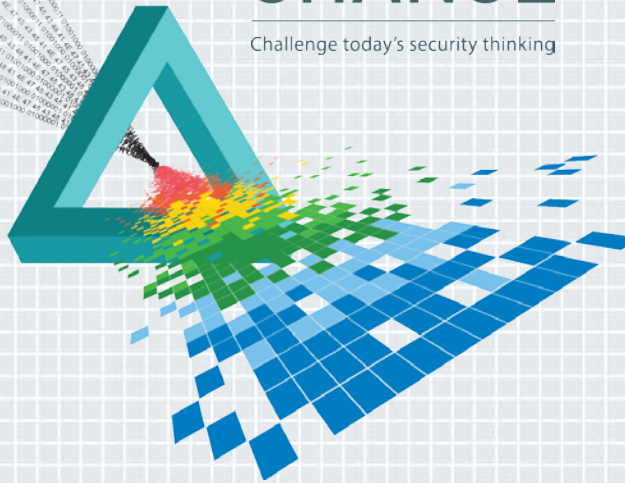
Information Security Leadership: Surviving as a Security Leader

Start Time	Title	Presenter
8:30 AM	As a New CISO – How to Assess Your Security Program for Success	Gary Hayslip
9:15 AM	Are You Fighting the Wrong Battles?	Bill Burns
9:55 AM	Being a CISO – What They Don't Tell You	Evan Wheeler, Amy Butler, Julie Fitton, Rick Howard, Jack Jones
10:30 AM	BREAK	
10:45 AM	Stepping Inside the Boardroom	Trey Ford

RSAConference2015
San Francisco | April 20-24 | Moscone Center

CHANGE
Challenge today's security thinking



SESSION ID: SEM-M02

As a New CISO – How to Assess Your Security Program for Success

Gary Hayslip

Chief Information Security Officer
City of San Diego, California
@ghayslip

As a New CISO – You'll have more questions than answers

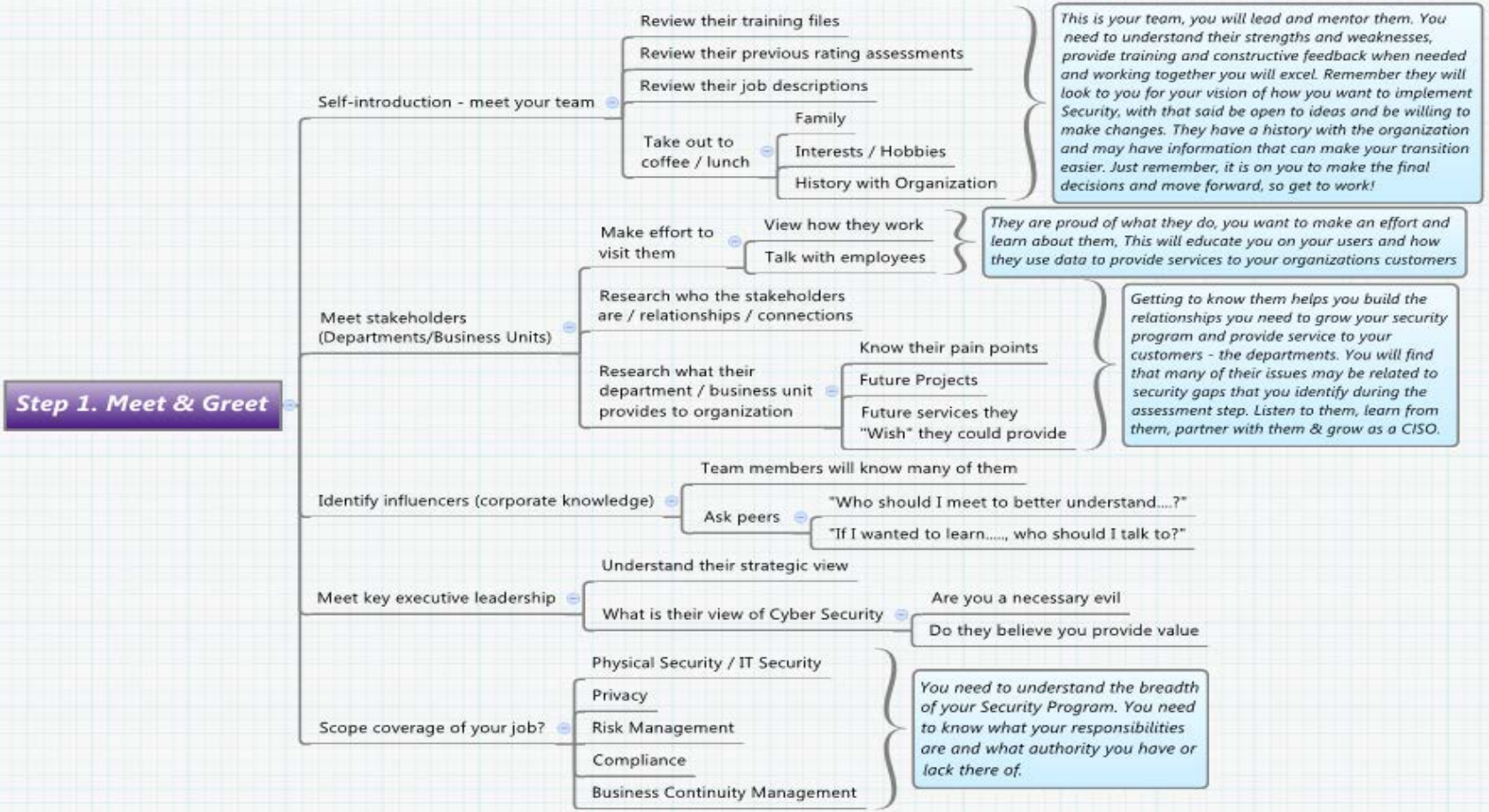
"Visibility"

“Cyber is a Business Enabler”

5 Steps I have used for Success

Step 1 – *"The Meet & Greet"*

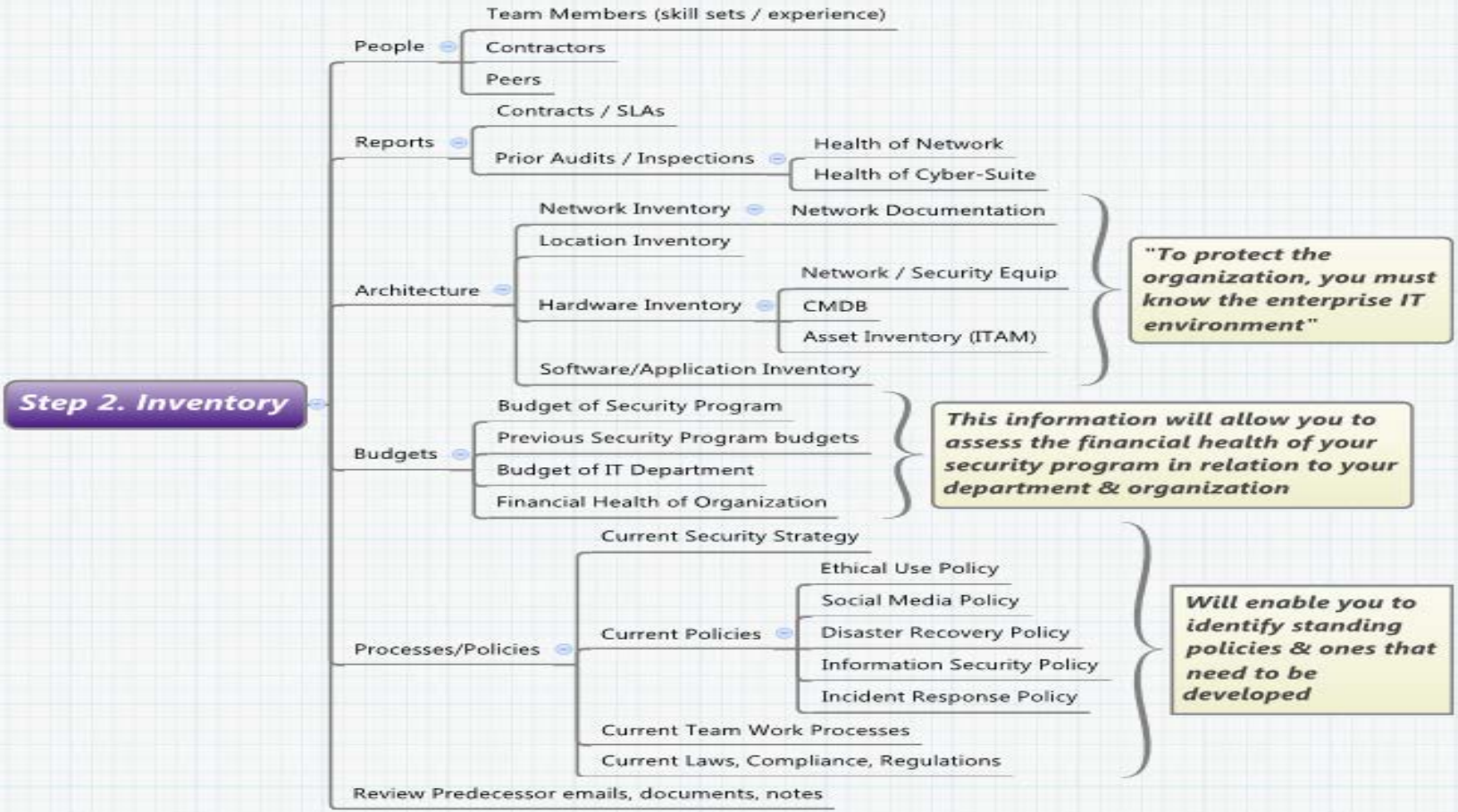
- "Security doesn't work in a Vacuum, however it works well in a Community"
  - Grow your "Human Network"
    - Meet your Team
    - Meet Your Stakeholders
    - Identify Influencers
    - Meet Key Executive Leadership
  - Know the responsibility & authority of your position
    - Sometimes its more than what you realize



https://app.box.com/RSA-CISOmindmaps

Step 2 – *"Inventory"*

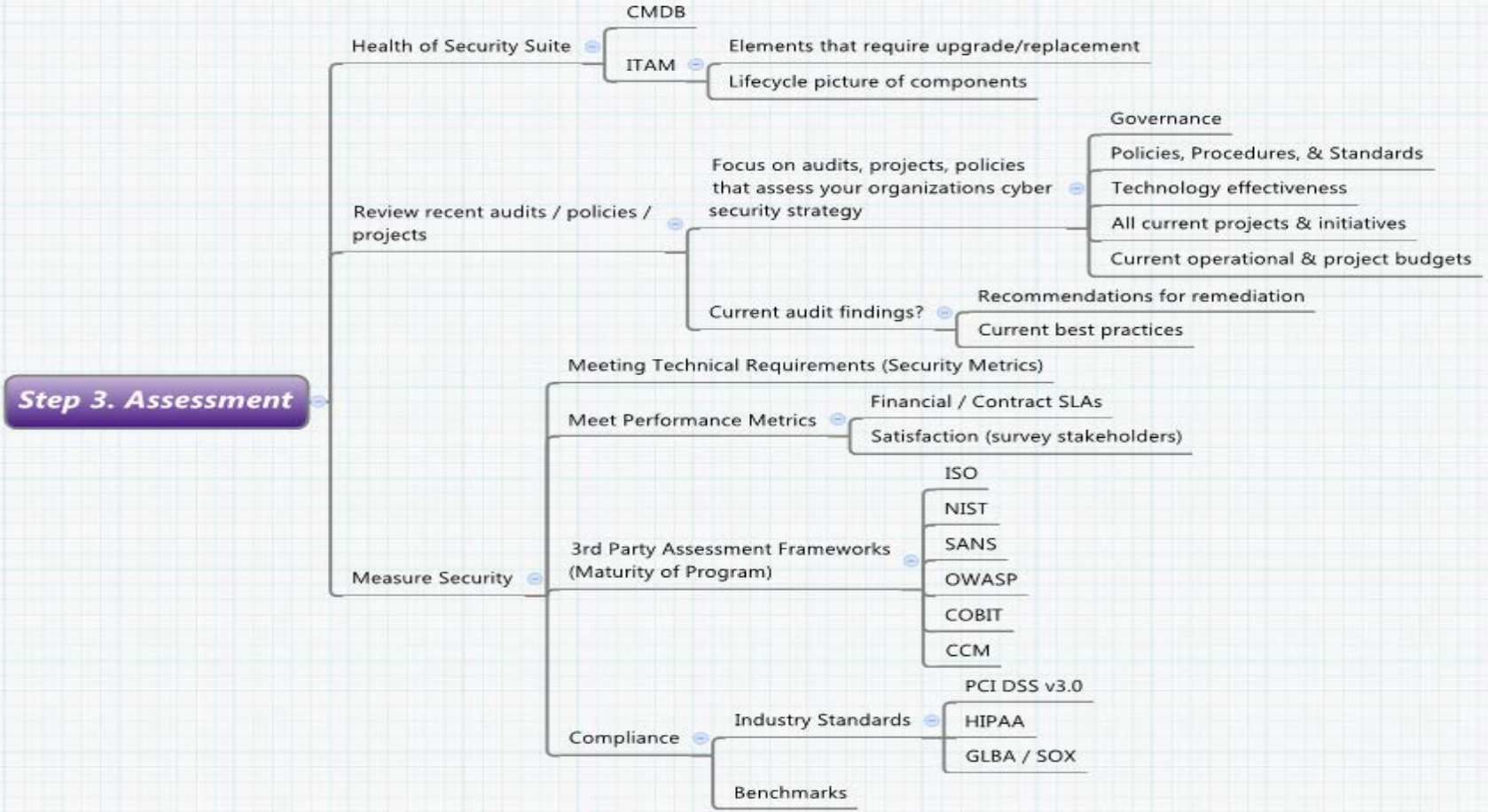
- "To protect your organization, know your enterprise environment"
  - People (Team Members, Contractors, Peers)
  - Reports (Contracts, Metrics, Prior Audits, Inspections)
  - Architecture (Network, Location, Hardware, Application, Cloud)
  - Budgets (Security Program, Department, Organization)
  - Processes & Policies
    - (Security Strategy, Policies, Workflows, Laws, Regulations, Compliance)
- Review your Predecessor's documents, emails, notes.
  - Now review their notes on your team members



https://app.box.com/RSA-CISOmindmaps

Step 3 – *"Assessment"*

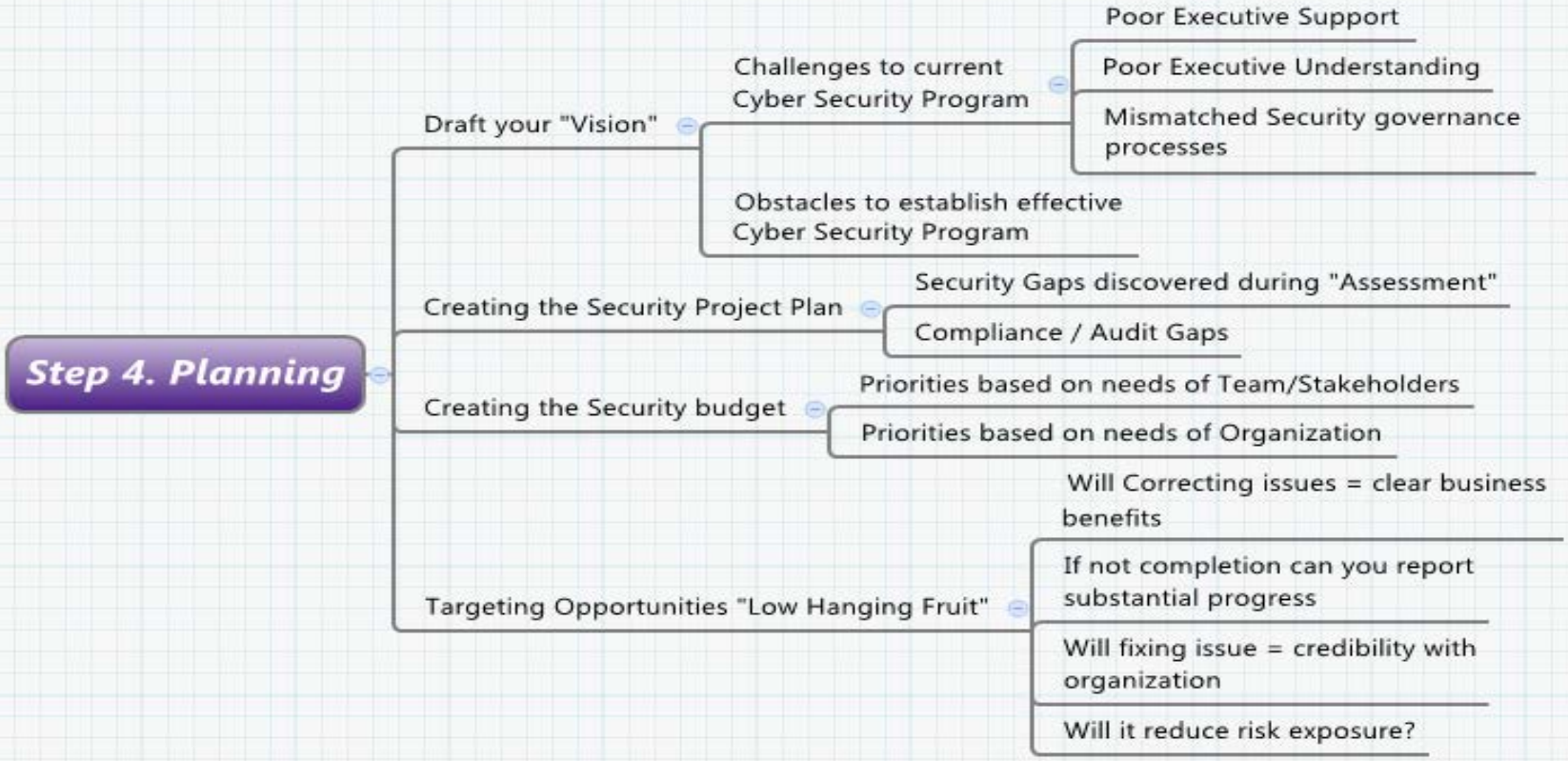
- "Continuous Assessment, establish and verify your baseline"
  - Health of your Security Suite
  - Review recent audits, policies, projects
    - Current audit findings, recommendations?
  - Measure Your Security
    - Are you meeting your security metrics?
    - Are you meeting performance metrics?
    - Are you meeting 3rd Party Assessment Frameworks?
    - Are you meeting Compliance Requirements?



https://app.box.com/RSA-CISOmindmaps

Step 4 – *"Planning"*

- "Your Security Program and Team are key to your Organization"
  - Draft your "Vision" of the Security Program
    - Challenges to the current program
  - Build your Strategic Security Project Plan
  - Use your Project Plan to build your Security Budget
  - Start Immediately (Momentum is key)
    - Will Correcting Issues = Clear Business Benefits?
    - Reduce Risk Exposure?
    - Will Fixing the Issues = Credibility for your Team?



https://app.box.com/RSA-CISOmindmaps

Step 5 – *"Communicate"*

- "Visibility = Executive Sponsorship = Budget"
  - Socialize your Security Vision
    - Vision = "Where we want to be"
    - Assessment = "Where we currently are"
    - Gap Analysis = (Vision – Assessment)
    - Gap Analysis = Strategic Security Project Plan = Security Budget
  - Socialize the Security Gap
    - Correcting findings brings value to the business

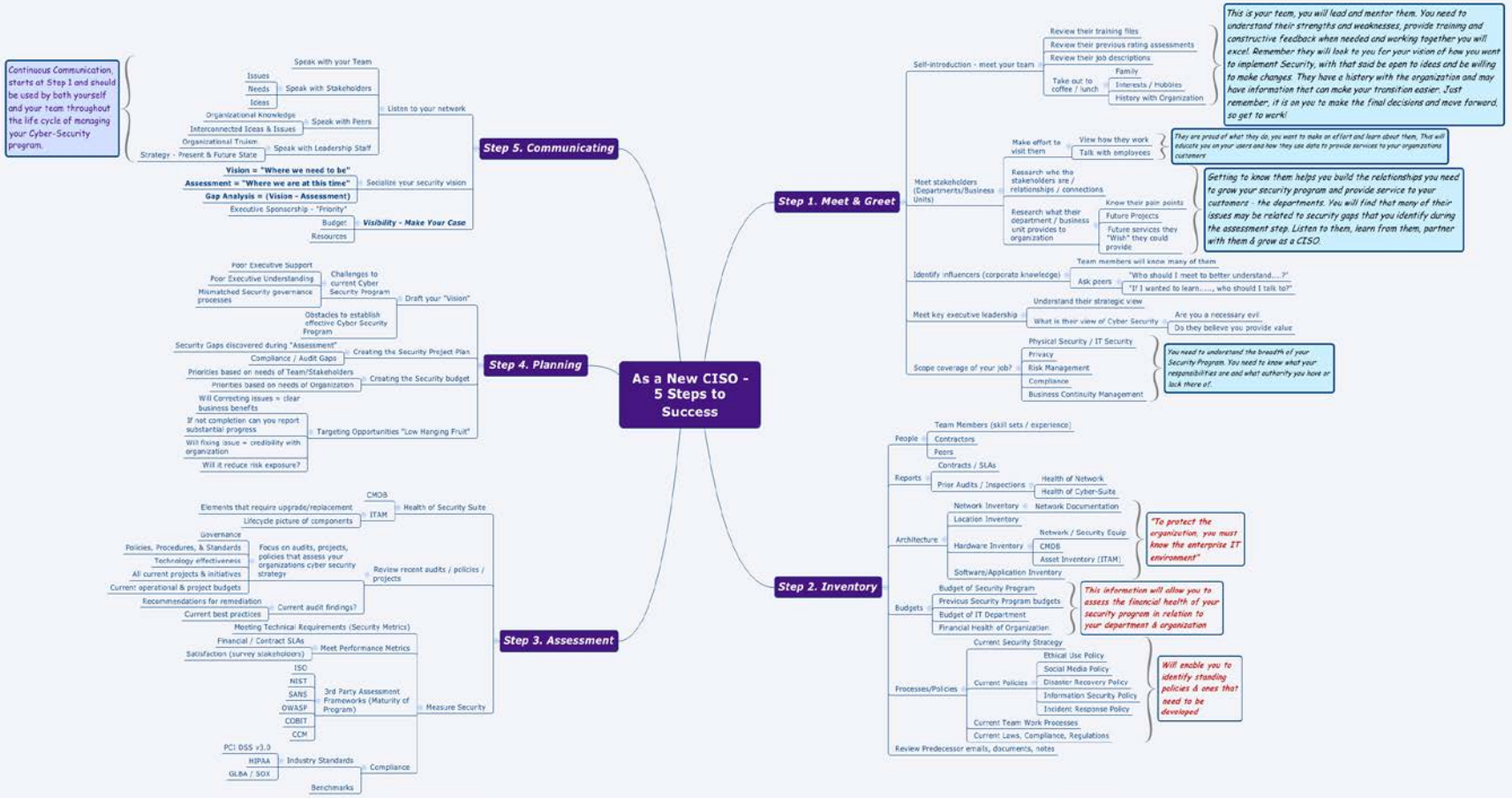
https://app.box.com/RSA-CISOmindmaps

Some points to remember

- You will be collecting and reviewing an enormous amount of data
  - This will take time, normally between 3-6 months
- Leverage your “Human Network”
  - Use your team, your peers, and stakeholders
  - Don’t be afraid to ask for help
- Share your information
  - Visibility is crucial for your Team and Security Program

Conclusion

- At the end of this 3-6 month journey, you will have:
  - A “Human Network” to help you drive Cyber in your organization
  - An updated Inventory of your Organizations Enterprise IT assets
  - You will know the maturity of your Security Program and your assessment baseline
  - You will have created your Strategic Security Project Plan
  - This plan will help you create your Security Program budget
  - Better understanding of how “Cyber = Business Value”
- So did you miss anything?
- When You get home, what are you going to verify?



https://app.box.com/RSA-CISOmindmaps

“Cyber, its all about the maybe”

Questions?

Gary Hayslip

ghayslip@gmail.com

@ghayslip

www.linkedin.com/in/ghayslip/

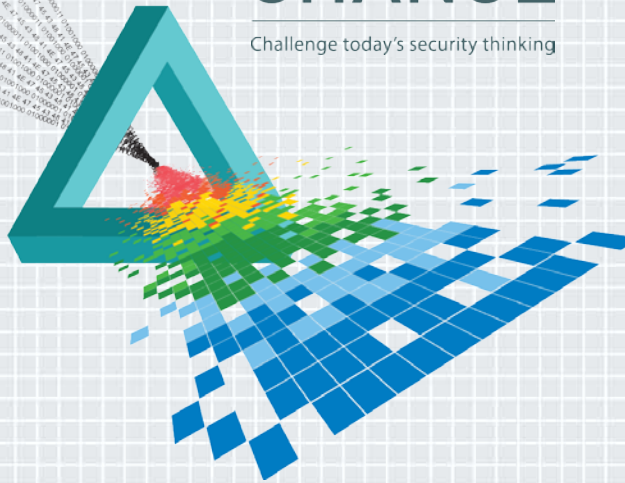
https://app.box.com/RSA-CISOmindmaps

Information Security Leadership: Surviving as a Security Leader

Start Time	Title	Presenter
8:30 AM	As a New CISO – How to Assess Your Security Program for Success	Gary Hayslip
9:15 AM	Are You Fighting the Wrong Battles?	Bill Burns
9:55 AM	Being a CISO – What They Don't Tell You	Evan Wheeler, Amy Butler, Julie Fitton, Rick Howard, Jack Jones
10:30 AM	BREAK	
10:45 AM	Stepping Inside the Boardroom	Trey Ford

RSAConference2015
San Francisco | April 20-24 | Moscone Center

CHANGE
Challenge today's security thinking



SESSION ID: SEM-M02

Are You Fighting the Wrong Battles?

Bill Burns

VP, CISO
Informatica Corp.
@x509v3 | Bill.Burns@informatica.com

My Background

- Current: VP, CISO @ Informatica
  - New ISO27k security/compliance program, new security product line, culture of security
- My previous lives:

  - Investing in InfoSec – Building VC Security Investment Thesis
  - Democratizing Trusted Cloud Security – AWS CloudHSM
  - Architecting, Building and Operating Security @ Scale

Why Are We Here?

- Who are you fighting for?
  - Shareholders, Owners
  - Employees, Teammates
  - Customers, Constituents
- Why do *you* do this job?!?
  - The Challenge, A Puzzle
  - Protecting Others
  - Sense of Duty, What's Right

As A Security Leader, You Are Fighting for

- Corporate Budget
- Skilled Resources
- Employees' Attention
- Raising The Security Bar On Your Watch
- Improving The Security State Of The Art

… Relevance

Frames of Reference — Being Relevant

1. **Risk** vs. Threats
2. **Data** vs. Opinion
3. **Relationships** vs. Transactions
4. **Business Impact** vs. Business Disruption
5. **Systems** vs. Tasks
6. **Security** vs. Compliance
7. **Value** vs. Cost
8. **Efficiency** vs. Effort
9. **Results** vs. Effort
10. **Being Heard** vs. Talking
11. **Feedback loops**

Risk vs. Threats

- Risk ~= Vulnerabilities * Threats * Impact
- You do not control **threats**
  - What the attackers could do
- You do have (some) control over **impact**, **vulnerabilities**:
  - Patching effectively
  - Incident response capability
  - Regular response plan testing
- **Focus on what you can control, being prepared**
  - Helps your program be seen as Being Proactive vs. Reactive

Data vs. Opinion

- Ask yourself: “Who has better data about this situation?”
  - Have fact-based conversations

1. Establish hypotheses
2. Run experiments to gather data (“A/B Tests”)
3. Measure results
4. Prove / Disprove your theories
5. Make decisions to improve security
6. Rinse, repeat

Relationships vs. Transactions

- Move beyond transaction-based personal interactions
- Industry and Peer benchmarks are powerful leverage
  - Establishes a neutral or trusted third-party, external expertise
  - Removes emotion, subjectivity
  - Ponemon, Gartner, Forrester, WiseGate, peers, etc
- Build & Maintain Relationships … With Your Security Peers
  - Salaries, Budgets, Product Reviews, Training, Feedback, Sanity :)
- … With Your Company's Peers
  - Pre-wiring meetings, Your Program's Support, Their Program's Support

Business *Impact* vs. Business *Disruption*

- Business Disruption:
  - Applying OS patches typically requires reboots
  - Critical infrastructure patches lowers availability
  - Pay down technical debt means we can't ship the new features
- Business Impact:
  - Compare security posture, features to your peers, industry benchmarks
  - Security can be a competitive differentiator, or a "must do", not a tax
  - Use events like "What if we had the same thing happen to us…?"
  - Speak to the business impact, not the technical details
  - Get this on record, have this conversation, build your case

Systems & Programs vs. Tasks

- We know security is an ongoing process, not a task or one-time checklist
- Task-focused security appears never-ending
  - Hard to show return on investment, results for effort
  - Minutiae obscures the value of security from project-level work
- Focus on higher-level metrics, regular cadence, objectives, accountability
- Build repeatable processes, automation, Programs
- Focus on what you can control
- Follow program management guidelines, best practices
  - Charter, Goals, Sponsorship, Metrics, Review, Cadence, RACI

Systems & Programs vs. Tasks (II)

- Example: Patching, Vulnerability Management is hard work. Never “done”.
  - Filing individual vulnerabilities & issues is not sustainable
  - Pre-wire conversations ahead of review meetings to re-affirm expectations, address concerns
  - Establish regular cadence with stakeholders to build accountability, credibility, measure progress
  - Prioritize the risk of what’s discovered, enabled
- Measure efficacy and efficiency, not effort
  - Move beyond “numbers of criticals”
  - Report “time to close” critical vulnerabilities
  - Not “100% patched”, but “close critical vulns within 2 days of release”
- Goal: Sustainable Security Programs

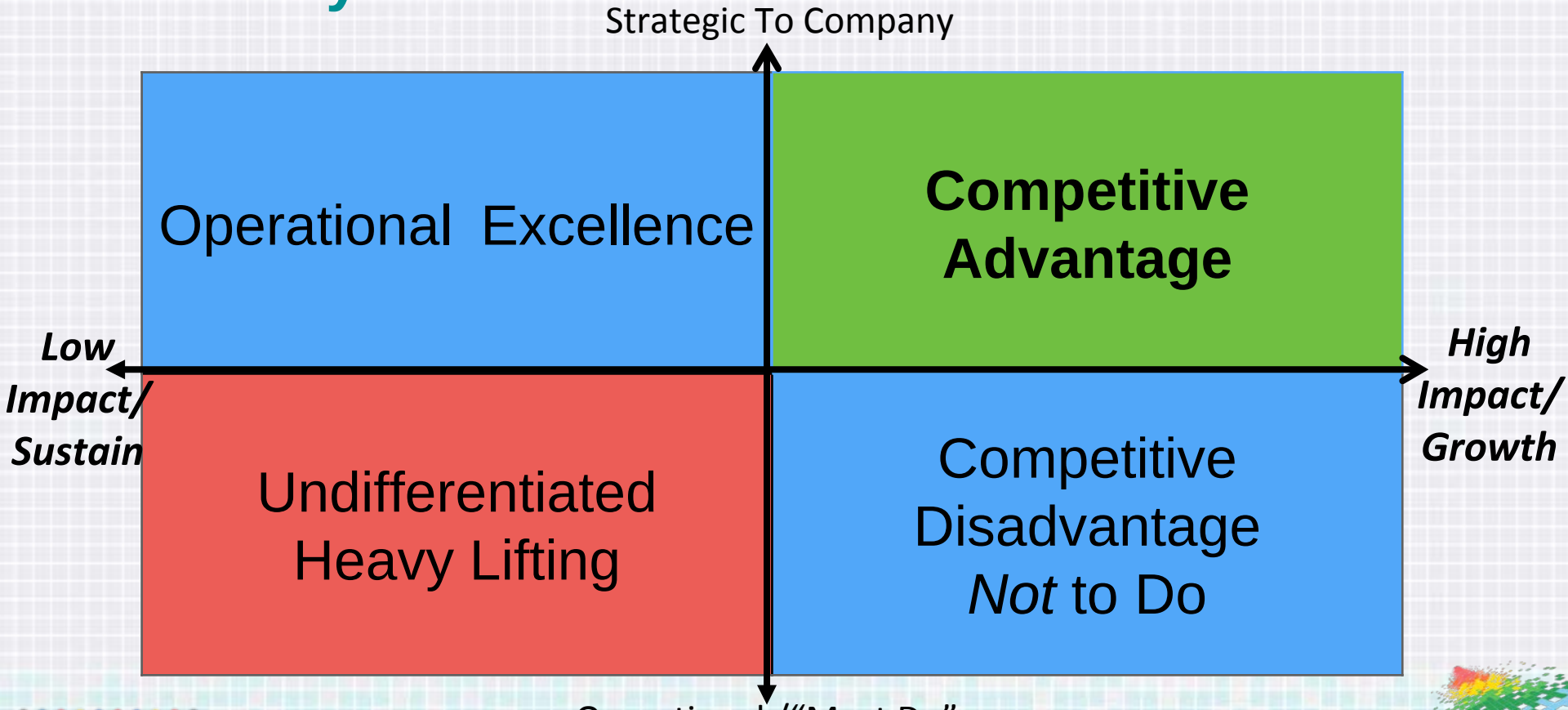
Security vs. Compliance

- Focus on solid security foundations
- Compliance will come along for the ride
  - “Say It” – Policies
  - “Do It” – Procedures & Guidelines
  - “Prove It” – Generate evidence to review
- Many standards, pick the best match for your company
- Already started with Compliance? Expand into Good Security

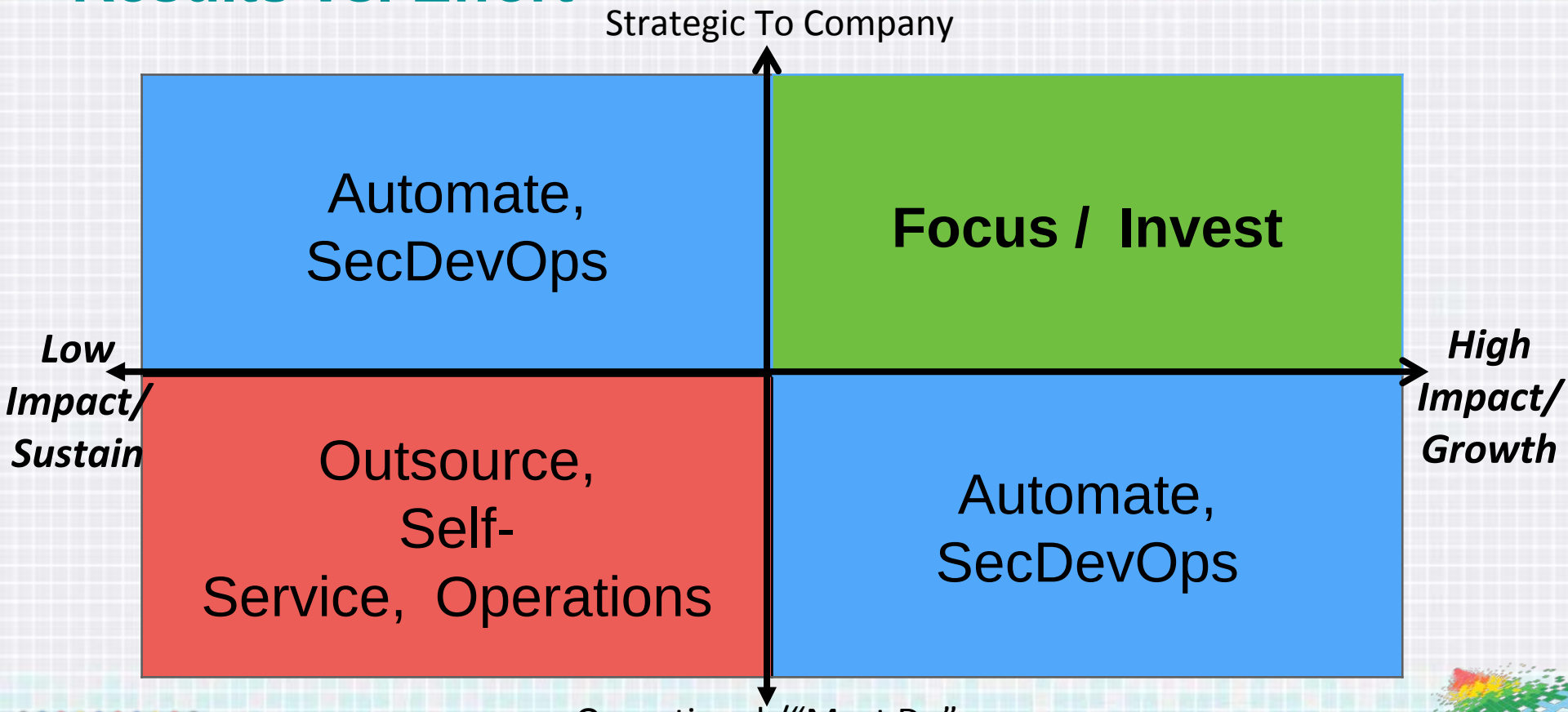
Assess once, comply many

Controls:	ISO 27000	SOX	GLBA	HIPAA	US-EU Data Privacy
Security Policy	✓	✓	✓	✓	✓
Organization of InfoSec	✓	✓	✓	✓	✓
Human Resource Security	✓			✓	✓
Asset Management	✓				
Access Control	✓	✓	✓	✓	✓
Cryptography	✓			✓	✓
Physical & Environmental	✓	✓		✓	✓
Operations Security	✓	✓		✓	✓
Communications Security	✓	✓	✓	✓	✓
System Acq, Dev & Maint	✓	✓	✓	✓	✓
Supplier Relationships	✓	✓	✓	✓	✓
InfoSec Incident Management	✓		✓	✓	✓
Business Continuity	✓	✓	✓	✓	
Compliance	✓	✓	✓	✓	✓

Efficiency vs. Effort



Results vs. Effort



Communicating vs. Talking

- Security is about influencing, selling, advising
- Communications is what The *Receiver Does*
- To be heard, use *their* vocabulary
- To be effective, use *their* communications vehicle
  - Avoid “Impedance Mismatches”
  - Operations: Change Requests & Tickets
  - Engineering: Bug Reports, Feature Requests
  - Automate filing audit tasks via your ticketing system
  - Create User Stories for desired security features

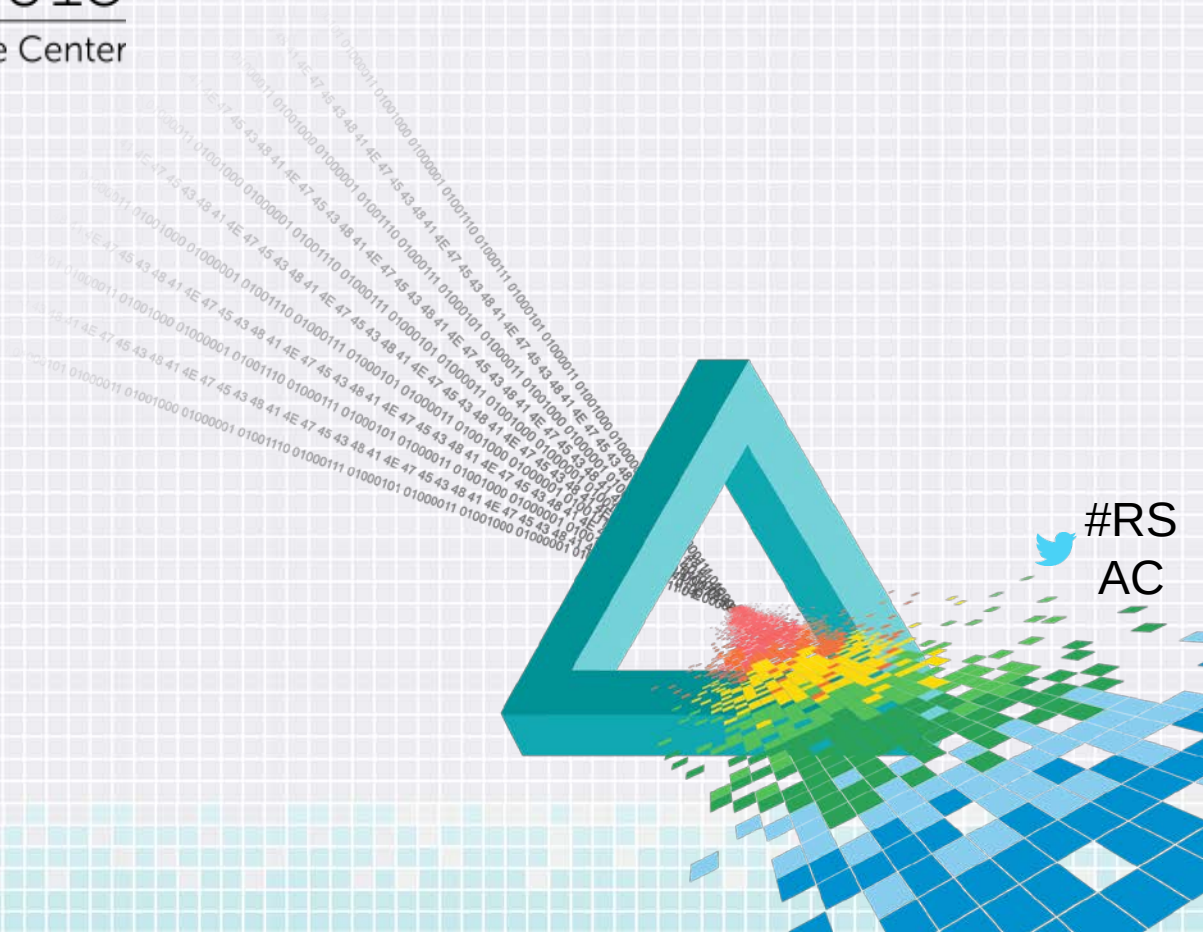
Feedback Loops

- Putting it all together …

- Create tight feedback loops with your stakeholders
  - Builds relationships, trust
  - Require metrics, measuring the Right Things
  - Establish data-based decision making
  - Reinforce / disprove your hypotheses
  - Increase your security velocity
  - This encourages Results, incremental improvements

RSAConference2015

San Francisco | April 20-24 | Moscone Center



#RS
AC

Recap

It's All About Results. Do The Following:

- By Next Week
  - Time map: Evaluate where [you | your team] is spending its energy
  - Take your [CIO | Operations Peer | Engineer Peer] to lunch
- With Next Quarter
  - Assess what metrics are truly impactful. Eliminate the rest.
  - For a month, measure your time-to-remediate vulns on one critical system or subnet
  - Identify 3 repeatable tasks you can automate
- By the End of This Year
  - Take your [General Council | Chief Product Officer | etc] to lunch. Share top metrics.
  - Automate at least 2 repeatable audit or security tasks
  - Create 1+ feedback loop on a task with your Operations or Engineer peer

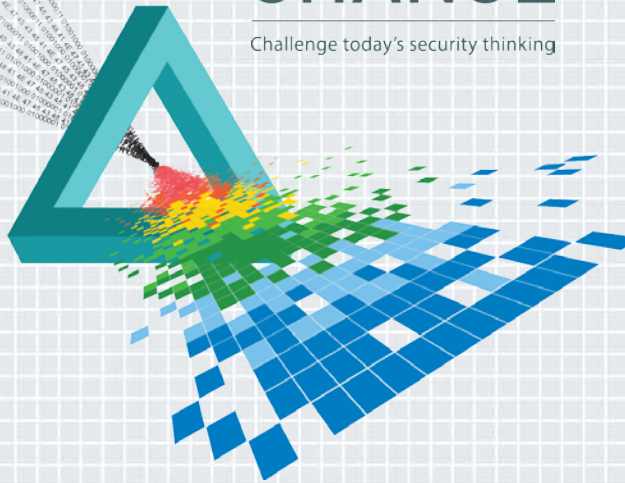
Information Security Leadership: Surviving as a Security Leader

Start Time	Title	Presenter
8:30 AM	As a New CISO – How to Assess Your Security Program for Success	Gary Hayslip
9:15 AM	Are You Fighting the Wrong Battles?	Bill Burns
9:55 AM	Being a CISO – What They Don't Tell You	Evan Wheeler, Amy Butler, Julie Fitton, Rick Howard, Jack Jones
10:30 AM	BREAK	
10:45 AM	Stepping Inside the Boardroom	Trey Ford

RSAConference2015
San Francisco | April 20-24 | Moscone Center

CHANGE
Challenge today's security thinking

SESSION ID: SEM-M02



Being a CISO – What They Don't Tell You

Evan Wheeler - Moderator

Amy Butler
George Washington University

Julie Fitton
EMC Rubicon Cloud Services

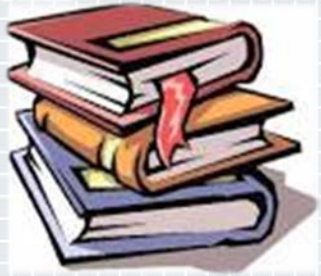
Jack Jones
CXOWARE

Rick Howard
Palo Alto Networks

Architect?

Police?

Everything



Lawyer?

Politician?

Apply Slide

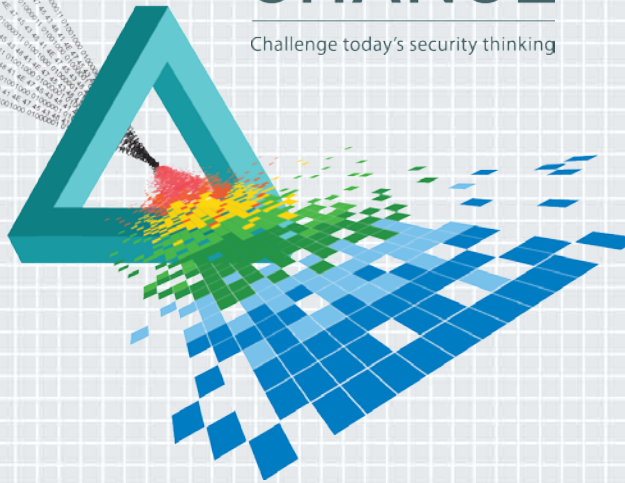
- Develop your team's culture to match the business, not as a sub-culture of security
- Should set aside time for strategic planning
- To be successful, you must be able to keep people calm, shield your team from pressures, and handle the stress yourself
- Developing and maintaining strong peer networks is key
- You must get comfortable "living in the grey"
- Educate yourself about the business

Information Security Leadership: Surviving as a Security Leader

Start Time	Title	Presenter
8:30 AM	As a New CISO – How to Assess Your Security Program for Success	Gary Hayslip
9:15 AM	Are You Fighting the Wrong Battles?	Bill Burns
9:55 AM	Being a CISO – What They Don't Tell You	Evan Wheeler, Amy Butler, Julie Fitton, Rick Howard, Jack Jones
10:30 AM	BREAK	
10:45 AM	Stepping Inside the Boardroom	Trey Ford

RSAConference2015
San Francisco | April 20-24 | Moscone Center

CHANGE
Challenge today's security thinking



SESSION ID: SEM-M02

Stepping Inside the Boardroom

Trey Ford

Global Security Strategist
@Rapid7
@treyford

Agenda

- Introductions
- Boardroom Disciplines
- The Security Executive's Challenges
- The Obvious Questions
- Affecting Change – Rapid7 Research Project

Introductions - Me

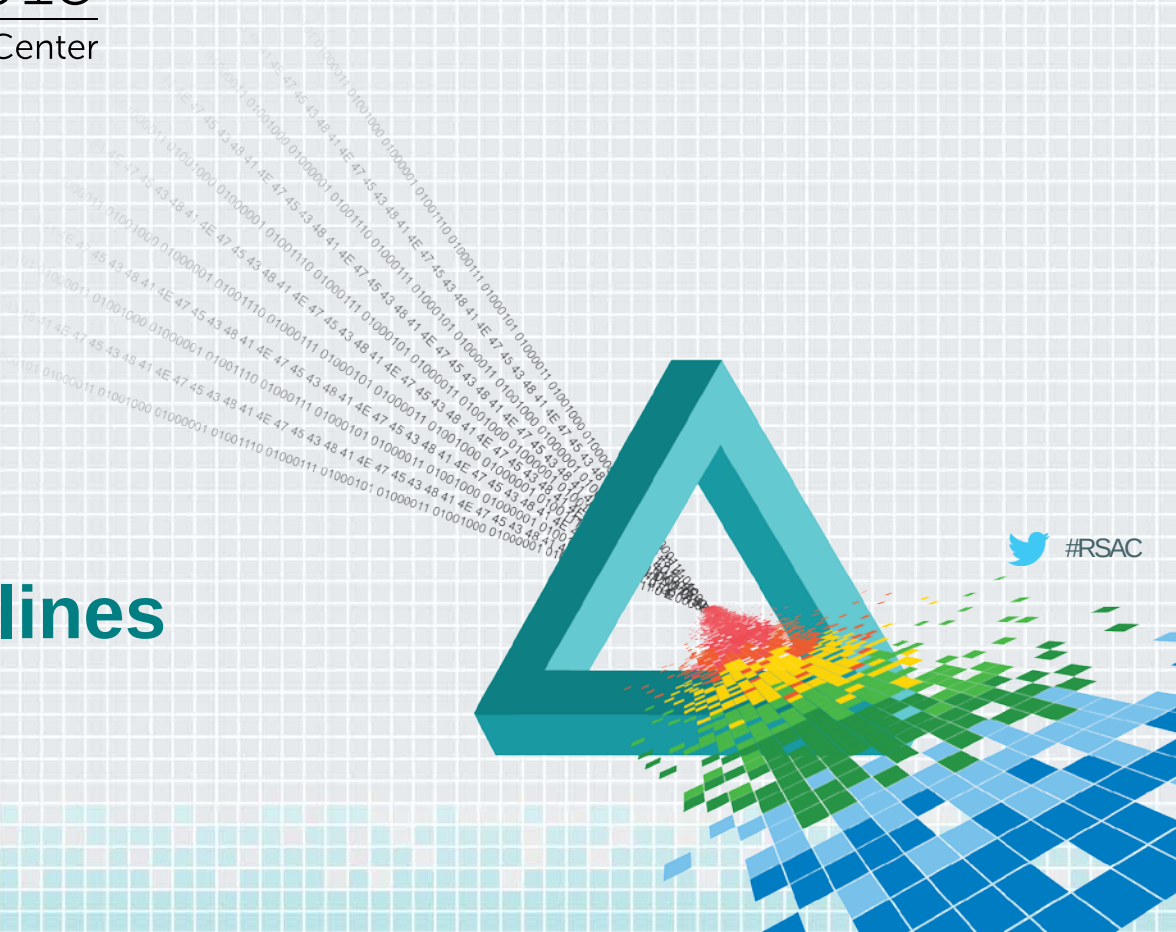
- Trey Ford, Global Security Strategist
  - Industry Advocate, Community Outreach, Spokesperson at Rapid7
  - Former GM at Black Hat, IR at Zynga, PM at McAfee, WhiteHat Security
  - Earned a gold star on a science project

Introductions - You

- What generation CISO are you?
- Board Presentations – have you given one?
- What kind of board are you preparing for?

RSAConference2015

San Francisco | April 20-24 | Moscone Center



Boardroom Disciplines

Established Professions

- Medicine
- Law
- Engineering
- Accounting

Boardroom Technology

NCR – 1884

IBM - 1911

RSAConference2015

San Francisco | April 20-24 | Moscone Center

The Security Executive's Challenges

Information Security

No Real ‘How To” Guide

Security Status Report

- Accounting has their GAAP
- Legal and Medicine has theirs
- What about Information Security?

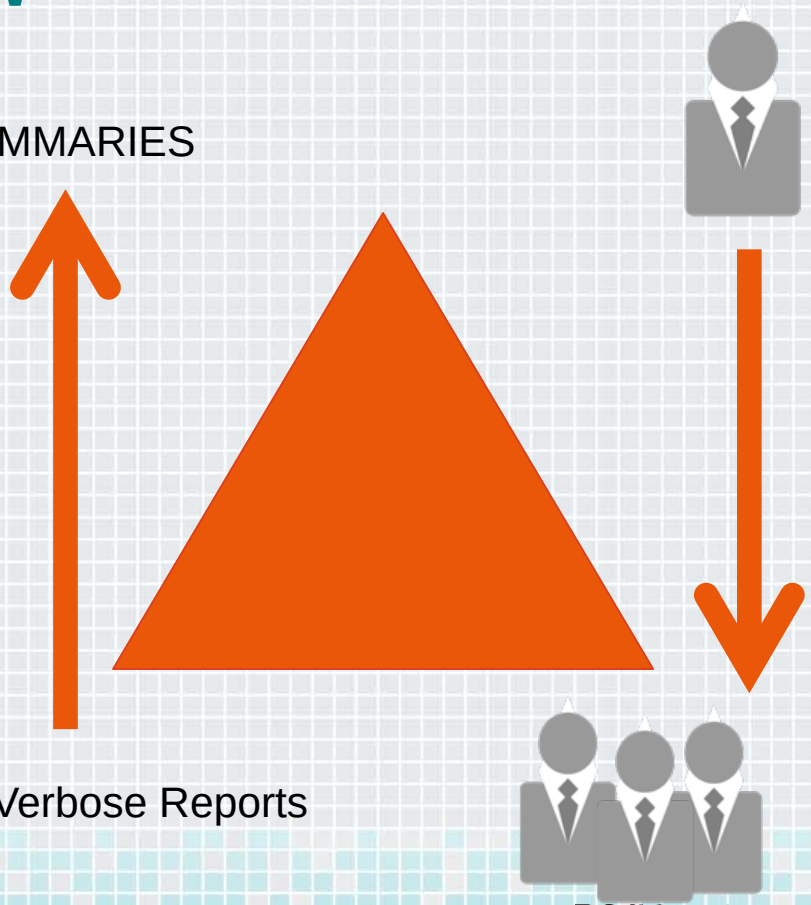
Communication Flow

WISDOM

KNOWLEDGE

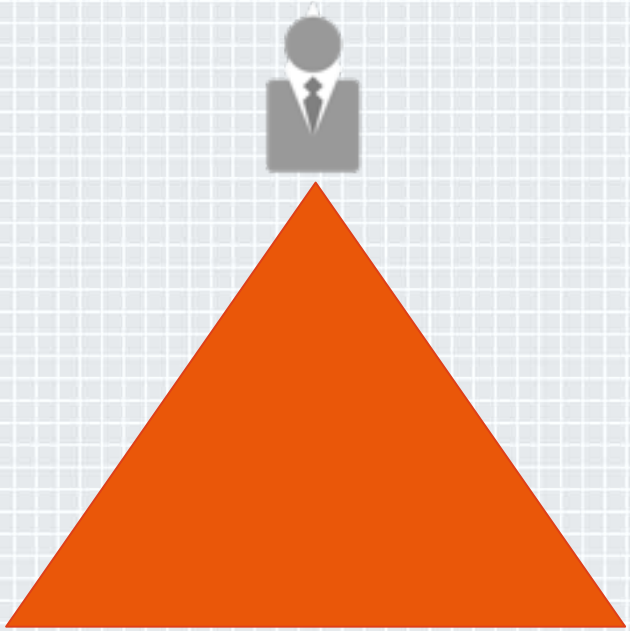
INFORMATION

DATA



Curse of Knowledge

- **Uncertainty at the Top**
  - Executives are Comfortable
  - Engineers are NOT Comfortable
- **The Secret**
  - Helping inform a point of view
  - The idea may be right or wrong



Vulnerability & External Audit Reports

BURY THEM!?!?!

Incidents Happen

- Unsafe to Discuss?
- Acknowledge bias:
  - Prevention vs. Response

Activating Incident Response

- Admitting Failure?
- Insurance Policy?

RSAConference2015

San Francisco | April 20-24 | Moscone Center

#RSAC

Asking the Obvious Questions

Obvious Questions

- Executive interactions must always answer:
  - What do I need to know?
  - Why does it matter? / What do I care?
  - What do you need from me?

- This is both SIMPLE and HARD!

Obvious Questions – know your audience

- Are you the first “CISO” to present?
- Who are you presenting to?
  - For how long?
  - How often?
- How are the CIO/CFO/GC incentivized?

Obvious Questions – soul searching

Discussing

- Unknowns
- Vulnerabilities
- Incidents

suicide or demonstration of strength?

RSAConference2015

San Francisco | April 20-24 | Moscone Center

Affecting Change: Rapid7's Research Project

Affecting Change: Expanding the Survey

- A Quantitative and Qualitative Survey
- Need > 250 CISOs and Non-Security Executives
- Takes less than 15 minutes of someone's time
- Results in an open source "Playbook" for CISOs
  - What should be reported? (Routine vs Special Requests)
  - Mapping to Common Security Frameworks

Affecting Change: Take it Yourself / Contribute

- Please take 15 minutes to complete the survey TODAY

bit.ly/CISOSurvey2015

- Then, pass it along:
  - 2 security colleagues
  - 3 non-security colleagues!

How to Apply What You've Learned

- Today you should:
  - Take Rapid7's CISO Reporting Survey
- In the next two weeks:
  - Evaluate what your teams are reporting
  - Think about how non-security executives will consume the results
  - Modify your metrics and report to focus more on business risk
- In the next 3 months:
  - Contact the consumers of your updated reports
  - Ask for feedback vs. previous months / years