Is The Security Industry Solving Our Problems?

And What Can We Do Without It?

Allan Alford, CISO

May, 2019

Version 1.6

NOTICE

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

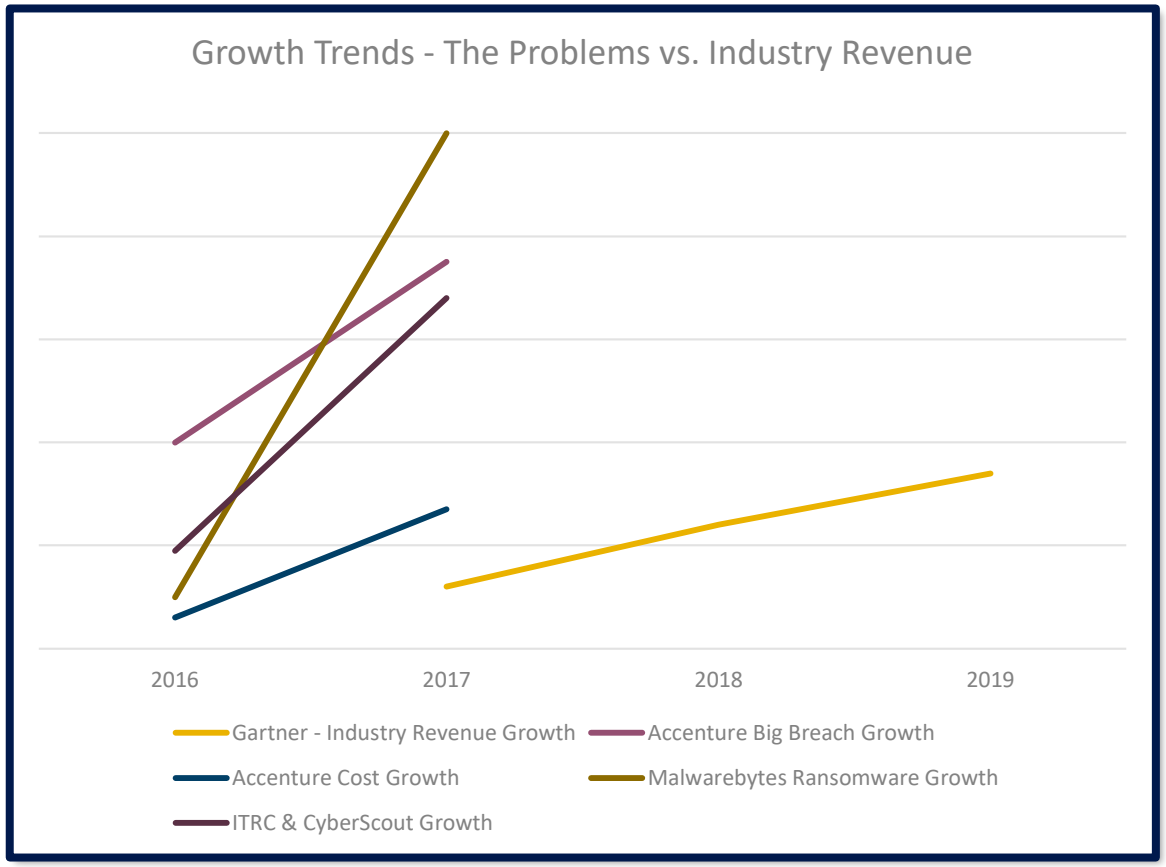
As such, the author's opinions are his own and do not necessarily reflect the opinions of any employer, academic institution or professional organization with which the author is or has been affiliated.

Is The Security Industry Solving Our Problems?

“There is an 80.9% correlation between the number of breaches and revenue growth for security companies".

Andrew Nowinski, senior research analyst at Piper Jaffray - August, 2016

We Are Not Keeping Up With The Problem – Despite Increasing Spend



In August, 2018, Gartner stated that the security industry was worth $114b, a 12.4% increase from 2017. 2019 was predicted to be at $124b, another 8.7% increase in growth.

In 2017, Ponemon/Accenture noted over 130 large-scale, targeted breaches, with a growth rate year-over-year of 27.4%. Average annualized cost of an incident was $11.7m, an increase of 22.7%.

In 2017, Malwarebytes reported that ransomware had grown by 90% from 2016.

The Identity Theft Resource Center/CyberScout reported a 44.7% increase year-over-year in breaches from 2016 to 2017.

But What About All That Innovation? Disruption? The Revolution?

Innovation is in our DNA

Because of the revolutionary real-time, cloud-based, massively scalable…

Reinforcing the Revolution

…driven by innovation…

…the security revolution in tools & training…

Security gurus share the secrets of emerging markets that are being shaped by disruption…

Is this the start of an EDR revolution?

the catalyst for the cybersecurity revolution

…disrupting the massive traditional antivirus industry…

…at the forefront of cloud security innovation…

Don't start the Blockchain revolution without making security a top priority

*** All Phrases Captured Verbatim from Vendor Websites and Trade Articles**

The Bar Is Low for a Cybersecurity Startup

- True Disruption Is No Longer Required
- Solving New Problems or Old Problems in Truly New Ways Is No Longer Really Required
- **Solve The Same Old Problems With Any of These & YOU CAN GET RICH!**

  - Slightly Fewer False Positives
  - Slightly Less Cost
  - Slightly More Speed
  - Slightly Less Overhead
  - Less Functionality but for Correspondingly Less Cost
  - Same Statistical Results but via Flashy New Means

(To Be Fair to the Industry)

- True Disruption Does Happen Every Now and Again:
  - UEBA fixed SIEM…
  - EDR beats traditional AV hands-down…
  - DLP and CASB didn't use to exist…
  - (And the big guys can innovate sometimes without startups)

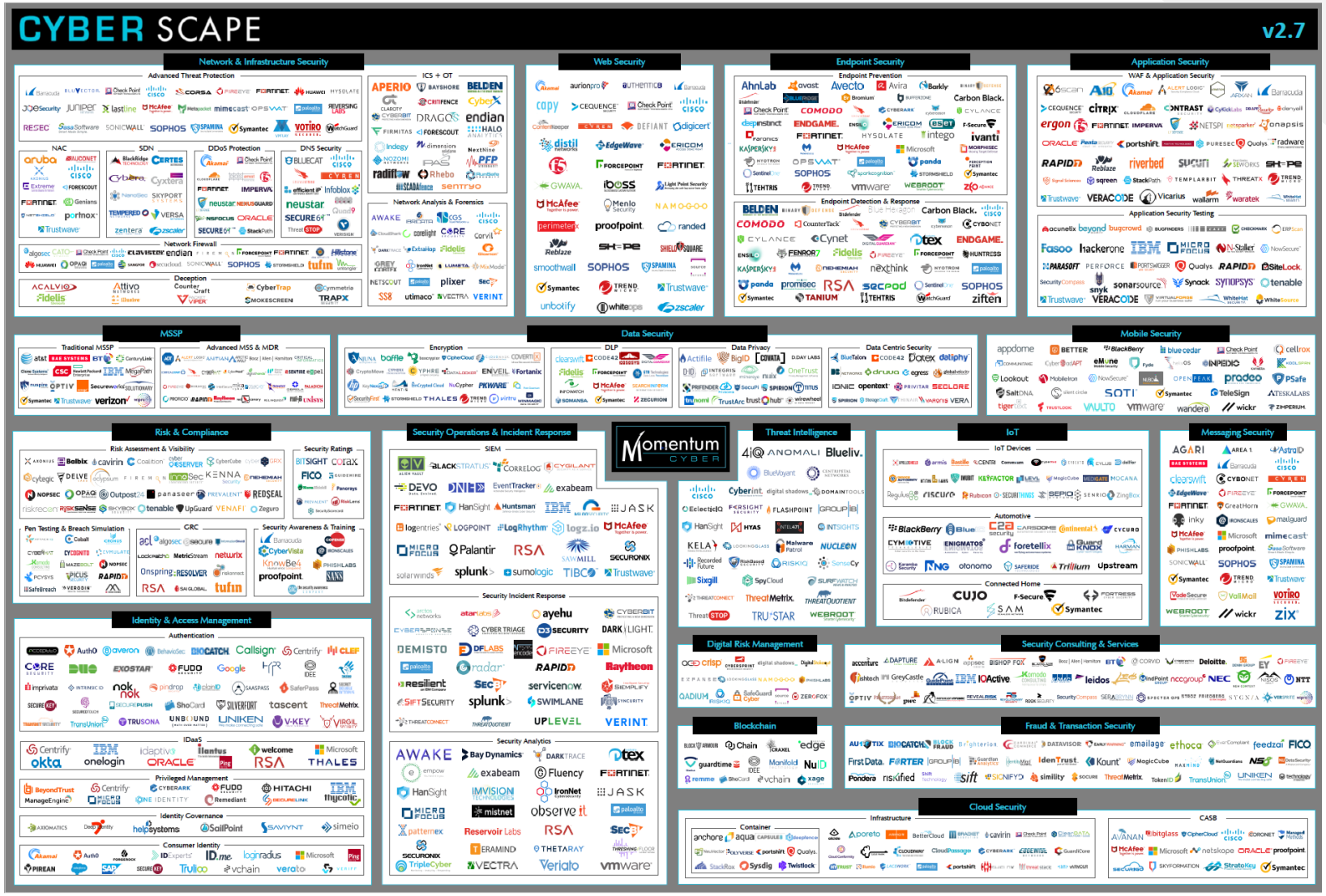
But the industry does not actually *need* real innovation to survive and even thrive.

But Why Is The Bar So Low? The Industry's Business Model Is Broken…

- Most cybersecurity startups (who don't fail) exit by way of acquisition rather than IPO: ~90% according to one anonymous venture capitalist source.
- *Startups do not necessarily have to solve any of the actual problems that you and I actually have as customers…*
- **The truth is that you only have to be good enough to make the established players *just nervous enough* to want to buy you!**
- The game is no longer about solving problems – it's about being just enough of a differentiator to be bothered with from an investment perspective…

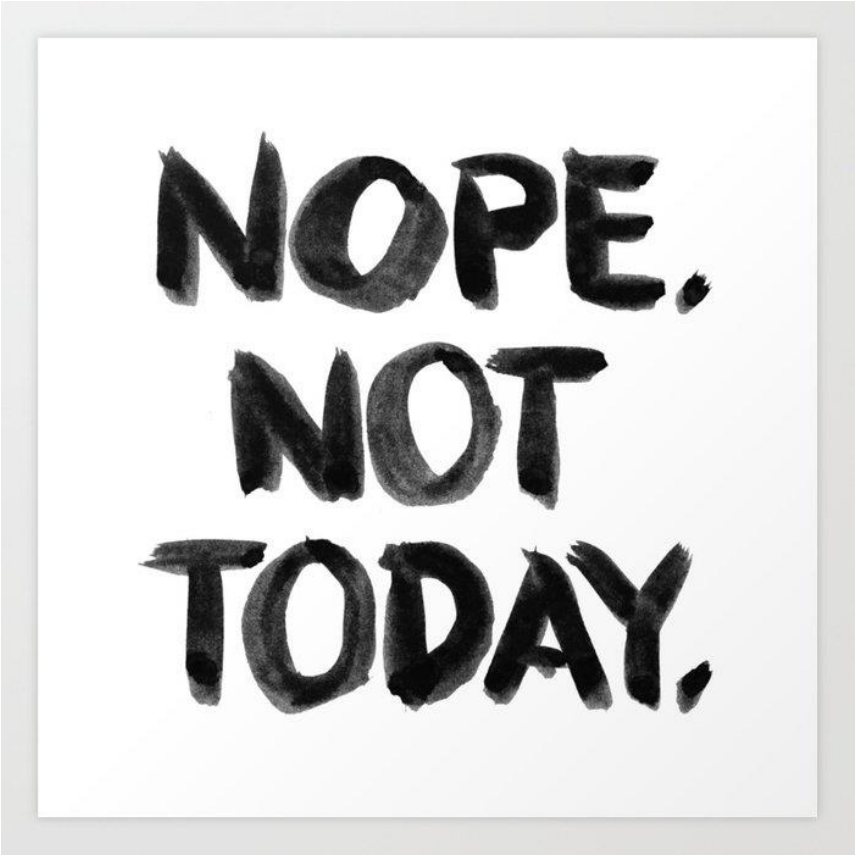
THIS IS WHY WE SEE SUCH MARKET SATUARTION IN OUR INDUSTRY

And There is a LOT of Market Saturation…



Also note that all of these “market landscape” maps are incomplete…

Do We Need The Industry As Badly As It Says We Do?



For One Thing, Your Organization Is Unique. Does Tool X *Really* Help You?
Are Your Security Concerns The Same As Mine? As His? As Hers?

What Can We Do About All This?

Don’t Get Suckered In!

You have a job, and you already know how to do it.

What follows is just a friendly reminder…

High-Yield Projects You Can Lead Without a Cutting-Edge Security Tech Stack

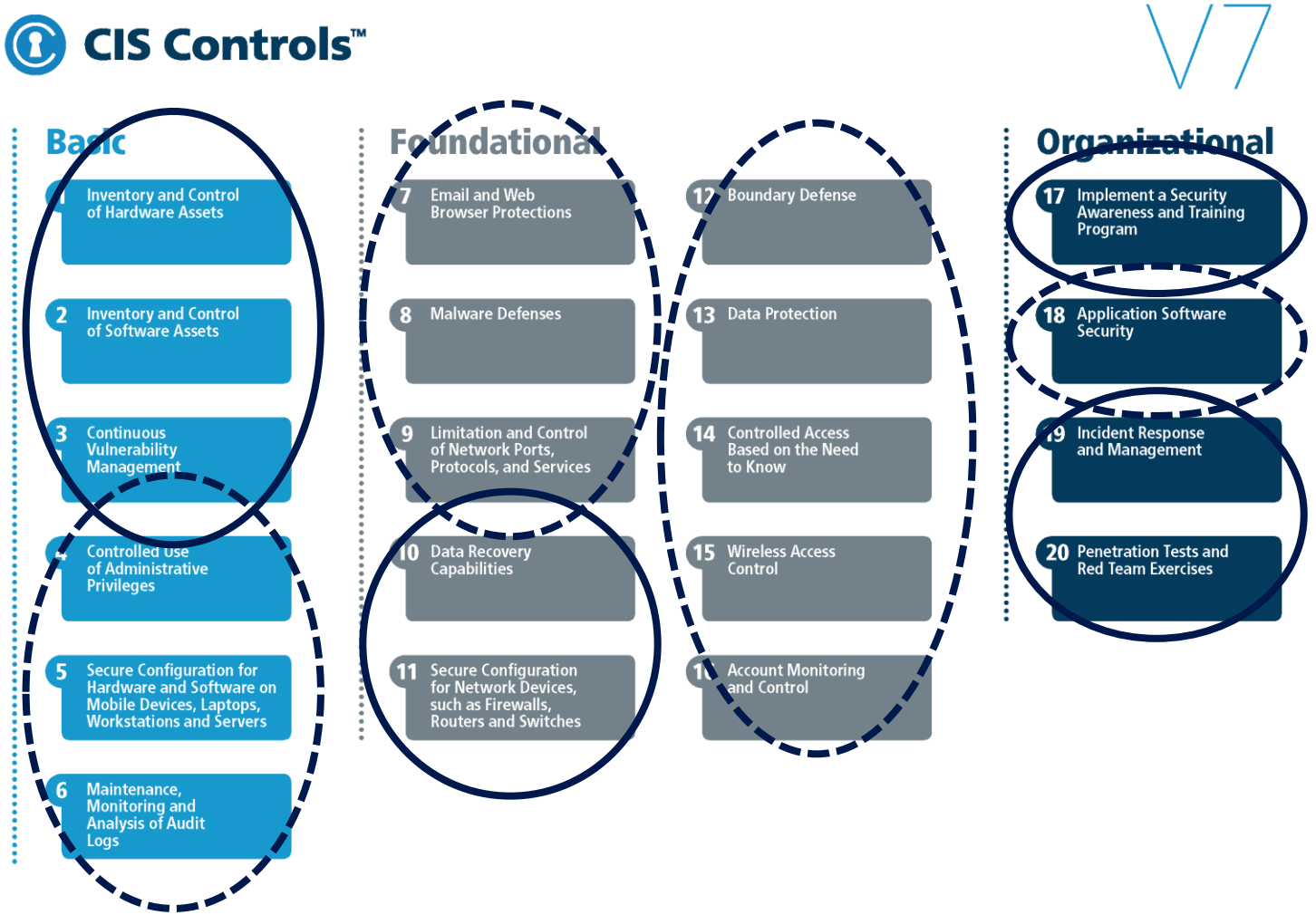
We can succeed in our mission if we get back to the basics.

What follows is a quick analysis of various security control frameworks.

Some key first steps, independent of any one framework, are also outlined.

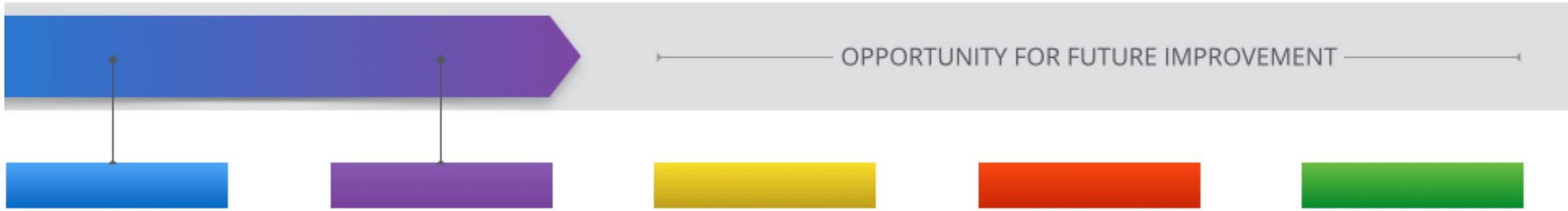
You Can Start with an Accessible Controls Set – CIS CSC 20

How much of this can be performed without consulting that market landscape map?



Growth Vector: You Can Even Evolve from CSC to NIST CSF

Your Turn: How much of this can be performed without a flashy security tech stack?



IDENTIFY

- Asset management
- Business environment
- Governance
- Risk assessment
- Risk management strategy

PROTECT

- Access control
- Awareness and training
- Data security
- Information protection and procedures
- Maintenance
- Protective technology

DETECT

- Anomalies and events
- Security continuous monitoring
- Detection process

RESPOND

- Response planning
- Communications
- Analysis
- Mitigation
- Improvements

RECOVER

- Recover planning
- Improvements
- Communications

Or Use CSC 20 to Fulfill CSF and Chart a Growth Plan to ISO 27001!

Category	Subcategory	Year One Plan - CIS CSCv7 Top 6 - Basic Controls	Year Two Plan - CIS CSCv7 Remaining 14 - Foun
Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	ID.AM-1: Physical devices and systems within the organization are inventoried	CIS CSC 1	
	ID.AM-2: Software platforms and applications within the organization are inventoried	CIS CSC 2	
	ID.AM-3: Organizational communication and data flows are mapped	CIS CSC 2	CIS CSC 12
	ID.AM-4: External information systems are catalogued	CIS CSC 1	CIS CSC 12
	ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	CIS CSC 2, 3	CIS CSC 13, 14
	ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	CIS CSC 4	CIS CSC 16, 17,

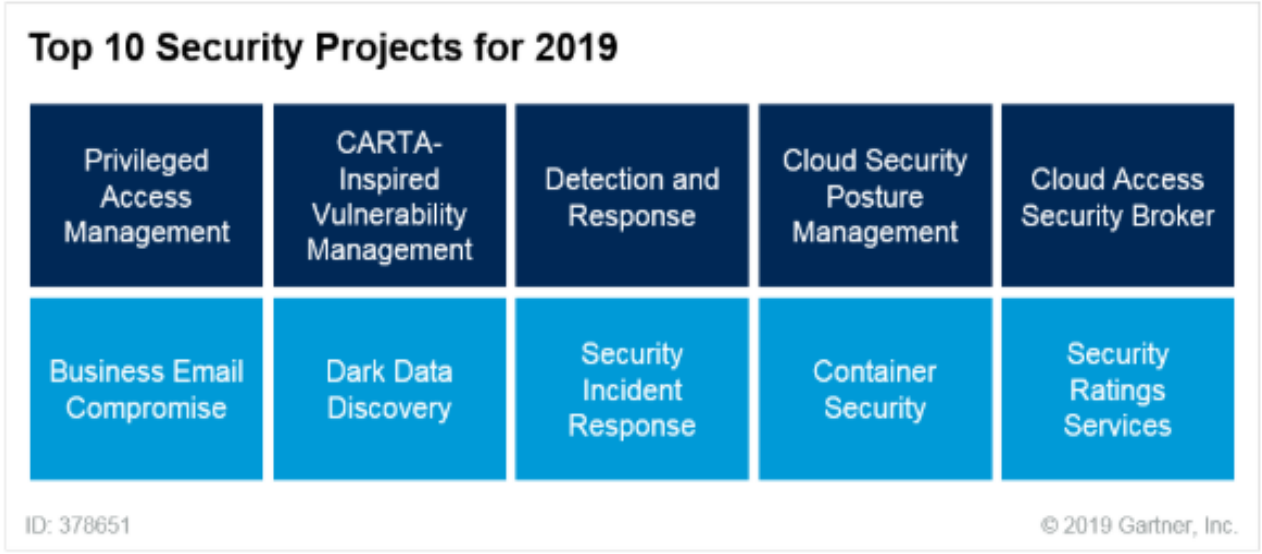
A 4-Year Plan Fulfilling NIST CSF via CIS CSC 20 evolving into ISO 27001 is Available on my Website

Side Note: Gartner Is Not Always Right

Gartner falls victim to the industry hype as much as anyone – if not more!

Shouldn’t Vulnerability Management and Security Incident Response be ahead of PAM?

Note: Again, many of the projects here can be implemented, at least partially, without the newest tech stack.



Source: Gartner (February 2019)

Where Does The CISO Thrive?

At the intersection of Risk and Business

Remember “Risk-Based Security”? It Is Still the Main Driver!

If you know your organization, and you know its core mission, and you measure your organization’s risks with that mission in mind…

The process of addressing those risks can be your focus without the latest in security technology.

You DON’T need a comprehensive risk management program to begin effectively managing key risks…

Spend Wisely & Manage Your Most Critical Risks

- Especially as an experienced infosec veteran, it is very easy to start implementing all the tools that you're used to having…
- But wait! Before you deploy DLP, are you sure that data exfiltration is as high a risk as, say, a data center full of unpatched servers?
- Use your GRC tool to measure the risks you find, and buy tools based on risk.
- Don't have a good GRC tool? A good FREE commercial option exists:

Disclaimer: An Austin colleague owns SimpleRisk. See the open-source *Eramba* too.

Asset Inventory – It's Boring, But It's Vital!

Steps #1 and #2 of the CSC Top 20 are asset inventory – hardware and software respectively.

There is a reason for this: You cannot secure what you don't know you have.

Asset inventory is the most important step in cybersecurity, and can be performed without any of the newest commercial infosec tools…

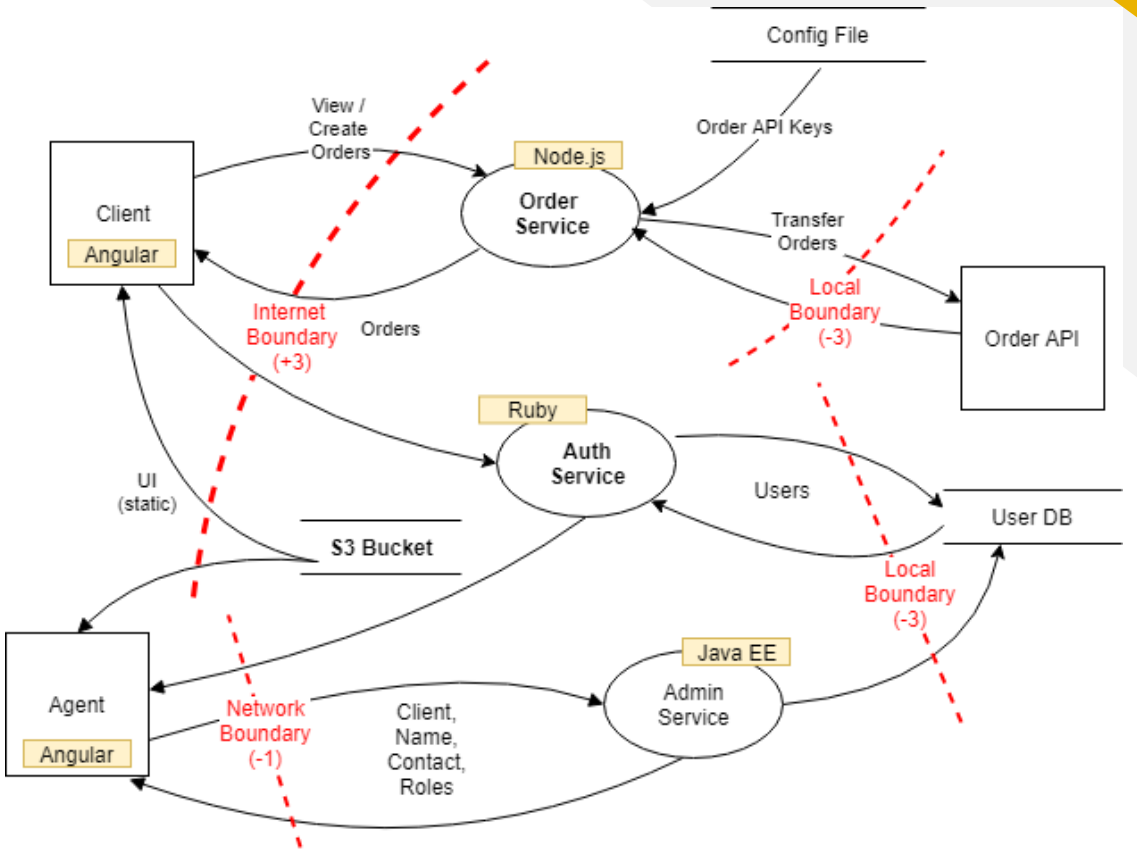
Again, start with what you know now, then grow!

What About Threat Modeling?

As important as asset management is, a threat modeling approach is equally valuable.

If you know your attack surface, and know the threats you face, you can begin to take steps towards securing your organization.

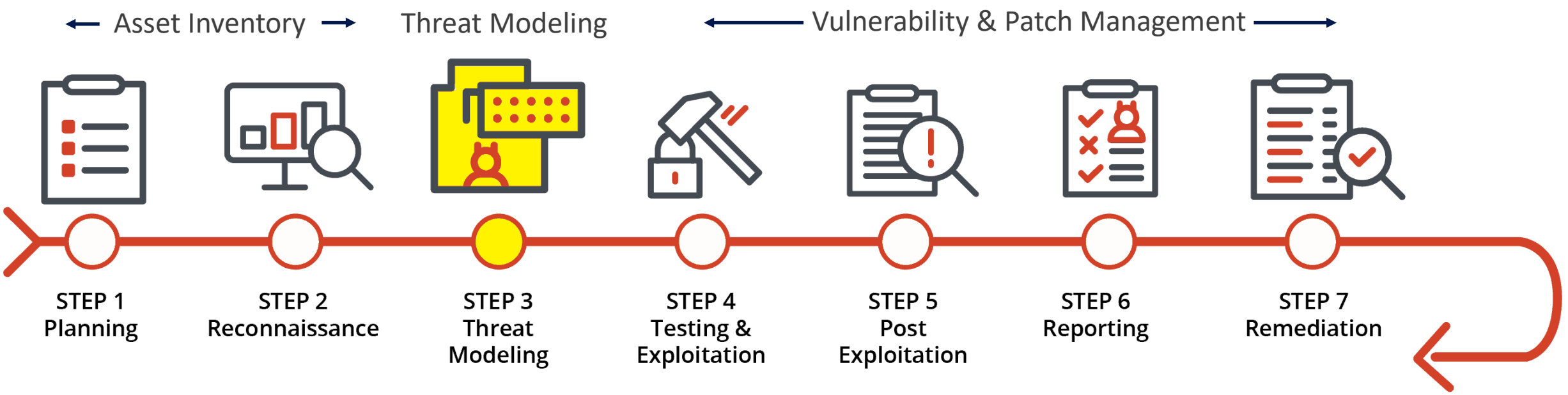
Again: You don't need a flashy tech stack, and you can start with what you know!



Vulnerability Management (and Patch Management)

This trifecta of asset inventory, threat modeling, and vulnerability (and patch) management feeds risk management and serves a key foundation in your security program.

Start with the systems most obviously related to your organization's central mission!



Crawl, Walk, Run

As you manage the risks most obviously related to your organization's core purpose, evolve the trifecta cycle over time.

Use that trifecta in the context of risk management while digging deeper and more broadly into your organization.

(Note: You are still operating without that saturated market!)

Don’t Forget Open Source and Free Tools!

GRC (SimpleRisk, Eramba)… pen testing (various) … monitoring, detection and response (Security Onion and Elkstack)… password managers (various)… two-factor authentication (twofactorauth.org)… cloud monitoring (Security Monkey)… WAF (Modsecurity)… risk measurement and prioritization (OpenFAIR)… OS monitoring (osquery & Sysmon)… PAM (Secret Server Free)… Antivirus (ClamAV), training (cybrary.it), Etc. Etc.

And Don’t Forget Your People!

People are the best possible alternative to a tech stack.

Incentivize your employees while investing in them!

Training is a great benefit both to the employee and to your organization.

Conclusion

- With all the hype the industry puts forth, it's hard to remember what really matters. Don't believe the hype, and don't forget what matters.
- A risk-based approach, aligned with your organization's mission, goes a long way towards achieving the right security goals.
- Don't wait for perfection! Dive in and get started!
- The most important work we do does not necessarily require a paid-for tech stack. Asset inventory, thread modeling, vulnerability & patch management are more important than anything cutting-edge security tools can provide.
- Free and open source tools exist that supplement our needs when the work does in fact require tools – but much of the work does not even require security-specific tools in the first place.

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 (including RSS feed!)

Join Me on LinkedIn!

I have a network of 18k 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…

References

Research

- https://www.crn.com/news/security/300081720/study-data-breach-numbers-continue-to-rise-creating-growing-security-opportunity-for-solution-providers.htm
- https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019
- https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf
- https://press.malwarebytes.com/2018/01/25/malwarebytes-annual-state-malware-report-reveals-ransomware-detections-increased-90-percent/
- https://www.idtheftcenter.org/2017-data-breaches/

References Pt. 2

Tools & Materials (Partial List)

- https://www.simplerisk.com/download
- https://allanalford.com/4-year-map
- https://www.osehra.org/sites/default/files/csd-host-open-soruce-cybersecurity-catalog.pdf
- https://osintframework.com/
- https://github.com/sbilly/awesome-security
- https://github.com/meirwah/awesome-incident-response
- https://publications.opengroup.org/i181
- https://www.eramba.org/resources/download/

References Pt. 3

Training

- http://www.dcita.edu/
- https://fedvte.usalearning.gov/
- https://cybrary.it
- https://niccs.us-cert.gov/training/
- https://bkimminich.gitbooks.io/pwning-owasp-juice-shop/content/

Shameless Plugs

- https://cisoseries.com/subscribe-podcast/
- https://www.linkedin.com/in/allanalford

About The Author

Allan Alford has served as Chief Information Security Officer (CISO) at Mitel, Forcepoint and Polycom. In his CISO roles Alford has managed enterprise, cloud and product security strategy and overseen compliance with various frameworks and regulatory requirements such as DFARS, GDPR, ISO 27001 and others.

With more than 20 years of IT and Engineering security management experience, he has a strong product and cloud security background as well. Alford oversaw security for Mitel's UCaaS and UC cloud offerings and served at Pearson as Product Information Security Officer, where he created the security practice for a massive-scale, companywide cloud transformation program. Alford also built and led the product security program at Polycom, integrating it fully into the product delivery process by aligning security with the business.

He is co-host of Defense in Depth – a weekly podcast that focuses each episode on a specific, popular topic from the world of information security. Alford also works to give back to the security community by authoring articles, contributing original content on various social media sites, and presenting at conferences and summits.

A perpetual learner, Alford is pursuing 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. Alford holds a CISM certification.

Thank You.

Allan Alford, CISO

www.allanalford.com

LinkedIn – Allan Alford

Twitter - @AllanAlfordinTX