
Caspar Herzberg
VP, Cisco Consulting Services, APJ+GC

September, 2015
Technology has become Embedded in Modern Existence

We live in a digital world enabled by complex technologies; but what if technology “stopped working”?
Present: Internet of Things

50 Billion Connected Devices by 2020

Adoption rate of Digital infrastructure: 5x faster than electricity and Telephony

Source: Cisco Internet of Things Report; Cisco Consulting Analysis
Internet of Things already here today

...combined with latest Disruptive Technologies

- Cloud
- Mobile
- Big Data
- Social
- Security

Disruptive technologies that enable new business outcomes

...make ‘Internet of Everything’ a new frontier of opportunities

People, Process, Data and Technology gets interconnected to deliver new business value
By 2020, Every Business, Country and City will become a Digital Enterprise

- In 2015, 99.4% of the physical world is unconnected today.
- By 2020, 75% of businesses will become fully digital or preparing to be.
- 30% of these digitization efforts will be successful if they can reinvent themselves.

Source: Gartner Digital Business Transformation: Disrupt to Win Report; Cisco Consulting Analysis
The “Bad Guys” are evolving - Cyberattacks are increasingly Sophisticated and Dynamic

- **Viruses** (1990–2000)
- **Worms** (2000–2005)
- **Spyware** (2005–Today)
- **APT s Cyberware** (Today +)

- **Phishing, Low Sophistication**
- **Industrialization of Hacking**
- **Sophisticated Attacks**

- **75%** of all attacks take only minutes to begin data exfiltration
- **>50%** of attacks persist without detection for months or years before discovery
- **100%** of companies connect to domains that host malicious files or services

Source: Cisco Industrialization of Hacking white paper; Cisco Consulting Analysis
Dramatic Increase in Number and Scope of Security Breaches

- Number of detected incidents rose to 43M in 2014, a 48% increase from 2013.
- Since 2009, we have seen a 66% compounded annual growth rate of detected incidents.
- Costs of Breaches amount to $20M+ for large companies in 2014, almost double that of 2013.

The more valuable data becomes, the more attractive hacking is to hackers.
Achieving Cyber Resilience in Internet of Everything Era

Security is fundamental to the success of a company’s digital strategy.
Optimizing Security Readiness: How to Get There

Phased Approach to Security Organizational Enablement

Phase 1: Organizational Change
- Realign goals, refresh human capital and leadership

Phase 2: Solutions Convergence
- Secure existing enterprise IT network i.e. routers, switches, servers etc and move towards an integrated platform

Phase 3: Security Everywhere
- Pervasive, Integrated, Continuous and Open
- Deploy solutions that span across IT and external networks
- Network seen as a Sensor and Enforcer

End Vision: Integrated Threat Defence
- Global intelligence based on advanced algorithms
- 3rd Party Ecosystem Open Source
- Advanced Malware Protection Everywhere
- Predictive, agile and dynamic
Phase 1: Organizational Change

**Cultural Change**
- Security to be engaged at boardroom level
- Personnel to be embedded into business units

**New Metrics**
- Increase collaboration between work teams
- Direct or indirect revenue impact

**Talent Pool**
- Invest in human capital
- Training and Up-skilling

**Enablement**

*Renew corporate focus on Security*
Businesses of all sizes must embed security into heart of network to achieve **defense in depth**.

Ideally, solutions should move towards a **converged model** which minimize disparate point-product deployment.

A converged model will capture **real time information on network across all critical assets**, providing holistic view of internal and external threats.
Phase 3: Security Everywhere across End Points and Extended Network

Security Everywhere

1. PERVASIVE – to persist across all attack vectors
2. INTEGRATED – To share information, intelligence, and capabilities
3. CONTINUOUS – Allow for ongoing protection across full attack continuum
4. OPEN – Option to integrate with third parties
End Vision: Integrated Threat Defense

GLOBAL INTELLIGENCE

AGILE ARCHITECTURE AND PLATFORMS

ADVANCED MALWARE PROTECTION

Open Source

3rd Party Ecosystem

Open

Continuos

Telemetry Data

Threat Research

Advanced Algorithms

Integrated

Security Ecosystem

Contextual Sharing

Accelerated Containment & Remediation

Pervasive

© 2015 Cisco and/or its affiliates. All rights reserved.
Cisco can Accelerate your Digital Journey with Holistic Security Solutions

<table>
<thead>
<tr>
<th>PLAN</th>
<th>BUILD</th>
<th>RUN</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Network Security</strong></td>
<td><strong>Cloud / DC Security</strong></td>
<td><strong>Advanced Malware Protection</strong></td>
</tr>
<tr>
<td>Capabilities Assessment</td>
<td>Integration and Deployment</td>
<td>Managed Threat Defense</td>
</tr>
<tr>
<td>Architecture and Design</td>
<td>Security Optimization and Migration</td>
<td>Remote Managed or Hosted Services</td>
</tr>
<tr>
<td>Custom Threat Intelligence</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Looking Ahead into the Future: Canalys Top Predictions for 2015

- Cybercrime will reach new levels
- Connected Things will create a major security loophole
- Mobile Payment systems will mean new threats
- DDoS attacks will target hosting and cloud providers
- Increased level of regulation
- User will be at heart of every security strategy
- Security will shift from being technology-centric to platform-centric
- Security gets C-Levels buy-in
Embracing Change and Position for the Next Digital Disruption

- Hyper-Connectivity of People, Data, Processes and Things will usher in the next wave of digital disruption known as Internet of Everything (IoE)

- **Security is fundamental to the success of a company’s digital strategy** as all ‘things’ get connected

- ‘**Security Everywhere**’ enables organizations to be proactive in identifying and addressing cybersecurity risks

> “**Organizations no longer want to accept that compromise is inevitable. They are looking to the security industry to provide them with products that are reliable and resilient, and capable of deflecting even the most sophisticated threats.**” John N. Stewart, Chief Security and Trust Officer Cisco