RSAConference2018

San Francisco | April 16 – 20 | Moscone Center

SESSION ID: STR-W04

Ten Tenets of CISO Success

Frank Kim

Founder
ThinkSec
@fykim
www.frankkim.net

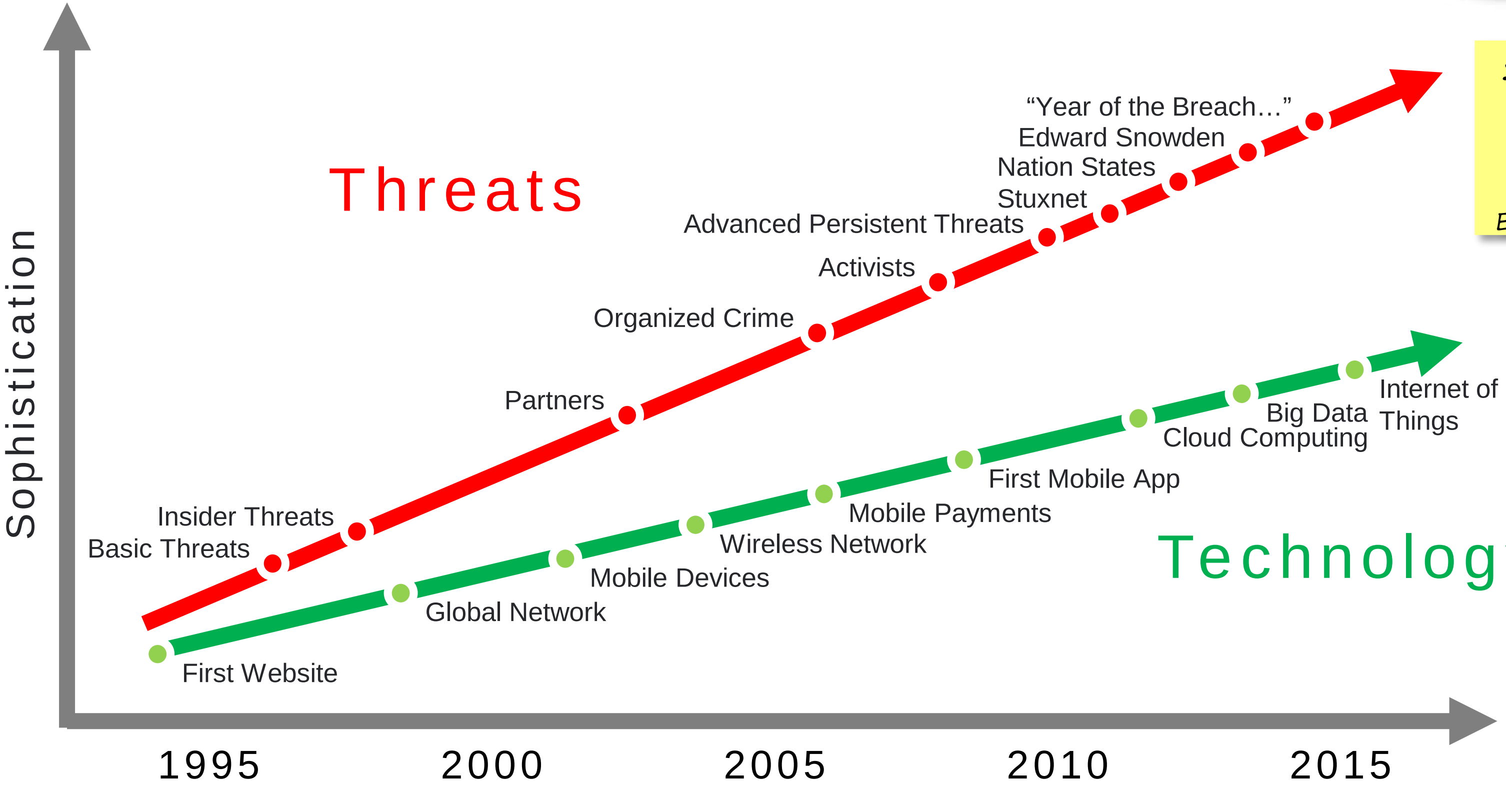
#1 Catch the Culture

Organizational Culture

> “Culture eats strategy for breakfast.”
>
> - Peter Drucker

#2 Relate to Risk

Business Risk



$1 Trillion
Cost of Cyber crime

– World Economic Forum

Graphic credit: Omar Khawaja

#3 Create Credibility

Creating Credibility

"A big part of being believable and building our trust is showing us how we compare to competitors, other industries, some kind of standards or benchmarks."

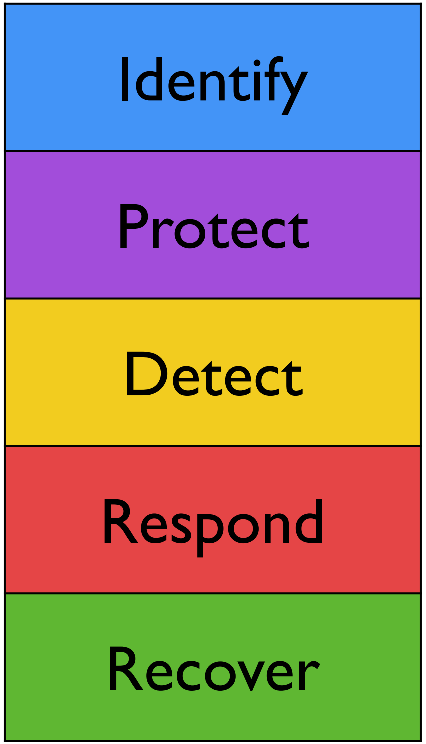
- Board Member

#4 Shape the Strategy

Identifying a Security Framework

- Security frameworks provide a blueprint for
  - Building security programs
  - Managing risk
  - Communicating about security
- Many frameworks share common security concepts
- Common *program* frameworks include:
  - ISO 27000 Series
    - 27001 – ISMS requirements
    - 27002 – Code of practice
    - 27003 – Implementation guidance
    - 27004 – Measurement
  - COBIT
  - ENISA Evaluation Framework
  - FFIEC Cybersecurity Assessment Tool
  - NIST Cybersecurity Framework

NIST Cybersecurity Framework


Identify

Protect

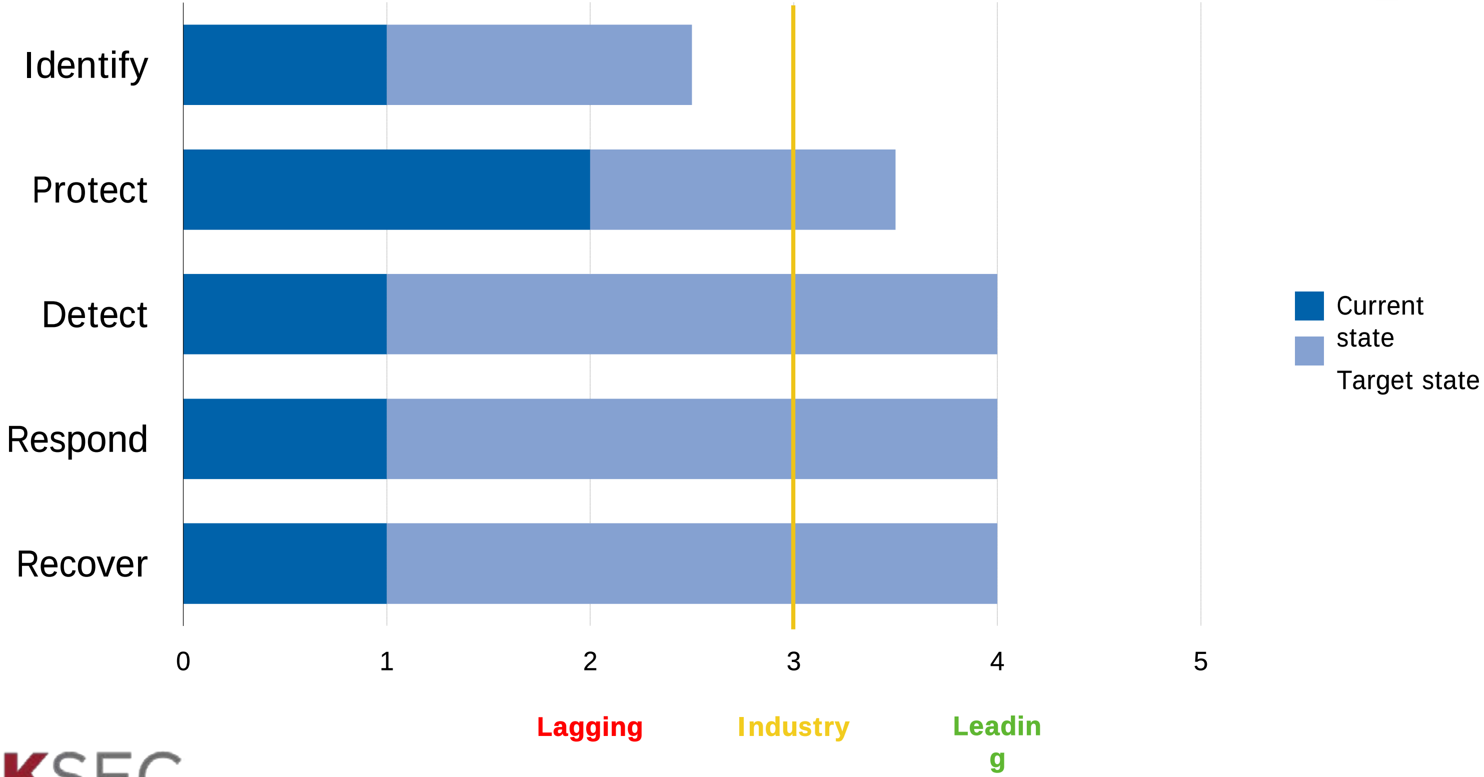
Detect

Respond

Recover

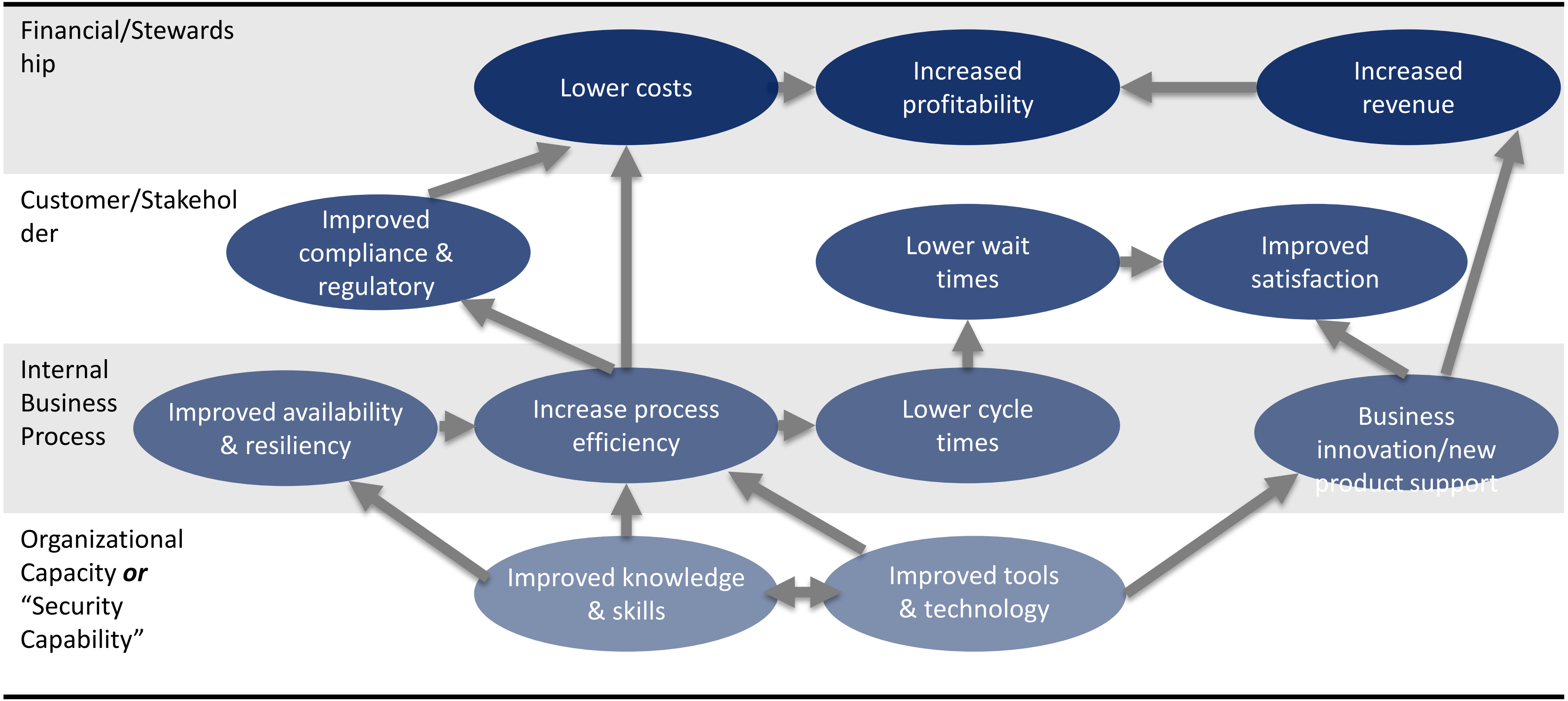
- Composed of three parts
  - Core, Implementation Tiers, Profiles
- Defines a common language for managing security risk
  - Core has five Functions that provide a high-level, strategic view of the security life cycle
- Helps organizations ask:
  - What are we doing today?
  - How are we doing?
  - Where do we want to go?
  - When do we want to get there?

Maturity Comparison Example



#5 Deliver the Deal

Mapping to Strategic Objectives


Financial/Stewardship
Customer/Stakeholder
Internal Business Process
Organizational Capacity *or* "Security Capability"
Lower costs
Increased profitability
Increased revenue
Improved compliance & regulatory
Lower wait times
Improved satisfaction
Improved availability & resiliency
Increase process efficiency
Lower cycle times
Business innovation/new product support
Improved knowledge & skills
Improved tools & technology

Provide Options

- Highlight trade-offs with business value, risk reduction, cost

	Option A	Option B	Option C
Business value	✓	✓✓	✓✓✓
Risk reduction	🔒	🔒🔒	🔒🔒🔒
Cost	$	$$	$$$

#6 Invest in Individuals

Putting Leadership Into Perspective

Boss ✗	Manager ✓	Leader ✓
Drives people	Manages things	Coach, mentor, and grow people
Thinks short-term	Thinks mid-term	Thinks long-term
Focused on self	Focused on process	Focused on people
Instills fear	Earns respect	Generates enthusiasm
Says “I”	Says “Our”	Says “We”
Micromanages	Delegates	Motivates
Places blame on roadblocks	Navigates roadblocks	Removes roadblocks
Dictates how it’s done	Shows how it’s done	Influences how it’s done
Takes credit	Shares credit	Gives credit
Commands	Asks	Influences
Says “Go”	Says “Let’s go”	Says “Way to go”

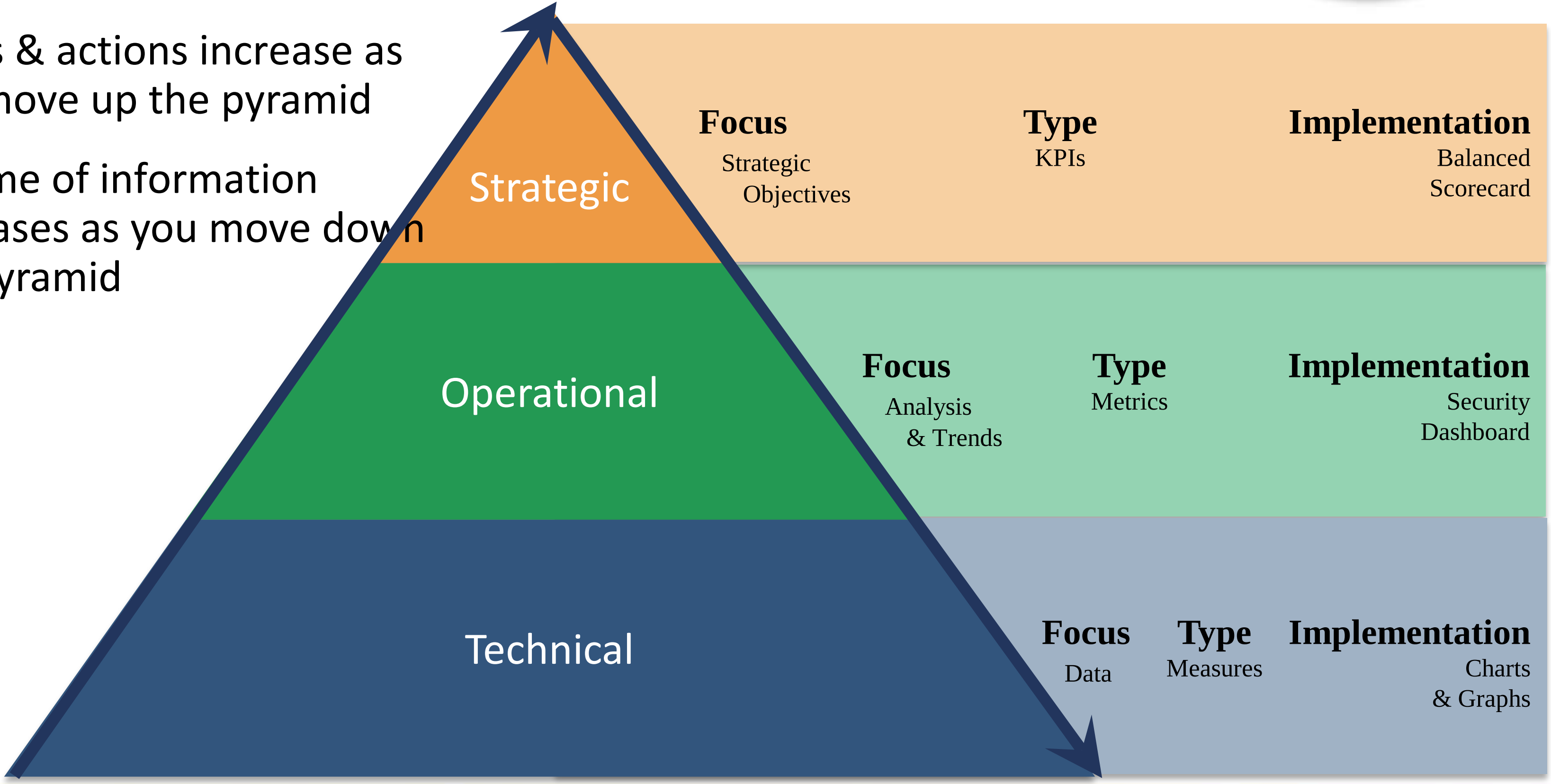
Career Management – P.I.E.

- Everyone should have a piece of the P.I.E.
- Performance
  - Perform exceptionally well
- Image
  - Cultivate the proper image
- Exposure
  - Manage their exposure so the right people will know them

#7 Make Metrics Matter

Metrics Hiearchary

- Focus & actions increase as you move up the pyramid
- Volume of information increases as you move down the pyramid



Strategic

Focus
Strategic Objectives

Type
KPIs

Implementation
Balanced Scorecard

Operational

Focus
Analysis & Trends

Type
Metrics

Implementation
Security Dashboard

Technical

Focus
Data

Type
Measures

Implementation
Charts & Graphs

Balanced Scorecard Example

Financial/Stewardship

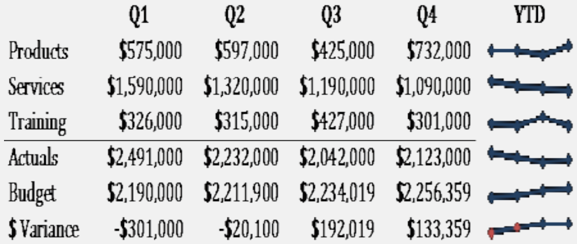
Q4 % Product Development Budget Allocated to Security

Target 5% ✓
Trend →

5%

- Increased support for legal as they piloted their case management system

Q4 & YTD Security Budget Allocation



	Q1	Q2	Q3	Q4	YTD
Products	$575,000	$597,000	$425,000	$732,000	
Services	$1,590,000	$1,320,000	$1,190,000	$1,090,000	
Training	$326,000	$315,000	$427,000	$301,000	
Actuals	$2,491,000	$2,232,000	$2,042,000	$2,123,000	
Budget	$2,190,000	$2,211,900	$2,234,019	$2,256,359	
$ Variance	-$301,000	-$20,100	$192,019	$133,359	

Customer / Stakeholder

Q4 % of Products Delivered On Time and On Budget

Target 95% ✓
Trend ↑

95%

- 18% increase over Q3 in on-time and on budget delivery. Security staffed temporary PMO team to meet goal

Customer Satisfaction

Target 90% ✗
Trend ↑

85%

- 8% increase over Q3 in customer satisfaction rating of 4 or higher out of 5 possible

Internal Business Process

Q4 % of Developers Training in Secure Coding Principles

Target 95% ✓
Trend ↑

97%

- 100% of flagship application developers completed training reducing overall risk to organization

Q4 % of Developers Attaining Certification

Target 95% ✗
Trend ↑

42%

- Mitigation plan: Follow-up with developers after training is complete for certification

Security Capability Example

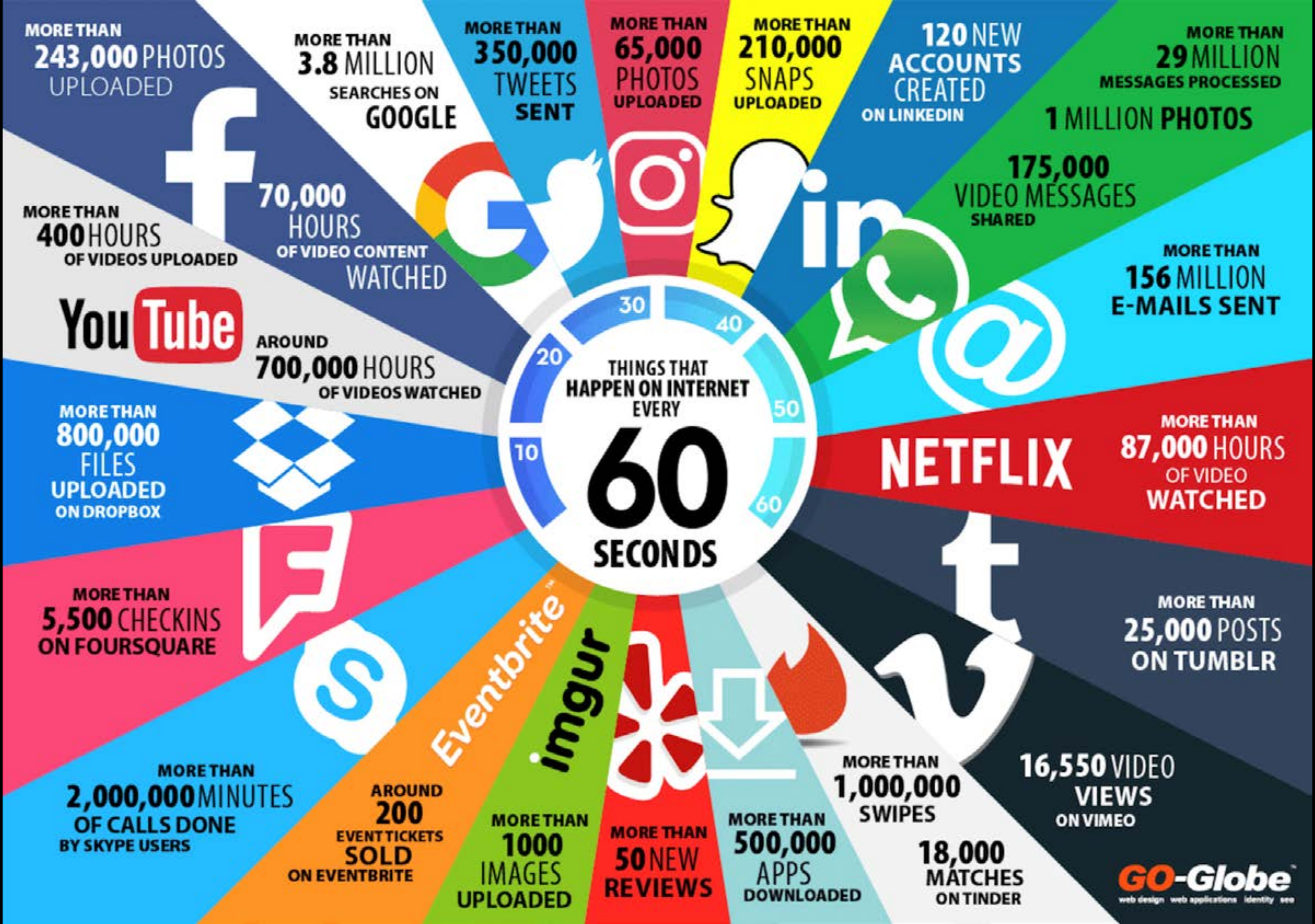
Security Capability	Status	Trend	Highlights
Identify: Manage risk to systems, assets, data, and capabilities	Yellow	↑	• 32% increase in unauthorized devices • 29% IT • 3 % HR • 27% increase in unauthorized software • Attributed to Q4 BYOD pilot
Protect: Ensure delivery of critical infrastructure services	Green	→	• 12% of users failed sponsored email phishing tests • 15% of employees have not passed security awareness assessments
Detect: Identify occurrence of a cybersecurity event	Green	↓	• 27% decrease in elevated access accounts • 275 total elevated access accounts
Respond: Take action regarding a detected cybersecurity event	Green	→	• 5% of database systems with sensitive information have not been scanned by vulnerability scanners
Recover: Maintain plans for resilience and to restore any capabilities or services that were impaired due to cybersecurity event	Red	↑	• 34% of systems not enabled with up to date anti-malware • Attributed to Q4 BYOD pilot

#8 Master Your Message

Effective Communications

"Security people don't speak our language. In fact, at each briefing they seem to speak a different language."

- Board Member



MORE THAN 243,000 PHOTOS UPLOADED

MORE THAN 3.8 MILLION SEARCHES ON GOOGLE

MORE THAN 350,000 TWEETS SENT

MORE THAN 65,000 PHOTOS UPLOADED

MORE THAN 210,000 SNAPS UPLOADED

120 NEW ACCOUNTS CREATED ON LINKEDIN

MORE THAN 29 MILLION MESSAGES PROCESSED

1 MILLION PHOTOS

175,000 VIDEO MESSAGES SHARED

MORE THAN 156 MILLION E-MAILS SENT

MORE THAN 87,000 HOURS OF VIDEO WATCHED

MORE THAN 25,000 POSTS ON TUMBLR

16,550 VIDEO VIEWS ON VIMEO

MORE THAN 1,000,000 SWIPES

18,000 MATCHES ON TINDER

MORE THAN 500,000 APPS DOWNLOADED

MORE THAN 50 NEW REVIEWS

MORE THAN 1000 IMAGES UPLOADED

AROUND 200 EVENT TICKETS SOLD ON EVENTBRITE

MORE THAN 2,000,000 MINUTES OF CALLS DONE BY SKYPE USERS

MORE THAN 5,500 CHECKINS ON FOURSQUARE

MORE THAN 800,000 FILES UPLOADED ON DROPBOX

AROUND 700,000 HOURS OF VIDEOS WATCHED

MORE THAN 400 HOURS OF VIDEOS UPLOADED

70,000 HOURS OF VIDEO CONTENT WATCHED

THINGS THAT HAPPEN ON INTERNET EVERY 60 SECONDS

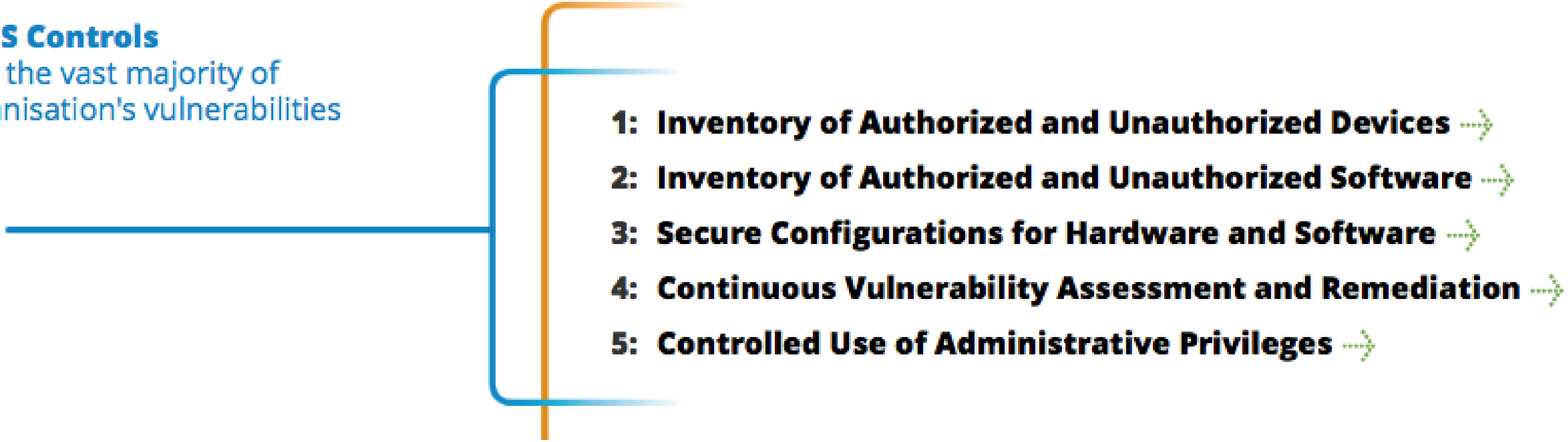
#9 | Champion Change

Breaking Down the Walls

- Agile
  - Break down walls between development and the business
- DevOps
  - Break down walls between development and operations
- SecDevOps
  - Break down walls between security and development, operations, business

Improve Effectiveness

CIS Controls



First 5 CIS Controls
Eliminate the vast majority of your organisation's vulnerabilities

1: Inventory of Authorized and Unauthorized Devices

2: Inventory of Authorized and Unauthorized Software

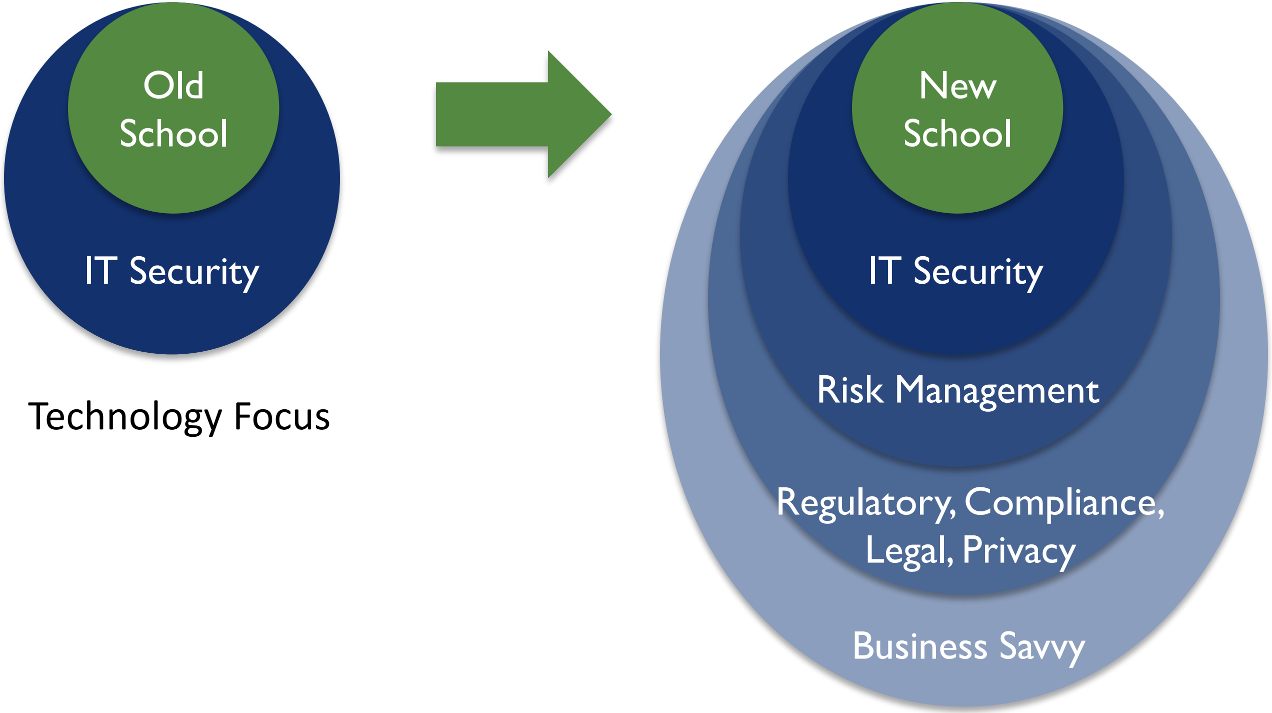
3: Secure Configurations for Hardware and Software

4: Continuous Vulnerability Assessment and Remediation

5: Controlled Use of Administrative Privileges

#10 | Solve Business Problems

Evolution of Security Leadership



Technology Focus

Business Focus

Graphic credit: https://www.rsaconference.com/writable/presentations/file_upload/prof-m07-from-cave-man_to-business-man-the-evolution-of-the-ciso-to-ciro.pdf

SANS MANAGEMENT
CYBER LEADER

CURRICULUM

Get the right training to build and lead a world-class security team.

FOUNDATIONAL

MGT512
SANS Security Leadership Essentials for Managers with Knowledge Compression™
GSLC

MGT414
SANS Training Program for CISSP® Certification
GISP

SEC566
Implementing and Auditing the Critical Security Controls – In-Depth
GCCC

MGT525
IT Project Management, Effective Communication, and PMP® Exam Prep
GCPM

CORE

MGT514
IT Security Strategic Planning, Policy, and Leadership

MGT415
A Practical Introduction to Cybersecurity Risk Management

NEW!
MGT517
Managing Security Operations: Detection, Response, and Intelligence

LEG523
Law of Data Security and Investigations
GLEG

SPECIALIZATION

AUD507
Auditing & Monitoring Networks, Perimeters, and Systems
GSNA

MGT433
Securing the Human: How to Build, Maintain, and Measure a High-Impact Awareness Program

MGT305
Technical Communication and Presentation Skills for Security Professionals

SANS Security Leadership POSTER

CISO Mind Map
Version 1.0

AND

Security Operations Center (SOC) Essential Functions

For Cyber Leaders of Today and Tomorrow

sans.org/curricula/management

CISO MIND MAP v1.0

Security Operations

□ Prevention
- Data Protection
  - Encryption, PKI, TLS
  - Data Loss Prevention (DLP)
  - Email Security
- Network Security
  - Firewall, IDS/IPS, Proxy Filtering
  - VPN, Security Gateway
  - DDoS Protection
- Application Security
  - Threat Modeling
  - Design Review
  - Secure Coding
  - Static Analysis
  - Web App Scanning
  - WAF, RASP
- Endpoint Security
  - Antivirus, Anti-malware
  - HIDS/HIPS, FIM
  - App Whitelisting
- Secure Configurations
- Active Defense
- Patching

□ Detection
- Log Management/SIEM
- Continuous Monitoring
- Network Security Monitoring
- NetFlow Analysis
- Advanced Analytics
- Threat Hunting
- Penetration Testing
- Red Team
- Vulnerability Scanning
- Human Sensor
- Data Loss Prevention (DLP)
- Security Operations Center (SOC)
- Threat Intelligence
- Threat Information Sharing
- Industry Partnerships

□ Response
- Incident Handling Plan
- Breach Preparation
- Tabletop Exercises
- Forensic Analysis
- Crisis Management
- Breach Communications

Legal and Regulatory

□ Compliance
- PCI
- SOX
- HIPAA
- FFIEC, CAT
- FERPA
- NERC CIP
- NIST SP 800-37 and 800-53

□ Privacy
- Privacy Shield
- EU GDPR

□ Audit
- SSAE 16
- SOC 2
- ISO 27001
- FISMA and FedRAMP
- NIST SP 800-53A
- COSO

□ Investigations
- eDiscovery
- Forensics

□ Intellectual Property Protection

□ Contract Review

□ Customer Requirements

□ Lawsuit Risk

Business Enablement

□ Product Security
- Secure DevOps
- Secure Development Lifecycle
- Bug Bounties
- Web, Mobile, Cloud AppSec

□ Cloud Computing
- Cloud Security Architecture
- Cloud Guidelines

□ Mobile
- Bring Your Own Device (BYOD)
- Mobile Policy

□ Emerging Technologies
- Internet of Things (IoT)
- Augmented Reality (AR)
- Virtual Reality (VR)

□ Mergers and Acquisitions
- Security Due Diligence

CYBER LEADER

Identity and Access Management

□ Provisioning/Deprovisioning
□ Single Sign On (SSO)
□ Federated Single Sign On (FSSO)
□ Multi-Factor Authentication
□ Role-Based Access Control (RBAC)
□ Identity Store (LDAP, ActiveDirectory)

Risk Management

□ Risk Management Frameworks
□ Risk Assessment Methodology
□ Business Impact Analysis
□ Risk Assessment Process
□ Risk Analysis and Quantification
□ Security Awareness
□ Vulnerability Management
□ Vendor Risk Management
□ Physical Security
□ Disaster Recovery (DR)
□ Business Continuity Planning
□ Policies and Procedures
□ Risk Treatment
- Mitigation Planning, Verification
- Remediation, Cyber Insurance

Governance

□ Strategy
□ Business Alignment
□ Risk Management
□ Program Framework
- NIST CSF
- ISO 27000

□ Control Frameworks
- NIST 800-53
- Critical Security Controls (CSC)

□ Program Structure
□ Program Management
□ Communications Plan
□ Roles and Responsibilities
□ Workforce Planning
□ Resource Management
□ Data Classification
□ Security Policy
□ Creating a Security Culture
□ Security Training
- Awareness Training
- Role-Based Training

□ Metrics and Reporting
□ IT Portfolio Management
□ Change Management
□ Board Communications

Leadership Skills

□ Business Strategy
□ Industry Knowledge
□ Business Acumen
□ Communication Skills
□ Presentation Skills
□ Strategic Planning
□ Technical Leadership
□ Security Consulting
□ Stakeholder Management
□ Negotiations
□ Mission and Vision
□ Values and Culture
□ Roadmap Development
□ Business Case Development
□ Project Management
□ Employee Development
□ Financial Planning
□ Budgeting
□ Innovation
□ Marketing
□ Leading Change
□ Customer Relationships
□ Team Building
□ Mentoring

Based on CISO MindMap by Rafeeq Rehman @rafeeq_rehman http://rafeeqrehman.com Used with permission.

Ten Tenets of CISO Success

- #1 Create Credibility
- #2 Catch the Culture
- #3 Relate to Risk
- #4 Shape the Strategy
- #5 Deliver the Deal
- #6 Invest in Individuals
- #7 Make Metrics Matter
- #8 Master Your Message
- #9 Champion Change
- #10 Solve Business Problems

Frank Kim

@fykim

www.frankkim.net

Material based on SANS MGT514
Security Strategic Planning, Policy, and Leadership