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

**Threats**

- Advanced Persistent Threats
- Activists
- Organized Crime
- Partners
- Insider Threats
- Basic Threats
- Mobile Devices
- Mobile Payments
- Wireless Network
- Global Network
- First Website
- First Mobile App
- Cloud Computing
- Internet of Things
- Big Data
- Nation States
- Stuxnet
- Edward Snowden
- "Year of the Breach…"

**Technology**

- Mobile Payments
- Wireless Network
- Global Network
- Mobile Devices
- Cloud Computing
- Internet of Things
- Big Data
- Nation States
- Stuxnet
- Edward Snowden
- "Year of the Breach…"

$1 Trillion Cost of Cyber crime

- World Economic Forum

Graphic credit: Omar Khawaja

Cost of Cyber crime

- World Economic Forum
#3 Create 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

- 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

Identify
Protect
Detect
Respond
Recover

Lagging  Industry  Leading

0 1 2 3 4 5

Current state
Target state
#5 Deliver the Deal
# RSA

**Mapping to Strategic Objectives**

<table>
<thead>
<tr>
<th>Financial/Stewardship</th>
<th>Customer/Stakeholder</th>
<th>Internal Business Process</th>
<th>Organizational Capacity or “Security Capability”</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lower costs</td>
<td>Improved compliance &amp; regulatory</td>
<td>Improved availability &amp; resiliency</td>
<td>Improved knowledge &amp; skills</td>
</tr>
<tr>
<td>Increased profitability</td>
<td>Lower wait times</td>
<td>Increase process efficiency</td>
<td>Improved tools &amp; technology</td>
</tr>
<tr>
<td>Increased revenue</td>
<td>Improved satisfaction</td>
<td>Lower cycle times</td>
<td>Business innovation/new product support</td>
</tr>
</tbody>
</table>

- Increased profitability
- Increased revenue
- Lower wait times
- Improved satisfaction
- Lower cycle times
- Business innovation/new product support
- Improved availability & resiliency
- Improved compliance & regulatory
- Improved process efficiency
- Improved knowledge & skills
- Improved tools & technology
- Improved availability & resiliency
- Improved compliance & regulatory
- Improved process efficiency
- Improved knowledge & skills
- Improved tools & technology
- Improved availability & resiliency
- Improved compliance & regulatory
- Improved process efficiency
- Improved knowledge & skills
- Improved tools & technology
- Improved availability & resiliency
- Improved compliance & regulatory
- Improved process efficiency
- Improved knowledge & skills
- Improved tools & technology
- Improved availability & resiliency
- Improved compliance & regulatory
- Improved process efficiency
- Improved knowledge & skills
- Improved tools & technology
- Improved availability & resiliency
- Improved compliance & regulatory
- Improved process efficiency
- Improved knowledge & skills
- Improved tools & technology
- Improved availability & resiliency
- Improved compliance & regulatory
- Improved process efficiency
- Improved knowledge & skills
- Improved tools & technology
- Improved availability & resiliency
- Improved compliance & regulatory
- Improved process efficiency
- Improved knowledge & skills
- Improved tools & technology
- Improved availability & resiliency
- Improved compliance & regulatory
- Improved process efficiency
- Improved knowledge & skills
- Improved tools & technology
- Improved availability & resiliency
- Improved compliance & regulatory
- Improved process efficiency
- Improved knowledge & skills
- Improved tools & technology
- Improved availability & resiliency
- Improved compliance & regulatory
- Improved process efficiency
- Improved knowledge & skills
- Improved tools & technology
- Improved availability & resiliency
- Improved compliance & regulatory
- Improved process efficiency
- Improved knowledge & skills
- Improved tools & technology
- Improved availability & resiliency
- Improved compliance & regulatory
- Improved process efficiency
- Improved knowledge & skills
- Improved tools & technology
- Improved availability & resiliency
- Improved compliance & regulatory
- Improved process efficiency
- Improved knowledge & skills
- Improved tools & technology
- Improved availability & resiliency
- Improved compliance & regulatory
- Improved process efficiency
- Improved knowledge & skills
- Improved tools & technology
- Improved availability & resiliency
- Improved compliance & regulatory
- Improved process efficiency
- Improved knowledge & skills
- Improved tools & technology
- Improved availability & resiliency
- Improved compliance & regulatory
- Improved process efficiency
- Improved knowledge & skills
- Improved tools & technology
- Improved availability & resiliency
- Improved compliance & regulatory
- Improved process efficiency
- Improved knowledge & skills
- Improved tools & technology
- Improved availability & resiliency
- Improved compliance & regulatory
- Improved process efficiency
- Improved knowledge & skills
- Improved tools & technology
- Improved availability & resiliency
- Improved compliance & regulatory
- Improved process efficiency
- Improved knowledge & skills
- Improved tools & technology
- Improved availability & resiliency
- Improved compliance & regulatory
- Improved process efficiency
- Improved knowledge & skills
- Improved tools & technology
- Improved availability & resiliency
- Improved compliance & regulatory
- Improved process efficiency
- Improved knowledge & skills
- Improved tools & technology
- Improved availability & resiliency
- Improved compliance & regulatory
- Improved process efficiency
- Improved knowledge & skills
- Improved tools & technology
- Improved availability & resiliency
- Improved compliance & regulatory
- Improved process efficiency
- Improved knowledge & skills
- Improved tools & technology
- Improved availability & resiliency
Provide Options

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

<table>
<thead>
<tr>
<th></th>
<th>Option A</th>
<th>Option B</th>
<th>Option C</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business value</td>
<td>✔</td>
<td>✔✔</td>
<td>✔✔✔</td>
</tr>
<tr>
<td>Risk reduction</td>
<td>⚠️</td>
<td>⚫️</td>
<td>⚫️</td>
</tr>
<tr>
<td>Cost</td>
<td>$</td>
<td>$$</td>
<td>$$$</td>
</tr>
</tbody>
</table>
#6 Invest in Individuals
## Putting Leadership Into Perspective

<table>
<thead>
<tr>
<th>Boss X</th>
<th>Manager ✔</th>
<th>Leader ✔</th>
</tr>
</thead>
<tbody>
<tr>
<td>Drives people</td>
<td>Manages things</td>
<td>Coach, mentor, and grow people</td>
</tr>
<tr>
<td>Thinks short-term</td>
<td>Thinks mid-term</td>
<td>Thinks long-term</td>
</tr>
<tr>
<td>Focused on self</td>
<td>Focused on process</td>
<td>Focused on people</td>
</tr>
<tr>
<td>Instills fear</td>
<td>Earns respect</td>
<td>Generates enthusiasm</td>
</tr>
<tr>
<td>Says “I”</td>
<td>Says “Our”</td>
<td>Says “We”</td>
</tr>
<tr>
<td>Micromanages</td>
<td>Delegates</td>
<td>Motivates</td>
</tr>
<tr>
<td>Places blame on roadblocks</td>
<td>Navigates roadblocks</td>
<td>Removes roadblocks</td>
</tr>
<tr>
<td>Dictates how it’s done</td>
<td>Shows how it’s done</td>
<td>Influences how it’s done</td>
</tr>
<tr>
<td>Takes credit</td>
<td>Shares credit</td>
<td>Gives credit</td>
</tr>
<tr>
<td>Commands</td>
<td>Asks</td>
<td>Influences</td>
</tr>
<tr>
<td>Says “Go”</td>
<td>Says “Let’s go”</td>
<td>Says “Way to go”</td>
</tr>
</tbody>
</table>
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
Focus & actions increase as you move up the pyramid

Volume of information increases as you move down the pyramid
Balanced Scorecard Example

<table>
<thead>
<tr>
<th><strong>Financial/Stewardship</strong></th>
<th><strong>Customer / Stakeholder</strong></th>
<th><strong>Internal Business Process</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Q4 % Product Development Budget Allocated to Security</td>
<td>Q4 % of Products Delivered On Time and On Budget</td>
<td>Q4 % of Developers Training in Secure Coding Principles</td>
</tr>
<tr>
<td><strong>Target 5% ✔ Trend ➔ 5%</strong></td>
<td><strong>Target 95% ✔ Trend ➔ 95%</strong></td>
<td><strong>Target 95% ✔ Trend ➔ 97%</strong></td>
</tr>
<tr>
<td>• Increased support for legal as they piloted their case management system</td>
<td>• 18% increase over Q3 in on-time and on budget delivery. Security staffed temporary PMO team to meet goal</td>
<td>• 100% of flagship application developers completed training reducing overall risk to organization</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Q4 &amp; YTD Security Budget Allocation</th>
<th>Customer Satisfaction</th>
<th>Q4 % of Developers Attaining Certification</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Target 90% ✗ Trend ➔</strong></td>
<td><strong>Target 90% ✗ Trend ➔</strong></td>
<td><strong>Target 95% ✗ Trend ➔ 42%</strong></td>
</tr>
<tr>
<td>• 8% increase over Q3 in customer satisfaction rating of 4 or higher out of 5 possible</td>
<td></td>
<td>• Mitigation plan: Follow-up with developers after training is complete for certification</td>
</tr>
</tbody>
</table>
## Security Capability Example

<table>
<thead>
<tr>
<th>Security Capability</th>
<th>Status</th>
<th>Trend</th>
<th>Highlights</th>
</tr>
</thead>
</table>
| **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
“Security people don’t speak our language. In fact, at each briefing they seem to speak a different language.”

- Board Member
THINGS THAT HAPPEN ON THE INTERNET EVERY 60 SECONDS

- 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 on LinkedIn
- 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 25,000 posts on Tumblr
- Netflix
- More than 87,000 hours of video watched
- More than 2,000,000 minutes of calls done by Skype users
- Around 200 event tickets sold on Eventbrite
- More than 1,000 images uploaded
- More than 500,000 apps downloaded
- More than 100,000 swipes
- More than 18,000 matches on Tinder
- 16,550 video views on Vimeo
- More than 50 new reviews
- Around 700,000 hours of videos watched
- More than 800,000 files uploaded on Dropbox
- More than 400 hours of videos uploaded
- More than 5,500 check-ins on Foursquare
- More than 65,000 photos snaps uploaded.
#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

Old School
IT Security
Technology Focus

New School
IT Security
Risk Management
Regulatory, Compliance, Legal, Privacy
Business Savvy
Business Focus

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