SecManiac

Security Zone
Making Sense of (in)Security

Dave Kennedy (ReL1K)

http://www.secmaniac.com

Twitter: Dave_ReL1K

About Me

- Creator of the Social-Engineer Toolkit, Fast-Track
- CSO of a Fortune 1000
- Co-Founder of DerbyCon
- Author of new book from NoStarch Press on Metasploit
- Back|Track Development Team
- Exploit-DB Development Team
- Exploit Writer
- Penetration Tester

What this talk is about…

Who here feels they’re company can withstand a targeted attack?

General Reaction…

Why?

We aren’t secure…

We are scared of….

SecManiac

Where were we…during…

We were here..

SecManiac

We prayed … please don’t let us be next.

So we watched and waited....

SECURITY


COMODO
Creating Trust Online™


SecManiac


MySQL®


SecManiac


SecManiac


HBGary
Federal


SecManiac

And a lot more…

So we hire…consultants…

to fix our challenges

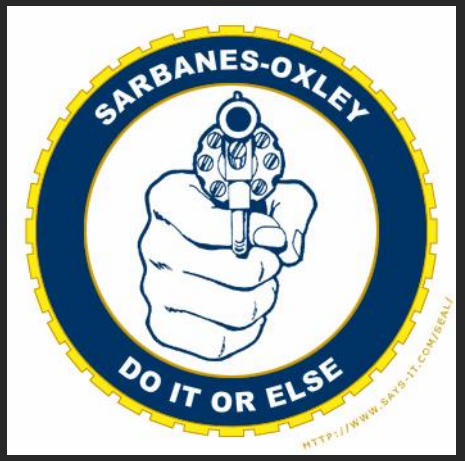
SecManiac

And we get..

certifications…

To expand our knowledge.

And we conform to..


SARBANES-OXLEY
DO IT OR ELSE


GLBA
Gramm-Leach-Bliley
Compliant


HIPAA

compliance…


PCI
Security
Standards Council
™
PARTICIPATING ORGANIZATION


NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION


SecManiac

To secure our organization.

SecManiac

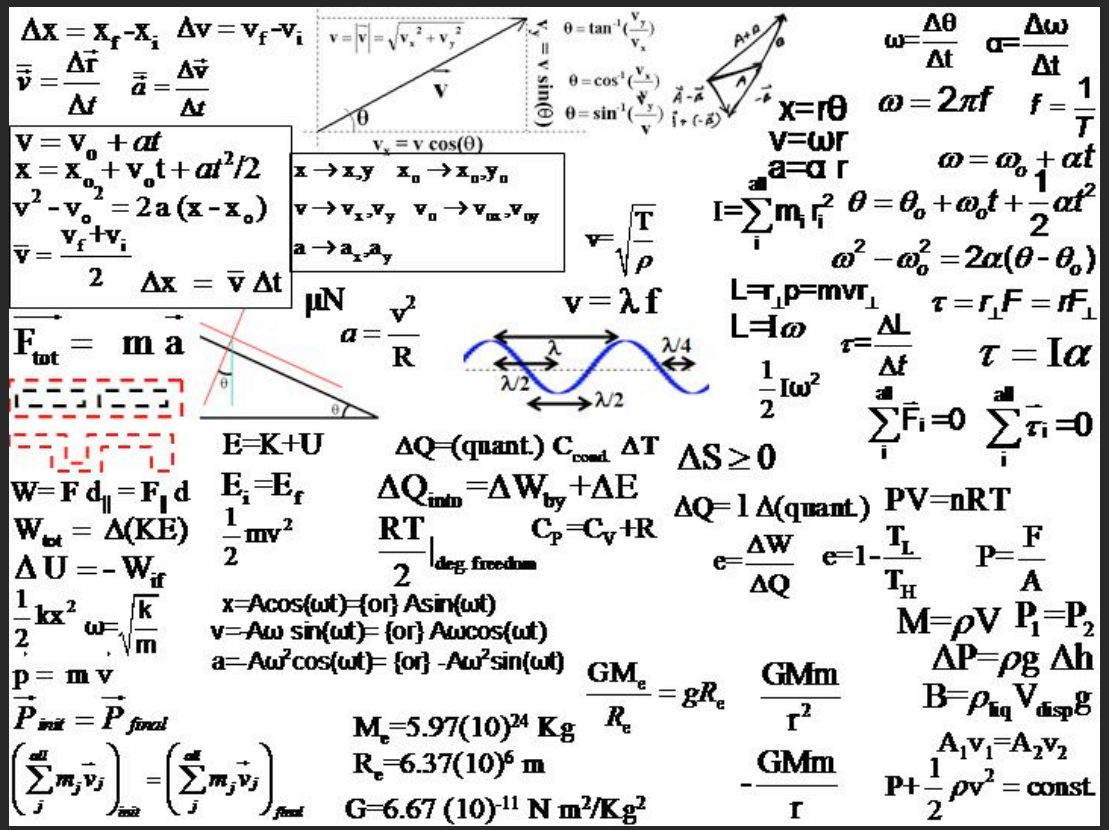
We prioritize our weaknesses with

risk management…

SecManiac

We create complexity

And add risk formulas



And spend…

SecManiac

For what??????

To be secure?

Are we?

We are a young industry.

Still finding our ways.

Is the path we are going right now the right one?

SecManiac

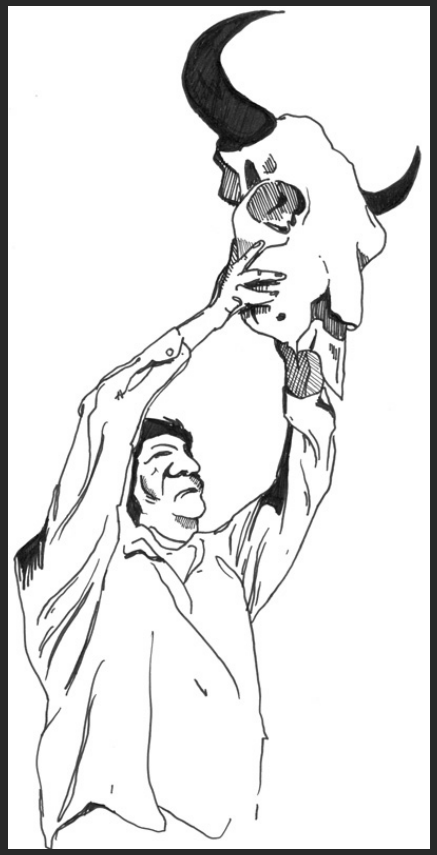
In order to answer this…

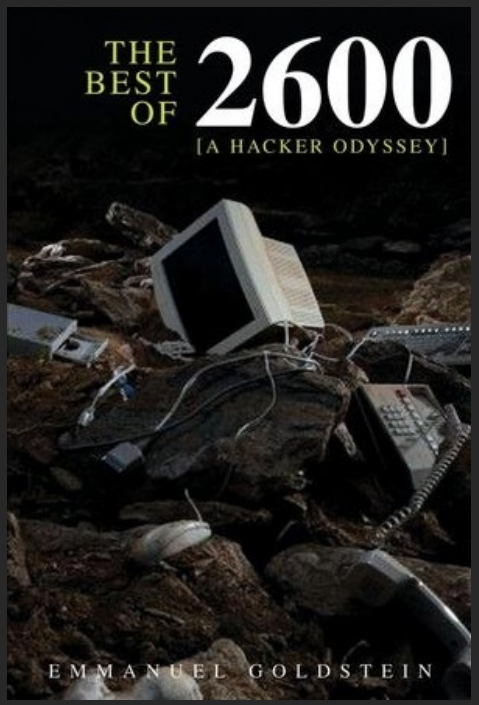
We need to understand

Maybe 15 years ago formally?

SecManiac

Before security, a breed of hackers were born…





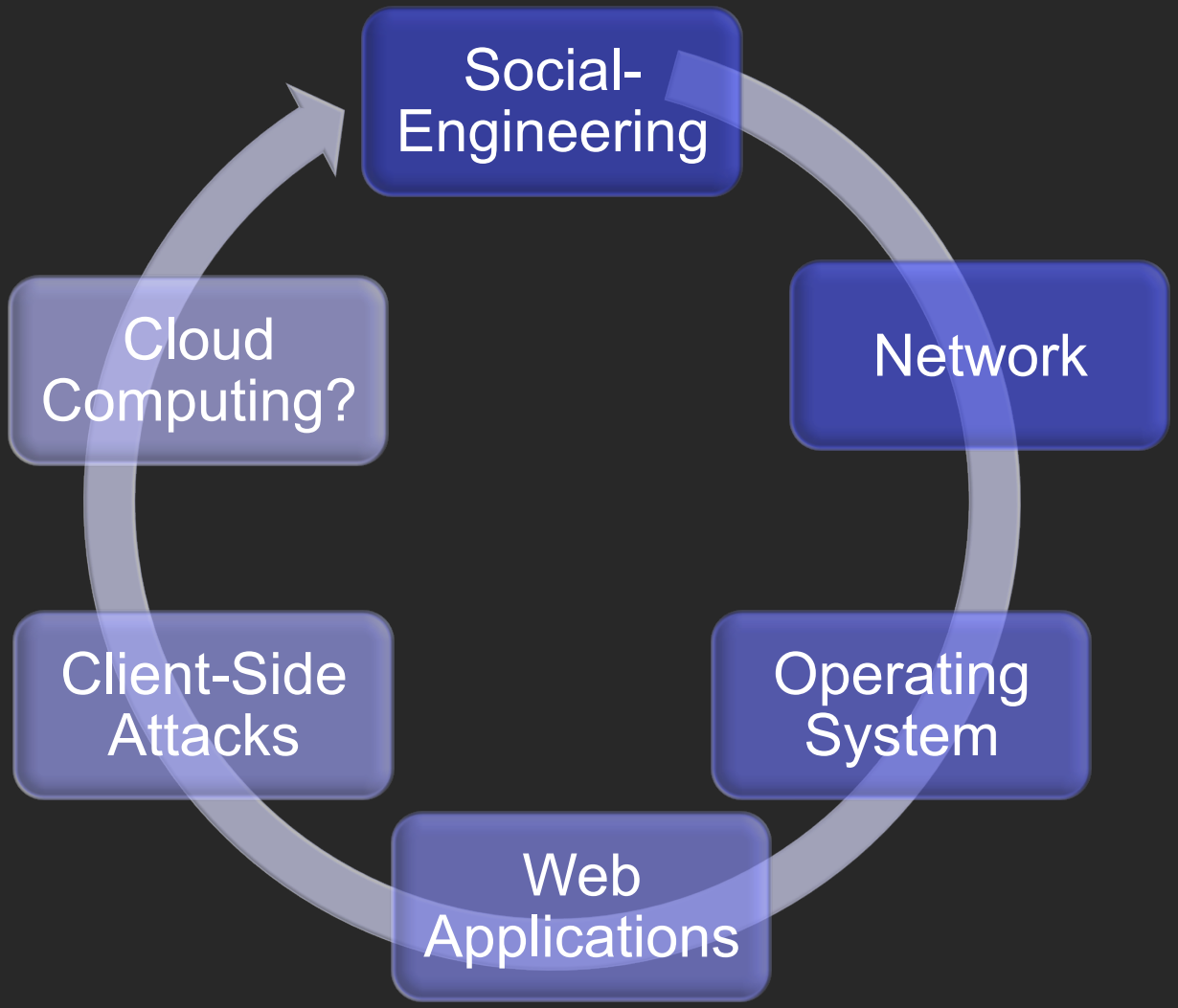
SecManiac

Technology progressed…

So did hackers…

SecManiac

Evolution of Hacking



SecManiac

A new era was born.

The Security Industry.

SecManiac

Flash forward - Today..

SecManiac

the present

SecManiac

2009 to 2010

- Security conferences reported record numbers.
- Security staffing decreased...then increased.
- Estimated 1 billion spent on Vista and Win 7.

SecManiac

2008 Breaches (PrivacyRights.org)

- In 2008 there was a total of 354 reported public data breaches.
- You might remember this one:
- RBS Worldpay, Atlanta Georgia

SecManiac

2009 Breaches (PrivacyRights.org)

- In 2009 there was a total of 252 reported public data breaches.
- We got better! … Wait?
- Largest breaches in history, largest amount of records disclosed, large amount of PII, PCI, PHI disclosed in one year ever.

SecManiac

2010 Breaches (PrivacyRights.org)

- We spent so much more this year… Estimated 34% increase on our budget.

- In 2010 there was a total of 594 reported public data breaches. Over double that of last year.

SecManiac

We are only the second industry that can continue to spend WAY more each year and get WORSE.

The first. Weatherman.

So we buy products to protect us.

But buy this, it will fix it.

Data Loss Prevention

But buy this, it will fix it.

Intrusion Prevention

But buy this, it will fix it.

Host Based Intrusion Prevention

But buy this, it will fix it.

Web Application Firewall

But buy this, it will fix it.

File integrity monitoring

But buy this, it will fix it.

Firewall

But buy this, it will fix it.

Anti-Virus

But buy this, it will fix it.

Whitelisting/Blacklisting

But buy this, it will fix it.

Patching Solution

But buy this, it will fix it.

Vulnerability Scanners

But buy this, it will fix it.

Network Access Control

But buy this, it will fix it.

APT Preventer

But buy this, it will fix it.

Data Loss Prevention

But buy this, it will fix it.

Anomaly Detection

But buy this, it will fix it.

Heuristics

But buy this, it will fix it.

Shiny stuff.

We buy technology to automate and prevent / detect human-based attacks.

So…

We have consultants.

Somehow they know our business better and how to secure us….

SecManiac

And we spend

And spend…

And spend...

Because we're told it will fix our problem…

SecManiac

This stuff doesn’t stop me….

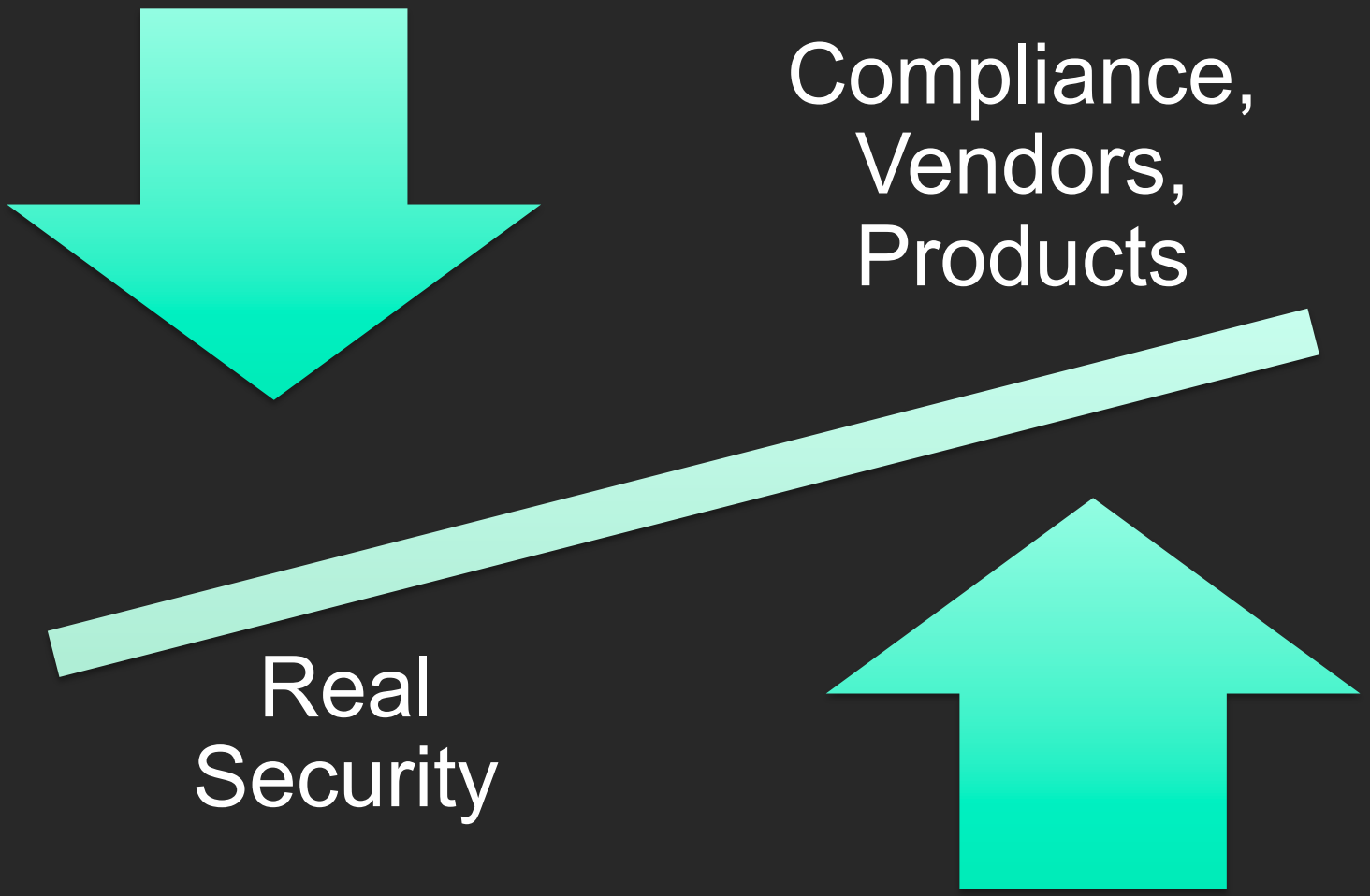
It barely stops her…

SecManiac

So why?

SecManiac

We aren't balanced….



SecManiac

SecManiac

We are taught risk management, risk acceptance, risk formulas. We are taught to be aligned with the business.

But we are in tune with “the business”

Does the business know security?

Do they know how to make decisions based on security?

Experience a Breach

SecManiac

Home of the Social-Engineer Toolkit

We are so scared of a breach.

Breaches can be a good thing.

SecManiac

It almost takes a breach for something to move.

Come to the realization that we will never win 100 percent of the time.

SecManiac

In most cases: A breach will not destroy your company.

SecManiac

Sometimes a breach isn’t as bad as it sounds..

SecManiac

It can help us.

SecManiac

So you can’t get security funded…..

Get breached.

SecManiac

Option 1

- You get popped.
- It sucks. Yea.
- But use this. Inject security into the company.

Option 2

- Simulate a breach.
- Penetration testing.

Who here has had a “penetration test”.

SecManiac

A penetration test was never what it was designed to be.

Our tests today are vulnerability scans and validation of testing.

How is that a simulated breach?

SecManiac

A penetration test is a simulation of an attacker attempting to cause impact to the companies ability to generate revenue.

SecManiac

They are designed to simulate a breach.

Penetration Test == Breach Simulation

SecManiac

You need to jack a company up.

SecManiac

You need to make them hurt, you need to be able to show you could destroy that company and everything it does.

SecManiac

Who here has had a “penetration test”?

SecManiac

So what now?

The Future..?

SecManiac

That’s up to us…

SecManiac

It could be this…

SecManiac

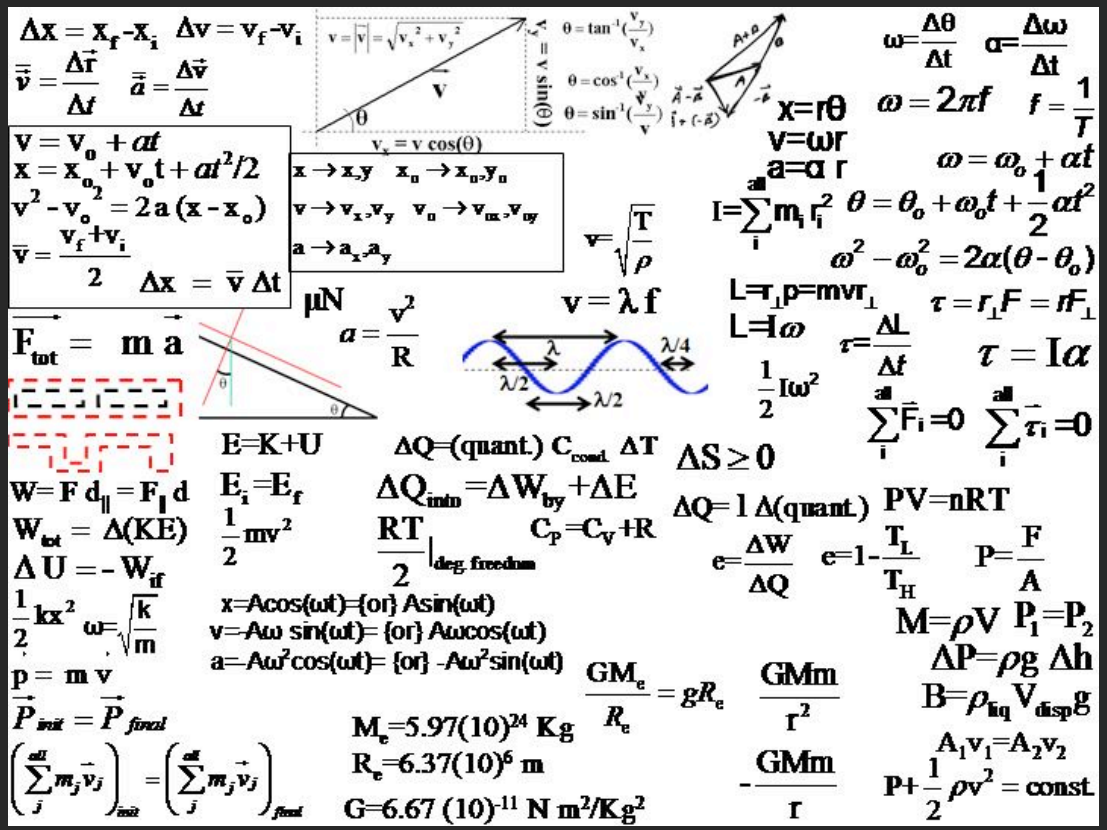
We need to invest in our people and do some hard work…

Or if we…

Impact change….

Secure critical assets that make companies money…

Move away from risk formulas and auditors…



Ignore the fear mongering…

SecManiac

Throw away the 5 year plans

SecManiac

And secure your stuff.. You got it.

The easiest thing to remember is

Find out what makes your company money.

Protect that.

Simple.

SecManiac

Invest in people.

Not technology.

Get Back to Reality

SecManiac

Breaking stuff.

SecManiac

Home of the Social-Engineer Toolkit

Thanks.

SecManiac

Home of the Social-Engineer Toolkit

davek@social-engineer.org
Twitter: dave_ReL1K