Information Security is a Marketing responsibility
Thank you!

Stephen Coates  Gallagher  Laura Bell  SafeStack
Andrew Kelly  Insomnia  Shahn Harris  Beca

(1) People - Process - Technology (that order)
(2) Infosec risks ≡ Business risks
(3) Governance: be wary of sneaky MVPs, proofs-of-concept, and digital disruption
Carlos Cordero | Principal
carlos.cordero@convergence.com
@Convergence
convergence.com

- Business consultant
- Work with the marketing organisation/function/team to make it more effective
Information Security is a Marketing responsibility

Problem is nobody has sent them the memo :(
The current situation
Hello Barbie Doll

“Chat with Barbie for a whole new way to play!”

“What Hello Barbie doll uses WiFi and speech recognition technology to engage in two-way dialogue”

“This is a US only product. The Hello Barbie companion app can only be found in US app stores.”

Source: Amazon’s product page

What Does Hello Barbie Say?

Hello Barbie converses using 4300 different sentences and expressions (lines). Mattel and ToyTalk “are consistently updating and enhancing the product’s vocabulary…”

Source: Hello Barbie Doll’s Lines document
Hello Barbie App, Hello Security Issues

Mobile App Security Issues

[1] “The app can be modified to reveal confidential information including authentication credential passwords.”

[2] “The app will connect a mobile device to any unsecured Wi-Fi network if it has “Barbie” in the name, allowing for a network spoofing attack to occur by an attacker impersonating the Barbie network to steal data.”

[3] “The app utilizes an authentication credential that can be re-used by attackers.”

[4] “The app shipped with unused code that serves no function but increases the overall attack surface.”

Server-Side Security Issues

[5] “Client certificate authentication credentials can be used outside of the app by attackers to probe any of the Hello Barbie cloud servers to look for more vulnerabilities.”

[6] “The ToyTalk server domain was on a cloud infrastructure susceptible to the POODLE attack, allowing attackers to downgrade connection security and listen in on communications to the server such as uploaded conversation from the doll.”

Source: Andrew Hayes (Director of Research at OpenDNS) and Bluebox Security (Bluebox Labs), “Hello Barbie App, Hello Security Issues”, published 4th Dec. 2015.
Availability

Authentication

Utility

Confidentiality

Integrity

Possession

Source: Andrew Hayes (Director of Research at OpenDNS) and Bluebox Security (Bluebox Labs), “Hello Barbie App, Hello Security Issues”, published 4th Dec. 2015.
How did we get here?
Marketers circa 1994

Image: Netflix
Marketers in 2016

Image: DreamWorks LLC, Paramount Pictures, Amblin Entertainment
Marketers ~1994
(In control of all the cards)

- Awareness
- Interest

Marketing objectives

Traditional media
Direct marketing

Marketing platforms

“database”

Marketing stack

Marketers in 2016
(Under extreme pressure. Customers have all the cards)

- Permanent Engagement
- Total Customer Experience

Extending products/services by using digital technologies

- Become stewards of the whole customer experience Lifecycle

Marketing performance and operational effectiveness

- Anything to enable and manage experiences, deliver digitally enhanced products and services, facilitate the customer journeys, and support marketing operations.

Highly fragmented.
Shadow IT: acquiring + developing
Syphons data all over the place.
Integration is a nightmare.
Current mindset of “The Marketers”
The marketer’s plate is REALLY FULL
MARKETERS ARE TRYING TO MAKE SENSE OF THEIR SITUATION
(1) What is their job about?  (2) How to do their job

Marketing Stack
Automation
Proactive Personalisation
Insights Big Data

Stewards of the Lifecycle
Total Customer Experience
Customer Journey Innovation
Operational Effectiveness

What does success look like?
Balance Creativity vs. Effectivity?
Ad avoidance?

Break Silos!
Partner CIO
New Capabilities
Agile!
What we do in the Shadows

Image: Shadow Pictures Ltd
Under extreme pressure and conflicting agendas something always ends up all screwed up

**PRIVACY**: a conflicting agenda

INFOSEC is **NOT** on the radar. (besides, that is ________ problem, not ours.)
Map of marketing related infosec Risks
Meet “Fluffy”
3 marketing-related infosec Risks

Products and services that are made with digital technology

(a) Digital technology is part of or the core of the product/service itself

(b) Digital layer that extends the core product/service

Marketing Stack (digital services/products + marketing operations)

Digital engagement & customer experience applications that “innovate” the customer journeys

Infosec Pros are not being invited to the digital transformation party (yet).
When Infosec Pros are not invited from day one…

Products and services that are made with digital technology

To patch your 2014 Jeep Cherokee you need a USB stick
Misconfigured MongoDB installation discovered by Chris Vickery, on 19th Dec. 2015, and disclosed to Sanrio.

Up to 3’300,000 user accounts were vulnerable - 186,261 belonging to minors (as confirmed by Sanrio’s investigation).
Highly fragmented. Shadow IT: acquiring + developing Syphons data all over the place. Integration is a nightmare.
Predictions and implications for INFOSEC Professionals
A combination of risk factors that we know well

<table>
<thead>
<tr>
<th>Extreme demands and expectations</th>
<th>No major catastrophe has occurred yet</th>
<th>Technology: complex and dynamic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ignorance</td>
<td>No punitive consequences have eventuated</td>
<td>Attitudes towards risks and uncertainty</td>
</tr>
<tr>
<td>Leadership vacuum</td>
<td>Clashing priorities: results/speed vs. quality/risks</td>
<td>IoT: new, untested, vast scale</td>
</tr>
</tbody>
</table>
January 28, 1986
Challenger
7 astronauts died

The causes were human nature (attitudes towards risks under conditions of uncertainty) and management practice that has clashing priorities.
We are fighting human nature and management practice that has clashing priorities

Experiences in developed countries over the past thirty years have demonstrated that the risks for road accidents can be substantially prevented. However, investment in road accident prevention in low and middle income countries is currently inadequate for meeting this growing public health concern; the implementation of cost-effective safety measures is not widespread.

Source: WorldBank’s website “Addressing the Road Safety Challenges in East Asia & Pacific Region”
February 1, 2003
Columbia
7 astronauts died

17 years later the causes remained the same.
Implication for Infosec Pros: we need to **catalyse** and **drive** the change in the organisation. To **lead**.

<table>
<thead>
<tr>
<th>Command the attention of marketers</th>
<th>Reduce the risk surface at the “concept” stage</th>
<th>Best of class technology management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Educate Train</td>
<td>Make the cost of a catastrophe very expensive</td>
<td>Timely and adequate risk assessments</td>
</tr>
<tr>
<td>Leaders setting priorities and driving change</td>
<td>Influence the priorities by surfacing risks</td>
<td>Frameworks “connected” to marketing praxis</td>
</tr>
</tbody>
</table>
What am I suggesting?
If the Lonely Mountain does not come to the dwarves, the dwarves have to go to the mountain...
Infosec Pros need to become leaders

<table>
<thead>
<tr>
<th>Win the Board as ally. Then win the Exec. Comm.</th>
<th>Lead the digital transformation (with IT guys)</th>
<th>Educate about technological risks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Join the process from the concept stage (its start)</td>
<td>Connect security incidents to brand damage</td>
<td>Co-develop risk assessment practices</td>
</tr>
<tr>
<td>Help marketing to adopt Agile approaches</td>
<td>Connect risk management to brand benefit</td>
<td>Reduce the friction for marketers</td>
</tr>
</tbody>
</table>
Leaders rise when the times call for them.

It is our time.
Thank you!

Happy to answer your questions at the pub ;)

(or just contact me: carlos.cordero@convergnce.com)