

FAIL SECURE

23 Ways to Undermine Your Security
Program

ISSA Central Maryland Chapter
August 28, 2019

Disclaimer

Security compliance is important

Some of my best friends do compliance

It's a tough job on the good days

Don't hate the playa, hate the game!

Tom Hallewell

Dad and Husband

Fed

Recovered system and network admin

Development Team Lead

Compliance

Software Assurance

Vulnerability Management

Incident Response

Malware Analysis

Policy Wonk

Identity Management

Network Defense

Irregular Blogger

Culture Clash? Nah.



This is Hopeless!

You have the power to transform security in your organization!

Listen

Collaborate

Prioritize

Explain

Support

Make connections

Help

You don't need permission!

Let's have a meeting!

We need more effective meetings with the stakeholders

Stakeholders are busy creating value for the business

They don't have time to listen to you read a list of deficiencies and schedules to them

People will love you if you can cut that 2 hour meeting down to 15 minutes!

Assign personal blame for deficiencies

Establish a "no bus" rule at your kickoff meeting

Agree to focus on resolution, not culpability

This doesn't mean to ignore root causes

Train don't blame

Security should come first

The mission comes first, and the things we are auditing/securing ARE the mission

It's our job to help them get to market on time, and securely, or we've failed the mission

There has to be a value proposition between the cost of breach and the cost of prevention

Management decides whether the risk is acceptable

The stakeholders don't care about security

The stakeholders care about the customer

They care about the mission

They care about the quality of their work

Stop talking about requirements and frame security in their language

Understand their interests and speak to them

Maybe they'll start to understand your interests

Use Cybersecurity as an HR Tool

Stakeholders will clam up if they think you'll use security data against them

This is not how you instill trust and transparency

Transparency is a two-way street!

Operate in stealth mode

They're your colleagues, not The Enemy

Black box testing is for red-teams, not auditors

The purpose of internal audit/accreditation is not to "catch" or "ding" people, it's to help your organization prevent an incident

Operate from a position of mutual benefit

They Failed the Test

No, we failed the test

The test is whether we can get this product out without rework

If we don't help them deliver, we failed

Our job is to show them how to pass

We feed them the answers so they can get an A

I don't care what you want to call it -
it's a deficiency

Words matter

People are passionate about the systems they build

They get defensive when you tell them there is a flaw in
their work

(Even if they know in their heart it's a hot mess)

Talk about findings, not flaws, problems, and deficiencies

If you call it a vulnerability, a smart team will make you
prove it before they'll fix it

Use Jargon and Acronyms

It's frustrating when someone throws a bunch of new acronyms and jargon at you

Speak plain English

Explain consequences in a context that your stakeholders can relate to:

Downtime **Loss of Revenue** **Schedule Delays** **Cost Overruns**

They'll get it

It's the system owner's job to figure out how to resolve findings

This has to be a partnership

Devs and Admins no hablan security

Hold their hands for a while and help them fix some findings

They'll gain confidence in you and their ability to resolve findings

Crawl Walk Run

Technology will solve all your security problems

Most shops are drowning in tech
Execution is the problem

They don't have the discipline to install, configure and maintain the systems they have

If you can't do it in a spreadsheet on a small scale, your fancy tool won't help

We Need More Data

You don't need much data to make better decisions than you're making now

Data costs money and time to collect, store, and interpret

Is the data you're trying to defend worth the price of the data you're gathering?

A treasure chest should never cost more than the treasure!

If you collect 5 data points, there is an 85% chance that the median will be in that range

Fix everything now, or you'll get hacked!

You're not allowed to exaggerate!

We need to look at risk based on real consequences

In general, the more "ifs" and "ands" in a statement of risk, the lower the risk

Prioritize the risks with the least "ifs" and the scariest "then"

Each conjunction adds an action for the attacker - and a point of detection for the defender

This agile, cloud and automation stuff is risky

So is maintaining the status quo

New technology mitigates old risks, but introduces new ones

Take the time to understand the technology before you
default reject it

You may find that some of it makes sense

Work on multiple issues in parallel

Say it takes a week to get one thing to 100%

If you work on 7 things at a time, then all of them will be at 10% at the end of the week That's still red

It will take 10 weeks to get everything to green

It will take 10 weeks before you can tell your boss you've completed anything

Show progress by focusing on something you all agree is important and achievable

You have to be 100 percent Compliant

You should strive for excellence, but accept that you didn't get to this point overnight - it took years

It's going to be a long haul

Make incremental progress

Identify low-hanging fruits for quick wins

Identify solutions that can solve multiple issues at once
(like patching acrobat on 20 machines will eliminate 40
Nessus High findings)

I'm the only one who cares about
security

18

Since you put it that way, maybe you are

We need more documentation

You need better documentation

Documentation is a lot of work

Documentation should be as lightweight as possible

Bullets and diagrams are better than prose

Auto-generated if possible

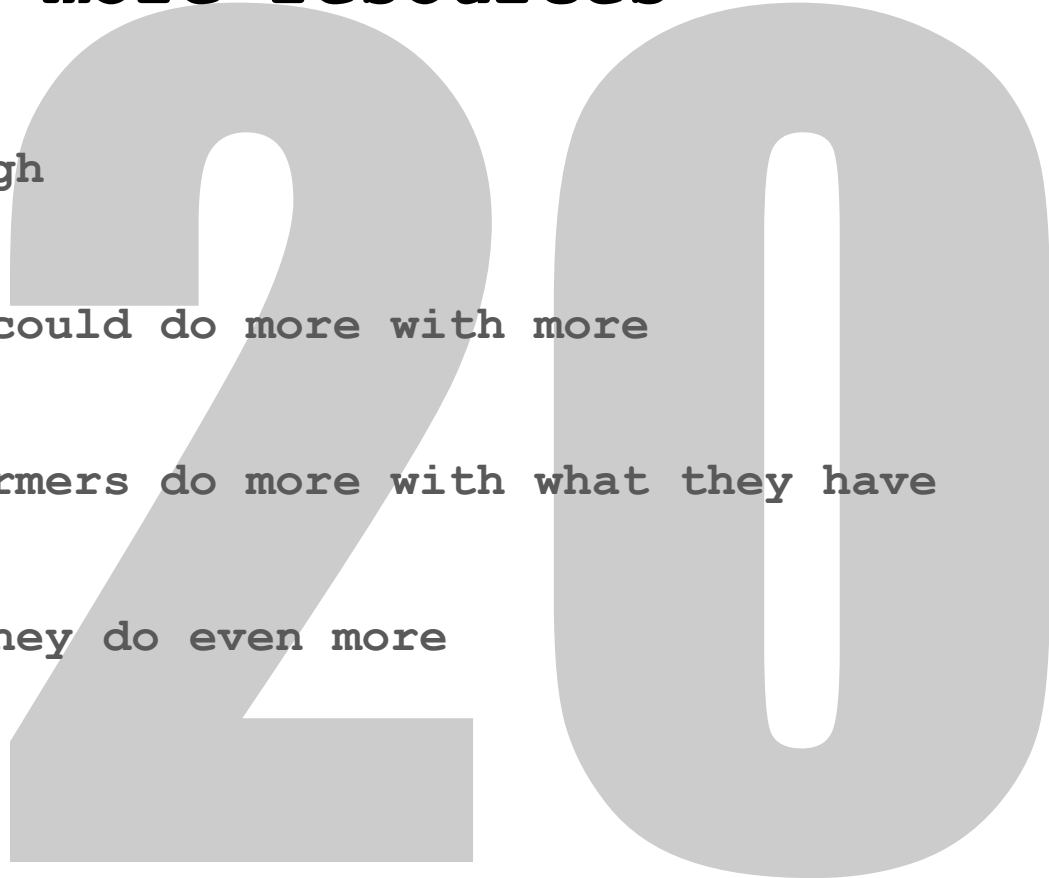
We need more resources

Life's tough

Everybody could do more with more

High performers do more with what they have

And then they do even more



I can't do this without buy-in from management

Top-down support is huge!

It opens doors

It makes everything easier

It's the right answer on all the certification exams

But you can make a difference by just showing up and doing the work

Once you make visible progress, management may buy in

I'm too busy to...

Busy is a choice

Never let them see how hard you work

Make it look easy

Have shorter, more frequent meetings

Don't run through status reports in meetings

Share them via email and focus on the three things you want to work on this week

Nothing I do will make a difference

Try to make a little progress every day!

You'll be amazed at what you can do in a month.

People will begin to notice your work and want to know your secret.

The secret is to get started.

Conclusion

Put some skin in the game

Stop aiming for "gotchas", instead help teams be successful

Create a collaborative, blame-free culture

Take tiny steps - you'll be amazed at what you can do

It gets easier

The Five Stages of Grief Applied to Software Security

Denial


These are false positives!



Anger

Those security idiots don't know anything about coding!

They're slowing down the whole sprint!!



Bargaining


Can we get an ATO if we just fix the HIGHs and CRITICALs?



Depression


All is lost!!!

Our velocity rate is slipping - we'll never make it through this backlog!



Acceptance

Let's just bite the bullet and get this done!



Inspiration

Behr, Kim, Spafford: The Phoenix Project

Wu: The Master Switch

Hubbard: How to Measure Anything

Singer, Brooking: Like War

Ries: The Lean Startup

Benson: Why Plans Fail

Ries, Trout: The 22 Immutable Laws of Marketing

Gladwell: Revisionist History Podcast

Tufte: The Visual Display of Quantitative Information

More Inspiration

More: Lean Security 101 Comic <https://www.eyrasecurity.com>

Carse: Finite and Infinite Games

Graeber: The Utopia of Rules

Adkins: Coaching Agile Teams

Taleb: Skin in the Game

Carnegie: How to Make Friends and Influence People

Seth Godin: Akimbo podcast <https://www.akimbo.me/>

Tim Ferriss: Anything

Contact

LinkedIn: <https://www.linkedin.com/in/hallewell>

Blog: <http://cybereffective.blogspot.com/>

Twitter: @Hallewell

Email: hallewellt@gmail.com