

The lost war on Information Security

hacker's corner

It happened, software ate the world, we lost control on our information and security is not better than before. What people could do?

Francesco Ongaro, Pasquale Fiorillo
Francesco.ongaro@isgroup.it
<https://linkedin.com/in/ongaro>



**INTERNATIONAL
JOURNALISM
FESTIVAL**

PERUGIA, ITALY | 6-10 APRIL 2016
X EDITION | FREE ENTRY

Francesco Ongaro - <https://linkedin.com/in/ongaro>

Francesco Ongaro is an Italian security expert and Hacker, living in Verona (the city of Romeo and Giulietta), specialized in **Network and Web Application Penetration Tests**. He performed several hundred of technical activities over the years for many of the most important and exposed customers in the private, public infrastructure, finance, banking, insurance and media fields. His research and advisories are published on USH (www.ush.it) and he founded an independent Tiger Team under the ISGroup (www.isgroup.it) umbrella.

The lost war on Information Security

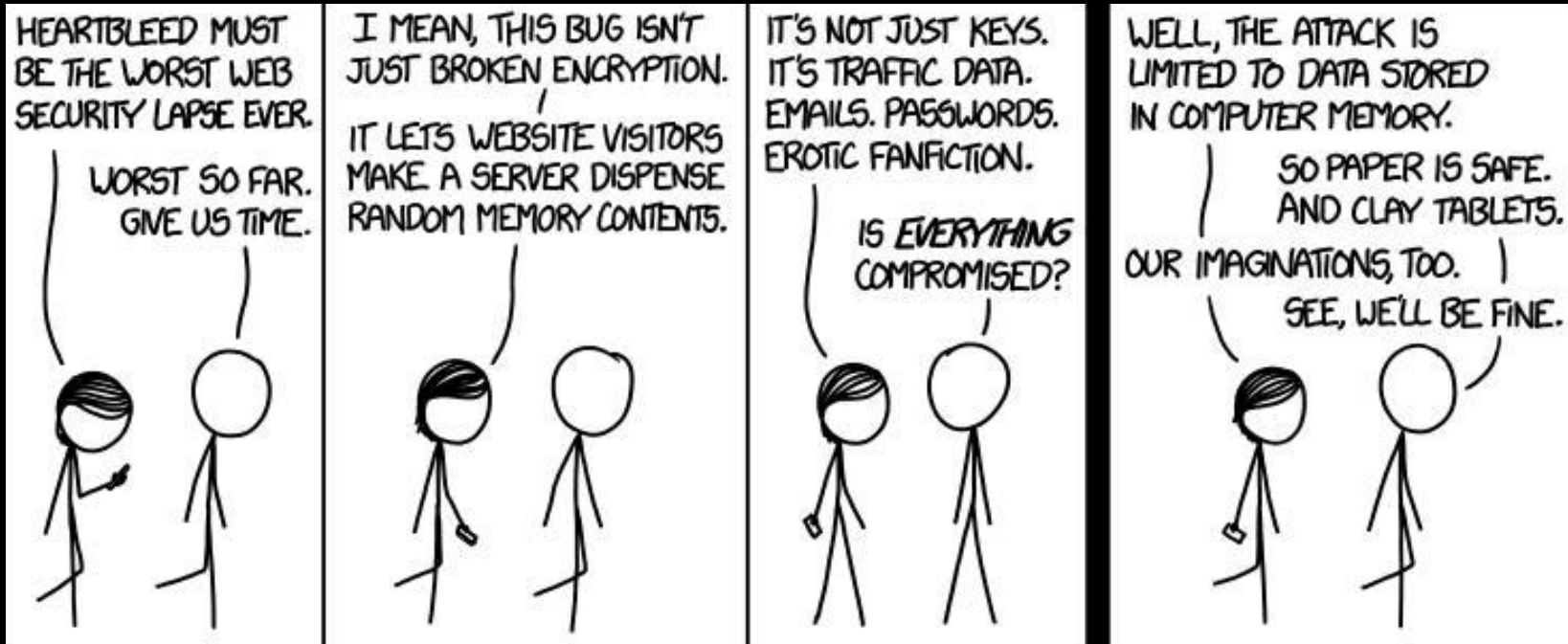
The lost war on Information Security

OR

CLOUD DANGERS

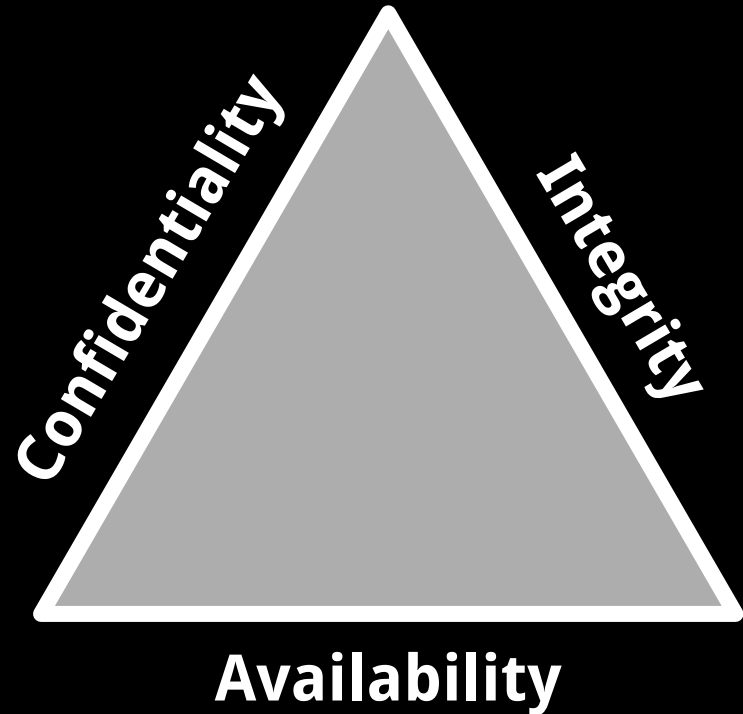
Vulnerability Definition

The ability to have an impact on Security



Security Definition

- CIA triad
 - Confidentiality
 - Integrity
 - Availability
- Extended security model
 - Authenticity
 - Non-Repudiation
 - Privacy
 - Accountability



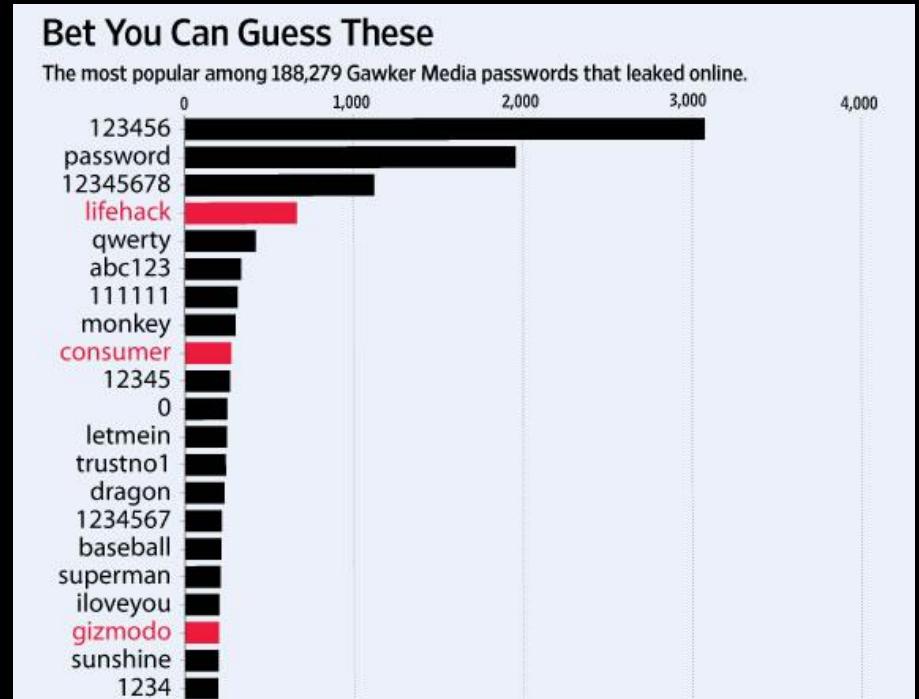
How are things Vulnerable?

- Implementation Vulnerabilities

- Weak PASSWORDS
- Improper DESIGN
- Unsafe DEPLOYMENT
- ...

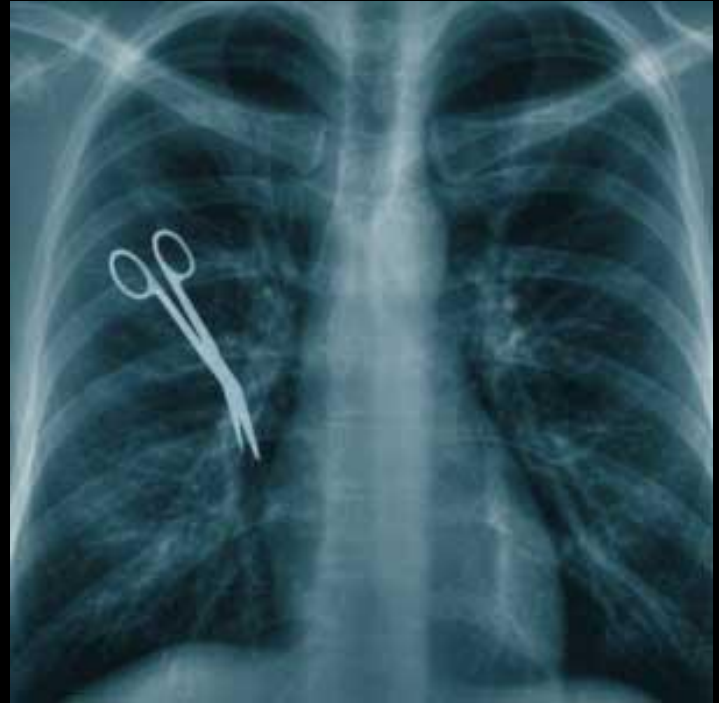
- Software Vulnerabilities

- Buffer Overflows
- SQL Injections
- Command Execution



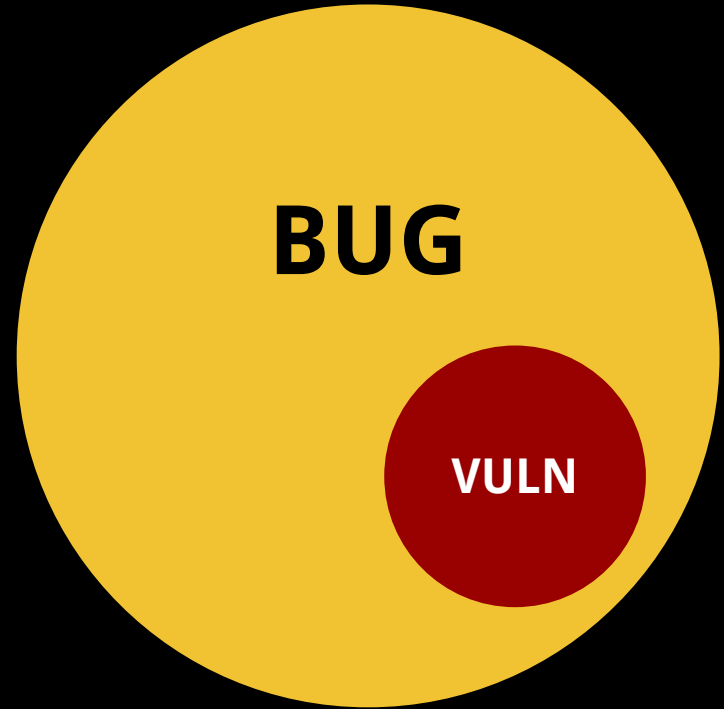
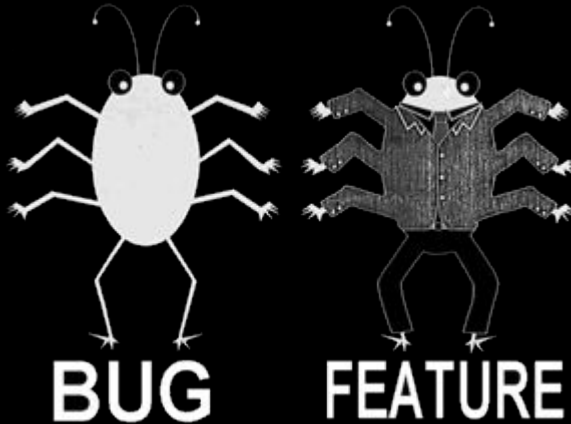
Why is Software vulnerable?

- It's written by humans
- Humans do mistakes
- It contains bugs

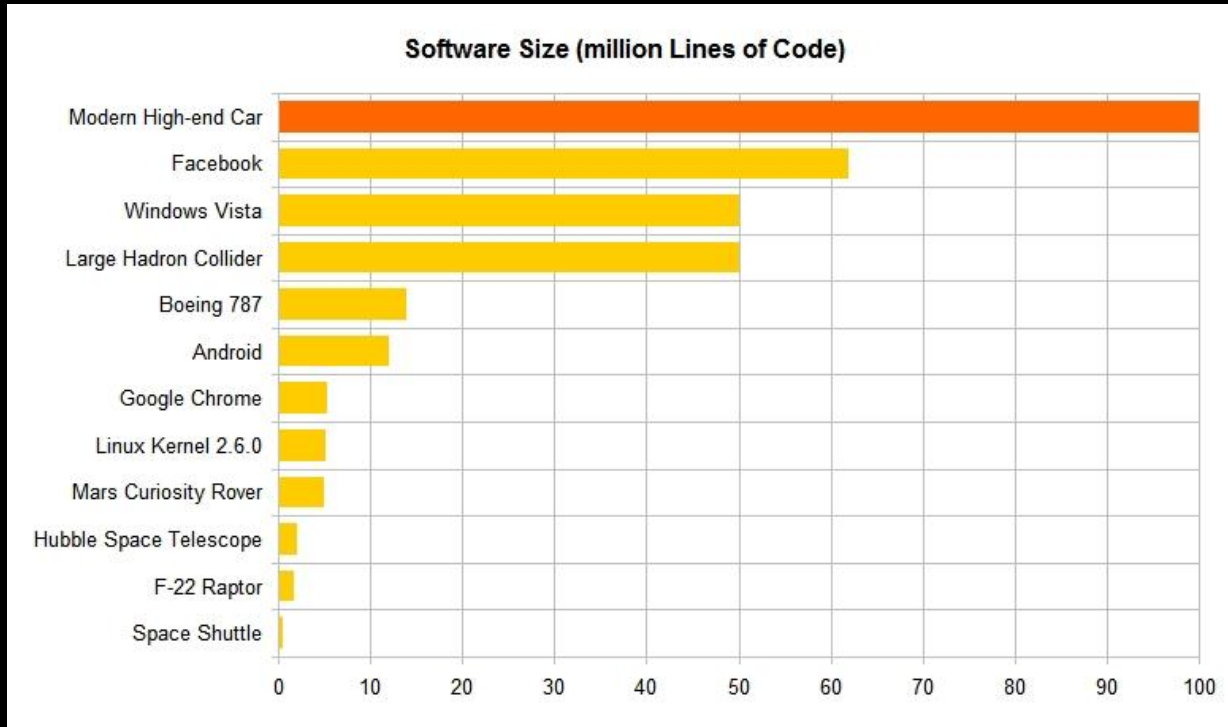


Bug vs. Vulnerability

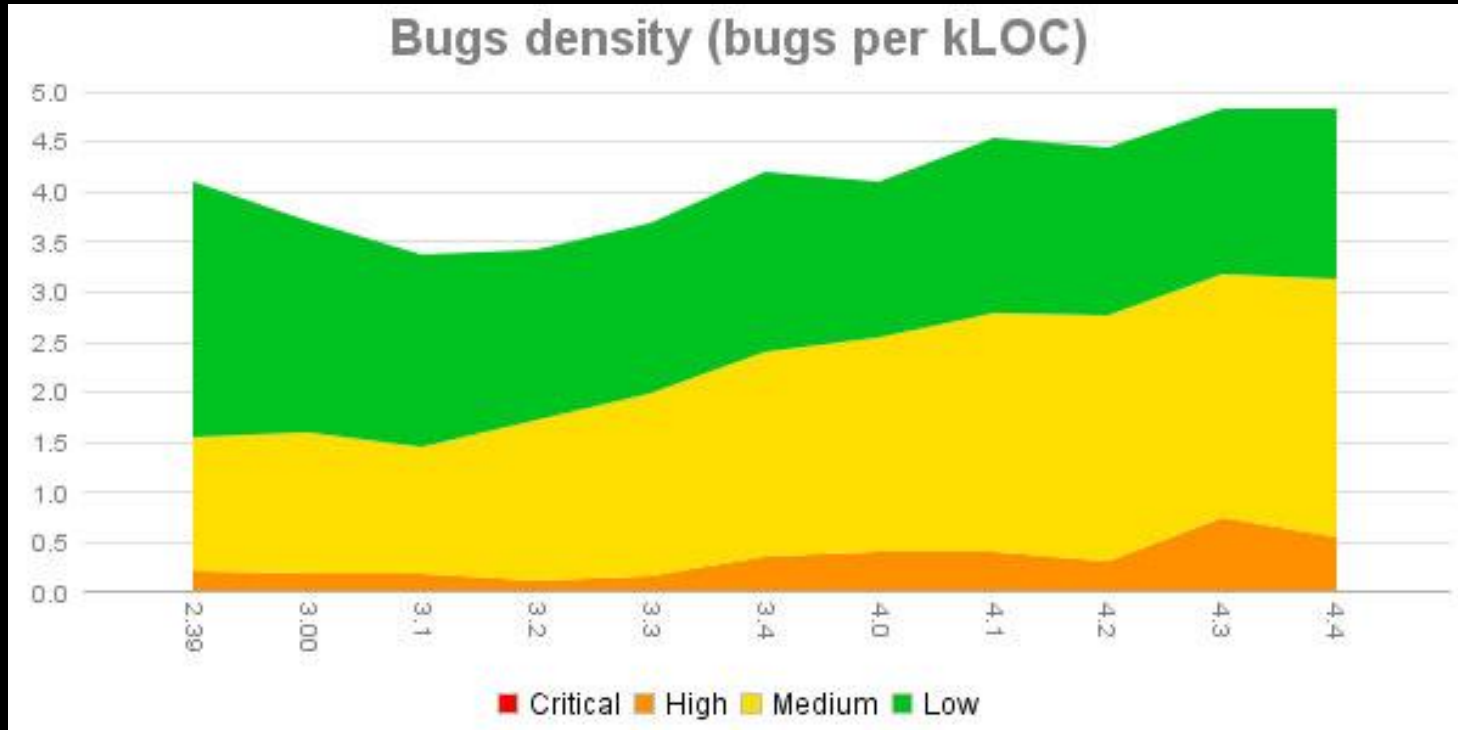
- Some Bugs are, also, Vulnerabilities
- http://www.pcworld.com/article/205318/11_infamous_software_bugs.html



Software Complexity



Bug % in software



It's a faith fact

1. There is a certain amount of bugs every KLOC (1000 lines of code)
2. A fraction of bugs are:
 - a. Risks
 - b. Defects
 - c. Software Failures
 - d. Vulnerabilities
3. The Linux Kernel is 2.5-15 M SLOCs
4. A Debian system is 55-419 M SLOCs

The Kernel example

- 1255 CVE for the Linux Kernel
- Not every vulnerability has a CVE
- It's the largest software project in terms of contributors
- It's the most audited software

Open Source Software - OSS



Given enough eyeballs, all bugs are shallow.

(Eric S. Raymond)

Other companies

- Not enough resources
- Even Microsoft before 2005
- Well..

IIS 7

MS15-034 (April 14, 2015)

<https://technet.microsoft.com/en-us/library/security/ms15-034.aspx>



Summarizing

Software

is made of

Bugs

And

Cloud

is made of

Software

What save us from total-failure is



Compartmentation

Separation of Duties

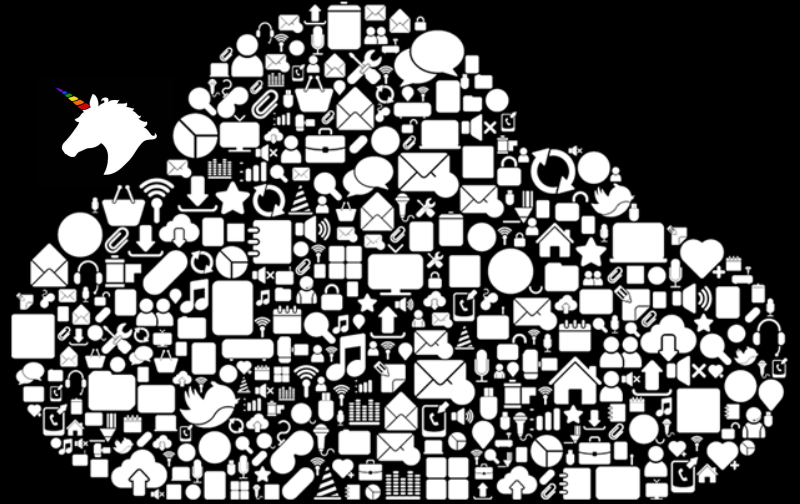
Layered Security

Defense in Depth

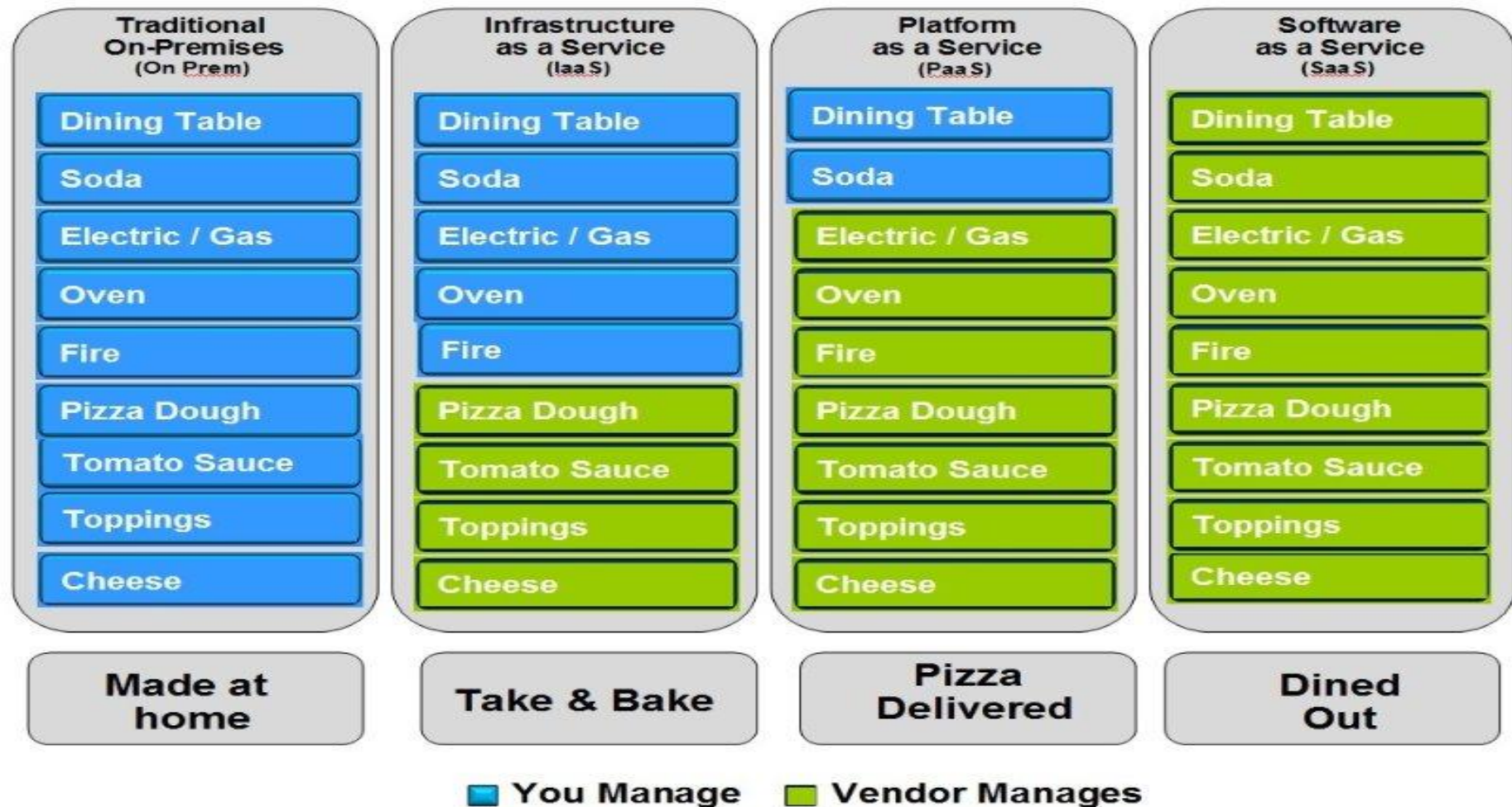
It's called

Security in the Architecture

1960 → 2016



Pizza as a Service



The Digital Disruption
has already happened



World's largest taxi company
owns no taxis (Uber)

World's largest taxi company
owns no taxis (Uber)

Largest accommodation provider
owns no real estate (Airbnb)

World's largest taxi company
owns no taxis (Uber)

Largest accommodation provider
owns no real estate (Airbnb)

Largest phone companies own
no telco infrastructure (Skype,
WeChat)

World's largest taxi company
owns no taxis (Uber)

Largest accommodation provider
owns no real estate (Airbnb)

Largest phone companies own
no telco infrastructure (Skype,
WeChat)

Most popular media owner
creates no content (Facebook)

World's largest taxi company
owns no taxis (Uber)

Largest accommodation provider
owns no real estate (Airbnb)

Largest phone companies own
no telco infrastructure (Skype,
WeChat)

Most popular media owner
creates no content (Facebook)

Fastest growing banks have
no actual money (SocietyOne)

World's largest taxi company
owns no taxis (Uber)

Largest accommodation provider
owns no real estate (Airbnb)

Largest phone companies own
no telco infrastructure (Skype,
WeChat)

Most popular media owner
creates no content (Facebook)

Fastest growing banks have
no actual money (SocietyOne)

World's largest movie house
owns no cinemas (Netflix)

World's largest taxi company
owns no taxis (Uber)

Largest accommodation provider
owns no real estate (Airbnb)

Largest phone companies own
no telco infrastructure (Skype,
WeChat)

Most popular media owner
creates no content (Facebook)

Fastest growing banks have
no actual money (SocietyOne)

World's largest movie house
owns no cinemas (Netflix)

Largest software vendors don't write the apps (Apple, Google)

Everybody's jumping on the Cloud bandwagon



Bonus: <https://github.com/panicsteve/cloud-to-butt>

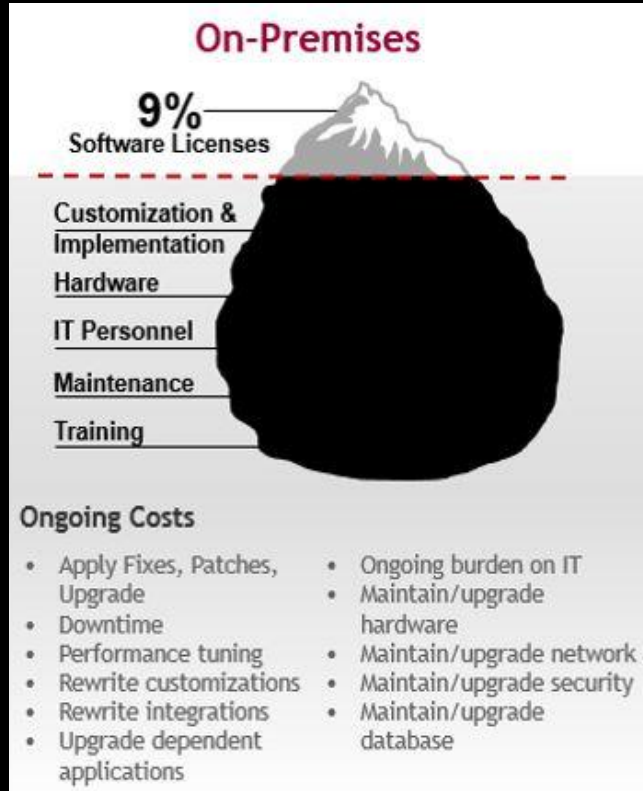
Wow! Liability shift

Management of security is 3rd party

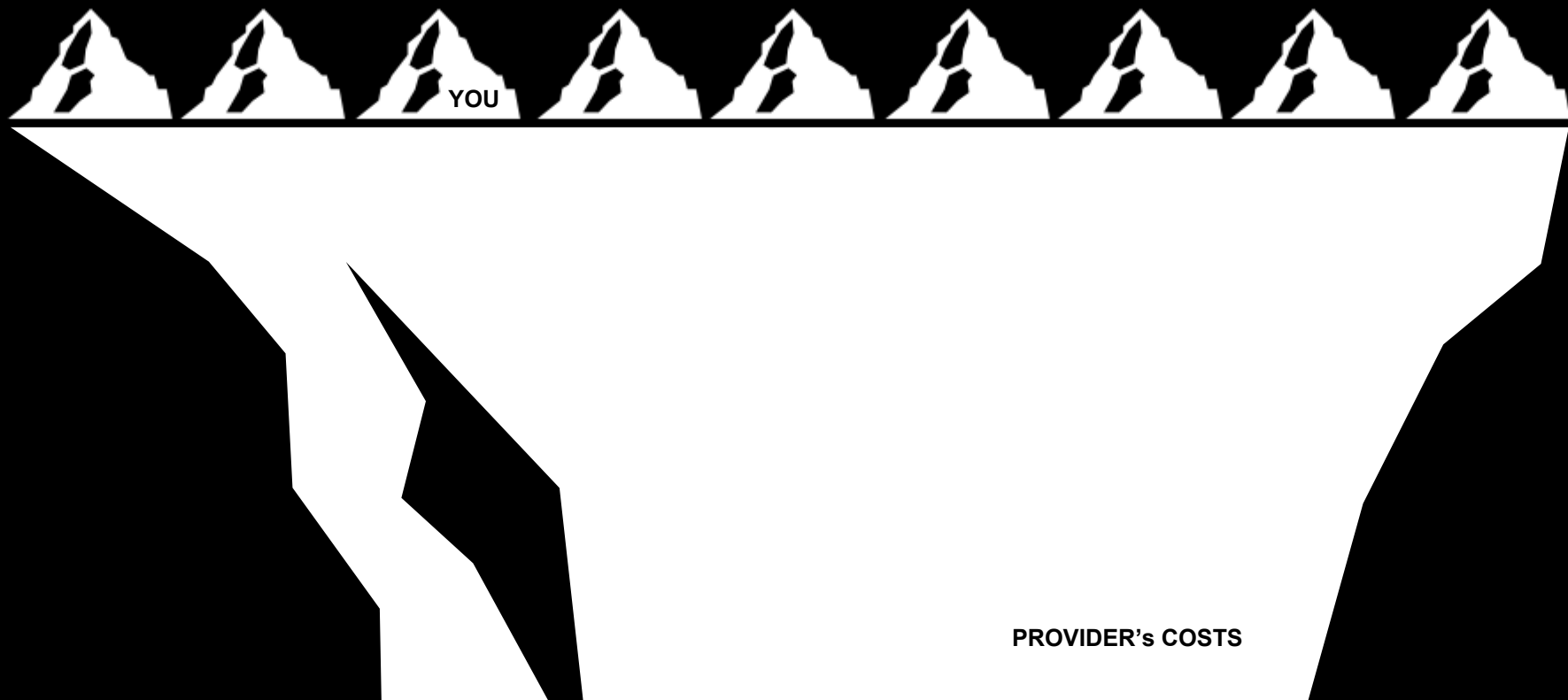
- Responsibility cannot be outsourced
 - It's the function that can be outsourced
 - It's your reputation, your data, your customers

Welcome to the **Third-party risk** Era

Wow! Cost reduction



Reality of off-premise / multi-tenant systems



Multitenant architectures

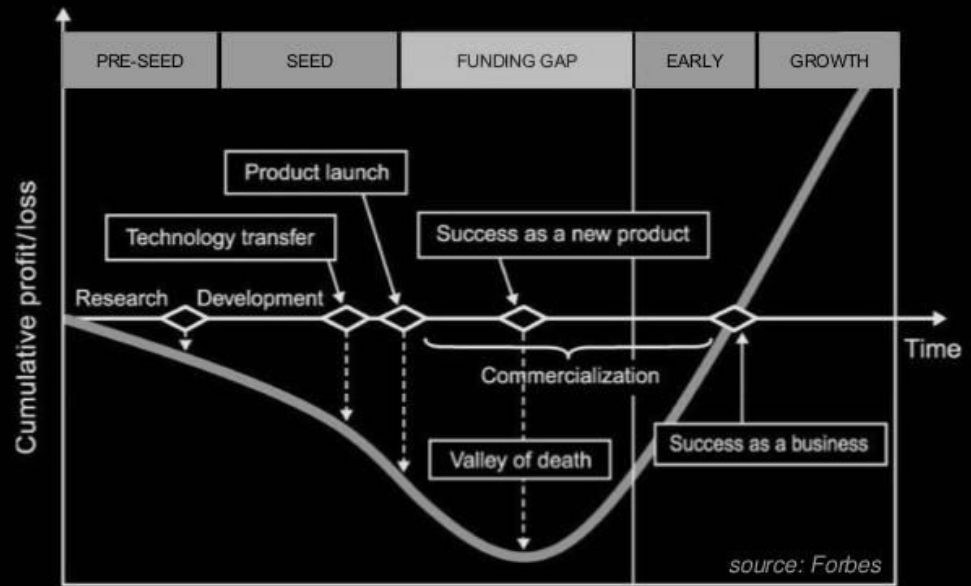
PROs

- Scale on demand
- Limit additional CAPEX with growth

CONS

- More complex
- Shared by design

the Valley of Death



The CLOUD *may lead to* lower levels of

Security in the Architecture

and thus increase the Risk

Random good-design rule #86

Don't mix trusted data with untrusted data

Don't mix trusted sources with untrusted sources

3rd party Javascript Inclusion

```
<script src=//code.jquery.com/jquery-2.2.1.min.js></script>
```

I have a dream!

Random good-design rule #471

Limit visibility of Administrative Interfaces

Compartmentalize at the lower level, both horizontally and vertically

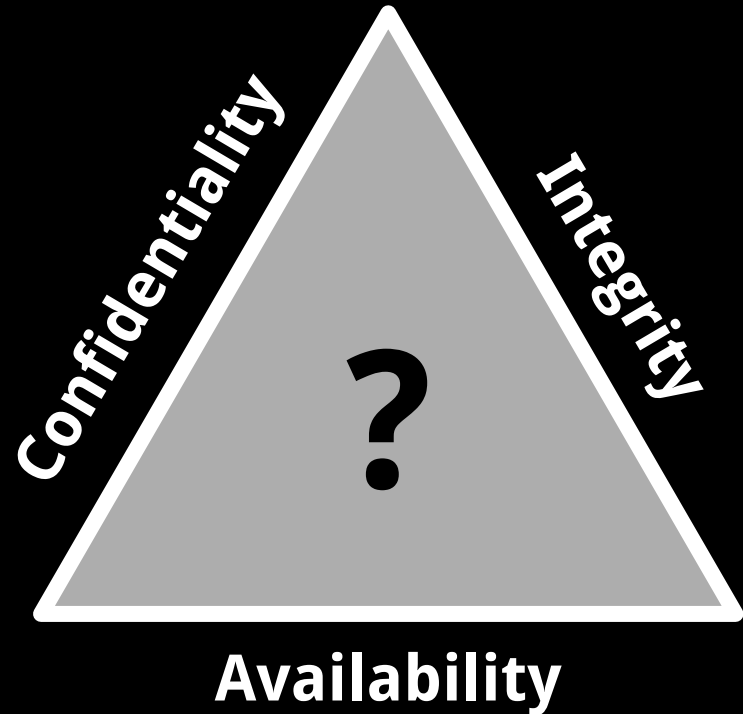
Your SaaS application will have an Internet Facing login

`https://www.facebook.com/records/x/login/`

Request Secure Access to the Law Enforcement Online Request System

CLOUD Security

- CIA triad
 - Confidentiality
 - Integrity
 - Availability
- Extended security model
 - Authenticity
 - Non-Repudiation
 - Privacy
 - Accountability



Problem #1 Immaturity (MVP)

Startups and immature SaaS services (and SaaS marketing is all about hype and traction)



Problem #2 Visibility

- More casual Attackers
- Collateral Damage
- Access Everywhere

Early Stage Benchmarks

	< \$5M	\$5M - \$20M
1 Year Revenue Growth Rate	50%	32%
Operating Income	- 19.8%	-13.6%
Sales Expense	32.2%	30%
Marketing Expense	21%	13.1%
Head Count	23	62
Net Cash from Operations as a % of Recognized Revenue	-50%	5%

Source: 2011 OPEXEngine Software Benchmarking Industry Report

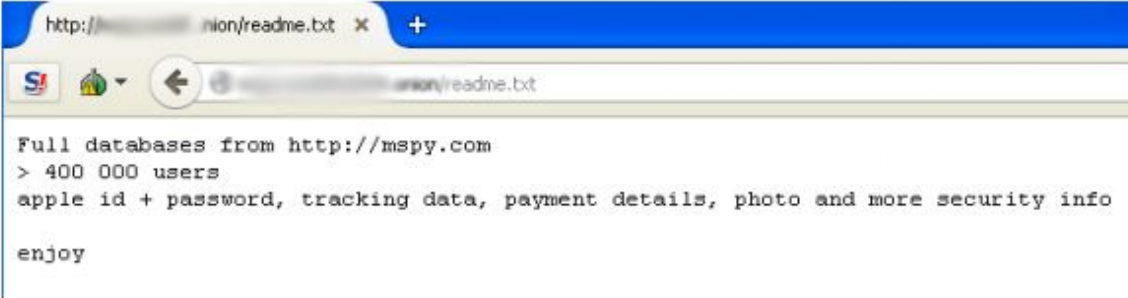
14 Mobile Spyware Maker mSpy Hacked, Customer Data Leaked

MAY 15



mSpy, the makers of a dubious software-as-a-service product that claims to help more than two million people spy on the mobile devices of their kids and partners, appears to have been massively hacked. Last week, a huge trove of data apparently stolen from the company's servers was posted on the Deep Web, exposing countless emails, text messages, payment and location data on an undetermined number of mSpy "users."

mSpy has not responded to multiple requests for comment left for the company over the past five days. KrebsOnSecurity learned of the apparent breach from an anonymous source who shared a link to a Web page that is only reachable via **Tor**, a technology that helps users hide their true Internet address and allows users to host Web sites that are extremely difficult to get taken down.



```
http://[redacted].onion/readme.txt x +
Full databases from http://mspy.com
> 400 000 users
apple id + password, tracking data, payment details, photo and more security info
enjoy
```

The Tor-based Web site hosting content stolen from mobile devices running mSpy.

SMALL

We've been hacked

BY MIKKEL SVANE ON FEBRUARY 21, 2013

We feel that it's important our customers receive an update from us on a recent security situation. We have an investigation underway and do not have the answer to every question.

We've become aware that a hacker accessed our system this week. As soon as we learned of the attack, we patched the vulnerability and closed the access that the hacker had. Our ongoing investigation indicates that the hacker had access to the support information that three of our customers store on our system. We believe that the hacker downloaded email addresses of users who contacted those three customers for support, as well as support email subject lines. We notified our affected customers immediately and are working with them to assist in their response.



BIG

Problem #3 Palatability

Economy of scale (for attackers too!)

NEWS ANALYSIS

Adobe hack shows subscription software vendors lucrative targets

Hackers jack 3 million credit cards, many tied to Creative Cloud software-by-subscription service



By Gregg Keizer

FOLLOW

Computerworld | Oct 7, 2013 7:44 AM PT

RELATED TOPICS

Security

Cybercrime & Hacking

Adobe on Thursday admitted that hackers broke into its network and stole personal information, including an estimated 2.9 million credit cards, illustrating the lucrative target that software-by-subscription providers have become to cyber criminals, analysts said today.

MORE LIKE THIS

Hackers steal data on 2.9 million Adobe customers

OOPS! Adobe abode hacked: Credit cards copied, source silently snatched

Adobe source code parked on hackers' unprotected server

on IDG Answers [➔](#)

How to use credit card machines over VoIP?

Zeus Trojan variant Targets Salesforce accounts and SaaS Applications


Thursday, February 20, 2014 Swati Khandelwal


 70

 Like 275

 Share 134

 Tweet 154

 Share 54

 Email 0

 share 887



Zeus, a financially aimed Banking Trojan that comes in many different forms and flavors, is capable to steal users' online-banking credentials once installed. This time, an infamous *Zeus*

Problem #4 Confidentiality, Accountability, Privacy

- Others looking at your data
 - Quis custodiet ipsos custodes?
 - Privacy impact
 - Low Accountability (transparency)
- Insider threat
 - Hackers are offering to pay \$23,000 for valid Apple employee login details
<http://bgr.com/2016/02/09/apple-employee-login-hackers/>
 - FBI director asks, 'What if Apple engineers are kidnapped and forced to write code?'
<http://www.techinsider.io/fbi-director-james-comey-on-apple-engineers-being-kidnapped-2016-3>

Problem #5 Shared by design

Shared hosting? Buu..



Cloud SaaS? Okay!

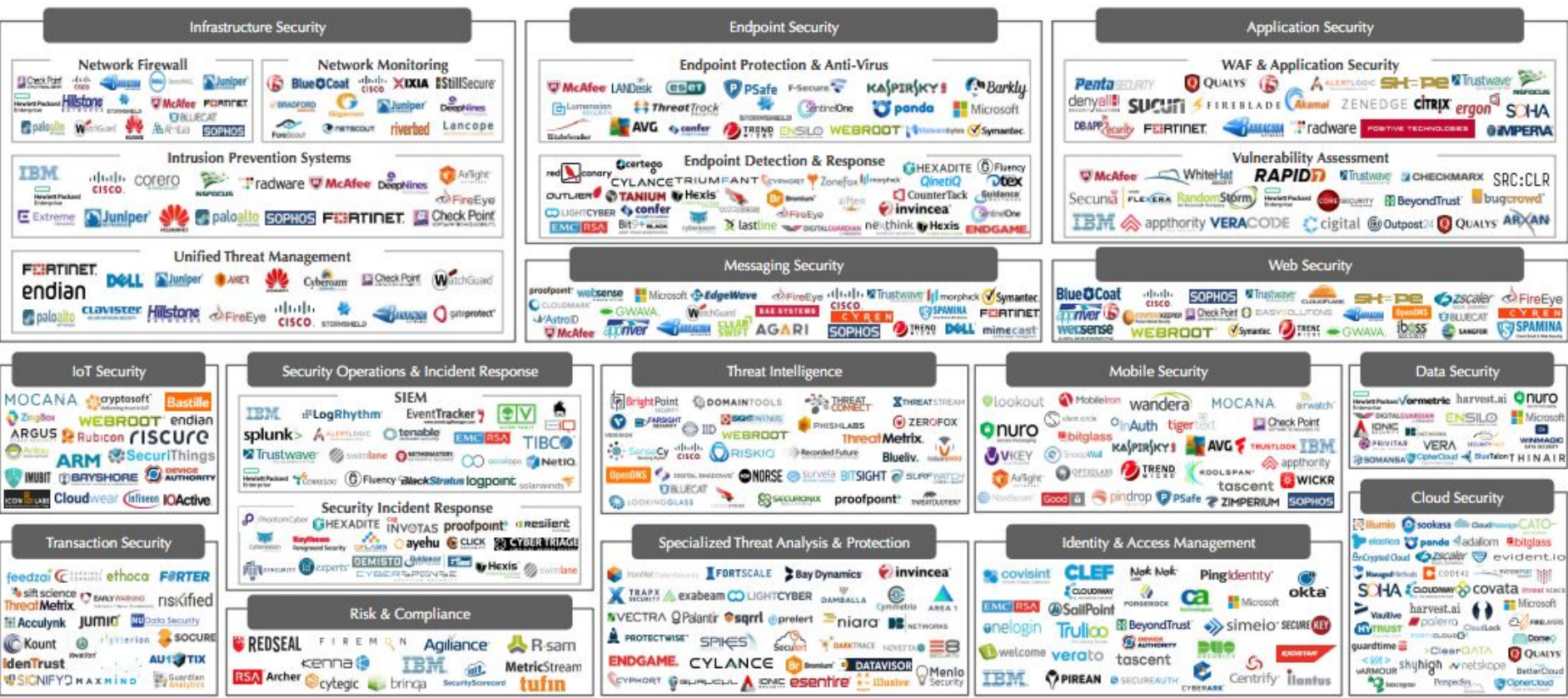


Problem #6 Weak standards

- Identity management
 - Integration of Authentication and Authorization
- Accountability
 - Logging of actions
 - Integration of logging
- Opacity
 - Vague statements about (security) policies
- Lack of standardization/interoperability

CYBERscape 2.0: Our Landscape Taxonomy

The Security Sector Is Dynamic And Vast. We Are Ceaseless & Vigilant In Our Coverage.



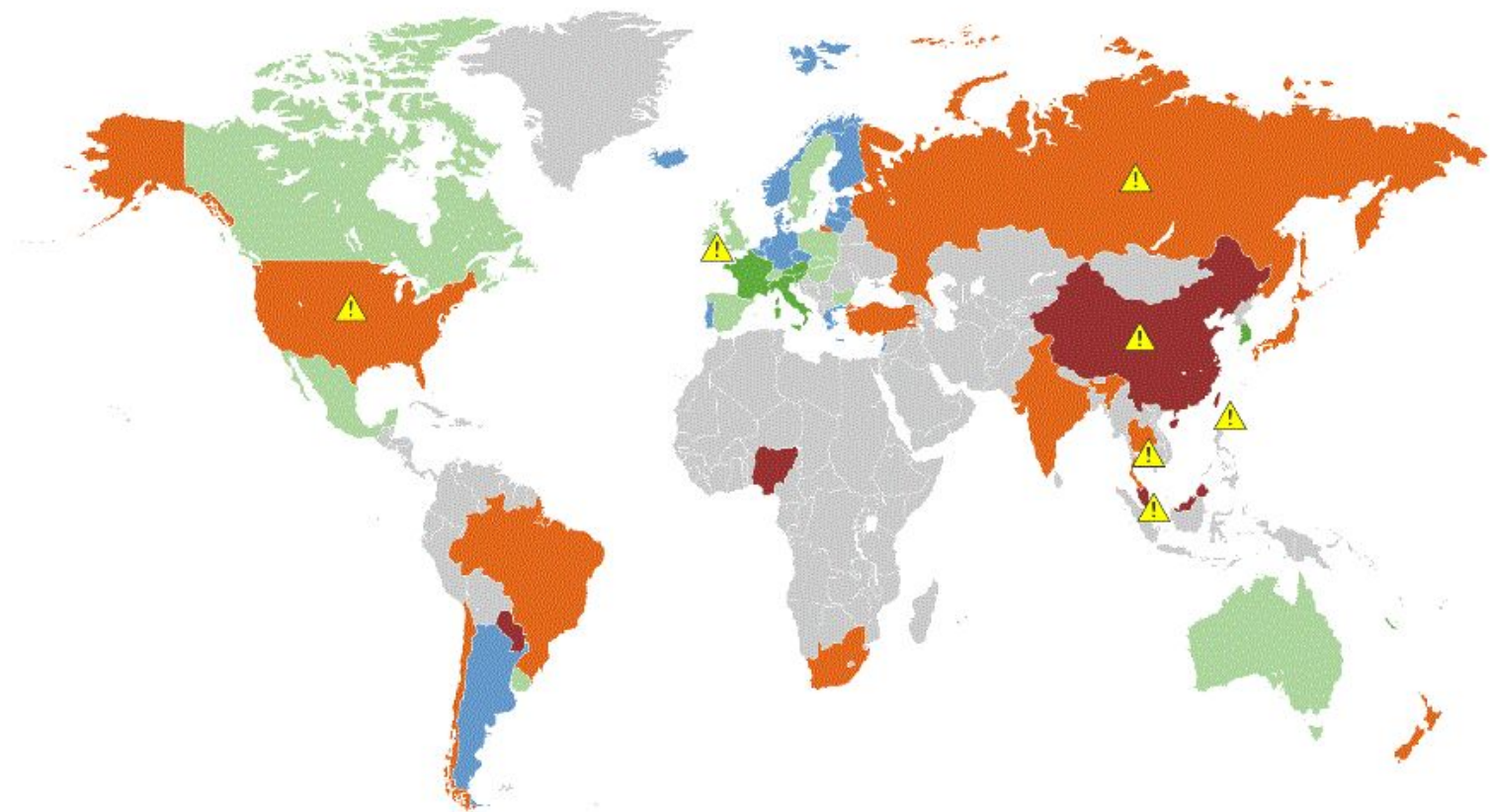
Source: Momentum Partners.

Problem #7 Jurisdiction 1/3

- Where is my data?

Microsoft to hide European data from the NSA with new German datacenters
<http://betanews.com/2015/11/11/microsoft-to-hide-european-data-from-the-nsa-with-new-german-datacenters/>

Max Schrems, European Law Student, Is Winning Against Facebook In A Data Privacy Case
<http://www.techtimes.com/articles/97276/20151020/max-schrems-european-law-student-is-winning-against-facebook-in-a-data-privacy-case.htm>



■ Most restricted
 ■ Restricted
 ■ Some restrictions
 ■ Minimal restrictions
 ■ Effectively no restrictions
■ No legislation or no information
 ⚠ Government surveillance may impact privacy

Source: US Department of Commerce and country-specific legislation

Problem #7 Jurisdiction 2/3

- Where is my data?

European Court of Justice Rejects Safe Harbor

<http://gmsmobility.com/corporate-relocation/knowledge-base/european-court-of-justice-rejects-safe-harbor/>

EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield

http://europa.eu/rapid/press-release_IP-16-216_en.htm

Problem #7 Jurisdiction 3/3

- How is data protected under the Law?
- Which are the differences between on-premise and
 - In USA cops need to obtain a search warrant to search your house, office and get access to digital evidences they may find
 - To get access to data stored on 3rd party systems they only need an easy to obtain subpoena
 - You may be not informed of the operation
 - The Patriot Act is often abused

https://en.wikipedia.org/wiki/Controversial_invocations_of_the_Patriot_Act

Problem #8 Gov's appetite 1/2

- Autistici/Inventati Crackdown
http://www.autistici.org/ai/crackdown/stampa/20050628_corriere.html
- Law enforcement or the NSA can easily access Cloud data
 - Convenient (remember PRISM?)
 - Zero knowledge systems are hard to implement
- You have basically no choice
 - Lavabit email service abruptly shut down citing government interference
<http://www.theguardian.com/technology/2013/aug/08/lavabit-email-shut-down-edward-snowden>

Problem #8 Gov's appetite 2/2

<http://www.wired.com/2016/03/feds-might-get-iphones-without-apples-help/>

“Justice Department has invoked the 200-year-old law All Writs Act to do it. But application of the Act requires the government to show that it has no other method of extracting data from the phones”

Problem #9 Liability

- Liability, if any
“Customer will indemnify, defend, and hold harmless Dropbox from and against all liabilities, damages, and costs (including settlement costs and reasonable attorneys’ fees) arising out of any claim by a third party against Dropbox and its affiliates regarding: (i) Customer Data; (ii) Customer’s use of the Services in violation of this Agreement; or (iii) End Users’ use of the Services in violation of this Agreement.”
- SLA is not a substitute of trust and evidence of good operations
- E&O (Errors and omissions) insurance is the most common risk shift

Problem #10 Ownership

- What Delete means in the Cloud?
- Who can use the data?
- Who is the owner of the data?
 - Facebook terms and conditions: why you don't own your online life
 - <http://www.telegraph.co.uk/technology/social-media/9780565/Facebook-terms-and-conditions-why-you-dont-own-your-online-life.html>

An example of miserable failure



The image shows a screenshot of a web browser displaying the Code Spaces website. The browser's address bar shows the URL `http://www.codespaces.com/`. A calendar widget in the top right corner indicates the current date is January 23, 2014, with navigation arrows for the months of December 2013, January 2014, and March 2014. The website header features the Code Spaces logo (an orange square with a gear icon) and the text "Code Spaces Source Code Hosting". To the right of the logo are "Sign Up" and "Login" buttons. Below the header, a central image shows a computer monitor displaying a code management interface. To the right of the monitor, a list of services is presented with green checkmarks:

- ✓ Subversion Hosting
- ✓ Git Hosting
- ✓ Project Management
- ✓ Fast, Reliable & Secure

At the bottom of the main content area, there is a green button with the Code Spaces logo and the text "Join Code Spaces Start your free trial in less than 60 seconds!". The footer of the page contains a row of logos for partner companies: ORACLE, macy's, Yellow Book, FedEx, smartWähler, RICOH, BOSCH, and TIBCO.

What you'll get from Code Spaces

Rock-Solid Repository Hosting

Revision 2.2 Further Enhancements to 2.x

Low Change Log

Revision 2.1 Any issues found with v2.0

Recent Subversion Commits

research And Development, revision 678 by Floyd Price (O 79 22:41)

research And Development, revision 677 by Floyd Price (O 79 22:29)

Code Spaces delivers first class Subversion and Git Hosting using the very best hardware and software combinations available. See our [Hosting page](#) for more information.

Full Redundancy & Snapshot Backups



Account settings / backups

Backups are taken everytime you updates your Subversion Data Best Time! Below is a list of the backups we have on file for your account.

Age	File Name	Download Size
about 1 month ago (March 07, 2011)	indip194.zip at 1557	Download (31.4 MB)
2 months ago (March 06, 2011)	shelldata195.zip at 1100	Download (13.7 MB)
3 months ago (February 18, 2011)	commercialturnerapath194.zip at 0909	Download (6.7 MB)
3 months ago (February 07, 2011)	turnerapath194.zip at 1901	Download (16.1 MB)

With Data Centers in 3 continents [we can guarantee 99% uptime](#). If our servers are not up for 99% of the time, we will give you that month's hosting for free - now *that's* a guarantee!

In-depth Reports & Project Analytics



Stay up to date with the progress of your projects with comprehensive analytics from Code Spaces. Our thorough reports ensure ease of management and accurate projections for teams, small and large.

Publicly Accessible Project Portals



Code Spaces Project Portal interface. The page includes a navigation bar with 'HOME', 'SUBMIT A BUG', and 'RSS'. The main content area displays project information for 'CODE SPACES PROJECT PORTAL', including a description, a link to the project page, and a table of project status details.

Project Name	Status
research And Development	Revision 678
research And Development	Revision 677

Keeping your clients up to date with the status of their project is a breeze with Code Spaces. Use our public portals to provide Wikis and deployment notifications, provide RSS feed updates, and allow clients to submit bugs.



We are experiencing massive demand on our support capacity, we are going to get to everyone it will just take time.

Code Spaces : Is Down!

Dear Customers,

On Tuesday the 17th of June 2014 we received a well orchestrated DDOS against our servers, this happens quite often and we normally overcome them in a way that is transparent to the Code Spaces community. On this occasion however the DDOS was just the start.

An **unauthorised** person who at this point who is still unknown (All we can say is that we have no reason to think its anyone who is or was employed with Code Spaces) had gained access to our Amazon EC2 control panel and had left a number of messages for us to contact them using a hotmail address

Reaching out to the address started a chain of events that revolved around the person trying to extort a large fee in order to resolve the DDOS.

Upon realisation that somebody had access to our control panel we started to investigate how access had been gained and what access that person had to the data in our systems, it became clear that so far **no** machine access had been achieved due to the intruder not having our Private Keys.

At this point we took action to take control back of our panel by changing passwords, however the intruder had prepared for this and had already created a number of backup logins to the panel and upon seeing us make the attempted recovery of the account he proceeded to randomly delete artifacts from the panel. We finally managed to get our panel access back but not before he had removed all EBS snapshots, S3 buckets, all AMI's, some EBS instances and several machine instances.

In summary, most of our data, backups, machine configurations and offsite backups were either partially or completely deleted.

This took place over a 12 hour period which I have condensed into this very brief explanation, which I will elaborate on more once we have managed our customers needs.

Thanks! And keep in touch ^_^

@ISGroupSRL

<https://linkedin.com/in/ongaro>

ascii@ush.it

Thanks! And keep in touch ^_^

@ISGroupSRL

Cloud

<https://linkedin.com/in/ongaro>

ascii@ush.it

Cloud