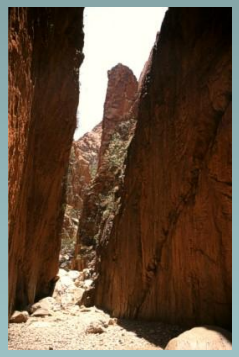
Security Chasm!



Dr. Anton Chuvakin

Security Warrior Consulting

www.securitywarriorconsulting.com

Hack in The Box

Amsterdam, The Netherlands

July 2010

Why Are We Here?

Risk of **DEATH** vs Risk of $60 fine?

Security Warrior Consulting
www.securitywarriorconsulting.com
Dr. Anton Chuvakin

Outline

- WTH is “security”?
- How we got here?
- Security *and/or/=/vs* Compliance?
- Security vs security?
  - Does what we do for security actually … improve security?
- Where it is all going?
- What can YOU do today?

Security Warrior Consulting
www.securitywarriorconsulting.com
Dr. Anton Chuvakin

For ADD Folks: Main Theme

1. There are “two security” realities: one *conceptual and fuzzy* + another *painfully real.* And a chasm between them!
2. This is not good – for security and for businesses!
3. What can we do about it?

Brief History First….

1950-1985 Stick Age: Security = door lock

1985-1990 Stone Age: Security = anti-virus

1990-2000 Bronze Age: Security = firewall

2000-2005 Iron Age: Security = IDS/IPS

2005-2010 Modern Age: Security = appsec

2010+ Cloud Age: Security = 

But this is technology only…?

Security Warrior Consulting
www.securitywarriorconsulting.com
Dr. Anton Chuvakin

OK, How About This View?

1950-1985 Stick Age: Local risks

1985-1990 Stone Age: Computer risks

1990-2000 Bronze Age: Network risks

2000-2010 Iron Age: **Regulatory** risks

2005-2010 Modern Age: Cybercrime risks

2010+ Cloud Age: All-of-the-above risks? ☹

Gross oversimplifcation, of course ☺

Security Warrior Consulting
www.securitywarriorconsulting.com
Dr. Anton Chuvakin

So, what are we doing?

Aka “What is Security?”

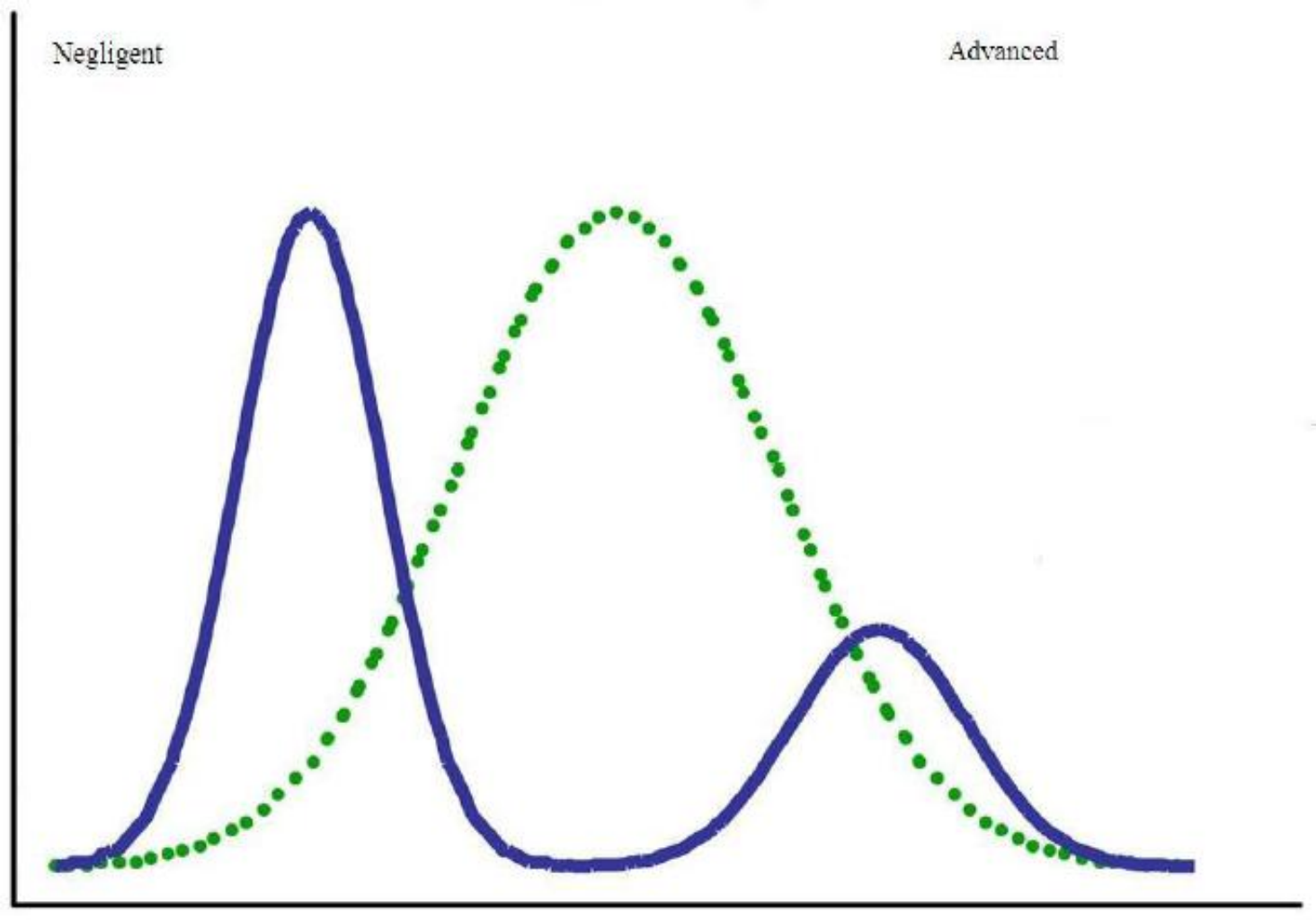
- Protecting the data
- Defending the network
- Guarding the IT environment
- Reducing “risk” (what risk?)

Yes, but really …

We ensure that organization *runs* and *wins*!

Security Warrior Consulting
www.securitywarriorconsulting.com
Dr. Anton Chuvakin

Leaders vs Losers



Security Warrior Consulting
www.securitywarriorconsulting.com
Dr. Anton Chuvakin

…and what if they still don't?

Then some regulatory body would come and beat them up ….

… and they'd continue to stay 0wned, of course ☺

Drilldown into “Compliancy”

Where Compliance Fears to Tread

<u>YOUR</u> DATA: Key Organization Data, IP, "Secrets", Trade Secrets	**<u>CUSTODIAL</u> DATA: SSN, PAN, ID, Addresses, Health records**
Usually not regulated	Usually regulated: PCI
Loss causes pain to you!	Loss causes pain to others!
You are responsible for protection	*You are responsible for protection*
Cannot be "killed"	Can be "killed"

Security Warrior Consulting
www.securitywarriorconsulting.com
Dr. Anton Chuvakin

Observations…

Protects OWN data, protects CUSTODIAN data
<LEADER>

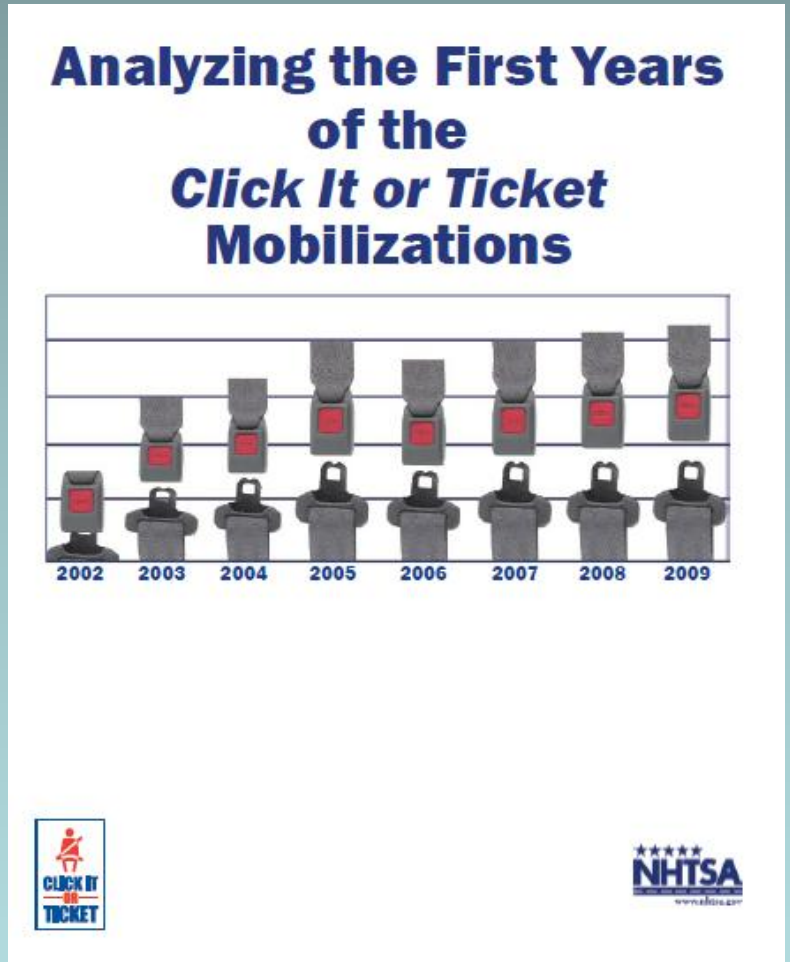
Protects OWN data, *fails* to protect CUSTODIAN data
<RISK TAKER>

Fails to protect OWN data, protects CUSTODIAN data
<IDIOT>

Fails to protect OWN data, *fails* to protect CUSTODIAN data
<LOSER>

Security Warrior Consulting
www.securitywarriorconsulting.com
Dr. Anton Chuvakin

Compliance Is…



Risk of **DEATH** vs Risk of $60 fine?

DOT study on seatbelts:

Compliance = (Awareness + Enforcement) / Security Benefit

Security Warrior Consulting
www.securitywarriorconsulting.com
Dr. Anton Chuvakin

Chasm Emerges!

PCI DSS is TOO EASY!
PCI is a joke. It is not security!
Playing scope games?
PCI makes you buy stuff you don't need
PCI is not risk management!

PCI DSS is TOO HARD!
What? 224 questions!!?
Firewall, IDS… what's all that?
You mean we now have to pay for AV updates?
What is that risk thing?

Security Warrior Consulting
www.securitywarriorconsulting.com
Dr. Anton Chuvakin

Compliance Mystery Solved!!

Compliance ***is*** the
"floor" of security

And a motivator to DO IT!

However, many prefer to
treat it as **a "ceiling"**

Result: **breaches, 0wnage, mayhem!**

Security Warrior Consulting
www.securitywarriorconsulting.com
Dr. Anton Chuvakin

Compliance vs Security

Compliance (PCI)	**Security (risk)**
Operates with “known knowns” or “unknown knowns”	Operates mostly with “known unknowns”
Can have a full TODO list	Can NEVER have a full TODO list
Can be counted	Can only be guesstimated
EASY (=EASIER)	**HARD**

Security Warrior Consulting
www.securitywarriorconsulting.com
Dr. Anton Chuvakin

How To “Profit” From Compliance?

Everything you do for compliance, MUST have security benefit for your organization!

Examples: log management, IDS/IPS, IdM, application security , etc

Security Warrior Consulting
www.securitywarriorconsulting.com
Dr. Anton Chuvakin

Back to Chasm…

Compliance is NOT the reason for a chasm, but it made it …

MORE VISIBLE!

Security Warrior Consulting
www.securitywarriorconsulting.com
Dr. Anton Chuvakin

SIDE 1: Consultant Comes In…

- Talks to senior management
- Scopes a “risk assessment” project
- Start talking to “stakeholders”
- Reading policies …
- …never touches “metal”
- Comes up with RISKS!

Are we secure now?

Security can be as dumb as compliance…

Security Warrior Consulting
www.securitywarriorconsulting.com
Dr. Anton Chuvakin

SIDE 2: Intrusion Tolerance …

… aka **Running an Owned Business**.

Why it is [*seen as*] OK?

- Non-critical assets affected
- Non-critical C-I-A dimension affected
- Assets operate while affected
- Other priorities override

Security Warrior Consulting
www.securitywarriorconsulting.com
Dr. Anton Chuvakin

Moreover: Assumed 0wnage!

- **Desktops**: banks now *assume* that online banking client PC is owned
  - If I see a PC now, I assume it is 0wned! ☹
- **Web applications**: not even "luck based strategy", but "lazy attacker strategy"
  - Static HTML is OK, of course ☺

If we cede desktop and web, where DO we fight?

What is the new line of battle?

Security Warrior Consulting
www.securitywarriorconsulting.com
Dr. Anton Chuvakin

Chasm?

Chasm!!

SIDE 1

- “Aligning strategy”
- Writing policies
- Talking risk and doing assessments
- Compliance vs security
- Inputs
- Try for “proactive” and fail

SIDE 2

- Gathering metrics
- Responding to issues
- Figuring out risks and implementing controls
- Keep the business running
- Output -> inputs
- Focus on responsive

Security Warrior Consulting
www.securitywarriorconsulting.com
Dr. Anton Chuvakin

Related Security Mini-Chasms

- Proactive vs reactive
- Risk vs diligence
- Policy vs technology
- Inputs vs outputs security
- Micro and macro security

What Does Future Hold?

- More regulation to compel the laggards
- More threats to challenge the leaders
- Less chance to do “intrusion tolerance”
- And - of course! – more clouds ☺

Longer term:

slow **trend toward chasm closure**

However….

Security Warrior Consulting
www.securitywarriorconsulting.com
Dr. Anton Chuvakin

Security 2020?

Added dimension to spice things up...

In 2020, security FAIL might mean you DIE!

Security Warrior Consulting
www.securitywarriorconsulting.com
Dr. Anton Chuvakin

Conclusions: How To Bridge The Chasm?

- Is **intrusion tolerance** the only way?
  - "Titanic DID have compartments"
- Use **compliance to drive security** – not whine about it
- NEVER **conceptualize without doing**! (*)
- Chasm exists – but you can start closing it at your organization by **always connecting mission with "metal"**

Security Warrior Consulting
www.securitywarriorconsulting.com
Dr. Anton Chuvakin

Action Item!

NOW LET'S ALL GO PRACTICE INCIDENT RESPONSE!!!

Security Warrior Consulting
www.securitywarriorconsulting.com
Dr. Anton Chuvakin

Questions?

Dr. Anton Chuvakin

Security Warrior Consulting

Email: anton@chuvakin.org

Site: http://www.chuvakin.org

Blog: http://www.securitywarrior.org

Twitter: *@anton_chuvakin*

Consulting: http://www.securitywarriorconsulting.com

More on Anton

- **Now:** independent consultant
- **Book author:** “Security Warrior”, “PCI Compliance”, “Information Security Management Handbook”, “Know Your Enemy II”, “Hacker’s Challenge 3”, etc
- **Conference speaker:** SANS, FIRST, GFIRST, ISSA, CSI, Interop*, many, many others worldwide*
- **Standard developer:** CEE, CVSS, OVAL, etc
- **Community role:** SANS, Honeynet Project, WASC, CSI, ISSA, OSSTMM, InfraGard, ISSA, others
- **Past roles:** Researcher, Security Analyst, Strategist, Evangelist, Product Manager

Security Warrior Consulting Services

- Logging and log management strategy, procedures and practices
  - **Develop logging policies and processes**, log review procedures, workflows and periodic tasks as well as help architect those to solve organization problems
  - **Plan and implement log management architecture** to support your business cases; develop specific components such as log data collection, filtering, aggregation, retention, log source configuration as well as reporting, review and validation
  - **Customize industry "best practices"** related to logging and log review to fit your environment, help link these practices to business services and regulations
  - **Help integrate logging tools** and processes into IT and business operations
- SIEM and log management content development
  - **Develop correlation rules, reports** and other content to make your SIEM and log management product more useful to you and more applicable to your risk profile and compliance needs
  - **Create and refine policies, procedures and operational practices** for logging and log management to satisfy requirements of PCI DSS, HIPAA, NERC, FISMA and other regulations

More at www.SecurityWarriorConsulting.com

Security Warrior Consulting
www.securitywarriorconsulting.com
Dr. Anton Chuvakin

Want a PCI DSS Book?

"PCI Compliance" by Anton Chuvakin and Branden Williams

Useful reference for merchants, vendors – and everybody else

Released **December 2009!**

Security Warrior Consulting
www.securitywarriorconsulting.com
Dr. Anton Chuvakin