Business Value of IT Security

Ricardo Mariano González
Head of Operational Risk & Control
Zurich Spain

Disclaimer: The opinions expressed in this presentation are those of the presenter, and do not necessarily represent the view of Zurich Seguros (Zurich in Spain), Zurich Insurance Company Ltd. or the Zurich Insurance Group
The problem

- Business leaders do not see IT Security as a competitive advantage. A necessary cost, or something to be avoided.
- High-profile cases help (for a while), but “it won’t happen to me”.
- What if we just…minimize the spending in IT Security?
The problem

- Budget is still scarce (cuts, scrutiny of spending and cash management)
- Concerns about IT: risks, decisions and implementations
- Interconnected risks (outsourcers, supply chain…)
- Business demand more open access to data and systems
- The gap is vast. It won’t get small.
Uncomfortable Questions

“Why you guys speak so funny? Nobody else in the Company can understand you.”

“Are we getting enough from what we’re spending?”

“If I give you more money, will I get more?”
Uncomfortable Questions

“Here’s the balance sheet: please explain to me how the ‘Information Security’ line translates into ‘Less Business Risks’, in a language I can understand”
Business Language, please

The story goes:

- Businesses run on IT, including IT Security (they already know this).
- (Via some financial processes) Finance assigns money to IT
- IT uses that money to run its hardware, software, people and services
- Later on, Finance should verify that IT used that money properly

…but…
Business Language, please

…Finance does not always do that,

…IT does not always ensure this verification happens, and then

…the value of IT is not always demonstrated

If you can’t prove is competitive, then is expensive
Business Language, please

Expectations:

- Business are used to immediate results.
- The CIO / CISO does not want to disappoint and might over promise.
- But IT projects do have delays:
  - From spending, to implementation
  - From implementation, to measurable return
- Results and benefits are difficult to measure
- Target DOES move: hard to prove you reached where you wanted
Information Security…

…does it really have a value of its own?
Finding Value

“What if we just…do not spend in IT Security?”

Figure 1: The cost of inaction – two illustrative scenarios for an organisation’s approach to Information Security

Key event

Total Lifecycle Cost of Information Security = Lifecycle costs of deploying and operating security solutions + Reputational value + Intellectual Property value + Operational effectiveness + Financial impact of incidents

Source: “Revolution or evolution?” The Technology Strategy Board & PWC
Finding Value

“Is there a way to spend thinking about maximum return?”

First think about “what to do”, then “how to do it”

- Commodities, infrastructure: price, or “how much”
- Laws and regulations: depth, or “how far”
- Investments: cost-benefit, or “how much to produce a desired outcome”
- Cave at: “Return of Investment” and “Business Value” are not synonyms!!!
Finding Value

“If we do better IT Security than the competition, will we be more Valuable?”

– Threshold condition
– Sufficient security
– Intellectual property
– Sales percentage

IT Security fosters Innovation

– Investment in Social, Mobility, Cloud, BYOD, Big Data…
– Peace of mind to try out new things and explore new products/services
– Customer & Shareholder trust
Managing Communications and Expectations

- Benefit: only if Business understand it
- Use standard presentation formats and value measures.
- Ensure you’re aligned with your CEO / CFO. Is easy.
Articulating Value

Do you know what your Business wants from IT? You’re sure?

Source: ValueBridge Advisors LCC, used by permission
Articulating Value

Another model, following Business Strategy:

**Growth:** ITSec can protect the business, safeguard revenue and free-up resources to increase revenue.

**Innovation:** Data needs to be secure, privacy is critical. ITSec can help demonstrate leadership.

**Optimization:** ITSec can optimize the costs of protecting information (not all of it in the ITSec function).

**Protection:** ITSec can demonstrate strong and effective monitoring, good governance and transparency.
Articulating Value

Invest where less money brings more effect
Articulating Value

Align…

— to your IT and Business strategy,
— to your Portfolio and Program management

Understand who will benefit, and meet them

Measure:

— Use **existing metrics**, already aligned to organizational objectives
— Use the **same value measures** in investment portfolios and daily operations (i.e. when deciding, and when reporting)
Examples...

- **Business Strategy**
  - **Growth**
    - **IT Alignment**
      - Commodity / Efficiency
    - **ITSec aligned task**
      - Free up Resources
    - **ITSec contr.**
      - Help demonstrate Leadership
      - Benchmark with peers & competition
  - **Innovate**
    - **IT Alignment**
      - Competitive Weapon
    - **ITSec aligned task**
      - Reduce costs
      - - Cost structure (function internal and external)
      - - Risk-based cost-saving opportunities
  - **Innovate**
    - **IT Alignment**
      - Reliable Business
    - **ITSec aligned task**
      - Protect Customer Privacy
      - # privacy requests received, complied
      - Compliance with privacy laws & regulations
  - **Innovate**
    - **IT Alignment**
      - Competitive Weapon
    - **ITSec aligned task**
      - Secure Big Data
      - Data volume & incident
  - **Innovate**
    - **IT Alignment**
      - Reliable Business
    - **ITSec aligned task**
      - Prove good governance
      - Measure and monitor according to proven Standards and Frameworks
Shifting from Cost-Centre to Differentiator

- Monitor alignment (ITSec initiatives, IT portfolio, Business portfolio)
- Engage the Risk Manager: how can I reduce business risks, and risks from IT?

- You can transfer some of those risks (and also have a handy quantification!)

- Give the next step: IT Risk Management
Final thoughts...

- IT Security is not only cost; it is a strategic investment in reduction of corporate risk, and a positive contribution to the realization of business value.

- There is no “one-size-fits-all” recipe. There is a right answer for your own organization, but you’ll need to find it.
Remarks…

“One positive trend has been the growing awareness of cyber risks among members of corporate boards” (Zurich & Atlantic Council)

“Cyber-security is no longer a technical problem, but rather a risk the Board and C-suit must understand and properly manage” (PWC)

“across industries, we continue to see evidence of executive recognition that security’s strategic value is more closely aligned with the business than with IT” (PWC)

“the information security function continues to take on a far more customer-facing, business-supporting, strategic value-building role” (PWC)
Endnotes

- Source: “Show Me the Money! Three Ways to Better Partner with Finance,” by Brian Barnier, ISACA Journal, Vol. 6, 2010© ISACA® All rights reserved. Reprinted by permission.
- Source: “Five Tips for Better Communication with ‘the Business’,” by Brian Barnier, @ISACA, Volume 14, 7 July 2010© ISACA® All rights reserved. Reprinted by permission.
- “Managing cyber risks with insurance”. PricewaterhouseCoopers LLP. 2014.

The ideas, views, expressions and comments expressed in this presentation are my own and don’t necessarily represent Zurich’s position, strategy or views.

This work is licensed under the Creative Commons Attribution-NonCommercial 3.0 Unported License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc/3.0/ or send a letter to Creative Commons, 444 Castro Street, Suite 900, Mountain View, California, 94041, USA.