MIS|TI™ PRESENTS

InfoSecWorld

Conference & Expo 2018

BIG THINGS, LITTLE PACKAGES – MAKING A DIFFERENCE WITH A SMALL TEAM

Jack Nichelson & Ed Pollock

Jack Nichelson

- Director, IT Infrastructure & Engineering for Medical Mutual of Ohio
- Previous Director of Infrastructure & Security for Chart Industries.
- 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.

I defend my companies competitive advantage by helping solve business problems through technology to work faster and safer.

Ed Pollock

- CISO for STERIS Corporation
- STERIS is a leading provider of infection prevention and other procedural products and services. The company is focused primarily on healthcare, pharmaceutical and medical device Customers.
- Member of the Ohio Attorney General's CyberOhio Advisory Board
- Member of a local hospital system's Cyber Security Advisory Committee
- Member of Bitsight Technologies' Customer Advisory Board

We want to be a business enabler for the organization, not "the team of No".

CHALLENGE OF SMALL SECURITY TEAMS

Leading a small cyber security team can be a challenge & rewarding

- Responsible for security but limited power to fix things
- Want to do more but don't have the people
- Generalization vs. Specialization…Jack of all Trades
- Justifying spending

I wish this was the size of my team

KEY POINTS

- How are You Telling Your Story?
- What are Your Force Multipliers?
- Are You Outsourcing the Right Things?
- Are You Indispensable?

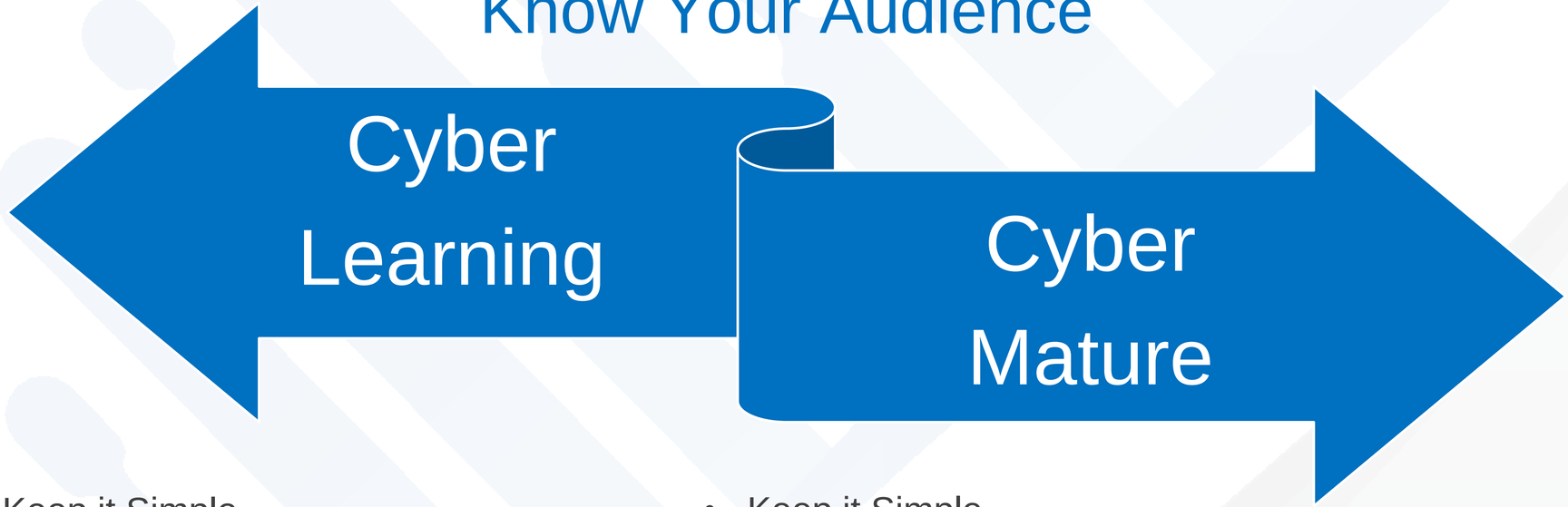
HOW ARE YOU TELLING YOUR STORY?

WHAT MAKES A GOOD METRIC

- Easily **measured**
- Easily **understood**
- Enables **decision-making**
- **Meaningful**
- **Consistent**
- **Quantitative**
- **Aligns** with your organization's **Risk Profile**

PRESENTING TO THE BOARD & SENIOR MANAGEMENT

Know Your Audience



- Keep it Simple
- Not Technical
- Based on Risk
- What is going well (GREEN)
- What needs their attention (RED)

- Keep it Simple
- Technical when they request it
- Based on Risk
- What is going well (GREEN)
- What needs their attention (RED)
- **How do we compare to others**
- **Progression against a Security Framework**

CYBER LEARNING

Boards & Senior Management in industries with historically low cyber security risk may still be learning

- Ask for guidance on what they want (they may not know)
- Keep short & simple
- What do you want from them?
- Report might be in an appendix
- Will become more important as cyber security becomes more important in your industry…only a matter of time

Build your program so it is ready

Cybersecurity Dashboard

Normal Activity | Increased Activity | Request Direction

Status	Areas of Interest	Description	Status	Requested Direction
G	Prevent	• Server/Desktop/Laptop • Network Protection • Data Loss Prevention	• New anti-malware protection purchased	
G	Detect	• Identify successful attacks • Notification • Third Party Monitoring		
B	Respond	• Incident Response Retainer with third party • Incident Response Plan	• Retainer in place • Added tools to increase response capabilities	
R	Recover	• Cyber Insurance • Disaster Recovery (DR)	• Completed annual comprehensive DR test	Recommend increasing current cyber insurance coverage from $10M to $20M to cover risk of new acquisition.
G	Cyber Attacks	• Malware, Ransomware, viruses • Data loss	• No impact to operations	

CYBER MATURE

Use grades that compare you to others in your industry
- BitSight Technology
- SecurityScorecard

How do we compare to others
- e.g. ,Top 10% in Network Protection
- e.g., Bottom 10% in Web Application Security – what is our remediation plan

Report status compared to a security framework
- Still keep it simple
- Show progress

Show impact of investments
- How did budget make things better
- Use trending

SecurityScorecard

B Application Security	A IP Reputation	A DNS Health	A Network Security	A Patching Cadence
A Social Engineering	A Endpoint Security	B Information Leak	C Hacker Chatter	A Cubit Score

Compromised Systems

Botnet Infections	B
Spam Propagation	A
Malware Servers	A
Unsolicited Communication	A
Potentially Exploited	D

Diligence

SPF Domains	A
DKIM Records	B
TLS/SSL Certificates	A
TLS/SSL Configurations	D
Open Ports	B
Web Application Headers	C

BitSight Technologies

InfoSecWorld Conference & Expo 2018

WHAT ARE YOUR FORCE MULTIPLIERS?

WHAT IS LEAN

- Eliminate **waste**…not **people**
- The **process** needs fixed…not the **people**
- Good for breaking silos
- Be sneaky…inject security

THE PUDDING – FINDING THE PROOF

Kaizen Mini Event to Improve Server Patching Process

- Automated 90% of patch process
- 50% improvement in number of patch cycles
- 42% improvement in time to patch a server

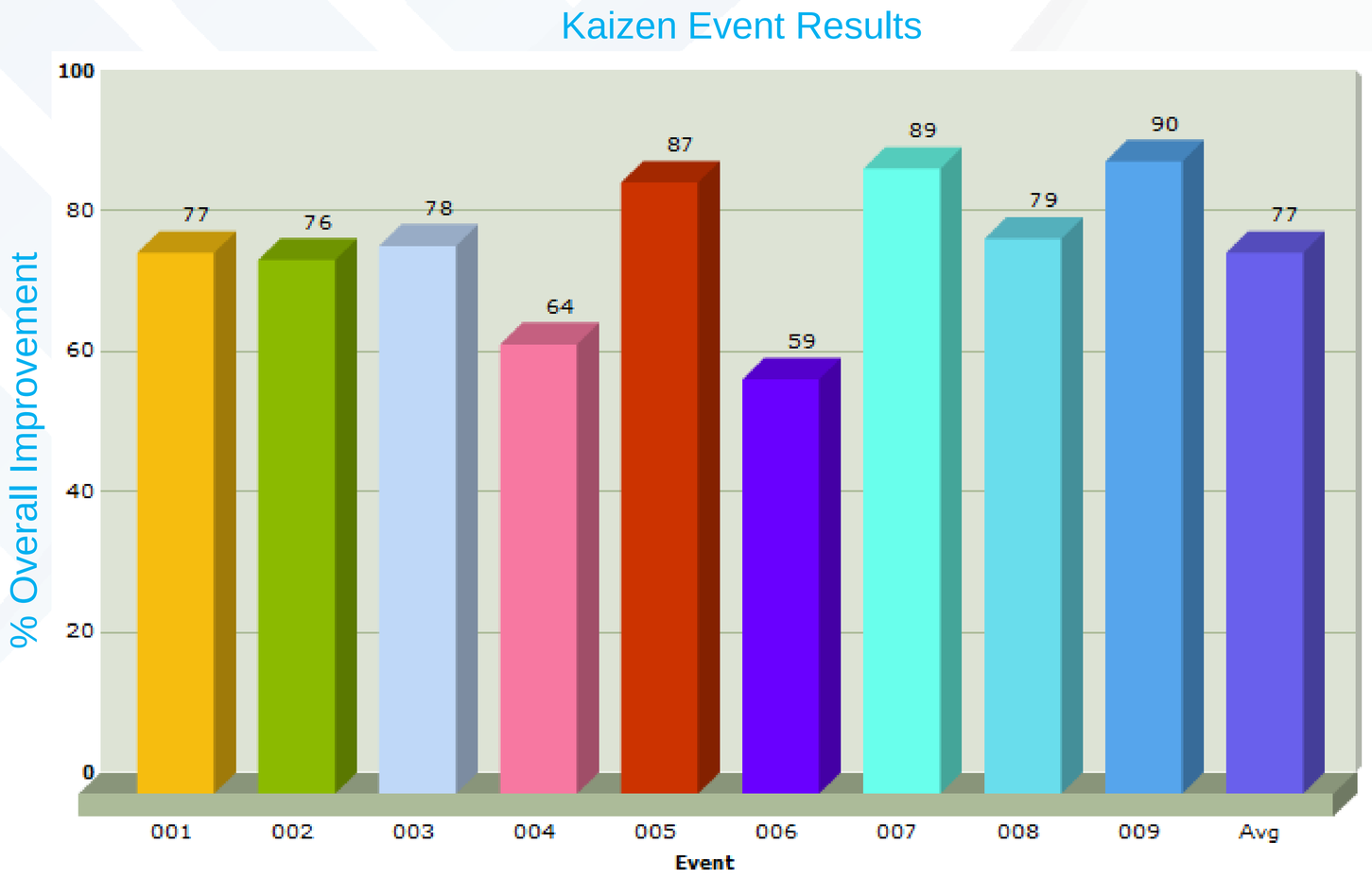
Kaizen Mini Event to Improve Server Provisioning

- Went from lead time of 6.7 business days to 12.7 hours
- Server Team came up with the idea of a Secure Gold Image to get me out of the process!

SQDC Boards

- +90% reduction in vulnerabilities
- **Teams start taking ownership for securing their systems & applications**

Breaks the silos



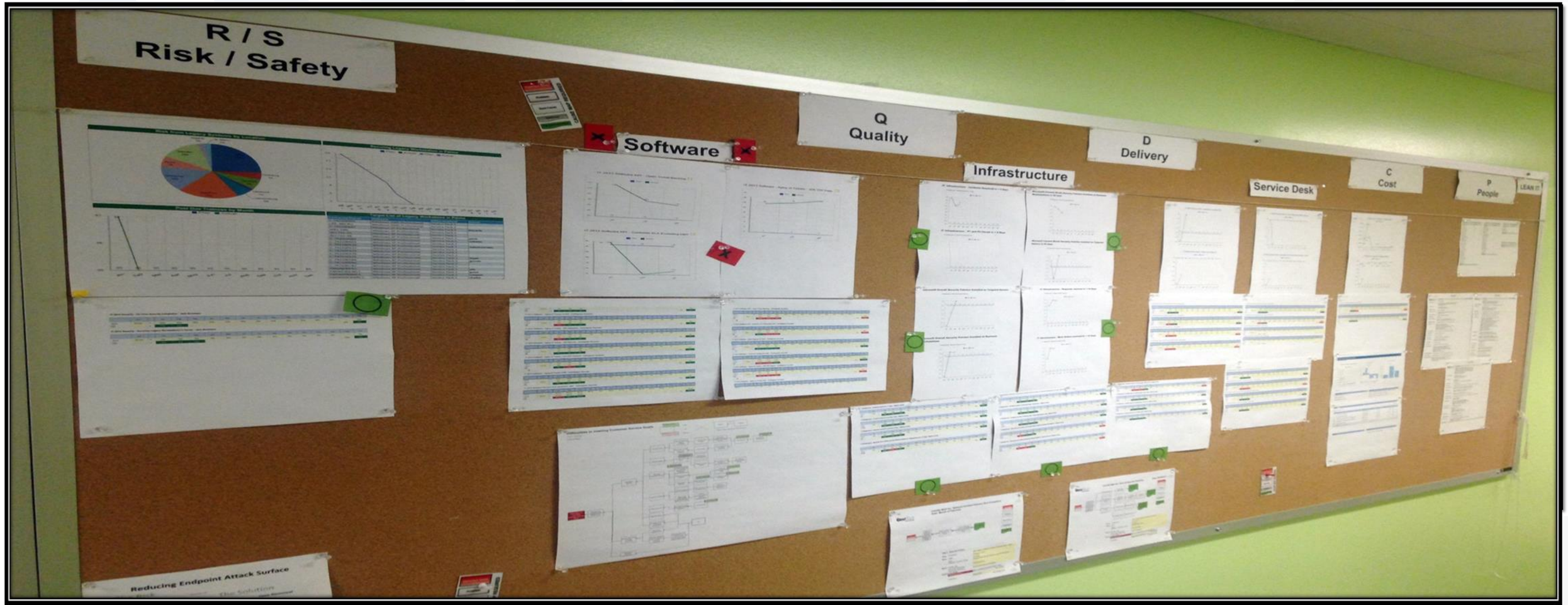
SQDC BOARDS

- Board of Metrics
- Visual
- Accountable
- Shows your pain points

Safety/Security, Quality, Delivery, Cost

CHART PERFORMANCE & ADJUST

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.



SECURITY IS EVERYONE'S RESPONSIBILITY – GETTING THERE?

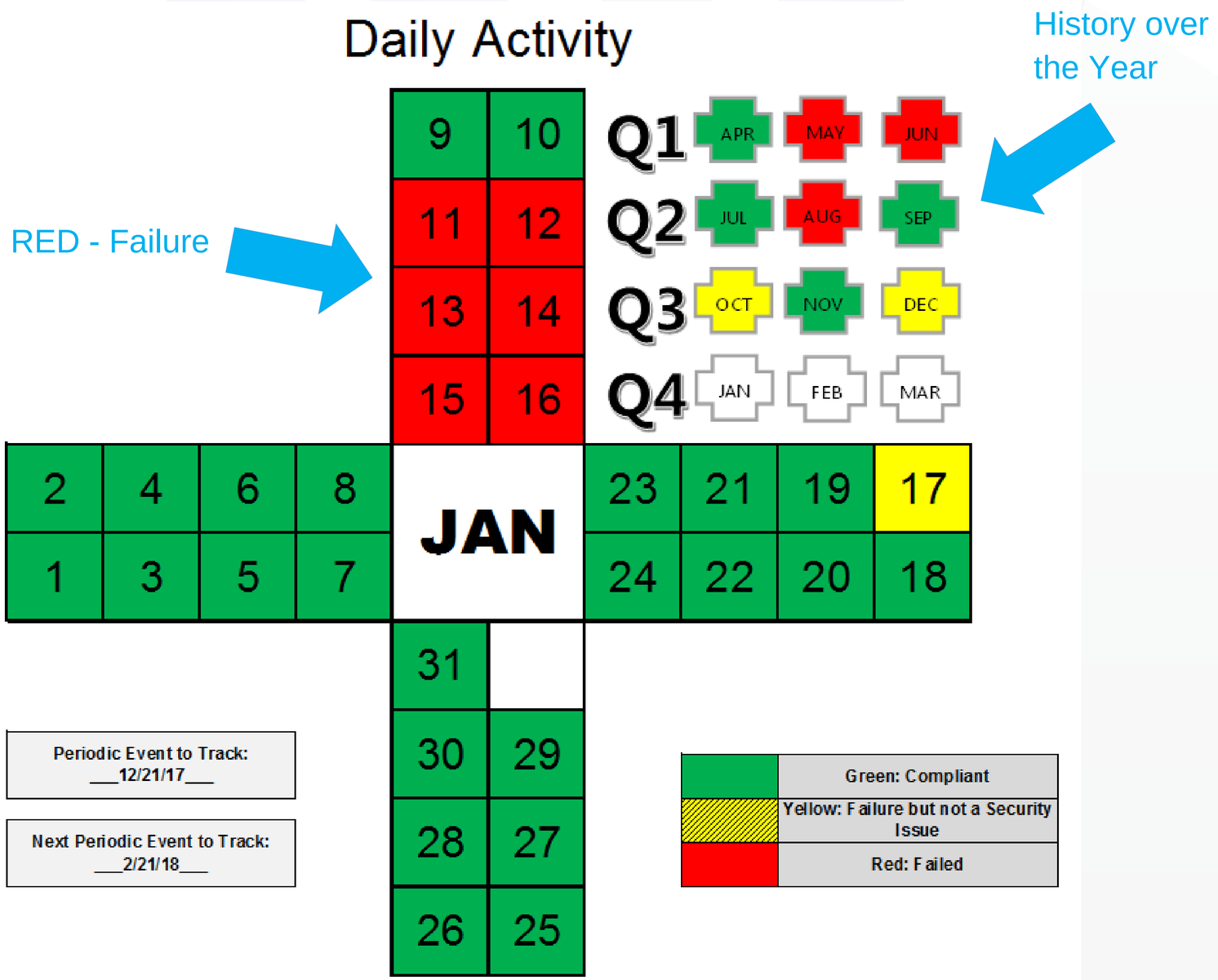
- Each Teams' Board has a metric on security examples:
  - Security Cross
  - Patching
  - Malware tickets
  - Code vulnerabilities
  - What would you like to see?

- Training Matrix - Development Team added Security as a skill…brought a tear to my eye ☺

SAFETY/SECURITY CROSS

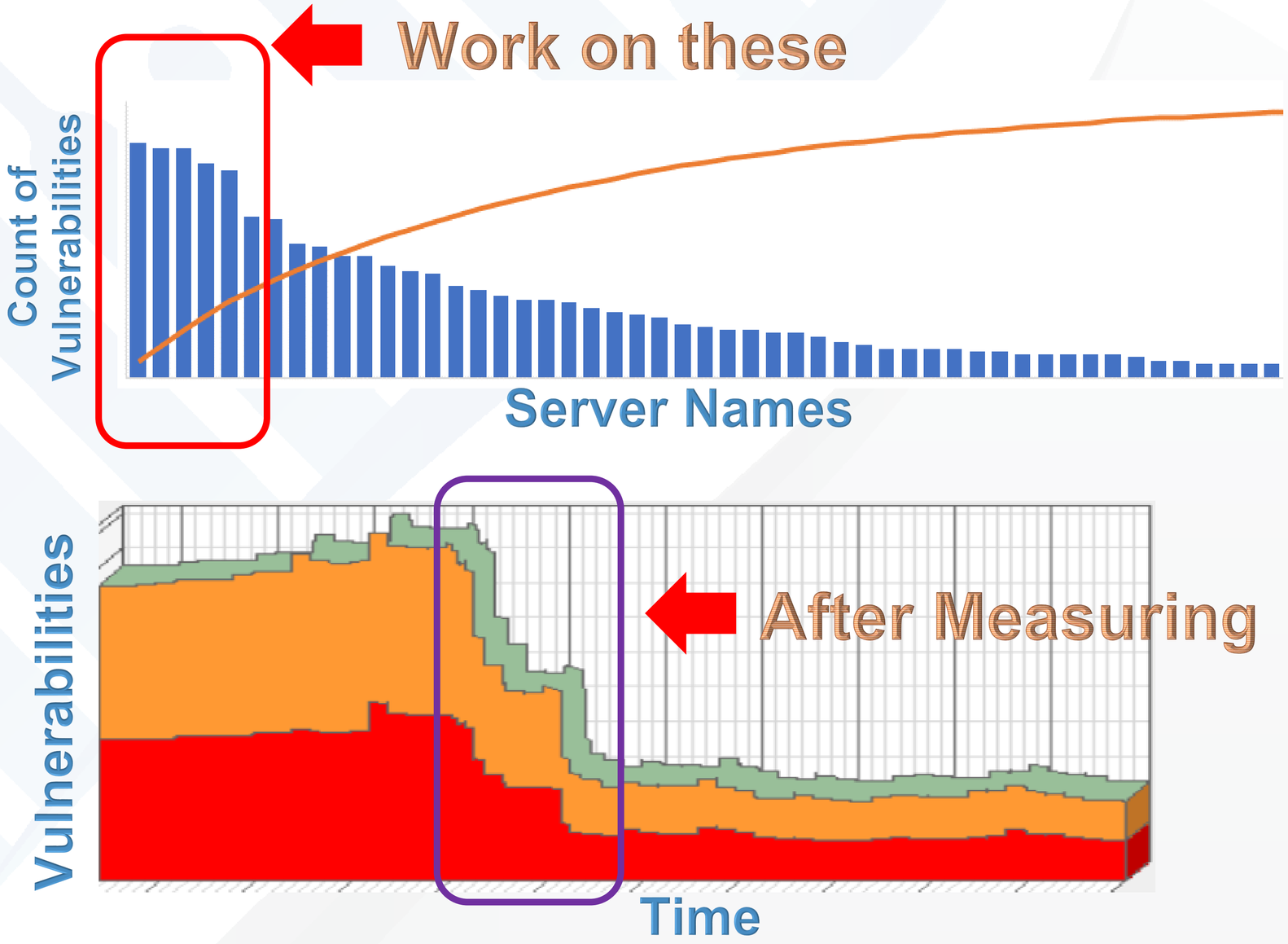
Stole from Manufacturing – used to track Safety incidents

Good for tasks that happen daily (e.g. PCI scan, system available, important daily financial report delivered on time, process completing on time, etc.)



PARATO CHARTS ARE YOUR FRIEND

- Highlights cause of problems
- Small bites of the elephant



STANDUP MEETINGS

- Standup Meetings
  - Multiple times a week
  - Review the REDs… Don’t fear the RED
  - Only review the RED, new metrics, & Thank You’s
  - Breaks down silos
  - 10 minutes or less in the morning
  - Use video to bring in remote team members

ARE YOU OUTSOURCING THE RIGHT THINGS?

OUTSOURCING

Where is your value?

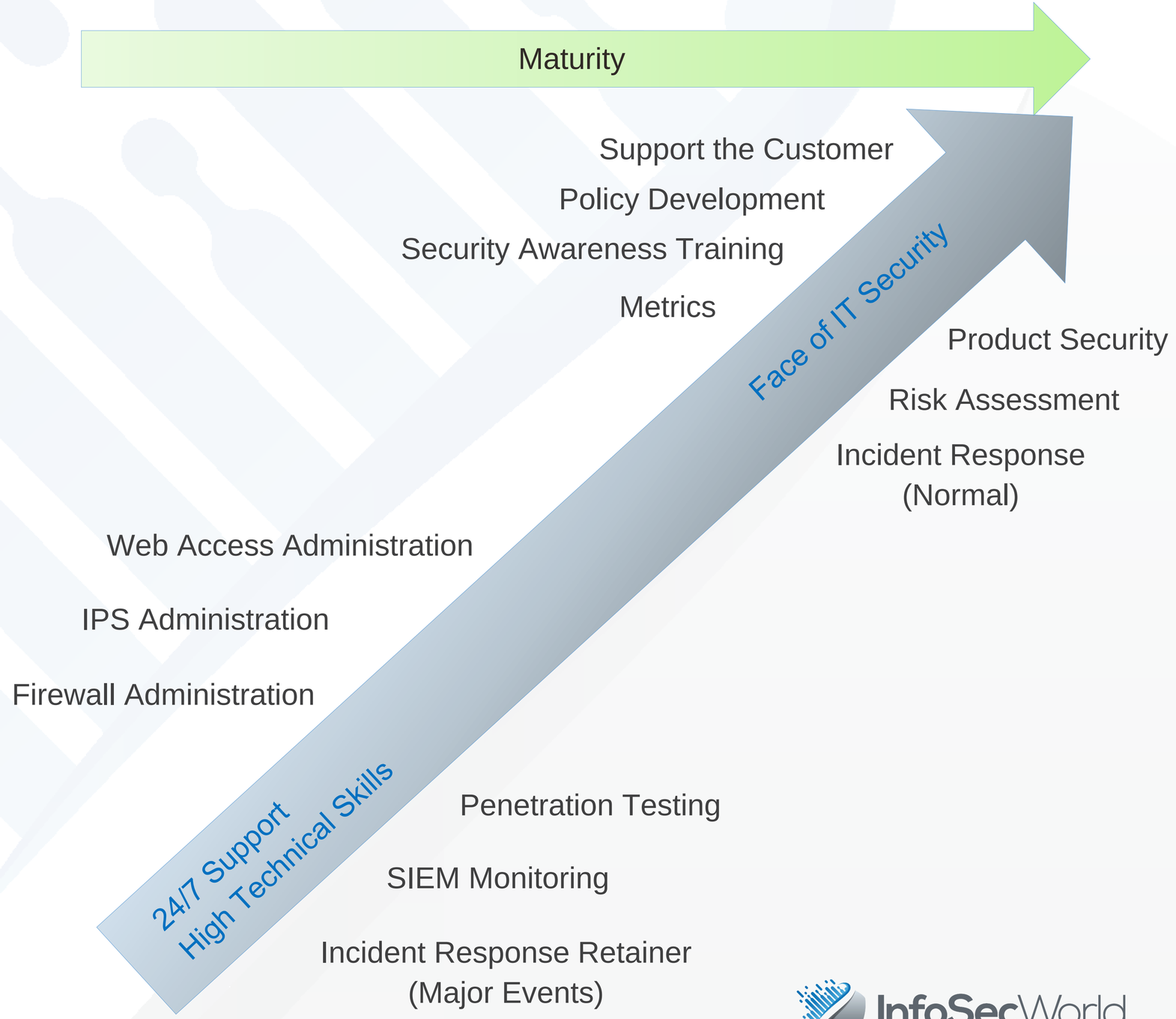
- Prioritizing
- Influencing Change
- Enabling the Business
- Senor Management knows you

Value of the Outsourced

- Frees your time
- 24/7 coverage
- Specialized skills

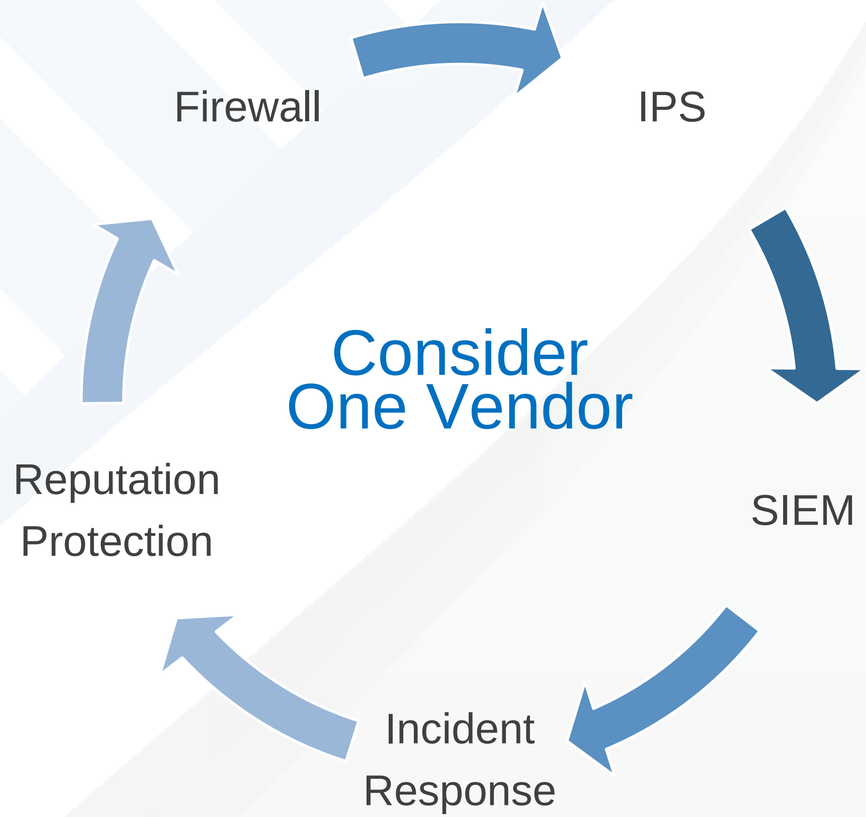
Can be outsourced to internal teams

Get the buy in from your team – how does it make them more valuable



OUTSOURCING CONSIDERATIONS

- Consider synergies when outsourcing
  - Firewall Management
  - SIEM Management
  - IPS Management
  - Incident Response
  - Reputation Protection
- Consider keeping separate
  - Penetration testing



ARE YOU INDISPENSABLE?

KNOW YOUR STAKEHOLDERS

To make stuff that matters, you have to know what matters so work on solving the right problems.

- 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

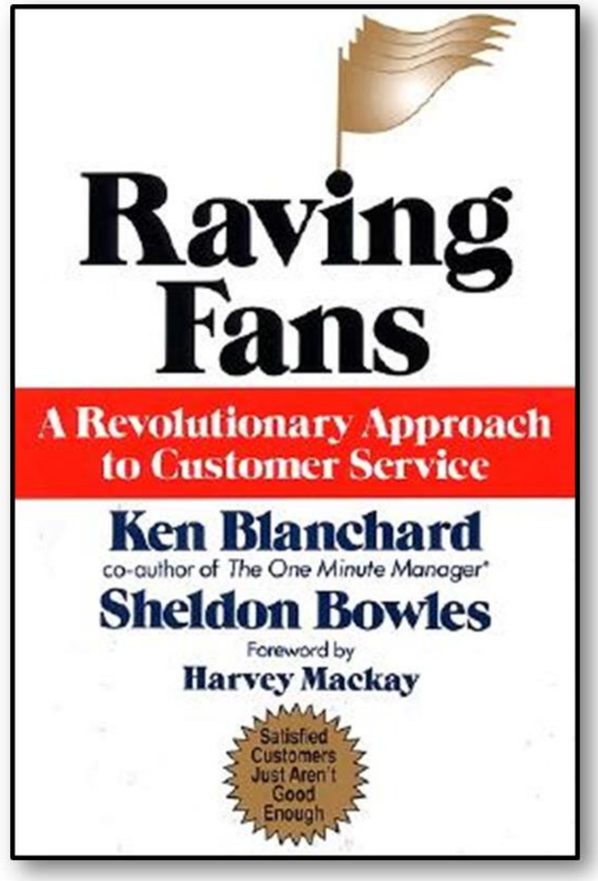
"No one cares what you know until you show them how much you care"

Effective managers take the time to identify stakeholders and know their pain points.

CUSTOMER SERVICE

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 subjects 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

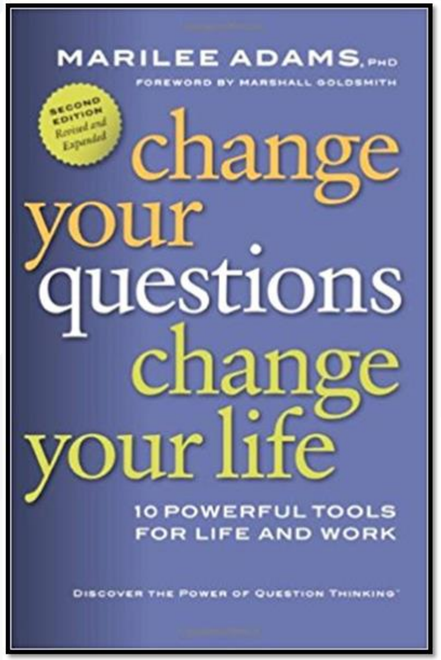


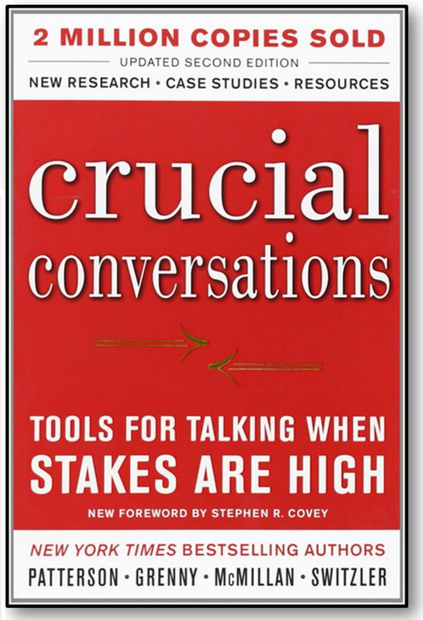
“The day people stop bringing you their problems is the day you have stopped leading them” - Colin Powell

JUST SAY MAYBE

Effective leadership requires collaboration and empathy for the other person.

- Security has often been the Department of “No”
- Taking a hard stance as a “cyber policeman” can seem to work…until you become perceived as an obstacle
- If you are an obstacle, process will begin to be routed around you





It’s OK to be uncomfortable with the results

BE PROACTIVE

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”

CONCLUSION

- Even small teams can make a big difference
- Tell your story using metrics
- Embrace Lean
- Outsource the day-to-day so you can add value
- Increase your value

MIS|TI™ PRESENTS

InfoSec World

Conference & Expo 2018

THANK YOU

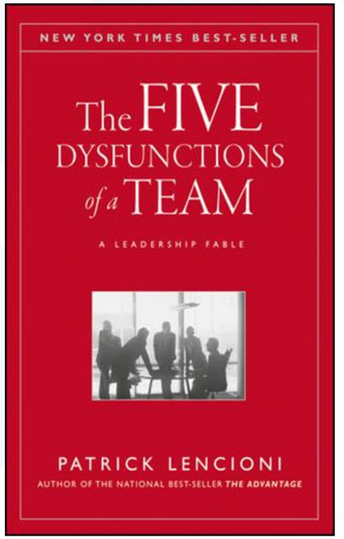
PLEASE FILL OUT YOUR EVALUATIONS!

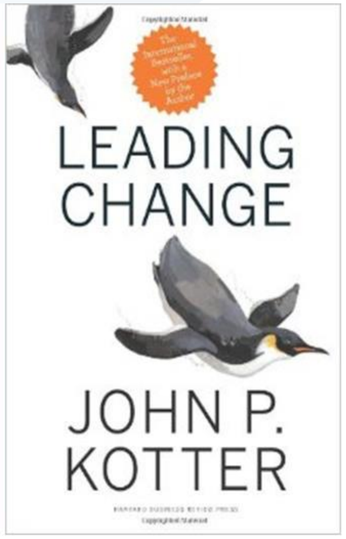
Jack Nichelson & Ed Pollock

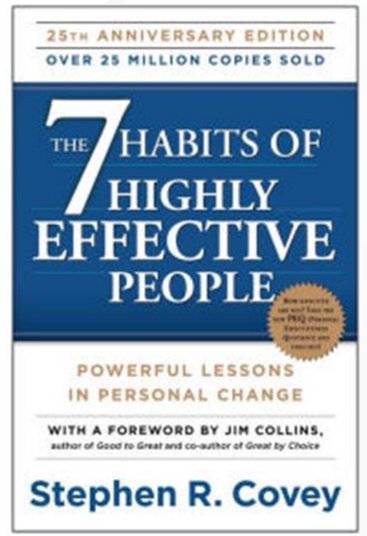
APPENDIX

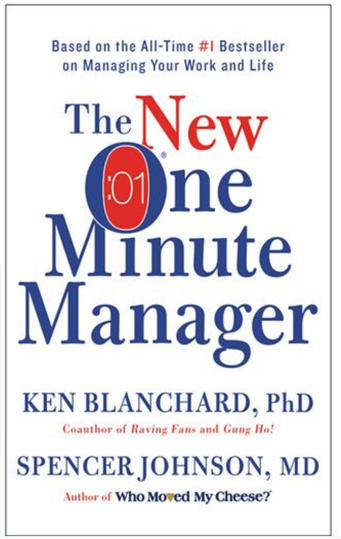
BOOK REFERENCES

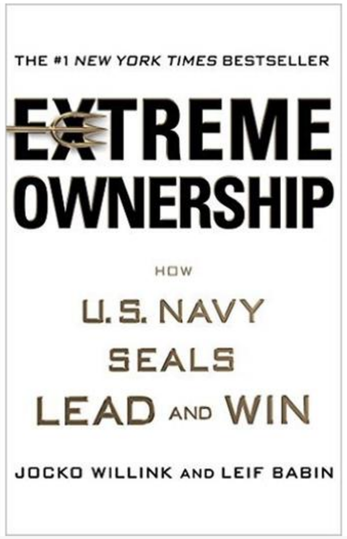
- **The Five Dysfunction of a Team** – Patrick Lencioni
- **Leading Change** – John Kotter
- **The 7 Habits of Highly Effective People** – Dr. Covey
- **The 1 Minute Manager** – Ken Blanchard
- **Extreme Ownership** – Jocko Willink
- **The Phoenix Project** – Gene Kim
- **What got you Here won't get you There** – Gooldsmith
- **Leaders Eat Last** – Simon Sinek
- **The Ideal Team Player** – Patrick Lencioni
- **Death by Meeting** – Patrick Lencioni
- **Everything I Know About Lean I Learned in the First Grade** – Robert Martichenko

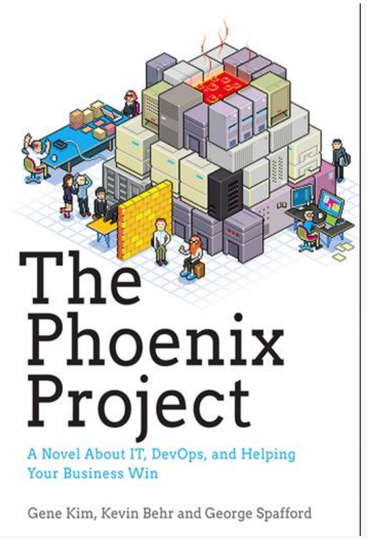










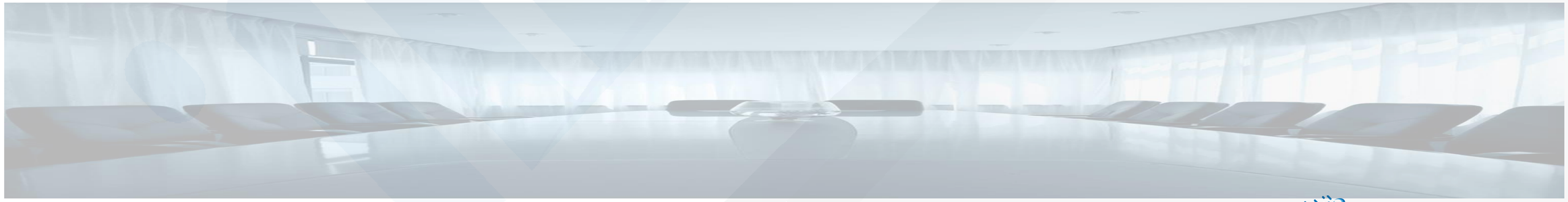


NETWORK

- No time like the present to put your soft skills to work
- Say hi to your neighbor…how can you help each other?

WHY METRICS

- Can only **improve** what you can **measure**
- Without measurement, security is purely **artistry** and **witchcraft**
- Because security wants a **seat at the big table**
  - *Business units that report to the board will have some way to demonstrate their performance*
- Because you need to know **what's working**, and what needs your attention
- Because you want to **buy more security toys** next year
- Because you want to **add more staff**



HOW WE'VE USED THEM

- **Drive** team performance
- **Explain** security to the board
- **Justify** past expense
- **Justify** FUTURE expense
- Keep myself **honest**

- **Influence** change…even with Marketing
- **Converse** with the CEO
- **Explain impact** of Acquisitions on our security posture
- **Built** a culture of security in other IT departments
- **Focus** the department's efforts

IMPLEMENTING LEAN IN IT

- SQDC (Safety, **Q**uality, **D**elivery, **C**ost) Board
  - Highlight your metrics
  - Shows trends
  - Kaizen Newspaper
  - Start with one board & expand from there
  - Put your energy with the believers…the others will come along
- Lean Steering Committee
  - Champions
  - Senior Leadership Sponsor
  - Partner with Lean/CI Department (if you have one)
- But your energy into the supporters not the detractors (they will come around)

SQDC BOARDS

The Rows

- Top Row – Trend for year
- Second Row – Trend for Month
- Third Row – Pareto chart on causes
- Forth Row – Kaizen Newspapers explaining what is being done to improve

Don’t be a hardliner…experiment & do what works for you

	5S	SAFETY	QUALITY	DELIVERY	COST
Individuals in the department enter data based on their responsibility and the metric	Average Site 5S Score	Site Safety Cross	Trend Chart for Quality	Trend Chart for Delivery	Trend Chart for Cost
		Trend Chart for Safety	Current Month Data for Quality	Current Month Data for Delivery	Current Month Data for Cost
Individuals in the department with Lean Champion guidance determine the root	Pareto SQDC scores by area	Safety Misses - Paretos by Root Cause	Quality Misses - Paretos by Root Cause	Delivery Misses - Paretos by Root Cause	Cost Misses - Paretos by Root Cause
Individuals in the department execute the countermeasure actions	5S Countermeasures	Safety Countermeasures	Quality Countermeasures	Delivery Countermeasures	Cost Countermeasures

IMPLEMENTING LEAN IN IT

- Partnering
  - Continuous Improvement Team if you have one
  - Consulting Company
  - Community College
  - Visit someone that is making the journey
- Training on Lean
- Kaizen Event
  - “Change for Better”
  - 4-5 day event to remove waste from a process
  - The problem is with the process not the people
  - Led by an experienced Lean professional
  - Participants become believers (if done right)

METRICS FOR IT

Use metrics to influence change

- Eliminate vulnerabilities
- Secure configurations
- Secure applications
- Make security a focus of ALL teams
- Accountability

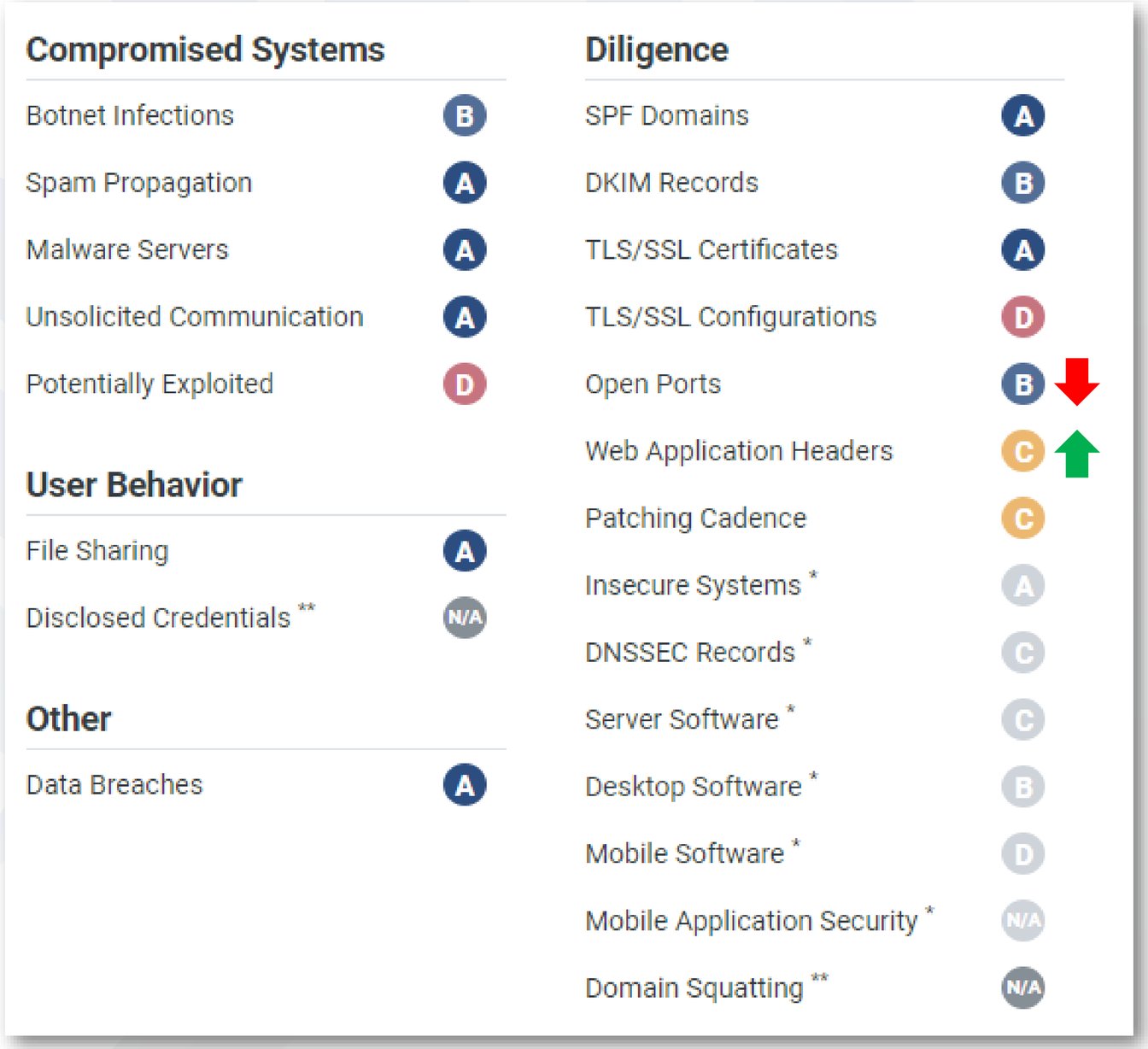
TARGET - IT

When you develop your metrics

- Use Grades - People understand & want “A’s”
- Show trends – good talking points
- Show targets – where do you want to be?

How metrics help

- Know your weaknesses
- Know where to target efforts
- Use to justify budget & change in technologies
- Near real-time alerting available when a grade changes



INCREASE YOUR VALUE

- Know the mission & support the mission
  - Do your products or brand need a security story?
  - Can you deliver fast & secure?
- Use metrics to show comparison to others
  - May not care about cyber security but do care how we compare to the competition
  - Customers seeing same scores in their Third-Party Risk Management monitoring
- Concentrate on high-value areas & outsource commodity services

WHAT TO CONTROL

Control processes that let you set direction & stop dangerous things

- Security Policy…but have to be more then paper policies
- High risk areas (firewall policy approval)
- Incident Response
- Risk Assessments