

Ultimate Hack

Hacking security into the business



Rafal M. Los ...aka „Wh1t3Rabbit“
Bsides – 2011

Hi ...I'm the Wh1t3 Rabbit

Twitter: "Wh1t3Rabbit"

Blog: <http://hp.com/go/white-rabbit>

What qualifies me...?

- IT since 1995
- InfoSec since 1999
- Built & led AppSec Program in Fortune 100
- More years *doing* then *talking*



Rules for this talk

(seriously)

CAUTION: The contents in this talk may make you uncomfortable as an information security professional.

1. Participate
2. Share your thoughts
3. If you share, be honest with your answers
4. There is an assignment at the end...



A riddle: What does an Information Security team DO?



NOW DO
YOU SEE
WHAT IT
TAKES
TO BE A
MANAGER?

SADLY,
YES.



Is 'security' a part of
your business, or
simply a bolt-on?



Our Goal as InfoSec Professionals

(what we tell ourselves)

- “secure the business”
- “reduce risk”
- “deploy security measures”
- “protect the company”
- “keep threats out”



Our Goal as InfoSec Professionals

When management hears this...

- “secure the business” ← *from what?*
- “reduce risk” ← *of what?*
- “deploy security measures” ← *why?*
- “protect the company” ← *from what?*
- “keep threats out” ← *of where? (and why?)*



Layers 8 & 9

“the layers beyond technology”

Management & Budget

necessary for...


- Organizational buy-in
- Push change from the top
- Create shift in policy & culture
- Credibility

Business Intelligence

answers questions...

- How does security **contribute** to the business goals?
- How does security **impact** IT performance?





**We are
responsible for
positively
impacting IT
performance,
business
objectives.**



Positively influencing business at Layers 8 & 9

My 7 Secrets to Success



Align to the Business

What does your business **do**?

Objective

Learn how your organization operates, what drives it –only then you can positively impact it.

Situation

Many IT Security Pros do not know business drivers

- Align to your business or organizational goals
 - Compliance with government regulations may be a goal
 - Expanding into new markets may be a goal
 - Developing a new prototype may be a goal
- Drive security like it was a 'business'
 - Understand cause:effect of security policy & vision
 - Don't spend \$10M to protect \$100k



Walk a mile...

Become a business analyst

Objective

**Learn to solve business
'security' challenges
without the typical need
for more technology.**

Situation

Understand the situations you are working against

- The security vs. business mentality is detrimental
 - Security analysts rarely see the 'big picture'
 - Try problem-solving without plugging in technology
 - "Work within the business framework"
- Try influencing business requirements
 - Understand the business, protect its assets rationally



Carrot & Stick

Balance consequences vs. rewards

Objective

Remember the old adage of “you can lead a horse to water, but you can’t make it drink”?

Embrace that, work with that mindset.

Situation

You can lead a horse to water, even put it IN water...

- Do better than “because security says so”
 - People avoid you because they can and will get away with it
 - Policy is a weak motivational tool
- Offer incentives to make ‘secure’ choices
 - Rewards, recognition, positive reinforcement
- When incentives fail, have real consequence
 - There must be real, concrete consequences to poor choices



Advisor vs. Operator

Segment your security practice

Objective

Separate out the 'advise' from the 'do' parts of Information Security to achieve higher credibility and better resource utilization.

Situation

Split the organization to optimize efficiencies

- Operational tasks move out to small operations team
 - Managing anti-virus, patches, IDM, firewall rules, etc
 - Manage the 'doers', validate with small nimble team
- Shift majority of team to advisory capacity
 - Much like internal consultants- provide sound advice, let others **do**
 - Formulate & dictate policy, push to ops teams to implement
- Optimize the use of your key talent
 - ...just in case you don't have a 100 person ITSec team



Risk, Compliance, Legal

Meet your new best friends

Objective

Align with the 3 most powerful parts of *any* organization; adopt their methods and leverage each others capabilities and expertise.

Situation

IT Security is not unlike legal, risk and compliance

- Get to know the practices of these departments
 - Understand their motivations and power capabilities
 - Understand their struggles with reaching goals
 - Offer technology-based approaches to their ills
- Leverage each others strengths to drive key strategy
 - What is good for me, is good for 'we'
 - Security's goals can often be accomplished by legal's requirements



Business-driven 'security'

Business must **need it**

Objective

If 'security' is perceived as a luxury, it will be marginalized.

Demonstrate 'security' as a core value, the business must aspire to be less risky.

Situation

Strive to make security a core business value

- Provide **free** assessments of IT risk to the organization
 - Define the appropriate format for your industry, market
 - Make reports readily available to **customers, auditors**
- Give reasonable alternatives to 'insecurity'
 - Make sure you understand good vs. good enough
- Offer a lower-cost, consolidated alternative to continually failing audit, scrambling to comply



Leverage Accountability

“Just sign here to accept risk”

Objective

Few things are more powerful than the realization of being held accountable for your actions; advise on risk and allow a business owner to accept that risk with a simple signature.

Situation

Accountability in a visible way is fundamental

- Provide objective assessment of risk
 - Research, then file a comprehensive risk profile report
 - Discuss the impact, cost, and assessed risk to the organization
- Give leaders the ability to choose
 - Accept risk on behalf of the organization
 - Sign off on the risk (literally) and be accountable
 - Remediate the risks



Measure Yourself (KPIs)

How do you know you've succeeded?

BONUS!

Objective

There are no more than 5 KPIs you must measure against; KPIs enable a non-technical conversation with management & leadership.

Situation

Can you measure security's business impact?

- Most organizations have lots of data & metrics
 - Consolidate data overload and noise into consumable KPIs
 - Spreadsheets, dashboards are often too complex and technical
- Do your KPIs pass the "so what?" test?
 - Does it impact the business (*positively*) ?
 - Does it impact revenue?
 - Are you improving proportionately to fiscal spend?



The Most Important Answer

If you want to shock your CIO, answer this question

When can we stop spending money?

The question isn't "are we secure?" ...

The **real** question is "are we good enough?" and "how do we know when we've arrived there?"



These are my secrets to succeeding

They've worked for me, they *may* work for you

Try this at home ...but make sure you are rational.

- There is no silver bullet, we're not baking cookies
- Every organization is different, approaches vary
 - Some assembly required, batteries not included
 - No warranties, no returns



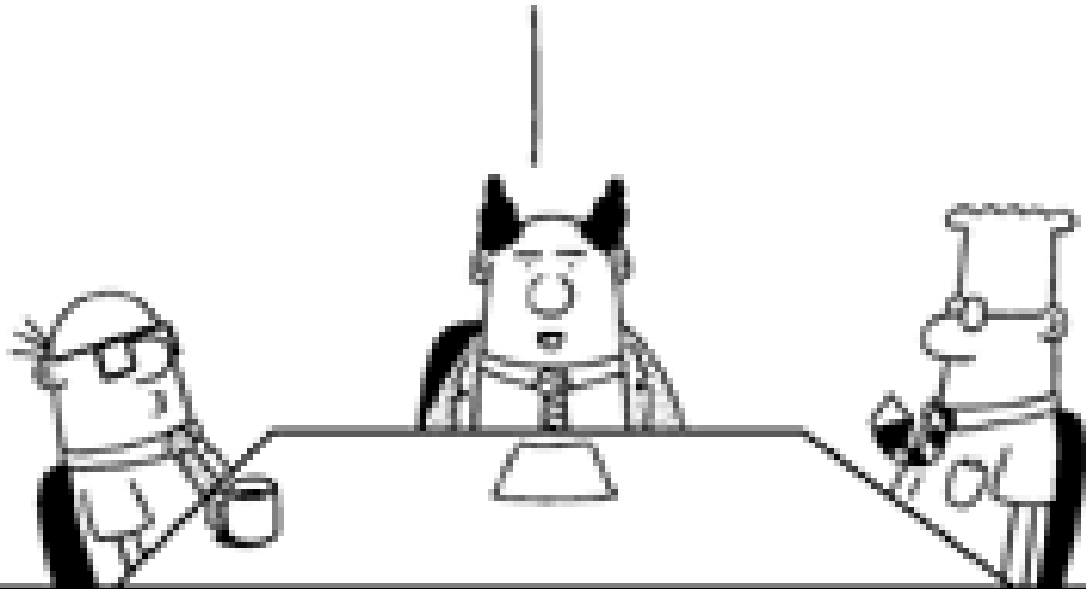
So What is it You DO ...here?

... please don't say 'security'

Make sure you can explain how what you do, impacts the organization positively or prepare for more of this...



WE'RE GOING TO
TRY SOMETHING
CALLED AGILE
PROGRAMMING.



Management
thru
buzzword
bingo.

A smart poker player knows...

- when to hold
- when to fold
- when to walk away
- when to *run like hell.*



Thank you

Did you learn something?

© Copyright 2011 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. Confidentiality label goes here

Rafal Los

[Twitter.com/Wh1t3Rabbit](https://twitter.com/Wh1t3Rabbit)

HP.com/go/white-rabbit

