The Data IPO: Don't Let It Happen to You

Carlos Casanova
President & Solutions Architect, K2 Solutions Group
Carlos.casanova@k2sg.com

Session Description

Security and risk management are not a one-and-done or spot solution activity. Similarly, neither are hacking or breaching corporate defenses. Both require various forms of persistent effort to reach a goal. This session will look at how the governance support structures from ITIL fall right in line and support the principle of implementing security in layers. Everything must work together to support and improve business outcomes. Resilience through comprehensive governance, drawn from various frameworks, is the only way to keep your data from filing for an IPO. (Experience Level: Fundamental)

Speaker Background

Carlos Casanova is Founder and President of K2 Solutions Group, Inc., and co-author of The CMDB Imperative: How to Realize the Dream and Avoid the Nightmares (2009). He is an Executive and Sr. Leadership adviser specializing in operational effectiveness and efficiency initiatives with firsthand experience in various operational areas including Security, Risk Management, Disaster Recovery and Business Continuity. He guides organizations through their challenges associated with strategizing, designing, and executing real-world organizational change.
The individual or thing within any given system that is the most adaptable and has the most flexibility has control over the system...

If we don’t change how we protect our most precious assets, we become vulnerable to attackers, those seeking to do us harm and expose our information...

Is it in your genes to protect?
Governance:
Broadly refers to
- Mechanisms
- Processes
- Relations
by which there is control & direction.

Do you have the right mindset?

Sometimes a layered three legged model is necessary for system survival and data safety!
Complex Process
• Flexible
• Prevent
• Observant

“Advanced targeted attacks make prevention centric strategies obsolete”

Neil MacDonald
VP Distinguished Analyst at Gartner
There is no chance, no destiny, no fate, that can circumvent or hinder or control the firm resolve of a determined soul.

Compliance alone is NOT Sufficient

It’s just a legal manifestation of a false security
Sharing feedback across all areas of the organization is essential to providing a corporate environment that is safe...

...and protected to the extent possible.

Coordinated Efforts
+ Working in Unison
Reliable Governance
Disasters evolve from breaches
Are you prepared?
Can you respond?
Can you recover?
How long will it take?
How resilient are you?

What business outcome are you trying to avoid?
Financial Loss, Public Relations, IP Theft, Safety...
The survival of your most precious asset, your data, is based on if you are prepared for what could threaten it!

Resilience is the state when you have achieved adaptability.
What doesn’t kill you, makes you stronger

Security
2015 KPMG survey*

4 out of 5 health execs say company data has been compromised

*223 U.S.-based health care executives at companies having at least $500 million in revenue

### Top 10 Breaches

<table>
<thead>
<tr>
<th>Breach</th>
<th>Number of Data Records</th>
<th>Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>Various Retailers*</td>
<td>160,000,000 (2012)</td>
<td></td>
</tr>
<tr>
<td>ADOBE</td>
<td>152,000,000 (2014)</td>
<td></td>
</tr>
<tr>
<td>Ebay</td>
<td>145,000,000 (2014)</td>
<td></td>
</tr>
<tr>
<td>Heartland</td>
<td>130,000,000 (2009)</td>
<td></td>
</tr>
<tr>
<td>TJX</td>
<td>94,000,000 (2007)</td>
<td></td>
</tr>
<tr>
<td>AOL</td>
<td>92,000,000 (2004)</td>
<td></td>
</tr>
<tr>
<td>Anthem</td>
<td>80,000,000 (2015)</td>
<td></td>
</tr>
<tr>
<td>Sony PSN</td>
<td>77,000,000 (2011)</td>
<td></td>
</tr>
<tr>
<td>JP Morgan Chase</td>
<td>76,000,000 (2014)</td>
<td></td>
</tr>
<tr>
<td>US Military</td>
<td>76,000,000 (2009)</td>
<td></td>
</tr>
<tr>
<td>Ashley Madison</td>
<td>37,000,000 (2015)</td>
<td></td>
</tr>
<tr>
<td>Adult Friend Finder</td>
<td>3,900,000 (2015)</td>
<td></td>
</tr>
<tr>
<td>Match.com UK</td>
<td>?? (2015)</td>
<td></td>
</tr>
<tr>
<td>US Off. Prsnl Mgmt</td>
<td>4,000,000 (2014) 1st Breach</td>
<td></td>
</tr>
<tr>
<td>US Off. Prsnl Mgmt</td>
<td>21,500,000 (2014) 2nd Breach</td>
<td></td>
</tr>
<tr>
<td>Premera</td>
<td>11,000,000 (2015)</td>
<td></td>
</tr>
</tbody>
</table>

*Over eight years, a hacking ring targeted banks, payment processors and chain stores, to steal more than 160 million credit and debit card numbers, targeting more than 800,000 bank accounts.

**Over 1 BILLION data records compromised**


Total Breaches

<table>
<thead>
<tr>
<th>Year</th>
<th>Number</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>2014</td>
<td>312</td>
<td>(23%)</td>
</tr>
<tr>
<td>2013</td>
<td>253</td>
<td>(62%)</td>
</tr>
<tr>
<td>2012</td>
<td>312</td>
<td></td>
</tr>
</tbody>
</table>

Breaches with More Than 10M Identities Exposed

<table>
<thead>
<tr>
<th>Year</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>2014</td>
<td>4</td>
</tr>
<tr>
<td>2013</td>
<td>8</td>
</tr>
<tr>
<td>2012</td>
<td>1</td>
</tr>
</tbody>
</table>

Top Causes of Data Breaches, 2014 & 2013

<table>
<thead>
<tr>
<th>Cause</th>
<th>Number of Incidents</th>
<th>Percent</th>
<th>2014</th>
<th>2013</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attackers</td>
<td>153</td>
<td>49%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Accidentally Made Public</td>
<td>67</td>
<td>22%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Theft or Loss of Computer or Drive</td>
<td>66</td>
<td>21%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Insider Theft</td>
<td>26</td>
<td>8%</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

It’s not so much a matter of **if** you will be successfully attacked, but **when**.

33% - Financial Gain
24% - Disrupt Service
19% - IP Theft


- White Hats
- Black Hats
- Grey Hats
- Script Kiddies
- Hacktivists
- State Sponsored
- Spy/Corp Espionage
- Cyber Terrorist

They’re coming at you from all directions
Vigilance
2012 → 2013

2013 Year of Mega Breach
8 Breaches exposed more than 10M identities each


2013 → 2014

113% increase in Ransomware attacks driven by more than 4,000% increase in crypto-ransomware attacks.

Are you asleep at the wheel?
Ethical Hacking?

“If ignorant both of your enemy and yourself, you are certain to be in peril”

~Sun Tzu

EVERY person in EVERY Department is responsible for Detection, Readiness & Response
What Next?

**Educate** yourself & teams on CyberSecurity (i.e. awareness, detection, response...)

**Evaluate** your data protection strategy related to both storage and transmission

**Improve** operational efficiency and effectiveness efforts related to patches and secure configurations
What Next?

**Governance** must be improved around incidents and events. Don’t assume they’re always benign. Find the patterns.

**Harden** environment by retiring weak platforms and/or buying more secure ones

**Simplify** Less things to attack means less to protect. Keep It Simple!

Frameworks to Leverage

**COBIT 5** - Control Objectives for Information & Related Technologies (ISACA)

**ISO 27000/1/2** - 27001 defines requirements 27002 defines operational steps of info security program (International Standards Organization)

**NIST SP 800** Info Security Standard and Best Practices (National Institute of Standards & Tech)
Cyber resilience is **NOT** something you do, It’s something you are.

Is the knowledge to protect and keep data private in your genes?

“It is not the strongest of the species that survives, nor the most intelligent, but the one most responsive to change.”

-Charles Darwin, 1809
Thank you for attending this session.

Please don’t forget to complete an evaluation form!