
Anmol Singh
Security for the Next Generation of Threat

- A pervasive digital presence is expanding into business, industry and society
- Once networked, this digital presence substantively alters risk for digital businesses
- Digital security is the next evolution in cybersecurity to protect this pervasive digital presence
Security Macro Trends You Face in the Age of the Pervasive Digital Presence

- Risk and Resilience Seek Balance
- Security Disciplines Converge
- Secure Digital Supply Chain Needs Grow
- Security Skills Options Expand
- Adaptive Security Architecture Embraced
- Security Infrastructure Adapts
- Data Security Governance Arrives
- Digital Business Drives Digital Security
Risk and Resilience
Seek Balance
Security Moves to An Embedded State in the Organization

RISK
- Governance
- Compliance
- Control
- Privacy
- Safety

RESILIENCE
- Reliability
- Speed
- Assurance
- Transparency
- Value
Security Principles for Trust and Resilience

Business Outcomes

Risk-Based

Facilitator

Data Flow

Detect & Respond

Principle of Trust & Resilience

People-Centric
People-Centric Security Continues to be Embraced
Takeaways: Risk and Resilience Balance

- Revisit the security organizational structure to ensure it reflects current mission
- Revise the methods used to calculate IT risk to incorporate new variables and factors
- Develop fast-track methods of addressing security requirements
- Refine the security communication and education process to emphasize agility
Security Disciplines Converge
“Digital Safety" Becomes a New Force and Responsibility

The "CIAS" Model of Digital Security

Data

Confidentiality

Integrity

Availability

People

Environments

Graphics: canstockphoto.com

© 2016 Gartner, Inc. and/or its affiliates. All rights reserved.
Takeaways: Security Convergence

- Establish security governance and planning relationships with physical and industrial counterparts
- Improve cross-discipline procurement methods for security requirements
- Modify security architecture to include additional layers where required
- Investigate changes in security management and operations that may be required to accommodate convergence
Secure Digital Supply Chain Needs Grow
Public and Private Clouds Make Traditional Security Controls Obsolete

Consuming entities

Layer of abstraction

Resource provider

- Workloads decoupled from hardware
- Workloads become mobile
- Security policy based on physical attributes breaks

Requirements

Results

Internet technologies
Service-based
Metered by use

Scalable, shared, automated and elastic implementation

Provider
Cloud Brokers: Single Consoles for Multiple Controls Over Multiple Services

- Single Sign-On
  - IDaaS
- Mobility
  - Device Management
  - Data Recovery
  - Discovery Investigation
  - Threat Control
- Other
  - Confidentiality
  - Compliance
  - Activity
  - Destination

Cloud Access Security Broker
Takeaways: Securing the Cloud (Supply Chain)

- Develop an enterprise public cloud strategy
- Implement and enforce policies on usage responsibility and cloud risk acceptance
- Follow a cloud life cycle governance approach
- Develop expertise in the security and control each cloud model used
- Implement technologies to fight cloud diffusion complexity
Security Skills
Options Expand
Assess the Most Critical Skills Impacts of Digital Security

Already, Traditional Security Strategies Are Shifting To:

- Contextual Security Monitoring and Response
- Data Classes, Data Governance
- Embedded Security
- Ubiquitous Identity Management
- Security Awareness, Privacy & Behavior
- Network Segmentation, Engineering
- Physical Security Automation
Takeaways: Accelerate Skills Generation and Convergence

- Build a long-term security workforce plan
- Make coaching and skills development first task
- Embed security skills within the lines-of-business
- Change security specialists to ‘versatilists’
- Mix traditional and agile recruitment techniques
- Evaluate current skills gaps
Adaptive Security Architecture Is Embraced
Software-Defined Everything, Including Security

"Control Plane"

Northbound APIs

API
API
API
API

Applications

Platform APIs

"Data Plane"

Southbound APIs

API
API
API
API
Develop an Adaptive Security Architecture

Policy

Continuous Visibility and Verification

Users
Systems
System activity
Payload
Network

Predict
Risk-prioritized exposure assessment
Anticipate threats/attacks
Baseline systems and security posture

Respond
Design/model policy change
Investigate incidents/retrospective analysis

Compliance

Prevent
Harden systems
Isolate systems
Prevent attacks

Contain incidents
Confirm and prioritize risk
Detect

Adjust posture
Implement posture
Monitor posture
Threat Intelligence Platforms Allow You to Visualize, Correlate and Gain Context

Open-Source MRTI Feeds
- Emerging Threats
- Shadowserver
- ZeuS Tracker
- Abuse.ch

Commercial Feeds
- Norse
- Internet Identity
- Cyveillance
- Malcovery

OSINT Sources
- News
- RSS Feeds
- Websites

Enrichment Services
- GeoIP
- Malware Lookup
- Domain Tools

Threat Intelligence Platform
- Analytics
- Visualization
- Forensics
- Threat Intelligence Processing
- Reporting
- Threat Intelligence Sharing

People
- Incident Response
- Fraud
- Threat Analyst

Process
- SOC Analyst
- Management
- Malware Analyst
- Help Desk

Technology
- Circle of Trust Sharing
- Workflow/ Escalation
- Communication
- Secure Web Gateway
- IPS/IDS
- NGFW
- Logs

Fraud

Incident Response

Management

Malware Analyst

Help Desk
Takeaways: Adaptive Security Architecture

- Shift security mindset from "incident response" to "continuous response"
- Spend less on prevention; invest in detection, response and predictive capabilities
- Favor context-aware network, endpoint and application security protection platforms
- Develop a security operations center
- Architect for comprehensive, continuous monitoring at all layers of the IT stack
Security Infrastructure Adapts
Develop a Pragmatic Application Security Strategy

Drivers: Fear of losing IP and revenue, global distribution of software

Applied at:
- Programming and build

Executed at:
- Operations

Application

- Software application firewall
- Code-hardening and self-repair
- Code obfuscation
- Application code
New Network Security Concerns in the Pervasive Digital Presence

- Attacks Through Local Wireless Networks
- Lower Defense Capabilities
- Risk Aggregation
- Aggregators
- Controllers
- IoT Platform
- Sensors
- Actuators
- Things
- Attacks Through Internet or Wireless Networks
- Attacks Through Local Wireless Networks and Users / Endpoints
Model of A Trusted Execution Environment (TEE)
Takeaways: Security Infrastructure Adapts

- Seek engineering skills to expand your application development portfolio
- Re-evaluate your network design for further segmentation as endpoint requirements change
- Review current wireless security standards for alternative connectivity requirements
- Trial trusted execution environments with workforce use cases where consumer mobile device use is needed
Data Security Governance Arrives
Develop a Data-Centric Audit and Protection Approach

Data Security Policy
- Data Classification and Discovery Policy
- Data Security Controls

Activity Monitoring
- Assessment of Users and Permissions
- User Monitoring and Auditing

Protection
- Analysis and Reporting
- Blocking, Encryption, Tokenization and Data Masking
Takeaways: Data Security Governance

- Prioritize organization-wide data security governance and policy
- Identify and implement risk-appropriate data security controls by data type where possible
- Implement a DCAP strategy that includes disciplined and formal product selection
- Incorporate big data plans and unique requirements into security strategy
Digital Business Drives Digital Security
Securing a Pervasive Digital Presence (the Internet of Things)

- **Security requirements**
  - Policy management, enforcement
  - Monitoring, detection and response
  - Access control and management
  - Protect data, apps, network, platform

- **Key challenges**
  - Scale
  - Diversity (age and type)
  - Function
  - Regulation
  - Privacy
  - Standardization

Recommendations: Focus on small scenarios. Use risk-based prioritization. Emphasize segmentation and access initially.
Cyber Risks and Consequences in an IoT Solution

**Edge**
- Device Impersonation
- Device Hacking
- Device Counterfeiting
- Snooping, Tampering, Disruption, Damage

**IoT Platform**
- Platform Hacking
- Data Snooping and Tampering
- Sabotaging Automation and Devices

**Enterprise Consumer**
- Business Disruption
- Espionage and Fraud
- Financial Waste
IAM Trends of 2015-2016 That Include an Identity of Things
Takeaways: Digital Business Drives Digital Security

- Risk and Resilience Seek Balance
- Security Disciplines Converge
- Secure Digital Supply Chain Needs Grow
- Security Skills Options Expand
- Adaptive Security Architecture Embraced
- Security Infrastructure Adapts
- Data Security Governance Arrives
- Digital Business Drives Digital Security
Recommended Gartner Research

- Cybersecurity Scenario 2020 Phase 2: Guardians for Big Change
  Earl Perkins and F. Christian Byrnes (G00279414)

- Predicts 2016: Security for the Internet of Things
  Ray Wagner, Anmol Singh et. al. (G00293187)

  Gregg Kreizman, Anmol Singh et. al. (G00292678)

- Cloud Security and Emerging Technology Security Primer 2016
  Jay Heiser (G00293190)