One CISO's Opinion...

Overcoming CISO Communication Issues

And The Issue of Cybersecurity Excuses

Allan Alford, CISO

February, 2020

Version 1.0

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.

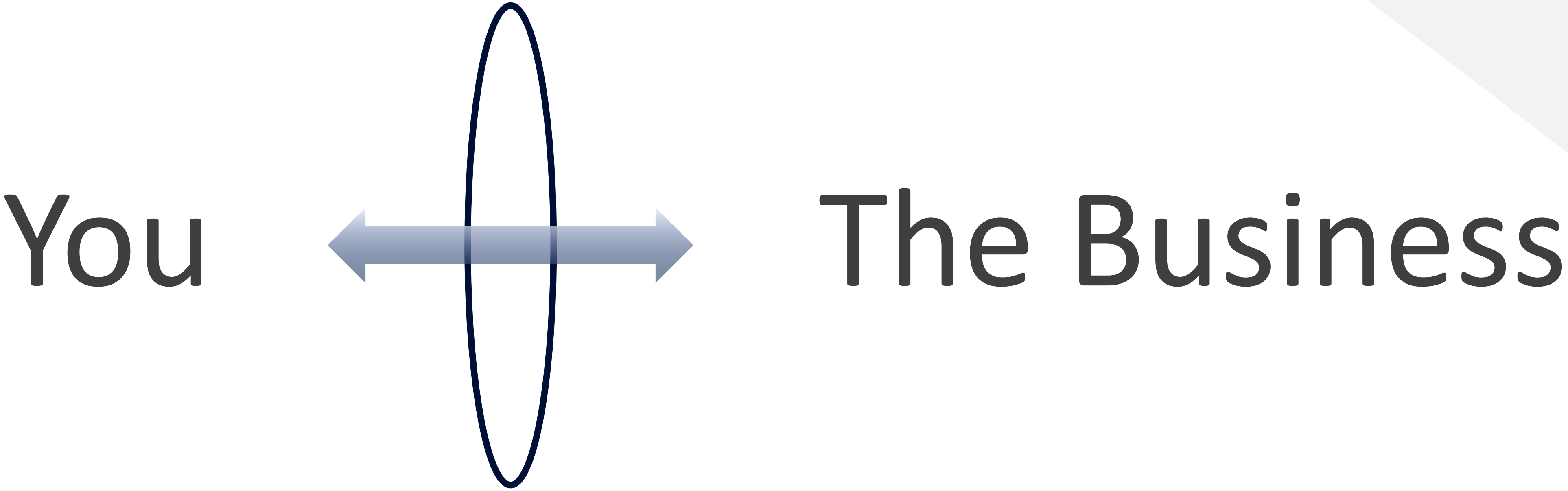
Most Common Cybersecurity Excuses

- *“You are slowing down the business!”*
- *“You are interfering with productivity!”*
- *“We do not need this much security!”*
- *“You own this risk, not me!”*

Other People and Departments

Sound Familiar? We all battle this kind of pushback.

The Answer Is In Your Lens on the Situation



You

The Business

“Secure Them Where They Live!”

Commit time (1:1 meetings, interviews, team meetings) to learning their perspectives, processes and tools so you can create:

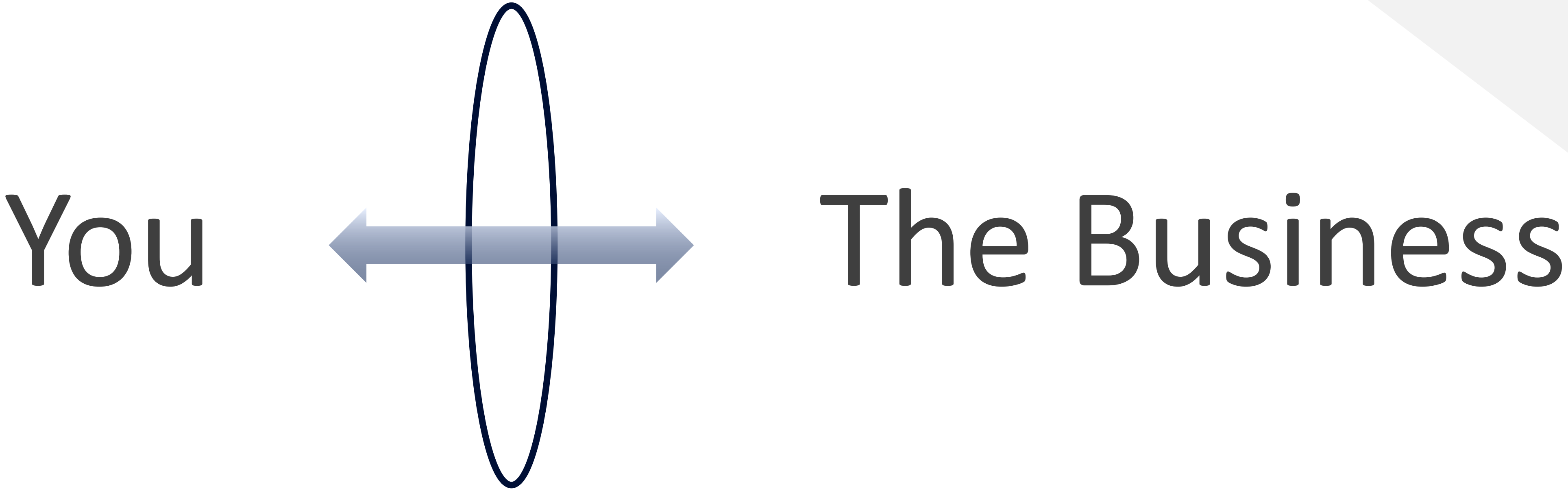
viable, usable, adoptable security that flows with existing business processes…

Business Streamlining - Examples

- Marketing insist on using Macs? Maybe you're rolling out Jamf…
- Executive notebook got stolen? Start with that guy for Bitlocker
- Engineering admins have headaches logging into 10 disparate systems? PAM or a Password Vault!
- Remote users hate VPN client? Perfect time for your proxy solution!

"Unusable Security Gets Bypassed!"

Now That You’re Looking Through the Proper Lens…



There Is An Even Better Perspective!

You **ARE** The Business

“The business” is just many disparate priorities, missions and teams coming together for common cause. Sacrifice and compromise are required in this process.

That IS the business! The Infosec voice is NOT outside this process!

You Are The Business

- Enter every high-level business conversation and meeting you can
- When you are losing, be magnanimous, “It’s in the better interests of the business…”
- Speak in business terms first, and risk terms second. Tech is last!

But What About the Biggest Excuse of Them All?

> *“I have all the accountability for security risks, but none of the authority. I should not even own the risks! I don’t have a voice!"*
>
> Many CISOs

This can be dealt with. The Infosec voice can be more effective!

If You Cannot Insert Security Into the Business…

#1 - Insert the Business Into Security!

- Form a security council with members from all over the business.
- Target the VP level to start. (Don’t worry if you don’t get great attendance at first).

Instead of Security Competing With Other Departments

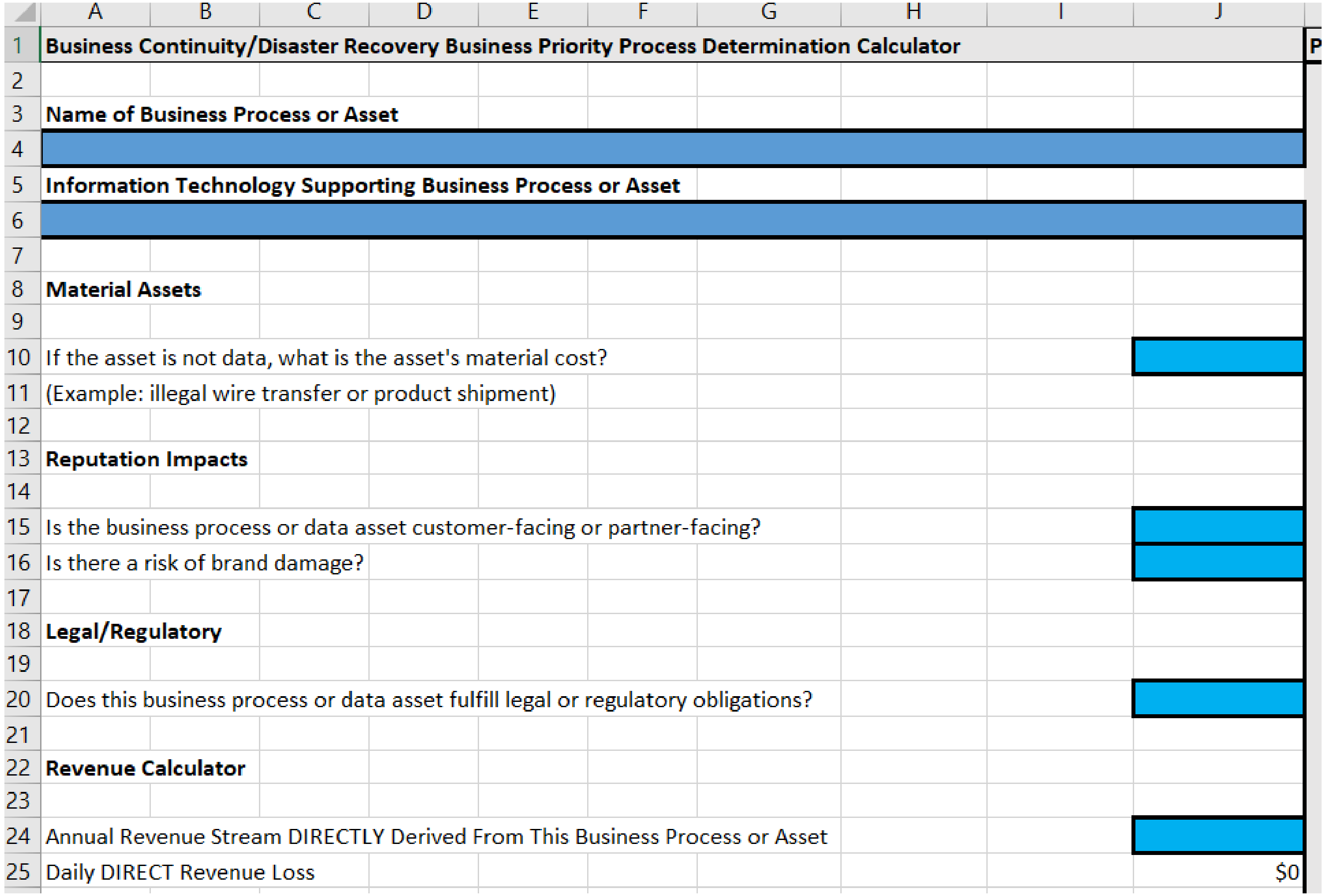
#2a – Have Other Departments Compete for Security!

- Those who attend the council will participate in your Business Impact Analysis Lite exercise (link below). This tool scores business processes and ranks them for programs like Business Continuity, Disaster Recovery, new protections rollouts, etc.

- Publish the results to all departments, especially those who do not participate originally in the council.

- State the priorities as crafted by the council. Make it clear that only those who attend get considered and ranked.

Business Impact Analysis Lite



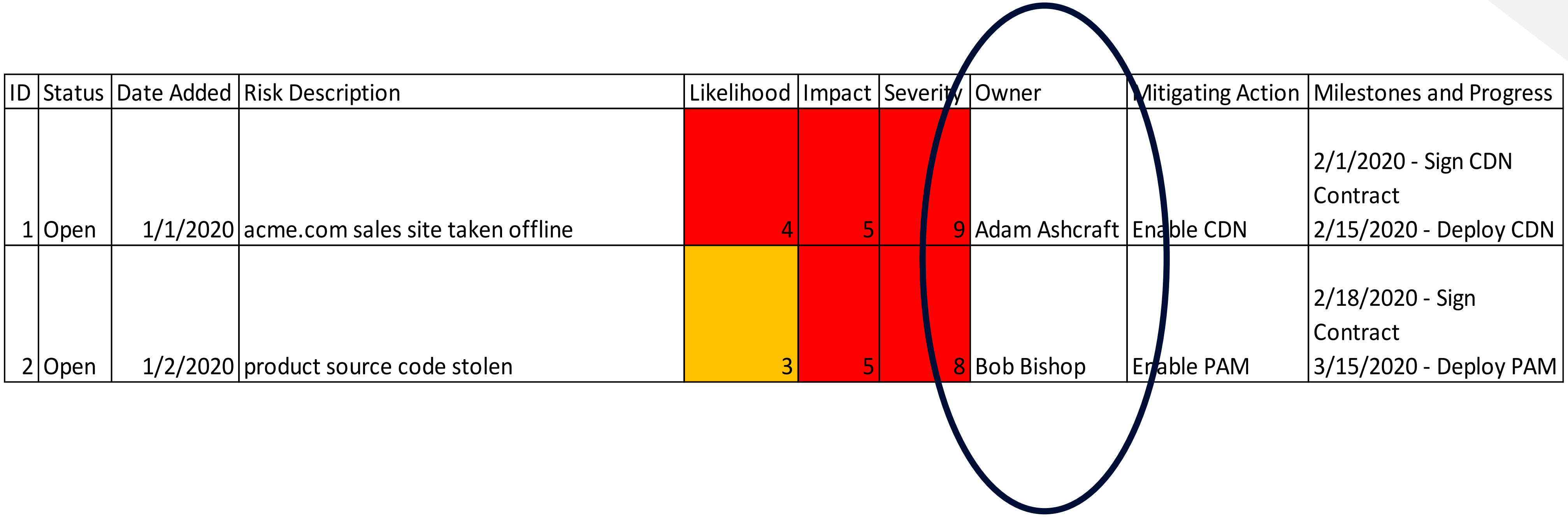
	A	B	C	D	E	F	G	H	I	J	
1	**Business Continuity/Disaster Recovery Business Priority Process Determination Calculator**										**P**
2											
3	**Name of Business Process or Asset**										
4											
5	**Information Technology Supporting Business Process or Asset**										
6											
7											
8	**Material Assets**										
9											
10	If the asset is not data, what is the asset's material cost?										
11	(Example: illegal wire transfer or product shipment)										
12											
13	**Reputation Impacts**										
14											
15	Is the business process or data asset customer-facing or partner-facing?										
16	Is there a risk of brand damage?										
17											
18	**Legal/Regulatory**										
19											
20	Does this business process or data asset fulfill legal or regulatory obligations?										
21											
22	**Revenue Calculator**										
23											
24	Annual Revenue Stream DIRECTLY Derived From This Business Process or Asset										
25	Daily DIRECT Revenue Loss									$0	

Instead of Security Competing With Other Departments

#2b – Have Other Departments Compete for Security!

- You can also have the council jointly create a risk register – what business risks most need mitigation!
- Use the same physics you used with business process prioritization. Show them the cost of not participating. The highest risks get the most security attention.
- You cannot overcommunicate. Arrange 1:1 meetings with the departments who did not attend or participate.

Risk Register

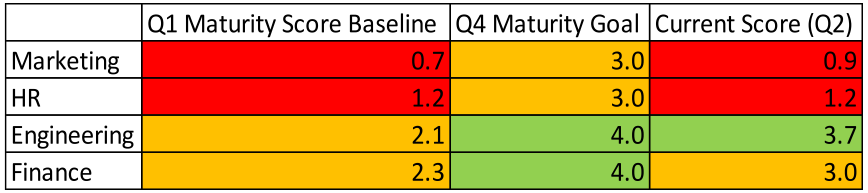


ID	Status	Date Added	Risk Description	Likelihood	Impact	Severity	Owner	Mitigating Action	Milestones and Progress
1	Open	1/1/2020	acme.com sales site taken offline	4	5	9	Adam Ashcraft	Enable CDN	2/1/2020 - Sign CDN Contract 2/15/2020 - Deploy CDN
2	Open	1/2/2020	product source code stolen	3	5	8	Bob Bishop	Enable PAM	2/18/2020 - Sign Contract 3/15/2020 - Deploy PAM

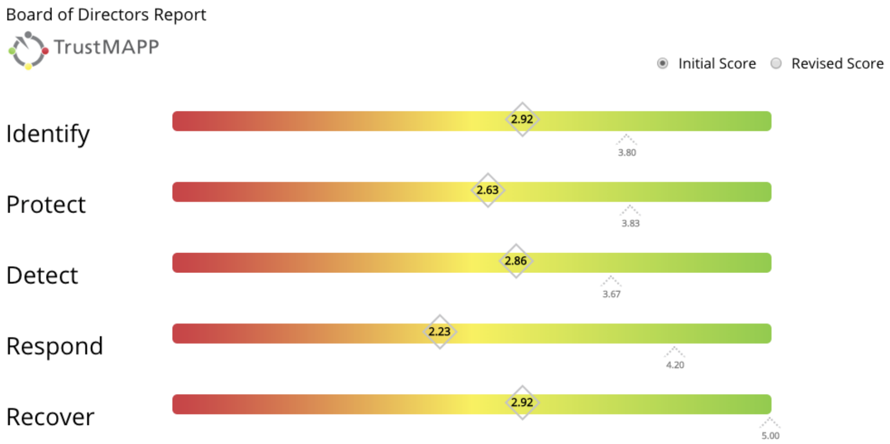
Not You!

Make Security A Competitive Sport

#3 – Wall of Fame and Hall of Shame



	Q1 Maturity Score Baseline	Q4 Maturity Goal	Current Score (Q2)
Marketing	0.7	3.0	0.9
HR	1.2	3.0	1.2
Engineering	2.1	4.0	3.7
Finance	2.3	4.0	3.0



- Conduct a series of rapid maturity audits vs. a popular framework like NIST CSF or even CIS CSC. Conduct one audit **per business unit or department**.
- When you publish your report to the C-suite and/or the board, include the maturity assessment results (along with your risk register and BC/DR process prioritization if they want that much detail). Over time you track progress against these goals and assessments.
- DISCLAIMER: I’m on the Executive Advisory Board of TrustMAPP. Feel free to use other tools.

If You Are Worried About Repercussions

“Bad News Is Always Better than Unpleasant Surprises!”

This is something you say to them, but also a warning to you – don’t put anyone on the HoF/WoF without a prior conversation…

Conclusion

- The business will always view security as an obstacle to be overcome until you figure out ways to use it to not interfere – and ideally streamline – their productivity.
  - Popular programs include SSO, passwordless, PAM, Proxy instead of VPN, etc.
  - Pilot all projects with “friendlies” – even over expense concerns – if you can
- You ARE the business!
  - Couch the conversation in business and partnership terms and ALWAYS speak to business risk and maturity
  - Fake it until you make it!
- The security game is won when all players compete to be more secure

A Shameless Plug

Please listen to the *Defense in Depth* podcast – co-hosted by me and David Spark, producer of the CISO Series.

We discuss security issues like this each week and go into them… "In depth!"

Available nearly everywhere podcasts are available…

Join Me on LinkedIn!

I have a network of 21k people, almost exclusively information security practitioners and vendors, CISOs, CIOs and CTOs.

I post original content on a near-weekly basis, in the form of questions that promote dialogue.

I always end up learning something, and you might learn something too…

Resources

- The BIA Lite Calculator is Available At:
  - https://allanlaford.com/resources

- This Presentation and Others are Available At:
  - https://allanalford.com/articles-%26-interviews

About The Author

Allan Alford is Delivery CISO (Chief Information Security Officer) at NTT Data Services, governing all security concerns for delivered IT and business services.

With 20+ years in IT and Engineering, Alford formerly served as CISO at Mitel, Forcepoint and Polycom. Alford has managed security strategy and led compliance with various frameworks and regulatory requirements such as NIST CSF, GDPR, ISO 27001, HIPAA, PCI DSS, DFARS and others.

Alford secured Mitel’s enterprise and UCaaS environments and served at Pearson as Product Information Security Officer, where he created the security practice for a company-wide cloud transformation program. Alford also built and led the product security program at Polycom, integrating it fully into the product delivery process.

Alford has a master's degree in Information Systems & Security from Our Lady of the Lake University and received a bachelor's degree in Liberal Arts with a focus on leadership from DePaul University. He also holds a CISM certification.

One CISO's Opinion...

Thank You.

Allan Alford, CISO

www.allanalford.com

LinkedIn – Allan Alford

Twitter - @AllanAlfordinTX