

Perspectives on Cyber Confidence

Tom Podnar ---- Tom.Podnar@gmail.com

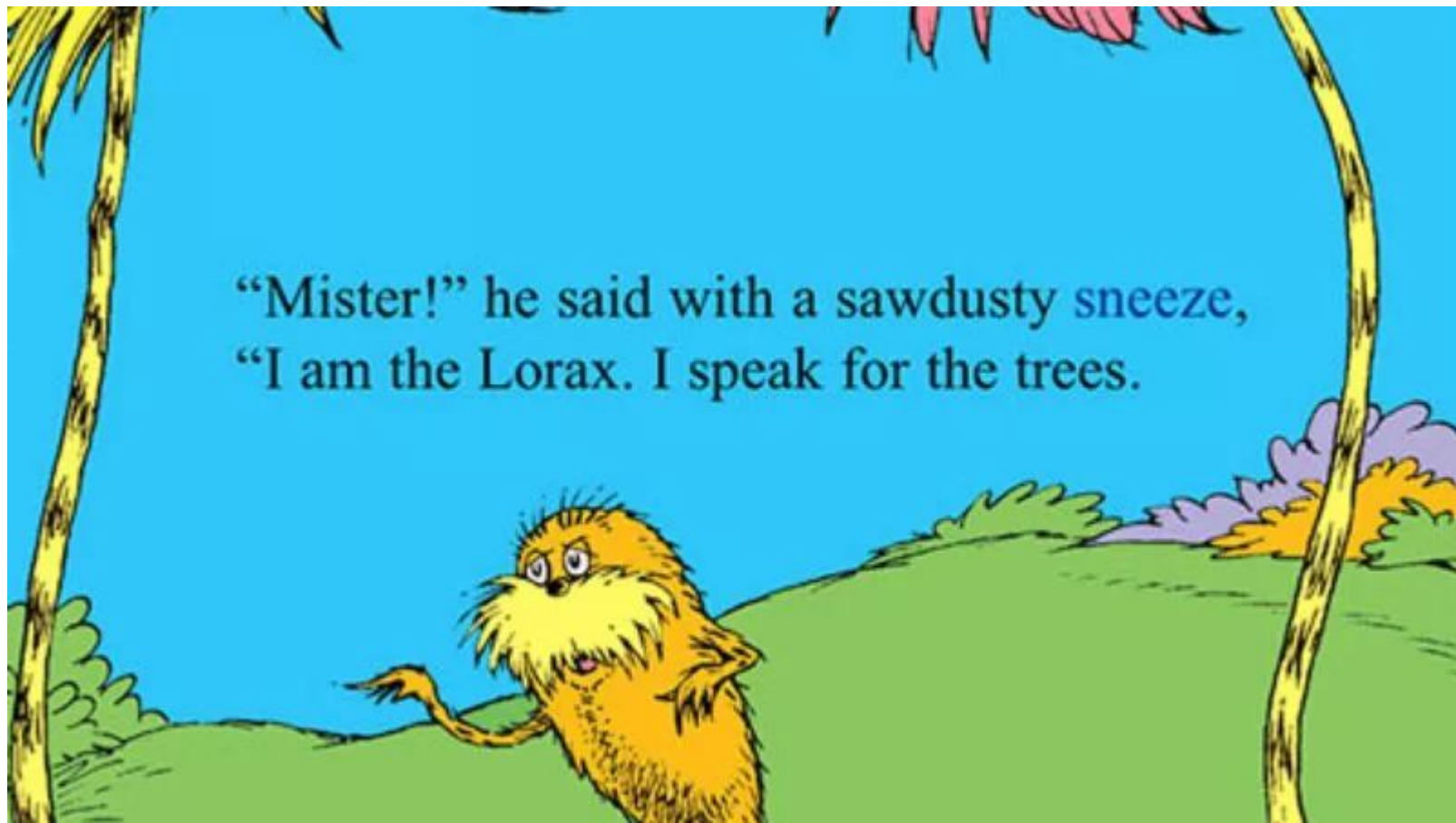
Tom's Story

- **CERT / Carnegie Mellon** - 4.5 years
 - architect/deliver realistic cyber warfare exercises to US Army
- **La Roche College** – adjunct faculty – Adv Computer Security
- **University of Pittsburgh** – 7 years
 - Systems Architecture Team Manager
 - All Enterprise Systems
- **Fiserv** – 4 years - E-Commerce Systems Manager
- many different startups - 20 years cyber & data center experience



Certified Information
Systems Security Professional

“Mister!” he said with a sawdusty sneeze,
“I am the Lorax. I speak for the trees.”





Cyber Confidence

Cyber Confidence Goals

1. Define **Cyber Confidence**
 - definitions and examples

2. **Increasing Cyber Confidence is guaranteed to benefit your teams**
 - technical and team dynamics perspective



End Result = Improved Cyber Security



Why Care About Increasing Cyber Confidence?

Traditional Challenges of Defensive Cyber Security

- **Threat landscape** - more diverse / ever increasing
- **Adversary** - advanced - emboldened - better financed
- **Workforce** - skill set and personnel gaps
- **Cloud** - security integration and traffic visibility
- **Business as usual** - just another IT cost center (ie: low priority for the bean counters)
- **Silver Bullets?** - Artificial Intelligence? Big Data? latest security policy frameworks?

Defensive Cyber... Additional Challenges...

- **Defensive Cyber Security is often not fair**
 - “Best” teams frequently lose
 - Only as strong as your weakest link
 - Terrible teams often never impacted
- **Defensive Cyber Security scenarios are often in the realm of “complex”**
 - Complex issues must be handled differently than “complicated” issues
- **Complicated issues**
 - Hard to solve -- but follow rules and can be solved with set processes
 - ex: rebuilding a car engine
- **Complex issues**
 - Many unknowns
 - Cannot be reduced to rules or processes
 - Unpredictable
 - many interdependencies and inter-communications



Defensive Cyber... Additional Challenges...

- **Aspects of Defensive Cyber Security can be intangible**
 - **Adversary**
 - Lack of defined physical presence
 - How to define/quantify risk of unknown threat?
 - **Leadership and Team Level**
 - Impacts traditional decision / prioritization models
 - **Funding allocation**
 - Factories, airplanes. ships or cyber?

Defensive Cyber... Additional Challenges...

- **National Security impact**
 - Strong nation state adversaries (Russia, Iran, North Korea, and China)
 - Well funded adversaries - zero days
 - Increasingly aggressive / emboldened
 - **Preference for Asymmetrical Warfare**
 - Adversary avoids direct conflict
- **Getting leaders and teams to care for the long term**
 - Impacts locally, large and small firms
 - 2013 - Target data breach
 - Supply Chain Attacks
 - Electrical Grid
 - Election infrastructure
- **Majority of national infrastructure is privately owned**
 - Boundaries of defense strategies / visibility



October 4, 2018, 5:00 AM EDT

The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies

The attack by Chinese spies reached almost 30 U.S. companies, including Amazon and Apple, by compromising America's technology supply chain, according to extensive interviews with government and corporate sources.

Third Quarter	
 Apple Inc. ▲ 1,091,000 ^[10]	
 Amazon.com ▲ 976,650 ^[11]	

Supply Chain Attacks



Apple



**Bloomberg
Businessweek**

October 8, 2018

The Big Hack

How China used
a tiny chip to
infiltrate America's
top companies

▲ Featured in *Bloomberg Businessweek*, Oct. 8, 2018. [Subscribe now.](#) PHOTOGRAPHER:



Moving the Supply Chain

While Bloomberg's story might have been a whopper, it does bring up the real and present danger of supply chain security. Being exposed to China, the supply chain is vulnerable and **less sophisticated attacks and exploits have happened before given this weakness.**

Prior to the publication of this story, Supermicro was well aware of this looming threat and was in the process of pushing more of its **supply chain over to Taiwan.** The trade war only accelerated this effort. In early May, Supermicro held a groundbreaking to mark the beginning of work on the second phase of a new 800,000-square foot factory in Taoyuan, Taiwan near Taipei.

Cyber Warfare



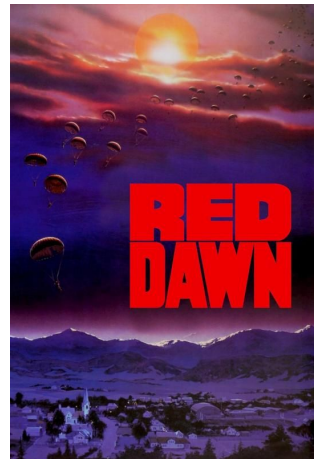
Waging Cyber War

Technical Challenges and Operational
Constraints

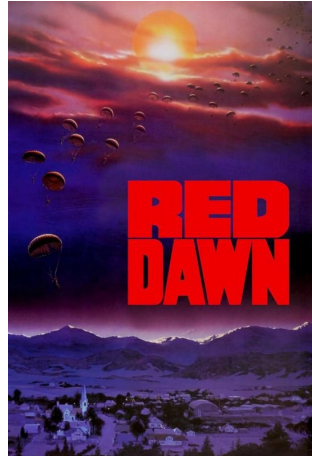
—
Jacob G. Oakley

Apress®

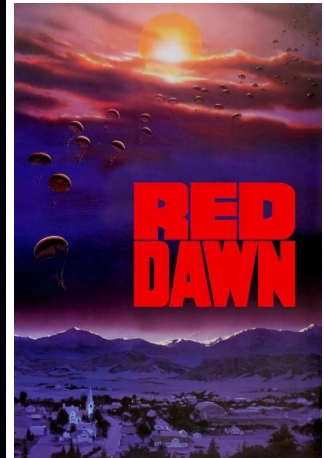
**— SOVIET UNION SUFFERS
WORST WHEAT HARVEST IN 55 YEARS.**




— LABOR AND FOOD RIOTS IN POLAND.
SOVIET TROOPS INVADE.



**— NATO DISSOLVES.
UNITED STATES STANDS ALONE.**





In our time
no foreign army
has ever occupied
American soil.

Until now.

**КРАСНЫЙ
РАССВЕТ
RED
DAWN**

AN AVAL KYRIE FILM A SIDNEY BECKERMAN PRODUCTION RED DAWN
STARRING PATRICK SWAYZE • C. THOMAS HOWELL • LEA THOMPSON • BEN JOHNSON
HARRY DEAN STANTON • RON O'NEAL • WILLIAM SMITH AND POWERS BOOTHE
SCREENPLAY BY KEVIN REYNOLDS AND JOHN MILIUS STORY BY KEVIN REYNOLDS
EXECUTIVE PRODUCER SIDNEY BECKERMAN PRODUCED BY BUZZ FEITSHANS AND BARRY BECKERMAN
DIRECTED BY JOHN MILIUS

PG-13

Parents Strongly Cautioned
Some Material May Be Inappropriate for Children Under 13

© 1984 Warner Bros. Entertainment Co. All Rights Reserved.





Defining Cyber Confidence

confidence **noun**

con·fi·dence | \ˈkän-fə-dən(t)s, -ˌden(t)s\

: faith or belief that one will act in a right, proper, or effective way

// have *confidence* in a leader

: the quality or state of being certain :!

// they had every *confidence* of success



trust **noun**

\ˈtrəst\

: assured reliance on the character, ability, strength, or truth of someone or something

Importance of using Confidence vs. Trust

Confidence vs. Trust

- seem nearly interchangeable

Trust

- trust -not- always based on past experiences
- is a **belief** that we have in another person not requiring evidence or questioning

Confidence

- confidence is based on past experiences
- believing that a team member has the potential and skills to do a task successfully

Confidence usage examples:

- a leader should have confidence in their team
- team members with confidence in their leader are more likely to be motivated followers

- we **trust** the team members or leaders that we have **confidence** in

Defining Cyber Confidence

Cyber - Computer & Network Security Related



Confidence

- Cyber Confidence is based on past experiences
- believing that a Cyber team member has the potential and skills to do a task successfully

Assurances, to organizational leadership, that based on past positive experiences, a cyber team has the proper leadership and team dynamics, and required technical skills, tools, and information, to successfully perform their defensive cyber mission.

THIS IS A TRUE STORY



You Tube

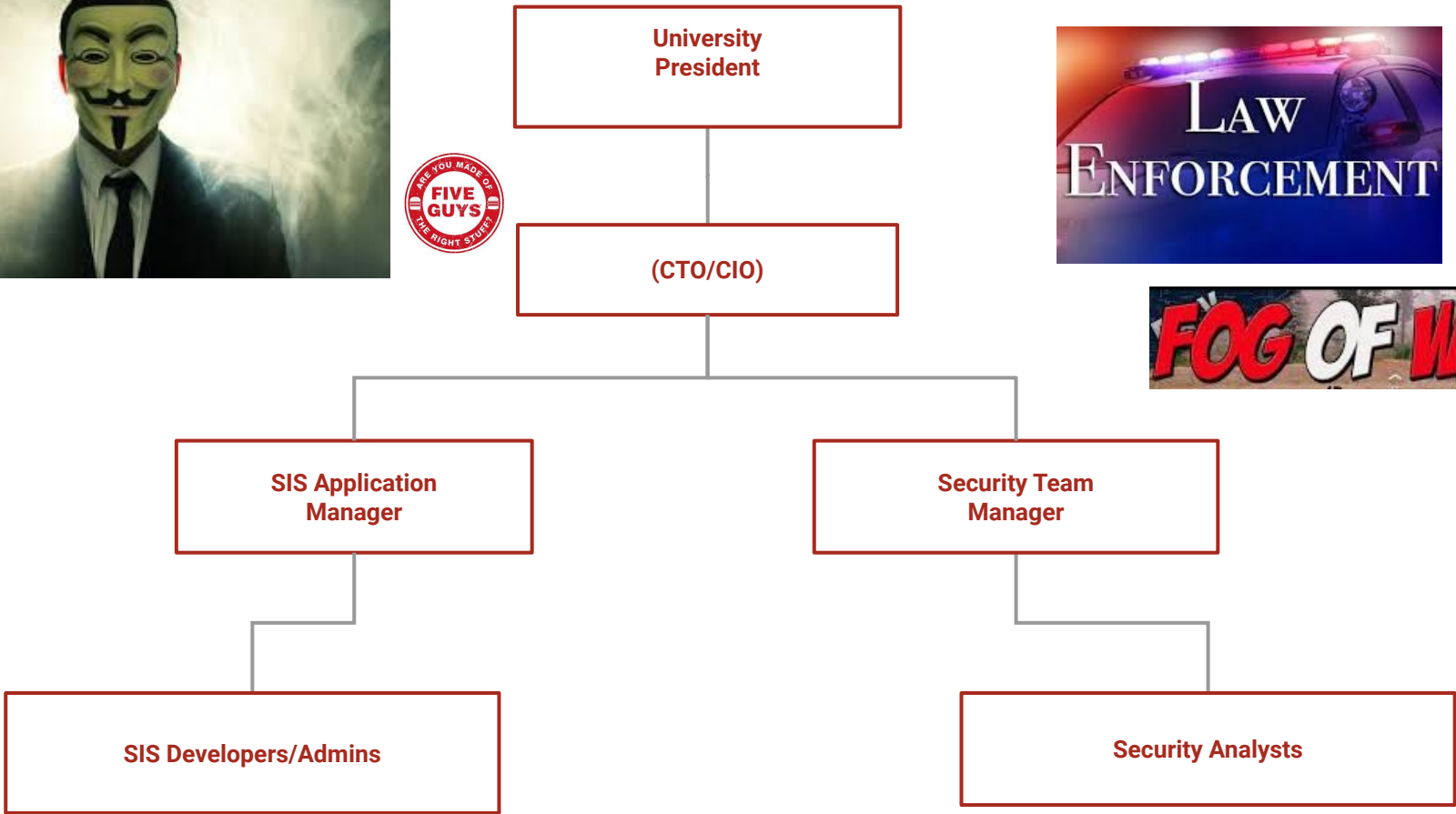


University President


UNLUCKY
LOTTERY

YOU'VE
BEEN
HACKED!

RANSOM



PROOF OF LIFE



Cyber Confidence from a Technical Perspective

Cyber Confidence from a Technical Perspective



Possibly Increase Cyber Confidence

- netflow
- firewall, authentication, web, application, and server logs
- Data Loss Prevention (DLP) systems

Possibly Decrease Cyber Confidence

- no intel - no IP or timeline
- impact of data retention policies
- shared database and admin passwords
- cloud migrations - multiple copies of data
- insider threat
- social engineered?




How to be confident that the event did not happen?

- proving that it -did- happen with logs would increase Cyber Confidence

Cyber Confidence from a Technical Perspective

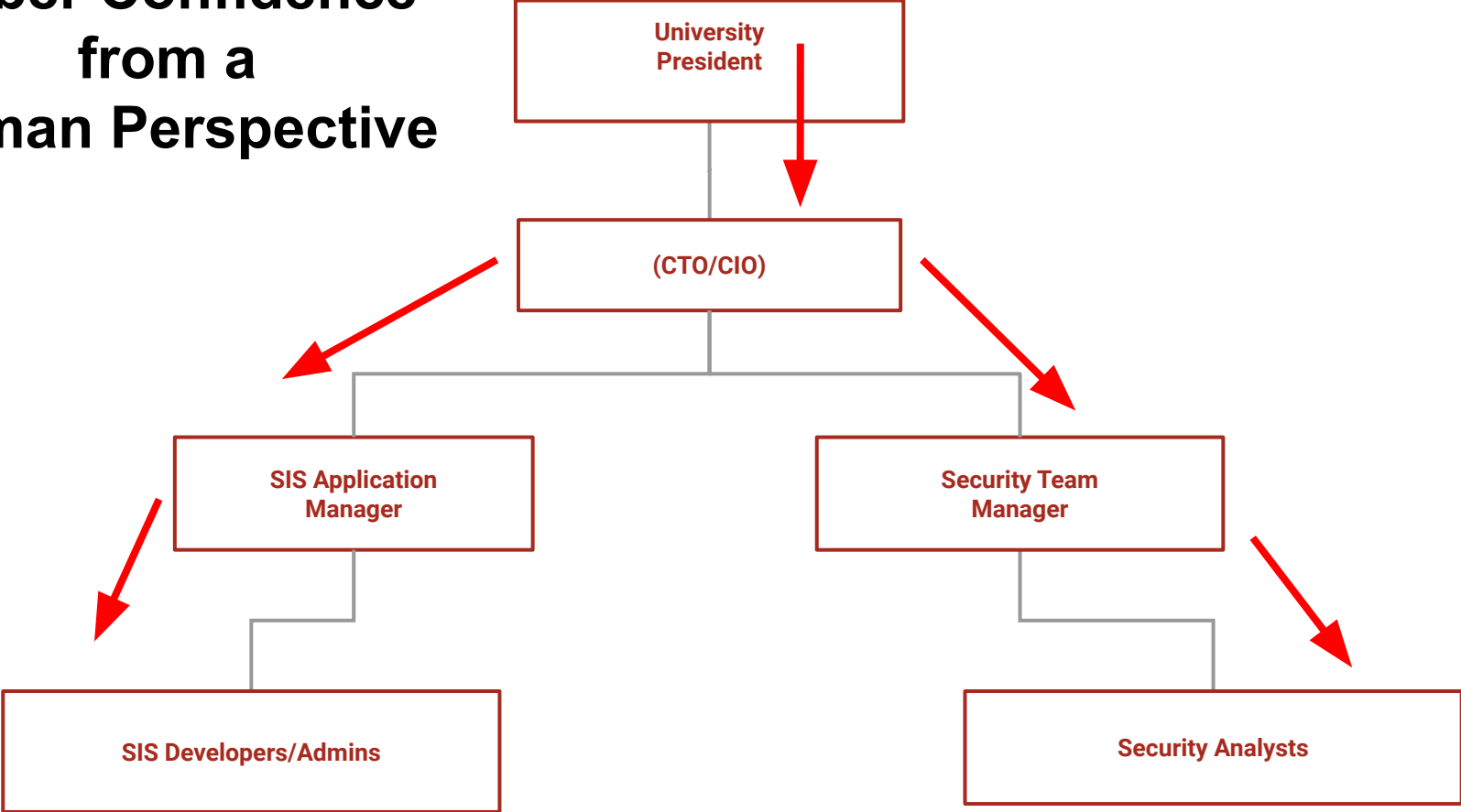
The analysts didn't find any proof, so it must not have happened??





Cyber Confidence from a Human Perspective

Cyber Confidence from a Human Perspective



If Increased Cyber Confidence Had Existed..

Technical Impact

- hard evidence found - help direct future security improvements
- prevent incident from ever occurring

Team/Leadership Impact

- Incident Response plan invocation speed
- lower remediation cost
- team dynamics - morale and longevity



Goals for Today

1. Define **Cyber Confidence**
 - definitions and examples

2. **Increasing Cyber Confidence is guaranteed to benefit your teams**
 - technical and team dynamics perspective

End result = Improved Cyber Security



How to Increase Cyber Confidence

Collecting & Storing Data

Categories for Data/Log Collection & Analysis

- **Network**
 - Proxy (Reverse & Forward)
 - DHCP, NAT, VPN, NetFlow, DPI
 - WAF
 - Network IPS & IDS events
 - Packet capture

- **Services/Applications**
 - DNS, HTTP/HTTPS proxies/interception
 - Authentication, Federation, AD/LDAP
 - Mail/Message Tracking, and Database
 - Host IPS & IDS events (AntiVirus)

Collecting & Storing Data

Categories for Data/Log Collection & Analysis

- **Server/Workstation/Appliances**
 - operating systems events, logins, processes, filesystem, network connections
 - PowerShell logging / command histories
- **On-demand data (scanning)**
 - active scanning looking for network hosts / services / ports
 - scanning hosts evaluating for known vulnerabilities
- **Configuration Management Database**
 - configuration changes
 - asset changes

Perspectives on the Collected Data

Why are you collecting all this data?

- collecting it -- not equal to being more secure
- analyze data -- find actionable events -- to become more secure

What about all this data?

- “we collect 10TB’s of data every day”
- Timely -- Properly -- Systematically - Automated

24x7x365



Perspectives on the Collected Data

Issues

- NTP - time sync
- overwhelming amounts
- is it the right data?
 - Intercepted SSL/TLS
- “good log messages” = easy parsing + correct details + timestamps
- keeping up - proper sensor locations - growing infrastructure / **acquisitions / cloud**
- tuning false positives = filters out some bad stuff too?
- adversary -can- impact your log files (diversions / deletions / mods)

Increasing Cyber Confidence

Perspectives on Increasing Cyber Confidence


- truly understand what's in the collected data - **“know your data”**
 - security analysts reliance on network, systems, and app administrators
- values of **data retention length**
 - adversary can be in your network for months/years
 - insider threat investigations can do on a long time



Network Security Through Data Analysis

BUILDING SITUATIONAL AWARENESS

Michael Collins



Additional Methods Increasing Cyber Confidence

Defensive Cyber Priorities

1. **Attend training and certifications**
2. **Cool tools**
3. **Lead, grow, and maintain the cyber team**
4. **And some really big monitors!!!**





Perspectives on Training and Certifications

Perspectives on Training & Certifications

- **Staff perspective**
 - formal training = birthright
 - certifications = career boost
 - Vegas and buffet jackpot
 - learn something new??
- **Mgmt perspective**
 - good metric to size up your team (all CISSP, CEH, etc.)
 - rewards good worker with happiness/retention
 - mgmt finally have someone who knows how to use the 500K tool you just bought



Industry wide - Cyber Training Budget/Hours - 2019



**100 Gazillion Hours
&
10 Gazillion Dollars**





Your Adversary



Are we 10 Gazillion \$\$\$
more Secure?

Increasing Cyber Confidence

- **Formal Training and Certifications**
 - they do help - at all levels even advanced including vendor product training
 - certifications are good to level set minimum skill requirements

- **Training Considerations for increasing Cyber Confidence**
 - **Benefits of “Stick Time” / Exercises and Mentoring**
 - senior cyber engineers should be mentoring junior engineers

 - All levels should be “exercising as a team” with realistic scenarios on their toolsets
 - these exercises are not just about technical items
 - technical event / incident & workflow management

Increasing Cyber Confidence

More Training Considerations for increasing Cyber Confidence

- **Internal Organizational Training**
 - network and servers teams - share about the infrastructure
 - application team / developers - share about apps
 - essential to becoming familiar with what is being defended
 - Build fusion centers - not an isolated SOC - breaks down team silos

- **Training by the Red Team**
 - red teams on their offensive tactics / techniques
 - customized training for attacking **the actual infrastructure** being defended
 - **-after-** a Red Team completes
 - to review actual sensor logs and events
 - Purple Teams (Red and Blue)

Defensive Cyber Priorities

1. Attend training and certifications
2. Cool tools
3. Lead, grow, and maintain the cyber team





Perspectives on Cool Tools

Perspectives on Tools

- **Before Tool Purchase Facts**

- cyber engineers love love love their tools
- cyber engineers cannot get enough new tools
- cyber engineers often sell “tool requests” as cyber silver bullets
 - “If I only had....”

- **Manager Myths**

- **buying an expensive tool or suite will automatically make an org more secure**
- no additional staff needs hired to manage the additional tool

- **After Tool Purchase Facts**

- the tool will likely require significant staff time investments for proper usage
- the time investment to manage the tool will persist for the life of the tool

- **cyber defenses are still only as strong as your weakest link**
 - (not measured by your most expensive tool)



Increasing Cyber Confidence

Tool Considerations for increasing Cyber Confidence

- **Evaluate staffing considerations**
 - why invest - cannot properly implement/maintain - no time
 - “free tools” - same boat
- **Try a tool before investing in it**
 - most defensive cyber operations are often very unique
 - Sales people falsehoods
- **Have a plan to review return on investment - ROI**
 - paying off in 6-12 months as expected?
 - if not used - lessons learned - not future repeats
- **Senior managers**
 - your role is more than just purchasing the tool
 - follow up on effectiveness - how to make better
 - encourage good tool usage
 - **hold teams accountable for poor tool purchases and usage**

Defensive Cyber Priorities

1. Attend training and certifications
2. Cool tools
3. Lead, grow, and maintain the cyber team



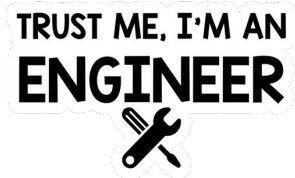


Perspectives on Cyber Teams

Perspectives on Cyber Teams

- **Cyber Engineers**

- you need engineers to do the work
- they often do a really good job and put in long hours and are really smart
- they can be **really** hard to manage
 - they often don't listen to mgmt types, and do whatever they want
 - have ability to overcomplicate a problem (over engineer)
- they can speak with a level of convincing authority
 - **in their mind - they are often convinced they are correct**
- they do -not- give a lot of slack/respect to “non-technical” managers
 - “street cred” before respect



Increasing Cyber Confidence

Cyber Engineers

- **Recommendations for increasing Cyber Confidence:**
 - **Participate in project plans, task lists, and deadlines**
 - despite what you think, these are invaluable to continued success
 - **Lose the attitude** - PowerShell & managers
 - **Mentor your management technically** - help inform them
 - simple as building diagrams, tutorials, lunch-n-learns
 - this will pay off for all

Increasing Cyber Confidence

Managers of Cyber Engineers

- **Recommendations for increasing Cyber Confidence:**
 - Cyber security is often complex -- it truly needs to be managed differently.
 - cyber leaders/managers are often former IT leadership - no **complex** problems
 - ability to know the “right questions to ask”
 - learn how to sort through the technical information
 - may take some deep dives into technical areas
 - **talk to multiple engineers to get varied opinions**
 - **Someone needs to be able to call B.S.**
 - else, engineers will run all over you

Increasing Cyber Confidence

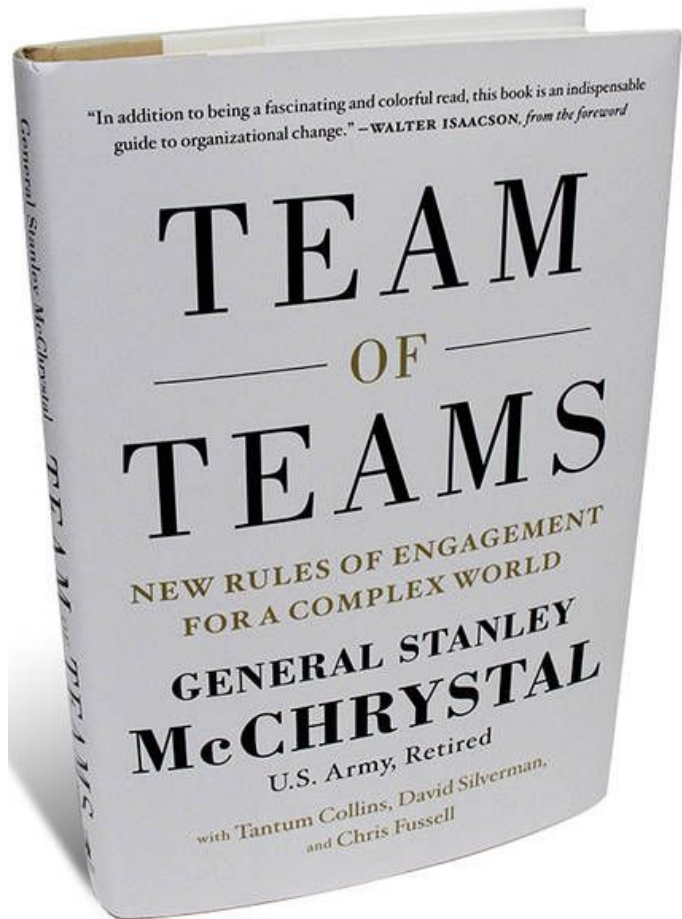
Cyber Team Senior Leadership

- **Recommendations for increasing Cyber Confidence:**
 - critical to involve non-technical & technical members for planning and decisions
 -
 - historically, engineers provide recommendations, but no “seat at the table”
 - today’s cyber security issues - “deep fast”
 - require technical skills to explain and advise --- **technical details matter**
 - recognize that true technical leadership is critical for an organization
 - make time for your cyber engineers -- eat lunch with them -- listen to them
 - old school mgmt techniques do not work



Increasing Cyber Confidence

- **What's the point of talking about Cyber Team members like this?**
 - These are similar problems you would see in any IT organization
 - Important to identify possible weaknesses of a team
 - leadership often ignores these problems to the detriment of the team
- **Working to identify and mitigate these issues helps improve Cyber Confidence**
- Very similar team structures and management techniques were used by the Army to defeat Al-Qaeda in Iraq in the early years of the Iraq War.
 - Al-Qaeda was treated as a “**complex adversary**”
 - All team members at all levels on daily briefings



Goals for Today

1. Define **Cyber Confidence**

- definitions and examples

2. **Increasing Cyber Confidence is guaranteed to benefit your teams**

- technical and team dynamics perspective

End result = Improved Cyber Security





Wrap Up
&
Some Fun

Five Reasons Why Defensive Cyber Security is Like an Alien Invasion Movie

- **always shows up when you least expect**
- **hard to estimate their size and power**
- **they likely have weapons more powerful than your defenses**
- **hard time figuring out if they've infiltrated you**
- **they can decimate your world for no good reason**



Questions?



Tom's contact info:

Tom.Podnar@gmail.com



The End