Security Challenges and Opportunities for IoE
Becoming an IoE Ready Organization

Steve Martino, Chief Information Security Officer, Cisco
Lokesh Sisodiya, President, ISC2, East Bay Chapter
Agenda

• IoE – Our View
• Enablers
• Challenges
• Meeting the Challenges
• Opportunities
• Resources
IoE – Connecting People, Process, Data and Things

**People** - Connecting people in more relevant, valuable ways.

**Data** – Converting data into intelligence to make better and quicker decisions.

**Process** – Delivering the right information to the right person/machine at the right time.

**Things** - Physical devices and objects connected to the Internet and each other for intelligent decision making; often called Internet of Things (IoT).

“Making the world more connected, more relevant and valuable than ever before.”
Key Enablers for IoE

- IPv6 Addressing Space
  - Scales our addressing capabilities from < 4 billion to $3.4 \times 10^{33}$

- Wireless technology advances
  - Smaller, longer battery life
  - Faster and more scalable – 802.11ac

- Explosion of cloud providers and business models

- Advancements in Big Data Analytics

- Industry demand...
“Almost everything that can be used for good can also be used for bad.”

Michele and others...
Cars of the Future: U.S. government probes medical devices for possible cyber flaws

BY JIM FINKLE
BOSTON | Wed Oct 22, 2014 7:13am EDT

Commentary: Not All Clouds Are Created Equal

Smartwatch Hacked, how to access data exchanged with Smartphone

Symantec: Wearables can be hacked to track workouts and even sexual activity

MIKE WHEATLEY | AUGUST 4TH

READ MORE

Here’s some jarring news for those who love to automatically tweet and track their exercise, sleep and sex routines. Aherents of “quantified self” might learn more about themselves, but they’re also making it possible for hackers to do the same.

At least that’s what Symantec Corp. researchers at BitDefender think. Using customized Raspberry Pi

©2014 Cisco and/or its affiliates. All rights reserved.
Some Facts to Add to the Challenges

**Security Postures Lagging**
- Most organizations still struggle with basic “block & tackle”.
- The average number of security vendor products use is > 40.
- BYOD was just the beginning...

**Attack Surface Exponential Growth**
- Hacking & malware still top for breach methods.
- Billions of new devices
- Embedded systems, sensor, wearables
- IP & non-IP
- Pivot attacks on the rise.

**Unparalleled Data Accessibility**
- 4 Exabytes of data in 2012 alone.
- 12 billion connected devices.
- 77+ billion apps in 2014.
- In 2017 Data Center hosted data will be 7.7 ZetaBytes

**Clouds, Clouds, and Cloud of Clouds**
- Explosive growth in the variety and number of Cloud vendors offerings.
- 64% of data will be in the Cloud (UP from 40% in 2012);
- Increase in “rogue” cloud deployments.
- Lack of visibility into the cloud.
Rising to the Challenge
Protecting Cisco, Securing Our Products, Protecting our Customers
2014-Sep-17

We are announcing the new Security and Trust Organization, which will be led by John Stewart as Chief Security and Trust Officer. John and his team will report to Gary Moore, President and Chief Operating Officer.

So, What Are We Doing?
The Security & Trust Organization will be responsible for ensuring trust and security across our entire product and service portfolio, and is charged with three things:

1. **Protecting Cisco before, during and after cyber threats.** To be the security leader, and be the #1 IT Company, protecting ourselves is paramount. Our customer and employee data needs to be secure. Our intellectual property needs to be protected. Our networks and our systems need resiliency and recoverability. Through all this, we'll gain significant threat expertise which we will share with our customers to help them. The new organization will continue to work closely with the Security Business Group, which is showing the market that we are the security leader.

2. **Product security and integrity.** To be clear, this part of our remit isn't about creating the market-leading suite of security products – that sits with our Security Business Group. Our customers expect us to design all our products with security high on the agenda. So we need to make sure that all Cisco solutions – cloud, Intercloud, collaboration, networking, datacenter – start out with security in mind. In partnership with the Engineering and Services teams, the Trustworthy Systems, Cisco Secure Development Lifecycle, and product security testing and certification are all part of this team's role.

3. **Protecting our customers.** This means providing customers with advanced threat intelligence, security expertise and Cisco-on-Cisco best practices while also making sure that we are compliant with imposed requirements and local laws where we do business. In partnership with the Security Services team, you will see new offers on tailored threat feeds, reporting, and protection. We are also forming a new router forensics team to help customers who are facing attack.
Optimal Link in the Kill Chain

Attack Continuum

BEFORE
Discover
Enforce
Harden

DURING
Detect
Block
Defend

AFTER
Scope
Contain
Remediate

The Kill Chain

Recon  Deliver  Control  Maintain

Weaponize  Exploit  Execute
A Day of Defending Cisco

- 14 billion NetFlows
- 4.7 billion DNS records
- 2 billion system events
- 6 million web transactions/day with about 143K blocked automatically (WSA)
- 5.4 million emails inspected, 4.1 million blocked
- 27TB traffic inspected – equivalent to 2.2K hours of blu-ray video per day.
- 1.2 trillion events throughout network
Key Pillars for Adapting our Strategy to Meet Needs of IoE

- Expert in “Block & Tackle” – the foundation
- Minimize attack surface – get to 100% visibility
- Manage and control our data – know your data
- Adapt our cloud engagement and support model – shared services, not duplicate services
- Achieve pervasive identity based policy (4W1H)
Better, Faster, More Agile Block & Tackle
Know Your Basics & Your Gaps

- IT Security Architecture Bundle
  - Governance
  - Identity & Access
  - Trusted Device
  - Data Security
  - Detect & Contain

- Architecture led planning
  - Understand posture gaps
  - Focus on most critical areas & prioritize

- Secure Development Lifecycle with threat modeling

- Two foundational “Game Changers”

- Operationalization of 20 Critical Controls
Expanding Accountability in IT - Service Security Primes

1 or more Primes

- Establishes security technology baselines
- Formal approval for exceptions
- Establishes corporate security policies and guidelines
- CSO of the Service
- Single point of accountability
- Increase communication and awareness around security.
- Visibility with Service Exec thru Unified Security Metrics

Service Executive

Service Owner
- Security SMEs
- Security architecture reviews
- Trusted advisors

Partner Security Architect

Service Security Prime

Infosec Team
Expanding Visibility - Unified Security Metrics

IT Service Owners and Security Primes

- Service Security Score Cards, Pending Mitigation

IT Service Executives

- Vulnerability-Performance Metric and Trending, Top 10 Vs. Bottom 10

Service Review

- Performance Metric (‘Aging’) and Trending

Ensuring Consistency Across All Reporting Areas
Operationalization of “20 Critical Controls”

• Be sufficient in all 20 controls in Production & Extranet network

• Be sufficient in most critical controls across labs, engineering, and other non-IT

• Add compensating controls where culturally not appropriate

• Measure posture of acquisitions using 20 controls

• Automate Metric & Test portion of controls

• Self reporting when something goes wrong

• Score twice a year and report metrics

• Incorporate into Unified Security Metrics
Minimize the Attack Surface
Keys to Minimizing Attack Surface

- “Trustworthy Products”
- Full embodiment of Trusted Device Policy and technology to back it up
- Pervasive ISE with differentiated access
- Mature behavioral based anomaly detection
- Decrease “Mean Time to Detect” and “Mean Time to Contain”
- Instrument the network – Fireamp, NGIPS, Netflow everywhere
- Segment the network – control zones, security group tags, data-aware
Moving Towards 100% Protection of Assets

Security Challenges
- Managed/Unmanaged Desktops
- Spam/Malware
- DDoS
- Compromised Hosts Remotely Controlled
- Rapidly Changing Environment

Foundational Solutions
- Anti-virus
- Firewalls
- IDS/IPS
- IronPort WSA/ESA
- Network Segmentation
- Log Capture/Analysis
- Incident Response Team
We Must Achieve Near 100% Protection of Assets

**Advanced Threats**
- Targeted Spear Phishing Trojans
- Watering Hole Attacks
- Social Networking Attacks
- Nation State Attacks

**Security Challenges**
- Managed/Unmanaged Desktops
- Spam/Malware
- DDoS
- Compromised Hosts Remotely Controlled
- Rapidly Changing Environment

**Evolving Solutions**
- Expanded Data Collection
  - Netflow, IP-Attribution, DNS...
- Big Data Analysis & Playbooks
- DNS/RPZ, Quarantine
- On-line Host Based Forensics
- Threat/Situational Awareness
- Dedicated APT Team

**Foundational Solutions**
- Anti-virus
- Firewalls
- IDS/IPS
- IronPort WSA/ESA
- Network Segmentation
- Log Capture/Analysis
- Incident Response Team
Manage & Control Data
Data Security Governance Strategy

Govern the data

- Laws, contracts, and policies impose requirements on the data
- Roles, responsibilities, ownership, etc. sets the accountability
- Training, awareness, and metrics to manage behavior

Protect the data

- Manage use of data throughout the life cycle (i.e. collection → disposal)
- Access and rights management
- Incubate data-level security solutions

Securing the foundation

- System / Application / Data security
  - Monitoring and response
  - Risk management
## Data Security Framework – The Holy Grail

<table>
<thead>
<tr>
<th>Data Management</th>
<th>Data Protection</th>
<th>Environment &amp; Perimeter Security</th>
<th>Monitoring and Response</th>
<th>Data Security Intelligence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data inventory</td>
<td>Access management</td>
<td>Secure development</td>
<td>Forensics</td>
<td>Third party security</td>
</tr>
<tr>
<td>Data import /export</td>
<td>Rights management</td>
<td>Hardening</td>
<td>Investigations</td>
<td>Behavior analysis</td>
</tr>
<tr>
<td>Data retention</td>
<td>Data Privacy</td>
<td>Secure operations</td>
<td>Compliance monitoring</td>
<td>Threat mining</td>
</tr>
<tr>
<td>Data destruction</td>
<td></td>
<td>Threat modeling</td>
<td>Security monitoring</td>
<td></td>
</tr>
</tbody>
</table>

### Process
- Data inventory
- Data import /export
- Access management
- Rights management
- Secure development
- Hardening
- Forensics
- Investigations
- Third party security
- Behavior analysis
- Data retention
- Data destruction
- Data Privacy
- Secure operations
- Threat modeling
- Compliance monitoring
- Security monitoring
- Threat mining
- Tagging / Classifying
- Contextual Discovery
- Data Erasure
- Masking / Encryption
- Data Backup
- Access Rights Cntrl
- Data Loss Prevention
- API & SDKs
- Vulnerability Scanners
- App / Svc Catalog
- Patching
- Forensic Capabilities
- Event Monitoring
- Data Loss Detection
- Remediation
- Policy Engine
- Context Awareness
- Big Data Analytics

### Technology

### Governance (Policy & People)
- Laws and Regulation
- Principles and Policy
- Authority
- Ownership
- Third Party
- Training & Awareness
- Secure Design
- Metrics
Adapt & Mature Cloud Engagement Models
Scaling Cloud Engagements

- Governance & Remediation
  - Assessment Questionnaires
  - Architecture Engagement Process
  - Terms of Use
  - Compliance
- Security Architecture
  - Architecture Guiding Principles
  - Assessment & Design Reviews
  - Baseline Compliance Criteria
- Monitoring and Incident Response
  - Logging & Monitoring Strategy
  - Event Analysis
  - Incident Response
- Vulnerability Management & Remediation
  - Scanning methodology
  - Pen Testing Methodology
  - Remediation
Opportunities
Cisco Is Becoming an IoE-Ready Organization
Maximizing the Networked Connection of our Extended Enterprise – its People, Process, Data, and Things

Adaptive Technology: Cisco IT’s Internet of Everything Vision

Combine the power of big data, analytics, distributed processing, and network innovation:

• to simplify operations support
• to extend and improve security systems
• in service of speed and effectiveness in the business.
Key Take Aways

- Understand the benefits & risks
- Master the basics – block & tackle
- Increase trust level on all fronts
- Expand accountability, visibility, knowledge
- Minimize attack surface
- Maximize your data management
- Mature your cloud engagement models
Resources & Interesting Reads

- http://www.cisco.com/web/IN/about/leadership/cyber_security_ioe.html
Thank You