build trust that it is ok to show Red
• Cybersecurity Team may have to build the metrics for the other teams
• Empower the teams to build their own cybersecurity metrics
• Build a culture of “how do we succeed as a team” and not “who do we blame”
REPORT CARDS FOR THE BOARD (TRENDING)

Show change over time
- Simple
- Easy to understand
- Independent
- Highlights challenges

Set expectations that it can drop
- Acquisitions?
- Shadow IT?

Provide assurance that we monitor and address issues
SUMMARY – TAKE OWNERSHIP

If I just had a better team, I would do better. “Wrong”
If I am a better leader, my team will be better. That is what I had to learn as a leader and step up to make happen.

- Be Proactive – Focus on what you can influence
- Begin with the end in mind – Define practical outcomes
- Create a Problem Statement – A goal without a plan is just a wish
- Put first thing first – Plan weekly, act daily
- Chart Performance & Adjust – Shine a light on the problem

BIT SIGHT Security Ratings Report
December 7, 2016

Chart Industries, Inc. manufactures engineered equipment for the production, storage, and end-use of hydrocarbon and industrial gases worldwide. The company was incorporated in 1992 and is headquartered in Garfield Heights, Ohio.

SECURITY RATINGS

BIT SIGHT SECURITY RATING

770
Our ratings measure a company’s relative security effectiveness.

ADVANCED 900–740
INTERMEDIATE 740–640
BASIC 640–250

Engineering Industry Range
REFERENCES

- The Five Dysfunctions of a Team – Patrick Lencioni
- Leading Change – John Kotter
- The 7 Habits of Highly Effective People – Dr. Covey
- The 1 Minute Manager – Ken Blanchard
- Extreme Ownership – Jocko Willink
- The Phoenix Project – Gene Kim
- The Ideal Team Player – Patrick Lencioni
- Death by Meeting – Patrick Lencioni

- Security Rating Vendors
  [https://www.bitsight.com/](https://www.bitsight.com/)
  [https://securityscorecard.com](https://securityscorecard.com)
  [https://www.riskrecon.com](https://www.riskrecon.com)

- Security Rating Research
  Forrester: New Wave Cybersecurity Risk Rating Solutions, Q4 2018
  Gartner: Innovation Insight for Security Rating Services
THANK YOU!

Jack Nichelson (CISO, MRK Technologies)