One CISO's Opinion...

Security Innovation Awareness

Through Vendor Relationships

Allan Alford, CISO

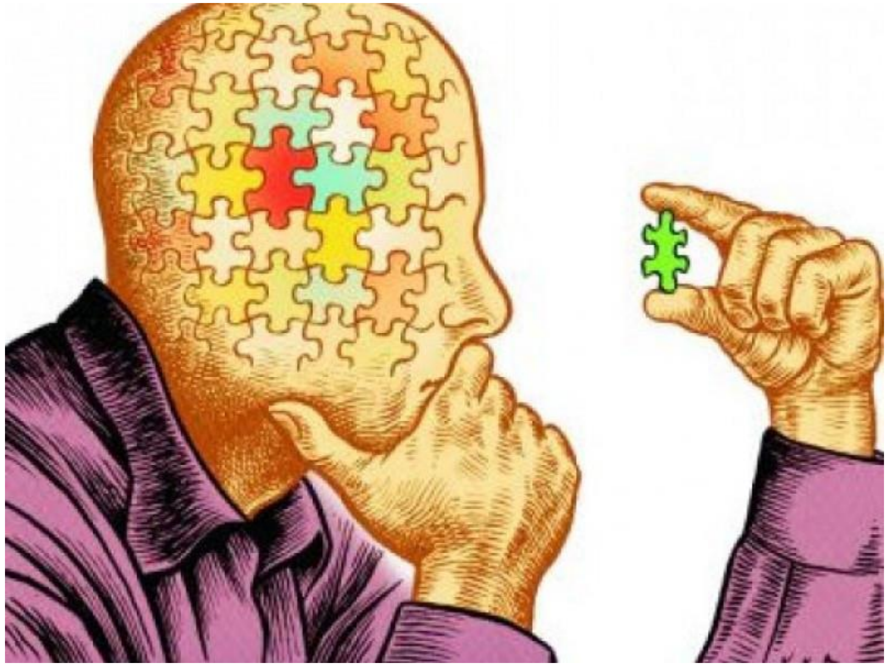
February, 2019

NOTICE

This presentation is part of an ongoing series: ***One CISO's Opinion***.

As such, the author's opinions are his own and do not necessarily reflect the opinions of any employer, academic institution or professional organization with which the author is or has been affiliated.

I Was a CISO in the Security Industry…



In my previous role I was CISO at a security company – a company that made solutions for Web/Email Protection, DLP, CASB, UEBA and NGFW.

The security industry is self-aware. It keeps up with itself, its technology and its innovators.

Casual hallway conversations would yield information not just about immediate competitors, but even those in the security space who were making innovations in other areas – like SIEM or Desktop Protection.

I Didn’t Know What I Had Until It Was Gone

After leaving the industry, that steady supply of information dried up overnight…

I had to find a new way to learn about industry innovations…

Awareness of Industry Innovation is REQUIRED

> *"During the last few years and particularly in recent months, we have been witnessing increased activity, coordination and even innovation from the bad guys."*
>
> Cyber Startup Observatory

The security world is an ever-changing landscape. At any given moment, something new and innovative arises *that exactly solves a problem you've been having*. The problem is that you probably don't know about it...

Threats change, solutions to address those threats change, but how do *you* change?

The Bad Guys BY NATURE think outside the box. We must too.

Five Methods for a CISO to Stay Abreast of Innovation

- Peer Groups
- Curators
- VARs, VARs, VARs
- Direct Vendor Engagements
- Podcasts, Blogs, Websites, Etc.

> *"Traditionally, CISOs gently balanced their precious resources between vendor education and securing their environment. With the number and aggression of security vendors increasing, CISOs are shutting down vendor communication in favor of CISO-to-CISO education".*
>
> David Spark, Co-Host and Producer of the CISO/Security Vendor Relationship Series

Peer Groups – Real and Virtual

- CISO Summits/Exchanges (Like This One)
  - In the last 4 months I have presented in Dallas, Toronto, Austin – Present something and the cost is low to meet with peers
- Local lunches/breakfasts (e.g., CISO Executive Network)
  - I attend weekly and monthly events in Austin and even San Antonio
- Local Chapters for ISSA, ISACA, ISC^2, OWASP, etc.
  - I admit I am remiss here, but plan to dive in
- LinkedIn Networking & Groups
  - > 16k Connections and 74 Groups
  - Don’t forget industry-specific, non-security groups!

The problem with peer groups is that they are a closed-loop system. Somebody has to be the first one to let the new technology or the new vendor into that loop.

Somebody has to step up and take one for the team.

Curators – Many Charge, But Some Don't

- Curators vet and sort the tech for you, usually with a specific focus – best of breed, most innovative tech, etc.
  - These are usually boutique affairs, and some charge a subscription fee for the CISO
  - Find the ones who do not charge to browse
  - My Favorite Free Curators:
    - **Cyber Startup Observatory** – Just download and read!
    - **The Roundtable Network** – I'll provide login credentials to browse their selection
      - *DISCLAIMER: I'm a member of both of the above*
- https://itkit.io is more of an aggregator than a curator, but is a quick resource nonetheless

Many More Exist – Ask Your Peer Networks

1 VAR Is Good…

Challenge your VAR Every Time and make them do the research

Arrange a VAR Demo Day where the VAR presents you 5-6 innovators that address problems you have given them to solve

… But 3 VARs Are Better!

Arrange a 3-VAR Showdown and give them the rules ahead of time:

1. You must find a new and innovative vendor who addresses my problem
2. Once one of the VARs has called 'dibs' on a vendor, no other VAR is allowed to submit that same vendor – latecomers have to work harder
3. Arrange another demo day and pick the best from the three!

* Credit to Josh Sokol at National Instruments for the 3-VAR Approach

What About the Venture Capital Community?

It would make sense that VC's would be a great resource for finding out about new and innovative technology. I've befriended quite a few both locally and nationally…

The problem with VC's is that their concept of "innovation" is 3-5 years in the future and, thus, usually not very practical for your current needs.

The other problem with VC's is that once they are invested in a given tech or company, they are really nothing more than salesmen when you talk about future innovations.

My Historical Approach to Vendors

Direct Vendor Engagements – Opening Up The Floodgates

The next few slides speak to a bold experiment and/or a fit of madness

You be the judge

In September, I announced the following on LinkedIn to what was then a total audience of roughly 11k folks (roughly 30% of them being vendors):

“For the next unforeseeable future, I'm going to commit 2 hours a week to new vendor chats.

I'm trying to limit folks to a 1/2 hour pitch, and figure some might spill to an hour, so let's call it 3 new vendor meetings a week. That's only 2 of my 60ish hours, so let's call it 3% of my time.

I'm refining my technique as to who I let in and why, but the idea is to tackle this "How do I stay current on disruptive tech?" question by deliberately exposing myself to new vendors on a routine basis.

(For the vendors in my network, this is not an automatic meeting - I'm focusing on areas of current need, etc.)

I'll keep you all informed as this progresses. *I suspect I will consider the time investment to be a payoff.*”

I Knew I was Inviting a Wave of Communications, But…

I also knew I was confining the experiment to LinkedIn, which I can handily ignore during the course of my workday.

But the reaction was far beyond what I anticipated. The chum was in the water and the sharks were circling…

- Within *just a few days*:
  - The post went viral. My network was only 11k and the post got 36k views.
  - I got roughly 1.5k vendor requests to connect
  - I was FLOODED with LinkedIn messages from vendors
  - I even got hit up via phone and email with vendors referencing my post

BUT: I was also starting to hear about new solutions to problems I was facing. The experiment was working, but I needed to adjust the signal-to-noise ratio rather dramatically…

(I also got invited to be a guest on the CISO/Security Vendor Relationship Podcast.)

Filtering the Flood

Four days after the initial post, I posted the following:

I have an update to “Operation Let The Vendors In”:

Cold calls are still ignored.

Unsolicited emails are still ignored.

A good pitch on LinkedIn might result in my sending you my email address for further communication.

What's a good LinkedIn message pitch?

One-sentence intro that ideally shows you have any clue about what I am up to. Example: In a recent article/interview, you said that you have a specific interest in automating compliance. Example 2: I see Mitel recently partnered with Google to leverage Google Cloud AI.

Short Paragraph One: Here is what we do. Example: We assess third-party libraries for vulnerabilities in your application development projects. Example 2: We employ analytics to reduce overhead associated with threat hunting red herrings.

Short Paragraph Two: Here is why we are the vendor you should go with in this space. Example: 80 of the Fortune 100 use our stuff. Example 2: Our AI is the only AI to have been proven to reduce false positives in an objective competition set up by the such-and-such consortium.

Conclusion: I'm hoping for a bit of your time, and I won't stalk you if you don't respond.

This Did the Trick

- Within *just a few days*:
  - The post went viral. My network was only 12.5k and the post got 55k views – As of the last time I was able to measure, this post got 87k views total vs. the original post maxing out around 45k.
  - ***It turns out that the vendor community was more hungry for guidance than for leads!***
  - I was FLOODED with LinkedIn messages from vendors – this time most of them were in accordance with my rules
  - (I still got hit up via phone and email with vendors referencing my post too)

BUT: The experiment was working! I was able to set a tentative block of my time on Friday afternoons each week to slot vendors into when they got my attention. I began conducting the 2 hours-per-week meetings.

Adjustments and Sustaining Phase

2019 Budget Planning Was Upon Me

- I was finding so much success with the experiment, and had so many areas where I wanted to learn about new solutions, that I upped the hours-per-week to more like 10 for a good several weeks. I learned a lot – and quickly.

- Vendors continued to honor my rules, though that began to trickle off. Every time I was interviewed on the CISO/Security Vendor Relationship Podcast, I referenced that I had rules, but nobody seemed to follow up. The podcasts drove traffic spikes nearly as much as the original posts did.

- I plan to re-publish my rules every few months as a reminder to the vendor community.

- I continue to allow vendors to connect, and actively seek connections with CISOs, CIOs, and security practitioners to keep the vendor ratio to around 30%-40% of my total connections.

- All in all, I'm calling this experiment a success, and plan to continue it indefinitely at the original 2 hours per week.

Other Resources - Podcasts

Podcasts for Tracking Innovators and/or Helping Manage Vendors:

- “The CISO/Security Vendor Relationship Podcast” – I’m a regular guest and contributor
- “Enterprise Security Weekly” – A solid all-around security podcast
- “Business Security Weekly” – Looks at business-specific security news
- “CyberWire Podcast” – Good all-around
- “Business of Security Podcast Series” - Google that exact phrase (I’ve been a guest here too)
- SHAMELESS PLUG:
  - “Defense in Depth” w/ Allan Alford & David Spark (3 episodes release so far!)

Other Resources - Websites

BLOGS:

- https://www.corelan.be
- http://www.irongeek.com

OTHER:

- http://kengilmour.com
- http://www.peerlyst.com
- https://www.iansresearch.com/
- https://www.thomsonreuters.com/en/products-services/technology/top-100.html (and interesting look at the big players' as innovators)

Other Resources

REDDIT:

- /r/netsec, /r/InfoSecNews, /r/security, /r/Information_Security, /r/cybersecurity, /r/Infosec

OTHER:

- OWASP Slack Channel
- Momentum Cyber’s Cybersecurity Almanac – They publish one of the more complete cyberscapes
  - (Also google “cybersecurity market map” and “cybersecurity landscape”)
- http://www.theroundtablenetwork.com. The following password is required to access the “featured vendors” tab: **trn.ciso**.

Suggestions from Attendees –
GDS Security Insight Summit, Dec 2018, Austin, TX

- Consortium Networks – Crowdsourcing of Product Analysis - https://www.consortium.net/
- Threatpost – Good News Site - https://threatpost.com/
- Incubators – Find some near you!
- VC Events – mimic how VC's vet companies – America's Growth Capital in particular has events where you can see how they evaluate startups - http://agcpartners.com/events/category/conferences/

Let’s Have a Discussion: Feedback?

- Do You Have Any Other VAR Strategies?
- Do You Know of Any Good Peer Groups?
- Do You Know of Any Good Curators or Aggregators?
- Have You Tried Direct Vendor Engagement via Some Other Means?
- Any Good Podcasts, Blogs or Websites We Should Know About?

- What Other Techniques Do You Employ To Learn About Innovation?

About The Author

Allan Alford is Chief Information Security Officer (CISO) at Mitel, formerly CISO at Forcepoint and at Polycom. In his CISO roles Alford has managed enterprise security as well as compliance with various frameworks such as GDPR, NIST SP800-171 and ISO 27001.

With more than 30 years of IT and Engineering security experience, Alford has a strong product and cloud security background, having served at Pearson as Product Information Security Officer (PISO), supervising the security of a massive-scale companywide cloud transformation program, and Polycom where Alford built and managed the product security program, integrating it fully into the business.

Alford is currently pursuing a master's degree in Information Systems and Security from Our Lady of the Lake University and received a bachelor's degree with a focus on leadership from DePaul University. Alford holds a CISM certification.

One CISO’s Opinion…

Thank You.

Allan Alford, CISO

www.allanalford.com

LinkedIn – Allan Alford

Twitter - @AllanAlfordinTX