The Fourth Leg of the Cyber Security Stool: PEOPLE

Jeff Felice
EVP, Partners & Alliances
Logical Operations
Cyber Clients

- Concise Networks
- Microsoft
- University of Rochester
- Wyndham Worldwide
- APL (Applied Physics Laboratory)
- U.S. Air Force
- Cisco
- Great-West Financial
- Perrigo
- SOTERA Defense Solutions
- Bank of Oklahoma
Threats are growing

83% view cyberattacks as one of the top 3 threats to business, but only 38% feel prepared for a sophisticated attack.

Visit: www.isaca.org/cybersecurityreport
The Stats Are Overwhelming

1. Over 169 million personal records were exposed in 2015, stemming from 781 publicized breaches across the financial, business, education, government and healthcare sectors.  
   – “ITRC Data Breach Reports – 2015 Year-End Totals” | ITRC

2. The average global cost per each lost or stolen record containing confidential and sensitive data was $154.  
   – “Cost of Data Breach Study: Global Analysis” | IBM/ Ponemon

3. In 2015, there were 38% more security incidents detected than in 2014.  

4. In 2015, even fewer SMBs (29%) used standard tools like configuration and patching to prevent security breaches, compared with 39% who did so in 2014.  

5. The median number of days that attackers stay dormant within a network before detection is over 200.  
   – “Microsoft Advanced Threat Analytics” | Microsoft

6. At least 52% of respondents felt that a successful cyberattack against their network would take place within the year.  
   – “2015 Cyberthreat Defense Report” | CyberEdge Group

7. As much as 70% of cyberattacks use a combination of phishing and hacking techniques and involve a secondary victim.  

8. 74% of CISOs are concerned about employees stealing sensitive company information.  
   – “SANS 2015 Survey on Insider Threats” | SpectorSoft

9. Only 38% of global organizations claim they are prepared to handle a sophisticated cyberattack.  
   – “2015 Global Cybersecurity Status Report” | ISACA International

10. 81%, report they had neither a system nor a managed security service in place to ensure they could self-detect data breaches, relying instead on notification from an external party. This was the case despite the fact that self-detected breaches take just 14.5 days to contain whereas breaches detected by an external party take an average of 154 days to contain.  
    – “2015 Trustwave Global Security Report” | Trustwave
93% of breaches are caused by human error

People: the weakest link in the cyber security chain. The Information Commissioner’s Office reported that 93% of incidents it investigated were caused by HUMAN ERROR.
Increased Security Awareness Among Employees

43% said they increased security training after a public breach.

41% said they established a formal set of security policies and procedures.

Source: Cisco 2015 Security Capabilities Benchmark Study
Traditionally businesses have relied on preventative measures to protect networks
  • Firewalls, antivirus software, etc.

Securing networks requires a multi-faceted approach
  • HW/SW solutions
  • Process
  • And People!

The key is ensuring all are working together to strengthen an organization’s security posture
How do we secure the entire organization?

Most security programs focus on training Security team only
Sample Cyber Training Plan

End User:
- All Staff
  - CyberSAFE

IT Professional:
- Foundational
  - Security+
- Intermediate
  - CFR
- Specialist
  - CSA+
  - CSC
  - *MMAD
- Manager/Other
  - CASP
  - CISSP
  - CIPP
  - CIPM
  - ISO 27001
  - RESILIA

Logical Operations: CyberSAFE, CFR, CSC, *MMAD
CompTIA: A+, Network+, Security+, CASP, CSA+
ISC2: CISSP
IAPP: CIPM, CIPT
OTHER: ISO 27001, RESILIA
*Coming Soon
"End-user awareness and training reduces security-related risks by 45% to 70%." - Reuters.com

Training and a Credential for the Weakest Link in the Security Chain: End-users

CyberSAFEcertified.com
End-user Knowledge Domains

- Compliance
- Social Engineering
- Device and Data Protection
- Online Security
Compliance

- Adherence to rules, regulations, or practices
- Imposed by the organization or government
- Requirements are often updated after breaches
- Self-imposed examples:
  - Password length
  - Password complexity
- Externally imposed examples:
  - GDPR
  - PCI DSS
Social Engineering

- **Definition:** the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.

- **Types**
  - Phishing
  - Whaling
  - Spear phishing
  - Vishing
  - Impersonation
  - Tailgating
Device and Data Protection

- Maintain Physical Security of Devices
- Use Passwords for Security
- Protect Your Data
- Identify and Mitigate Malware
- Use Wireless Devices Securely
Online Security

- Browse the Web Safely
- Use Email Securely
- Use Social Networking Securely
- Use Cloud Services Securely
"60% of companies will uncover a breach of sensitive data in 2015, while even more could go unnoticed."

– Forrester Research

CFRcertified.com
IT & Security Pro Knowledge Domains

- Threat Landscape
- Passive Data Driven Analysis
- Active Asset and Network Analysis
- Incident Response Lifecycle
The Phases of Cyber Security

- **Assessing** security risk and posture
- **Analyzing** threats

- **Collecting** real-time security intelligence
- **Analyzing** security intelligence

- **Responding and Investigating** incidents
Assess Security Risk & Posture

• Risk management has real strategic value in regards to information assurance
• Understanding of different risk assessment methodologies, including vulnerability assessments and penetration testing
• Specific strategies aimed at mitigating risks
Analyze Threats

• Baseline understanding of the numerous threat vectors affecting networks:
  • Reconnaissance incidents
  • Malware
  • Hijacking and impersonation
  • Denial of Service
  • “Persistent” threats
• Places onus on protecting data in cloud/mobile environments
Collect Intelligence

• Collecting network and host based logs
  • Proactive: as attacks occurs
  • Reactive: after attack occurs (but before it occurs again)
    • More likely
• Importance of analyzing after collection

• Active analysis vs. passive analysis
  • Active = Using Windows and Linux based tools to identify IOCs as threats are occurring
  • Passive = Using Windows and Linux based tools to parse logs and identify suspicious traces after a threat has materialized (whether known or unknown)
It’s no longer a question of if, but when
• Sound incidence response plan is needed
• Focus on the implementation of an incidence handling and response architecture
• Reinforces defensive security strategies, such as system hardening and isolation
The OTHER Factor in Cyber Security
Software Developer Knowledge Domains

• Common Secure Application Development Terminology and Concepts
• Job and Process Responsibilities Related to Secure Application Development
• Architecture and Design
• Risk Assessment and Management
• Application Implementation
Development Terminology and Concepts

• Understanding basic security principles
• Identify common hacking terminology and concepts
Job and Process Responsibilities

- Explain the software development lifecycle (SDLC)
- Understand the role of the designer/architect in creating secure applications
- Explain the role of the developer in creating secure applications
- Understand the role of the code reviewer in creating secure applications
- Understand the role of the application tester in creating secure applications
Architecture and Design

- Interpret use and abuse cases
- Understand architecture and design industry best practices
- Identify common regulations that relate to secure software development
- Explain the importance of organizational requirements to the development of secure software application
Risk Assessment and Management

- Classify common threats and vulnerabilities in terms of their impact on applications
- Compare and contrast common risk assessment and management best practices
Application Implementation

- Implement input validation
- Restrict the output of sensitive data
- Implement cryptography
- Implement authentication and access control
- Implement error handling and logging
- Implement communication security
- Implement application security parameters and configure security settings
- Implement secure database access
Summary

• Securing networks requires a multi-faceted approach, but ultimately begins and ends with people

• End-users need to be knowledgeable and vigilant

• IT and Security Professionals need to be involved before, during, and after events

• We need to consider that Software Developers
Next Steps

- Review your internal security strategy
- Determine the skills necessary to fulfill that strategy
- Support those skills with training and certification
Are YOU CyberSAFE? Take our complimentary CyberSAFE Readiness Test.

Measure your organization's level of preparedness against cyber threats with the CyberSAFE Readiness Test. Comprised of 15 questions that are designed to measure an individual's knowledge of how to detect and avoid cyber threats, this complimentary assessment provides you with a tool to determine how well your organization is protected from imminent cyber threats.

Simply follow the instructions below to take the CyberSAFE Readiness Test:

1. Go to http://cybersafecert.com and click Enter.
2. Under the New User section, enter CMXA1KTP4V as your Access Key.
3. Click the Enroll button.
4. Fill in all required fields in the enrollment form, including your username and password. You will now be on the CyberSAFE CHOICE homepage.
5. Log in under the RETURNING USER with your newly created username and password.
6. Click the course tile for your course.
Free ISSA Membership

Logical Operations provides any CyberSec First Responder (CFR) candidate who passes their CFR-210 exam a free ISSA membership *(valued at $95)* and pre-paid ISSA chapter dues for one year *(valued at up to $80 depending on location)*.
### 2017 Certification Product Roadmap

<table>
<thead>
<tr>
<th>Family</th>
<th>JAN</th>
<th>FEB</th>
<th>MAR</th>
<th>APR</th>
<th>MAY</th>
<th>JUN</th>
<th>JUL</th>
<th>AUG</th>
<th>SEP</th>
<th>OCT</th>
<th>NOV</th>
<th>DEC</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cyber Security Family</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CyberSec First Responder (Exam CFR-110)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>3/31</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CyberSec First Responder (Exam CFR-210)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CyberSAFE (Securing Assets For End-users) (CSF-111)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Application Development Family</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Master Mobile Application Developer (Exam MAD-111)</td>
<td></td>
<td></td>
<td></td>
<td>1/31</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cyber Secure Coder (Exam CSC-110)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4/30</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Master of Mobile Application Security (Exam MAS-110)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4/30</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>NCTA CloudMASTER Family</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NCTA Certified Cloud Technologist (NCT-110)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NCTA Certified CloudOps Specialist (NCO-110)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NCTA Certified Cloud Architect (NCA-110)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NCTA Certified CloudMASTER (NCM-110)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Certified Virtualization Professional (CVP) Family</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CVP - VMware vSphere v6.0 Level 1 (Exam CVP1-110)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CVP - VMware vSphere v6.0 Level 2 (Exam CVP2-110)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CVP - VMware vSphere v6.5 Level 1 (Exam Code TBD)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>6/30</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CVP - VMware vSphere v6.5 Level 2 (Exam Code TBD)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>6/30</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Internet of Things (IoT) Master</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>6/30</td>
</tr>
<tr>
<td>Exam Title TBD</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Instructor-Led Training Delivery Family</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Modern Classroom Certified Trainer (Exam MCCT-2015)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **End of Life**
- **Product Launch**
- **Exam Update**
- **Scheme Committee Meeting**

www.logicaloperations.com