



MANAGING LATENT CYBER THREAT VECTORS

ANDREW HALLBERG

ANDREW.HALLBERG@ABC.VIRGINIA.GOV

@ANDREW_HALLBERG

Everyone is aware of CSRM's process for managing system security (BIA -> Data Classification -> Risk Assessment -> System Security Plan), Right? Job's done, everything's secure? But there are obvious holes here... Not everything is a system.

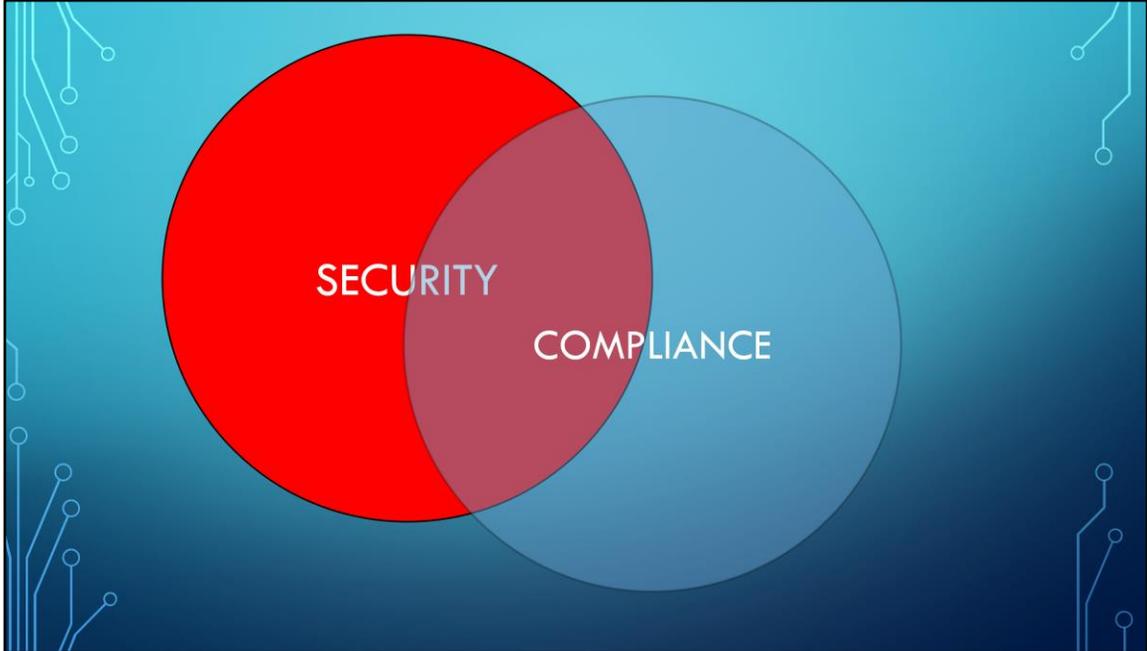
We found gaps

SEC501 is based on concept of "Information System"

Ignores agencies that have no Info Systems AND "things that aren't really systems"

IT Teams use this as leverage to create loopholes

XYZ is just a "tool" or "application", it's not a system



We KNOW that Security != Compliance, but what do we **do** about it? If you find an issue that DOESN'T meet SEC501, how do you track it? What if it *technically* meets SEC501 but is still a risk? What are you doing to address "Security" shortcomings that aren't identified in SEC501/ISO.

We ran into this problem and had to devise a way to identify and track issues across the board.

Here comes the cyber.



Using a wide range of the latest cyber research technology, the elite cyber warfighters at Virginia ABC used both strategic and tactical methods to identify latent cyber threat vectors.

There's a Cybersecurity Revolution and we are on the bleeding edge. Some of what we found were MAJOR agency-wide control deficiencies. Some were extremely minor. The wide range of complexity made it difficult to manage perception of customer value. Because of this, we had to develop a process to notify IT and the business when these threat vectors were identified. I assume this process looks a lot like the process used at your agencies as well.



<<< Here goes frantic chasing of threat vectors >>>

Bob your screen is unlocked

Hey boss, we don't have DR on ANYTHING

Somebody needs to fix these APA audit points

Why are there passwords in this source code?

It wasn't tested? What do you mean there's no test environment?

It's great that the developer fixed it, but why did the developer have access to production?

Should I even ask if there was a change control?

Our vulnerability guy found an unsecured IOT Device on the network.

Bob your screen is unlocked again...

Oh, you made your own "homegrown" encryption, great.

So the pentest found default "Admin:Admin" creds. Whose going to fix it? Better yet, how are you going to make sure it doesn't happen again?

So the payroll spreadsheet... With everyone's social on it... is on the shared drives...

Why can't I change my own password in this system?

So you used your AA account to add your COV account to the Admin group. Sweet.

Who left these Dormant Cyber Pathogens here?

Is that a SQL server under your desk?

Great, the APA is back. Has anyone done anything about last year's findings?

Somebody find Bob and tell him to lock his workstation!

We did this for a few years. Eventually, they tune you out. Then what?

THAT DIDN'T WORK, NOW WHAT?

- Report it out
 - Tell CIO
 - Tell Business
 - Tell Executives
 - Tell CSRM
 - Tell Auditors

When you can't get it fixed by breathing down someone's neck... You have to CYA. You can't keep it a secret because then you're just as culpable, so you report it out.

<<ANIMATE>>

This is great for CYA, and relieves us of the "burden" of knowledge... But doesn't actually fix the problems. Because what are these guys gonna do? At best they're gonna write you a "strongly worded letter" then...

WHAT NOT TO DO



Right? Because many of these issues are too small to address individually, or don't fall to their daily responsibilities. For example, CSRM doesn't care about single user issues like Bob's workstation, but these are genuine security problems. Or maybe it's not a genuine security issue, it's a compliance problem, but they are already on their third repeat audit finding.

Reporting out also creates a side effect that's worse: Us versus Them. *"Hide that from Security cause they'll make a big deal, then go tell everyone about it."*

IT (or sometimes business) starts to roadblock because "security finds problems so we don't want them to get in". Removing access to systems, keeping two sets of books, under documenting, leading to tribal knowledge hoarding, etc.



So how do we solve this? In order to manage the evolving cyber threat spectrum, we needed some way to catalog issues, assign ownership, and track to completion to deliver stakeholder value. So the elite cyber warfighters at ABC came up with a plan... We sent each other emails.



But emails get lost, and aren't good for categorizing or tracking so we needed to sharpen our cyber-pencils.

So once again, the elite cyber warfighters at ABC set our sights on resolving this systemic problem and RAISED THE BAR for the Commonwealth. *(Dramatic Pause)* Oh yeah, we went full-spectrum cyber.

<<CLICK>>

So we put them in a spreadsheet. We called it our "Control Deficiency" spreadsheet. Every Time we found a security issue, it went in the spreadsheet. This wasn't terribly bad, and lasted a good while.

Ultimately, we decided on a ticketing system. We wanted something that could eventually auto-mail users notification of age, Workflow to different queue, age-out old tickets, provide reports and metrics.

We were lucky enough to have a ticketing system already. If you have one, take advantage of it. If not, try the spreadsheet and see if it helps, or see if you can get a

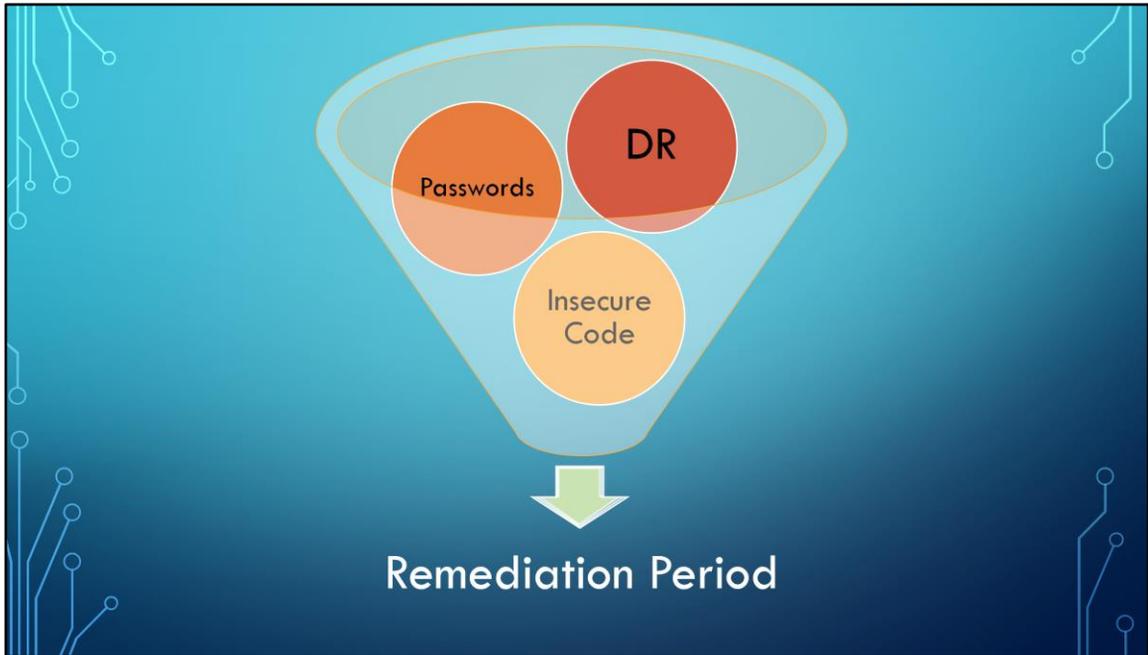
VCCC queue.



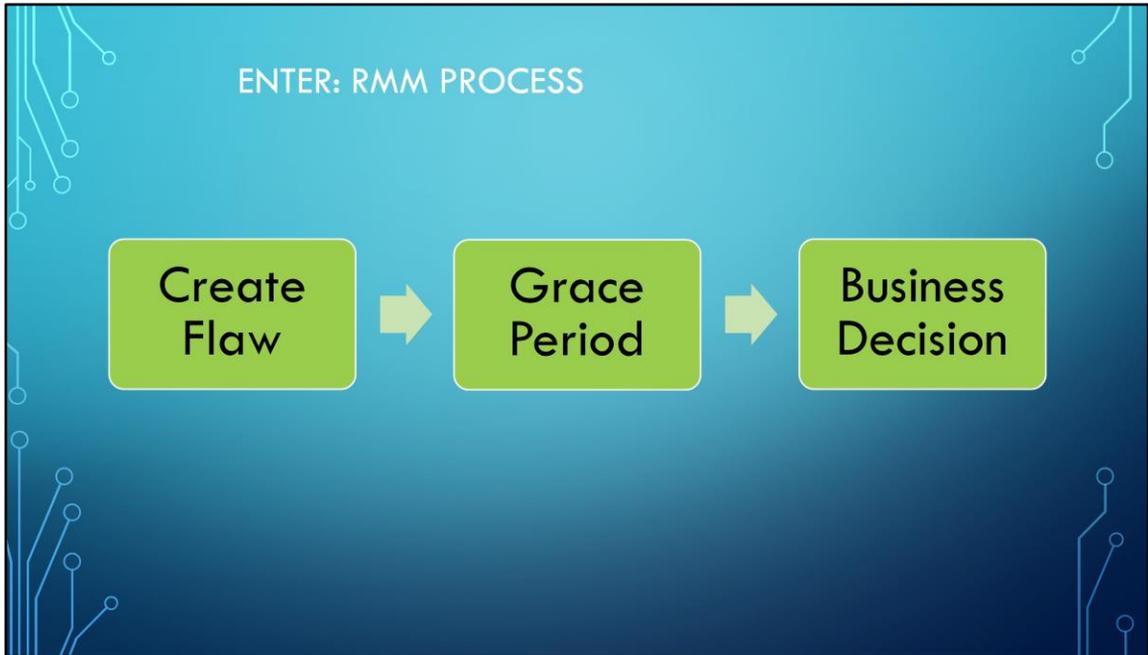
So now we have a way to **collect** all these random issues. It's a bucket. It gives us a way to deal with the question of Security-or-Compliance because they go to the same place.

(EX) You need to update your documentation or you won't be compliant – vs – You need to secure this spreadsheet or we're at risk of data breach

Which is fine, but not exactly groundbreaking. And still doesn't help with "Us Versus Them".



So we needed some way to turn this bucket into a funnel. A process that gives people opportunity to resolve and comment, but still keep moving towards business ownership of the risk decision.



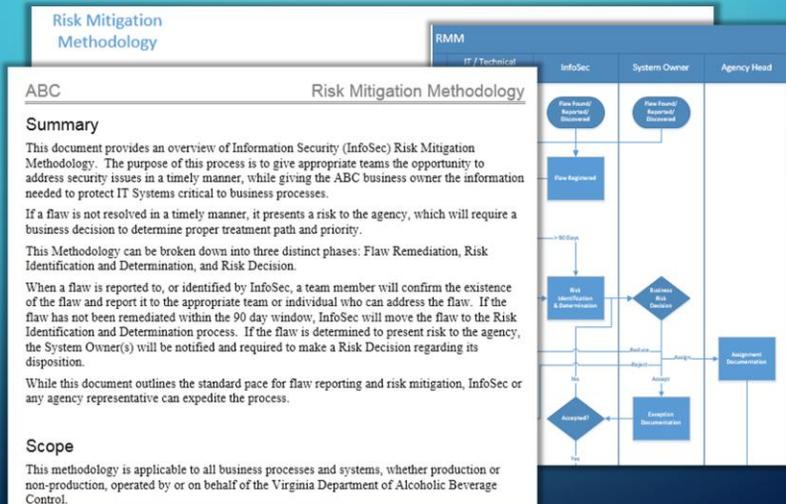
Risk Mitigation Methodology – It’s a terrible name for a great process. Through it’s simplicity it clears up many questions.

1. Infosec has a funnel to place ALL of the random Latent Cyber Threat Vectors
2. IT has an opportunity to address on their schedule, nobody breathing down their neck.
 1. Standard notification process (No question of email vs shoulder tap)
 2. Standard Grace Period
 3. Metrics
3. When it gets to the business, they know that someone has had an opportunity to address, it’s not a knee-jerk response.

After expiration, InfoSec determines the risk, present to business for decision
Present them with Options: fix it, Get exception, Disable it

Finally, this gives us a straightforward standard process so when we have an emergency like Heartbleed or Shell Shock, they know to listen.

RMM PROCESS – MATERIALS TO STEAL

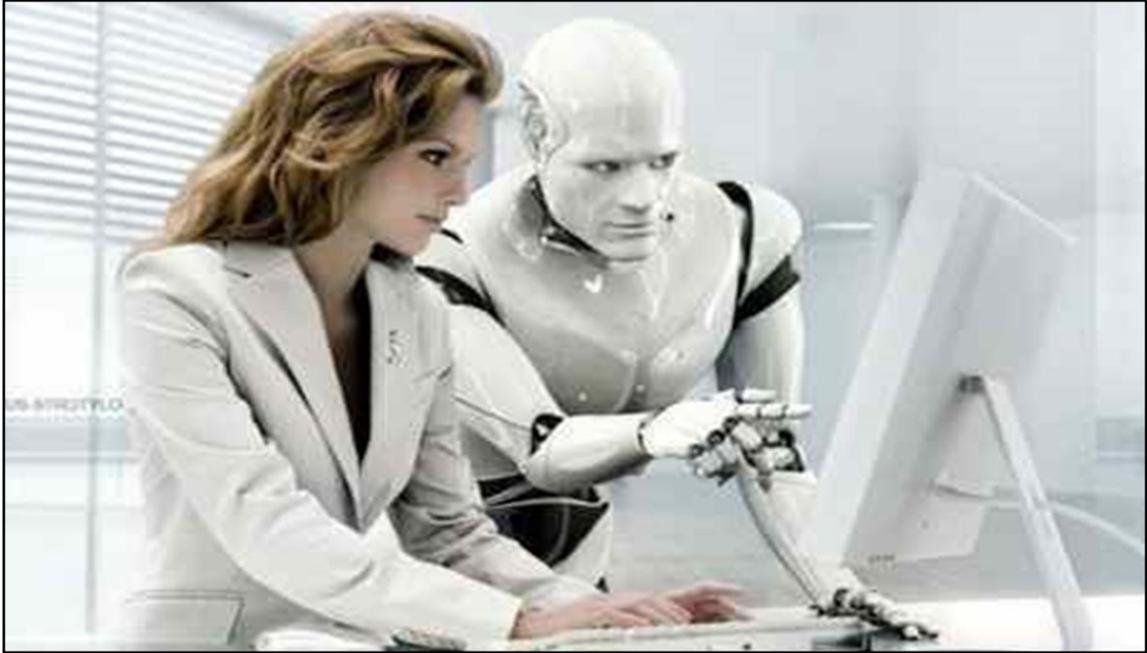


We've created process flows, swim lane diagrams, and a process/procedure

I love sharing, please take and use these

One Caveat – If you improve on it, give it back so others can improve as well. I'll post in knowledge sharing site, or email me.

<< DEMO Footprints and HR Test here >> (Comment that these are LIVE so FOIA exempt, please don't share)



Our goal was to provide an on-line, proactive Strategy to provide Scalable Benchmarks in managing the evolving threat landscape.

This morning, we heard from Eric O’Neal “There are no hackers, there are only spies.”

As we all know, and has been reiterated here today, hacking is no longer a basement dweller activity, but has morphed into organized attacks. Most of us in state agencies don’t have to deal with nation-state threat actors, <<Click for Anon>> but we do have to deal with hacktivists.

Mr. O’Neal also said “Amateurs attack computers. The professionals attack the people.”

<<Click for Robot>> I believe that is true for the defense as well. Barry said at lunch that this is a people business. THIS PROCESS isn’t about making technical changes, this is about hacking people to overcome resistance within your organization.

A decorative graphic on the left side of the slide, consisting of white lines and circles on a blue gradient background, resembling a circuit board or data flow diagram.

Andrew Hallberg

Andrew.Hallberg@abc.virginia.gov

[@Andrew_Hallberg](#)