Inspiring Your Cybersecurity Teams

Laura Lee
Executive Vice President
Circadence Corporation
laura.lee@circadence.com
This briefing explains what you can do to reduce the Cyber Risk to your organization.

Call to Action for Cyber Readiness:  

*Equifax is yet another wakeup call*  
October 2017

The year 2017 may be remembered as one of the most frightening in terms of cyber events, with hospital ransomware from WannaCry, the critical infrastructure attacks in the Ukraine from Petya, and the massive leak of financial data at Equifax. Unfortunately, this year is likely to be only the most frightening one to date. With 2018 around the corner, what can we do? What should we do?

1. Provide **interdisciplinary cyber training** that brings together interconnected roles in cyber (Executive, Developer, Security Operator, Defender, HR, Legal)

2. Move past individual work role concepts to define a team-based workforce and **train as cyber teams**

3. Enable **applied information sharing** by sector using realistic scenario exercises

4. **Reduce risk to the public and economy** through analysis of cyber relevant key terrain by forging Government, Industry, and National Guard relationships for planning how to prepare and respond to cyber attacks
50 Years of Technology Innovation

- 1969 host-to-host communication
- 1970 Email
- 1980 Personal Computers
- 1990 Network discovery with DNS
- 2000 WWW Web Pages in HTML
- 2010 Amazon, Yahoo, eBay
- 2020 iPhone

- Social Media
  - Facebook
  - YouTube
  - Twitter
  - Instagram

- E-commerce
- Internet of Things

- Too many attacks to even name
- 26 Billion Devices connected by 2020
Cyber Job Security

- No Easy Fix to Inherent Internet Structure
  - Internet Protocols = attack surface
  - Secure protocol standards need to be widely adopted (DNS → DNSSEC)

- Attackers are motivated
  - Espionage
  - Political Views
  - Financial

- Crypto Currencies enable Cyber Organized Crime
  - Hackerville (near Bucharest), Romania is a well-known incubator for cyber criminals
  - Everything can be hacked and there is a market for it

“The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards --- and even then I have my doubts” Eugene Spafford “Spaf”
Internet expert, Prof CSci, Purdue University

Image credit: istockphoto.com/rscyther5

Careers in Cybersecurity

• Gap of trained cybersecurity professionals to reach 3.5 Million by 2021

• Employers concerned that recent graduates lack practical skills and foundational understanding

1. https://cybersecurityventures.com/jobs/
Building and maintaining a cybersecurity team can seem daunting.
# NIST Cybersecurity Framework

<table>
<thead>
<tr>
<th>ID</th>
<th>PROTECT</th>
<th>DETECT</th>
<th>RESPOND</th>
<th>RECOVER</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IDENTIFY</strong></td>
<td>Key cyber terrain and risks</td>
<td><strong>PROTECT</strong></td>
<td>Organizational assets and data</td>
<td><strong>DETECT</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Asset Management</th>
<th>Identity Mgmt, Authentication and Access Control</th>
<th>Anomalies and Events</th>
<th>Response Planning</th>
<th>Recovery Planning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Environment</td>
<td>Awareness and Training</td>
<td>Security Continuous Monitoring</td>
<td>Communications</td>
<td>Improvements</td>
</tr>
<tr>
<td>Governance</td>
<td>Data Security</td>
<td>Detection Processes</td>
<td>Analysis</td>
<td>Communications</td>
</tr>
<tr>
<td>Risk Assessment</td>
<td>Info Protection Processes</td>
<td>Mitigation</td>
<td>Mitigation</td>
<td></td>
</tr>
<tr>
<td>Risk Management Strategy</td>
<td>Maintenance</td>
<td>Improvements</td>
<td>Improvements</td>
<td></td>
</tr>
<tr>
<td>Supply Chain Risk Management</td>
<td>Protective Technology</td>
<td>Perform Mitigation Activities</td>
<td>Respond</td>
<td></td>
</tr>
</tbody>
</table>

https://www.nist.gov/cyberframework  
https://www.nist.gov/file/448306
# Key Activities For NIST CSF

## What

<table>
<thead>
<tr>
<th>IDENTIFY</th>
<th>PROTECT</th>
<th>DETECT</th>
<th>RESPOND</th>
<th>RECOVER</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key cyber terrain and risks</td>
<td>Organizational assets and data</td>
<td>Unauthorized access &amp; data breaches</td>
<td>To Cybersecurity Events and Attacks</td>
<td>Normal Operations and Services</td>
</tr>
</tbody>
</table>

## Who (Cyber Roles)

<table>
<thead>
<tr>
<th>Harden</th>
<th>Monitor</th>
<th>Pursue</th>
<th>Coordinate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify assets, users, software, hardware</td>
<td>Tailor monitoring for key assets/threats</td>
<td>Perform Vulnerability Assessment</td>
<td>Assess threats, Manage Risk</td>
</tr>
<tr>
<td>Recommend policy/protection measures</td>
<td>Aggregate info, monitor all, triage alerts</td>
<td>Assess Risk Posture and Likely Areas</td>
<td>Prioritize Plan of Action</td>
</tr>
<tr>
<td>Respond to Events, Analyze Risk Areas</td>
<td>Improve monitoring and analysis</td>
<td>Find &amp; Analyze Artifacts (Malware)</td>
<td>Manage Incidents</td>
</tr>
<tr>
<td>Implement changes to respond to incidents</td>
<td>Improve Monitoring based on threat</td>
<td>Lead forensics and response options</td>
<td>Choose Course of Action</td>
</tr>
<tr>
<td>Document Change Management</td>
<td>Threat Attribution analysis</td>
<td>Report findings, share intel</td>
<td></td>
</tr>
</tbody>
</table>
Cyber Defense TEAMS

Risk Mitigation

Prevent Breach

Harden

Risk area, watch here...

Problem found, please mitigate...

Suspicious event, please check...

Suspicious event, please check...

Risk area, watch here...

INCIDENT RESPONSE

Assume Breach

 Pursue

Defeat Breach

MONITOR

COORDINATE (Lead, Intel)
Cyber “Basketball” Teams

- Offense and Defense is a blur
- Fast paced
- Need both big picture and tactical view
- Communication and passing is a must
- Team work is mandatory for success
- Specialization for career
  1. Point Guard – **Pursue** (Quick and Control the Court)
  2. Shooting Guard – **Coord/Intel** (Wing to assist in defense)
  3. Small Forward – **Monitor** (Pass the ball, Draw Fouls)
  4. Power Forward – **Coord/Lead** (Versatile)
  5. Center – **Harden** (Close to the Basket)
Notional Cyber Defense Team

Team Lead

Intel

Watch Keep

Pursue

Survey

Vulnerability Analysis

Risk Assessment

Hunt

System Integrity

Forensics

Monitor

Network

Host

MONITOR

Harden

Windows

Linux/Unix

Infrastructure

COORDINATE

PURSUE

HARDEN
SOCs Scale the Cyber Defense Team Model

SOC Director

**Intelligence**
- Intel Analysis
- Threat Analysis
- Vulnerability Analysis
  - Pursue/Harden

**Operations**
- Investigations
  - Forensics
  - Incident Response
  - Malware
    - Pursue
  - Lead

**Security Operations**
- Monitoring
  - Tier 1
  - Monitor
  - IT
  -硬

**Security Services**
- Security Service Engineers
- Security Service Operators
- Tech Policy and Config Mgmt
- Vulnerability Management
- Business Ops
- Compliance and Auditing
- Program Management
- Processes and Procedures
  - IT
  - Harden
  - IT
  - IT
  - IT
  - IT
  - IT

Coordinate (Lead)

Monitor

Monitor/Pursue
Growing Cybersecurity Staff

• **10,000 hours of practice are necessary to be a Master**, according to Malcom Gladwell’s book *Outliers: The Story of Success*
  
  “To become a chess grandmaster also seems to take about ten years. (Only the legendary Bobby Fisher got to that elite level in less than that amount of time: it took him nine years.) And what’s ten years? Well, it’s roughly how long it takes to put in ten thousand hours of hard practice. Ten thousand hours is the magic number of greatness.”

• **Project Ares is Circadence’s Cybersecurity Learning Environment and Assessment tool that makes 10,000 possible and engaging**
  
  - Real, evolving threats
  - Real, integrated toolsets
  - New Tactics, Techniques and Procedures (e.g., Ender’s Game)
  - Gamification (Skills/Badges earned, Leader Boards, Feedback)
  - Experiential learning (video, reading, practicing, experimenting)
  - Artificial Intelligence methods to reduce human instructor burden
  - Auto Scoring for immediate feedback
Influential References

• “Ender’s Game”
  o AI Games for Evolving Learning
  o Ender's Game is a 1985 military science fiction novel by American author Orson Scott Card and 2013 LionsGate Film.

• “Code Girls”
  o Attributes for Cryptanalysts
  o Identifying, training staff

“I need you to think of solutions to problems we haven’t seen yet. I want you to try things that no one has ever tried because they’re absolutely stupid.”

-- Ender Wiggin

“Code breaking required literacy, numeracy, care, creativity, painstaking attention to detail, a good memory, and a willingness to hazard guesses. It required a tolerance for drudgery and a boundless reserve of energy and optimism.”
Project Ares®
Project Ares Casual Cyber Games

https://cybergames.circadence.com/
Mission Play
(Individual, Crew and Team Play)
Strategy for Hiring/Retaining Cyber Experts

- **Be inclusive in hiring** (e.g., job postings) and educational requirements
- **Test and Place people**
  - Mentor and grow them
  - Provide sufficient lifelong training
- **Find people with the “Right Stuff”, particularly as the team lead**
  - Train them in the fundamentals of NIST CSF
- **Work the soft skills**
  - Teamwork and communications
- **Make work fun – build the bond!**

**Curious** – try new things; proactive; learn from everyone

**Creative** – try many different ways to solve the puzzle; think outside the box

**Tenacious** – don’t give up; try multiple ways; research new tools and techniques to try

**Proactive** – stay current on the latest threats, tactics and evolution of the field; continually learn

**Organized** – keep good notes on what they did and what the result was; their own best resource
Case Study:

Jack Voltaic Exercise
24-26 July 2018

COMPONENT 1
Governance and Planning Committee
- Trusted agents
- Planners knowledgeable in cyber and emergency planning procedures
- Members are representatives from their sector

COMPONENT 2
Table Top Exercise (TTX)

COMPONENT 3
Live-Fire Exercise (LFX)
Operational and Technical Staff Work Together to Develop the Incident Response and Recovery Plans

- Are you prepared for a likely cyber attack?
- Have you identified your critical data centers and systems?
- How do you manage security risks to physical, human and cyber elements of the critical infrastructure?
- What are the thresholds and escalation procedures during a cyber attack?
- Do you understand legal reporting requirements and/or consequences?
- What processes are in place to share essential information across sectors and between public/private players in the industry?
- Do you share lessons learned and best practices across the business sector? City? Region? Nation?
Scenarios to Exercise Each Sector

Jack Voltaic Exercise 24-26 July 2018
2019 Plans for Disaster Preparedness

• Day One Morning - Tool Orientation (Cyber Tools and Programs)
  ○ Regional Tools Available tied to NIST Cybersecurity Framework
  ○ Technical Talks on Hot Topics
  ○ Cyber Hiring Best Practices – address the huge short fall of qualified staff

• Day One Afternoon – Cybersecurity Control Workshop (IT Staff)
  ○ Training on the Tools and Evaluation Walk through
  ○ Training on Response and Recovery Processes in preparation for the Table Top Exercise (TTX)
  ○ Legal Policies Review for Cyber Risk

• Day Two (Table Top and Live Fire Ex) - (IT and Operations Staff)
  ○ TTX - Response and Recovery on coordinated cyber attack
  ○ LFX - focusing on NIST Framework and addressing Incident Response
Call to Action for Cyber Readiness:
Equifax is yet another wakeup call  
October 2017

The year 2017 may be remembered as one of the most frightening in terms of cyber events, with hospital ransomware from WannaCry, the critical infrastructure attacks in the Ukraine from Petya, and the massive leak of financial data at Equifax. Unfortunately, this year is likely to be only the most frightening one to date. With 2018 around the corner, what can we do? What should we do?

1. Provide **interdisciplinary cyber training** that brings together interconnected roles in cyber (Executive, Developer, Security Operator, Defender, HR, Legal)
2. Move past individual work role concepts to define a team-based workforce and **train as cyber teams**
3. Enable **applied information sharing** by sector using realistic scenario exercises
4. **Reduce risk to the public and economy** through analysis of cyber relevant key terrain by forging Government, Industry, and National Guard relationships for planning how to prepare and respond to cyber attacks

There is no time like the present to move forward in cybersecurity . . .
Let’s Play!