September 2019

Make Risk Management Real

Bruce Potter – CISO Expel

bruce.potter@expel.io

Don’t believe anything I say

- Fancy term – autodidact
- Real-life term – College dropout

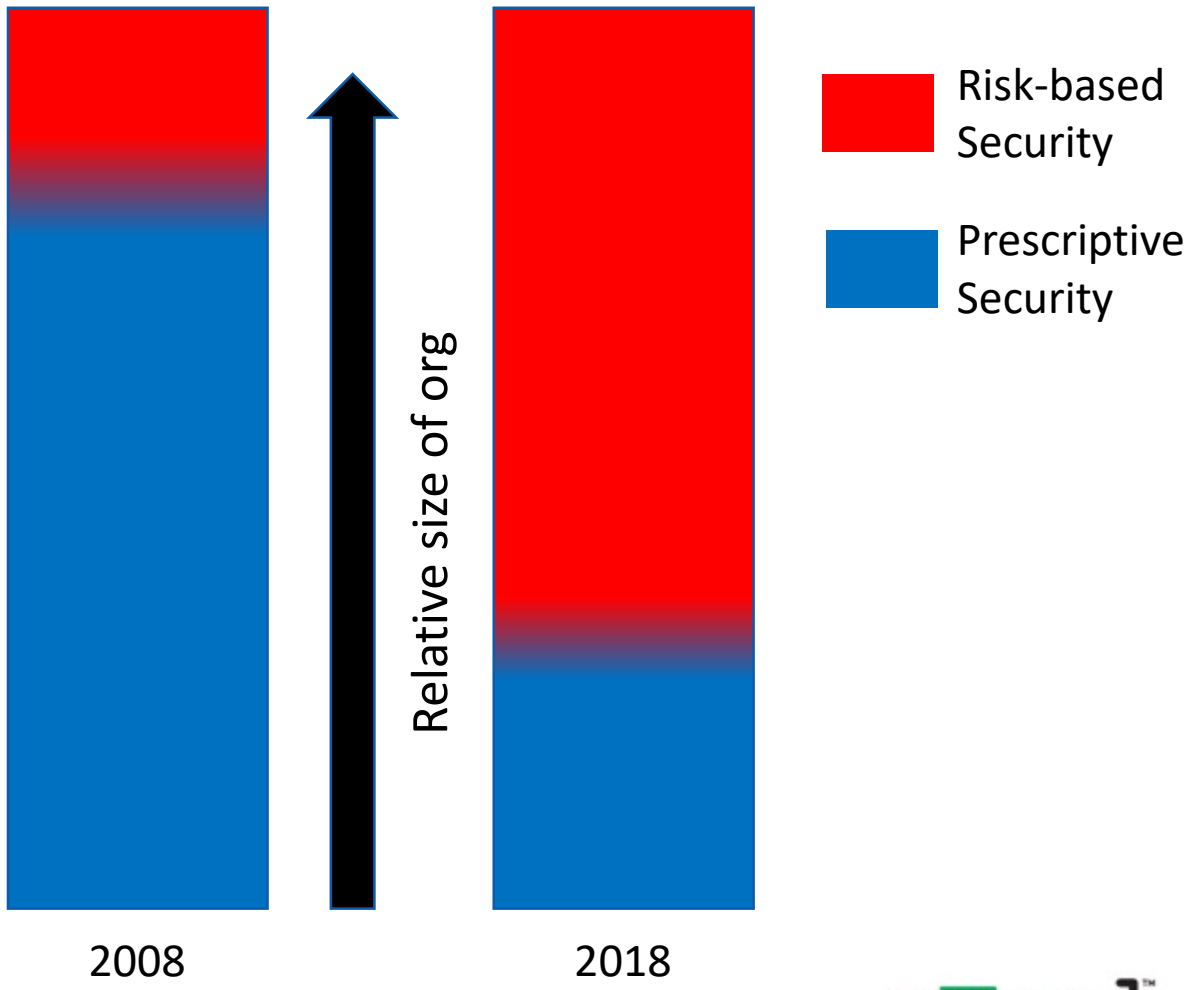
- CISO of Expel, an transparent MSSP based in Herndon, VA
- Founder – The Shmoo Group, help run ShmooCon

Risk is everywhere!

- We had to work hard for people to understand this in 2000
- In 2019, people are FREAKING OUT MAN and perceive risk even in places there is no risk

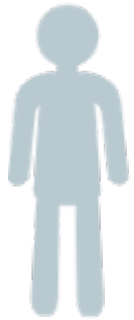
In 2019, risk management is everywhere

- Prescriptive security has limits, and those limits keep going down market
- Cyber risk used to be the domain of big orgs
- Now, smaller and smaller orgs (with fewer resources) are putting together cyber risk programs.



But how?

- Things we assume everyone knows how to:
  - perform risk assessments
  - make a threat models
  - determine their “risk appetite”
  - building a cyber risk program
  - use the CSF
  - create an incident response program
  - build 24/7 monitoring
  - perform an incident response table top exercise

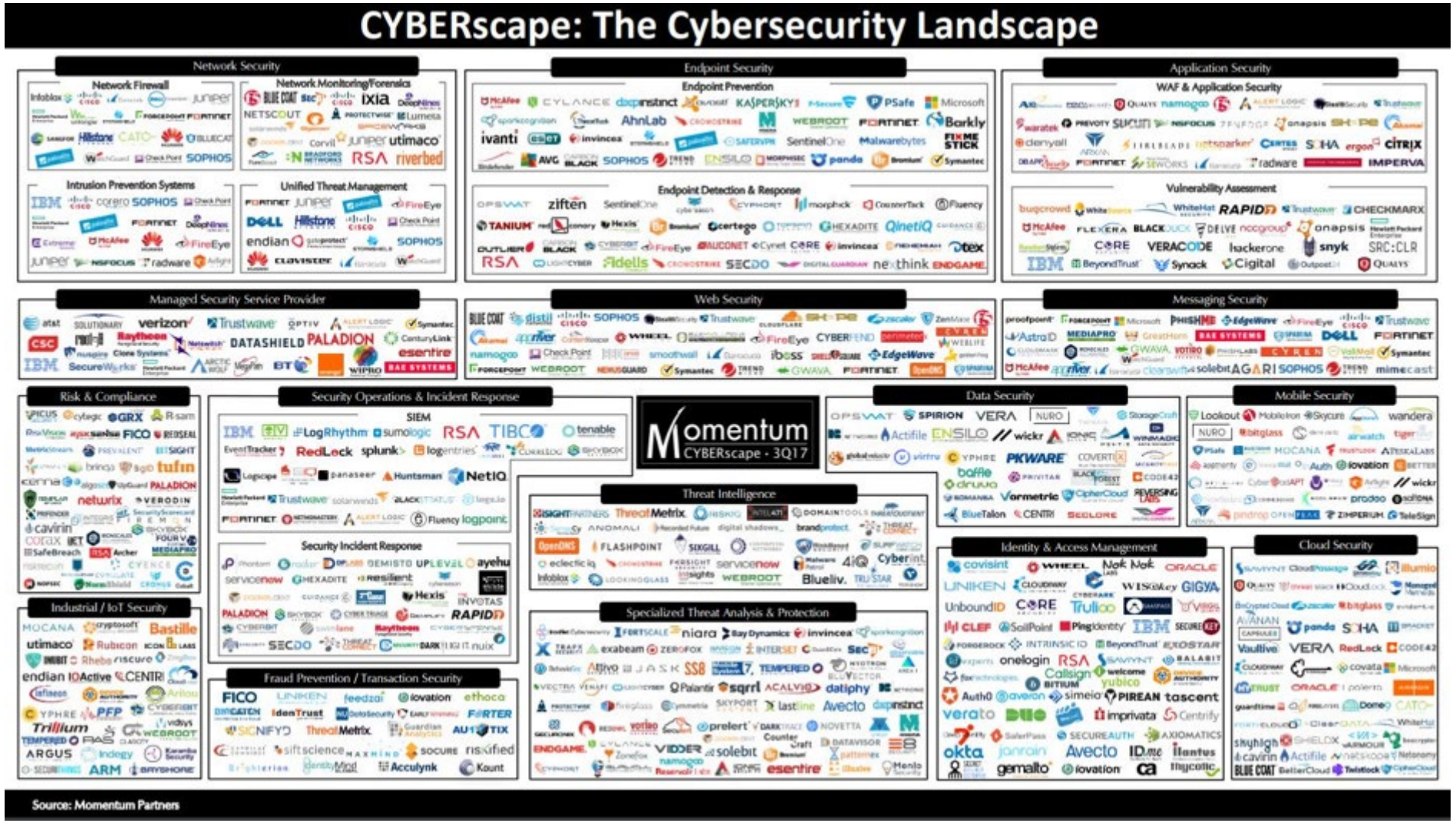


In reality…

- It is not trivial to know how to:
  - perform risk assessments
  - make a threat models
  - determine their ”risk appetite”
  - building a cyber risk program
  - use the CSF
  - create an incident response program
  - build 24/7 monitoring
  - perform an incident response table top exercise
- You are not alone if you’re trying to learn how to do these things
- This conference is great for learning what others are doing

The HOW is super important

What's the biggest risk to any cybersecurity program?


CYBERscape: The Cybersecurity Landscape
Network Security
Network Firewall
Network Monitoring/Forensics
Intrusion Prevention Systems
Unified Threat Management
Endpoint Security
Endpoint Prevention
Endpoint Detection & Response
Application Security
WAF & Application Security
Vulnerability Assessment
Managed Security Service Provider
Web Security
Messaging Security
Risk & Compliance
Security Operations & Incident Response
SIEM
Security Incident Response
Momentum
CYBERscape - 3Q17
Data Security
Mobile Security
Threat Intelligence
Specialized Threat Analysis & Protection
Identity & Access Management
Cloud Security
Industrial / IoT Security
Fraud Prevention / Transaction Security
Source: Momentum Partners

expel

An Example:

What's the first CIS control?

Inventory and Control of Hardware Assets

CIS Controls™ • CIS Control 1 *This is a basic Control*

Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.

Inventory and Control of Hardware Assets

CIS Controls™ • CIS Control 1

This is a basic Control

Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.

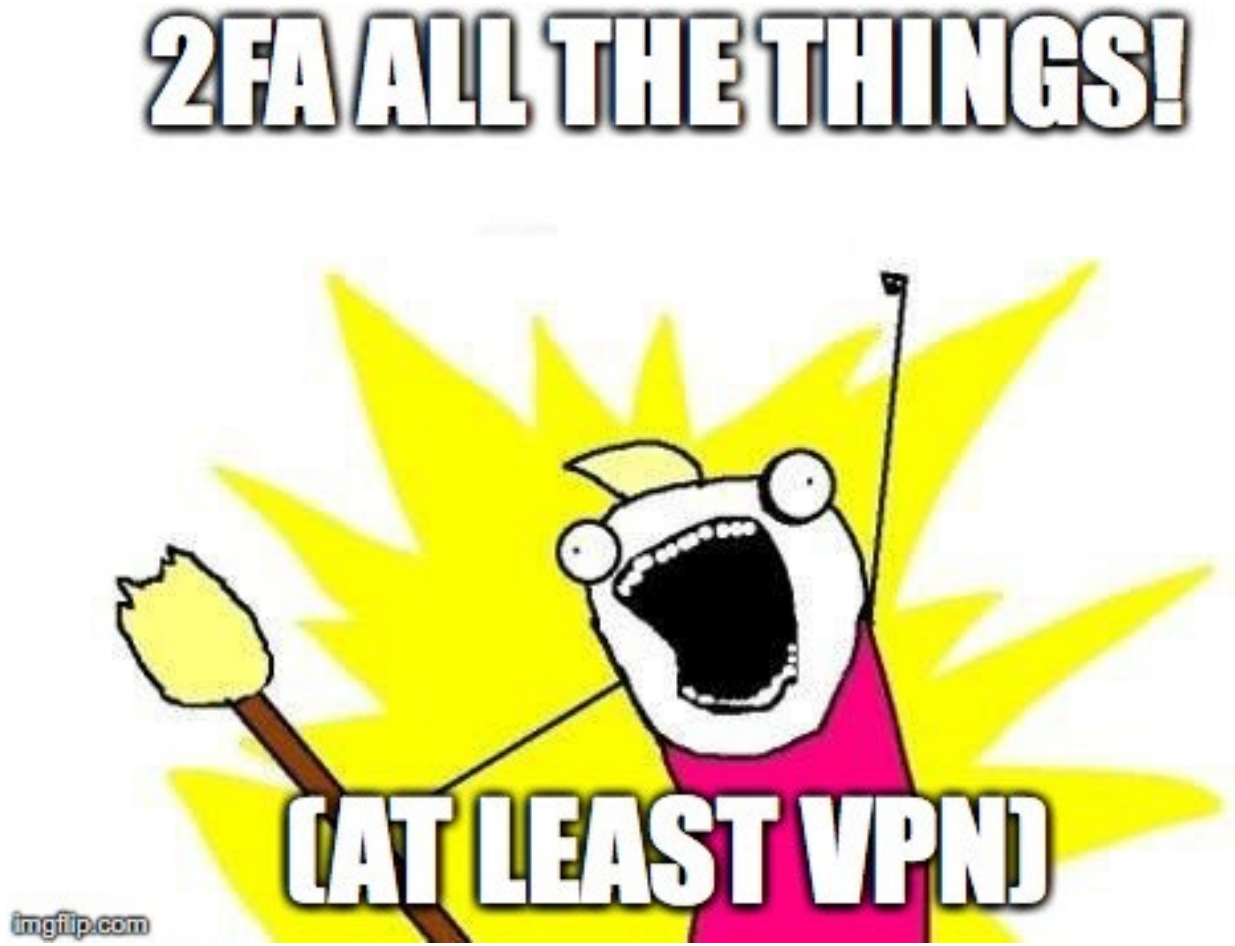
Inventory and Control of Software Assets

CIS Controls™ • CIS Control 2 *This is a basic Control*

Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.

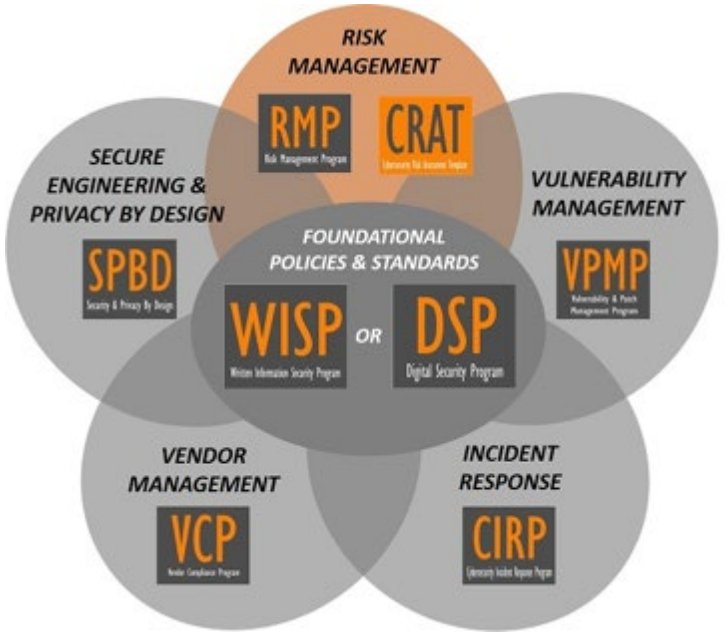
An Counter-example:

What's the first B(ruce)IS control?


2FA ALL THE THINGS!
(AT LEAST VPN)
imgflip.com

What does it take to run a risk program?

- Inventory and asset management
- Identity and asset management
- Network & endpoint controls
- Incident response
- DR/BC program
- Compliance
- Data at rest protection
- Data in transit protection
- …



https://www.complianceforge.com/digital-cybersecurity-risk-management/

http://www.cyber-risk.com.au/security-program/hello-world/

NIST CSF

Goal of an effective risk program

Minimize thinking

Maximize doing

expel

Minimizing thinking

- Thinking is dangerous!
  - The more you think, the more likely you are to make a mistake
  - Humans are bad as making risk decisions, especially in the moment

- Make your risk program only as complex as needed
- Everyone is directionally aligned from a risk perspective
- Everyone has a common conceptual model
- Risk-based decisions are planned in advance

- “Kentucky windage” works pretty well for most cyber risk decisions

- NOTE: That doesn’t mean your cyber risk management program should use “YOLO” as its core strategy

https://www.thoughtco.com/using-your-finger-like-a-weathervane-3444499

Maximize doing

- Implementing controls
- Improving controls
- Responding to incidents
- Measuring improvement
- Integrating with the business
- Leveraging 3rd parties
- Building a more resilient organization

Foundations of a risk program

- Where are you
- Where are you trying to get
- How will you get there

The NIST CSF

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness & Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes & Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies & Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

- The CSF is not something you can "do"… by design
- However, given your current state and where you want to go, you can use it to drive a process
  - First determine your current state
  - Then, determine your desired state

Here's one way to use the CSF

- There are many ways to use the CSF

- Tiers or no tiers?
- What metrics should I capture?
- How do I measure change over time?
- Excel? Sharepoint? Webapp?
- Should I build my own profile?
- Is there an industry profile I should derive my profile from?

The net is vast and infinite…
[and it's easy to build a risk program that is unmaintainable]

Example: Protect – Awareness and training

On a scale of **0 to 5**, **where are we** and were to do want **to be**?

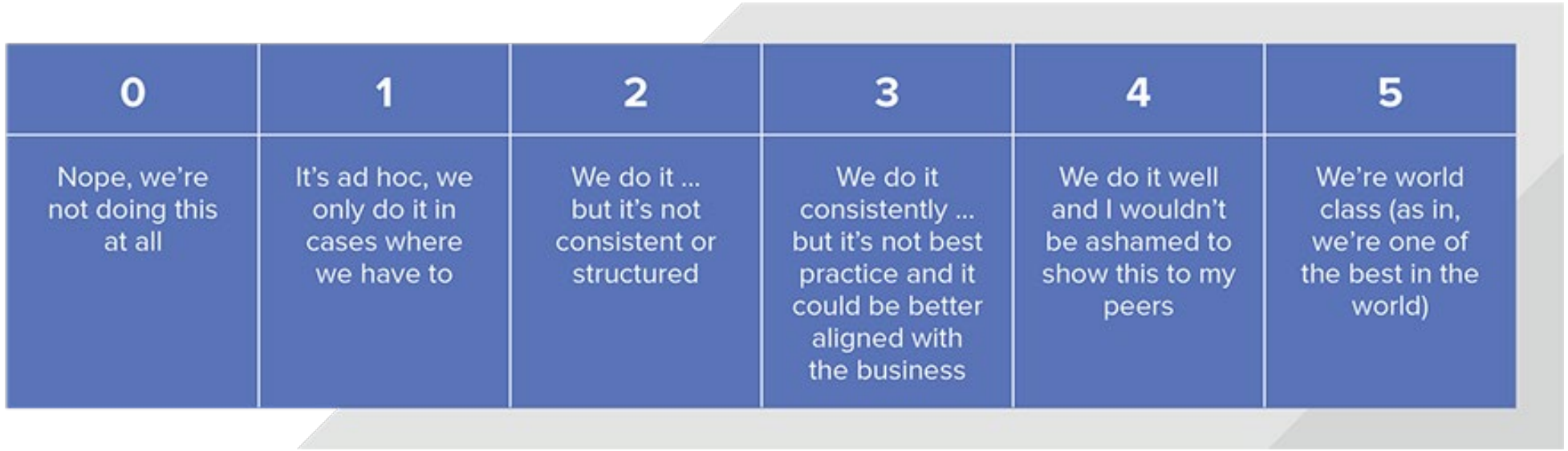
PR.AT-1: All users are informed and trained

PR.AT-2: Privileged users understand roles & responsibilities

PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities

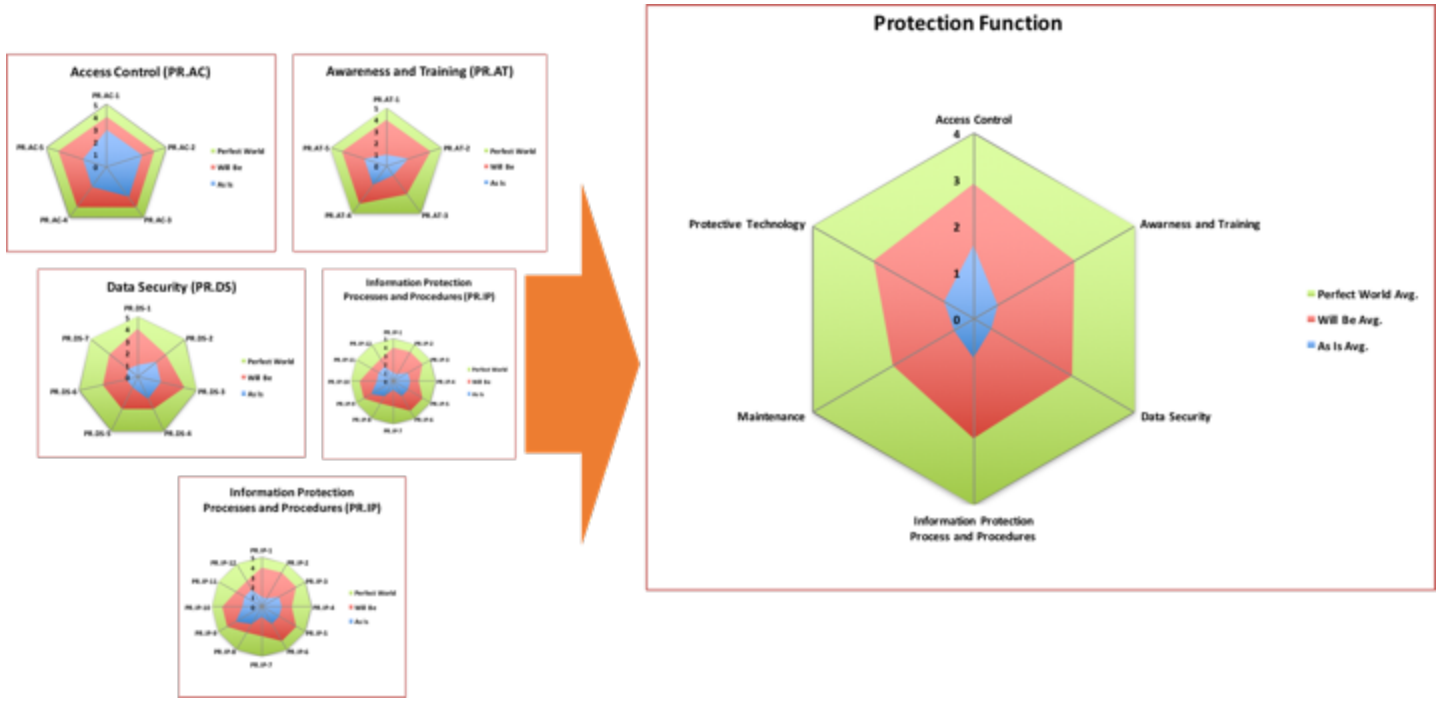
PR.AT-4: Senior executives understand roles & responsibilities

PR.AT-5: Physical and information security personnel understand roles & responsibilities



0	1	2	3	4	5
Nope, we're not doing this at all	It's ad hoc, we only do it in cases where we have to	We do it ... but it's not consistent or structured	We do it consistently ... but it's not best practice and it could be better aligned with the business	We do it well and I wouldn't be ashamed to show this to my peers	We're world class (as in, we're one of the best in the world)

Don’t over think it



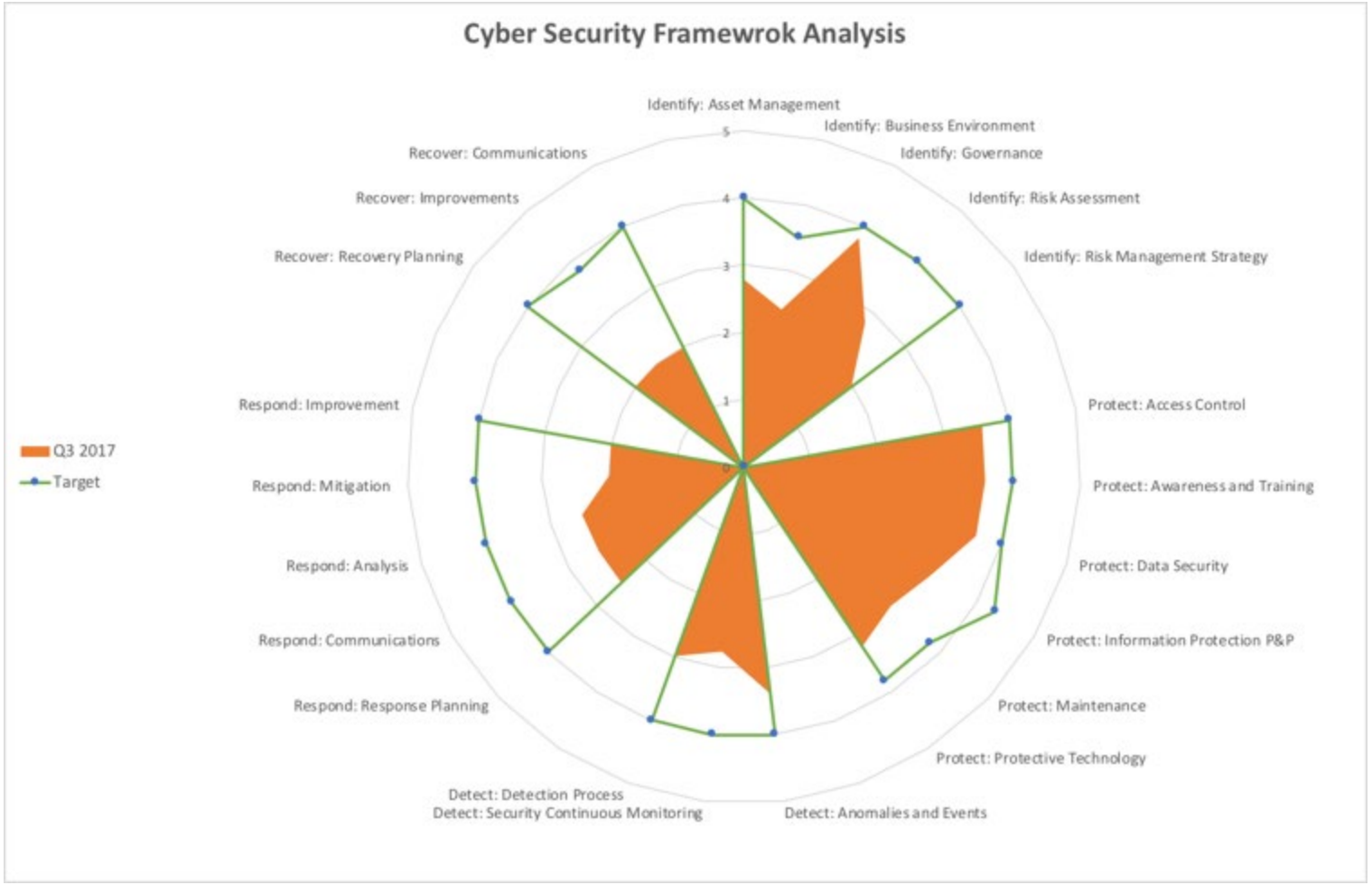
Your subcategories get rolled up to the categories.
Decimal points don’t matter

Don’t make it complicated

- Put it all together to get a picture

- Find the places you have the biggest **gaps**
- Find the places with the biggest **risks**
- Find the places you can have the **biggest gain**

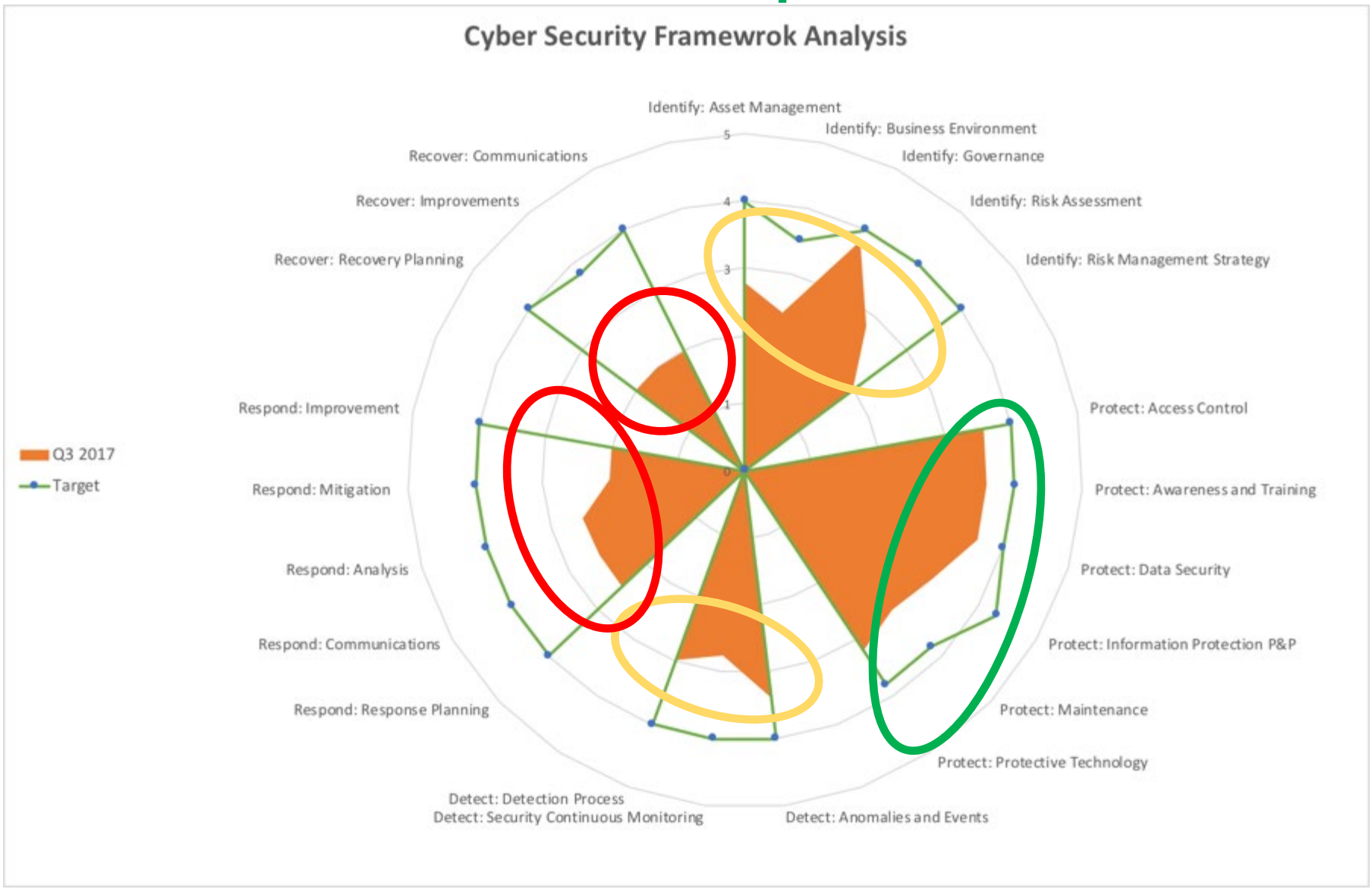
- Plan and execute



Measure progress

	Name	As-IS	To-Be	Q1
Identity Management, Authentication and Access Control (PR.AC) - Average	Identity Mgt	2	4	
Awareness and Training (PR.AT) - Average	Awareness and Training	2	4	
Data Security (PR.DS) - Average	Data Security	2	4	
Information Protection Processes and Procedures (PR.IP) - Average	Info Protection	2	4	
Maintenance (PR.MA) - Average	Maintence	2	4	
Protective Technology (PR.PT) - Average	Protective Tech	2	4	
Identity Management				
PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	PR.AC-1	2	4	2
PR.AC-2: Physical access to assets is managed and protected	PR.AC-2	2	4	3
PR.AC-3: Remote access is managed	PR.AC-3	2	4	3
PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	PR.AC-4	2	4	2

This is a common pattern…



Prescriptive

- **Protect**

Hybrid (Prescriptive And Risk-based)

- **Identify**
- **Detect**

Risk-based

- **Respond**
- **Recover**

Also can be viewed through the lens of maturity

expel™

Leveraging an MDR for rapid improvement

- Very few purchases have as big an impact on your CSF scores as onboarding an MSSP/MDR
- For most organizations, the cost of implementing a SOC and associated analysts is far more expensive than buying MSSP/MDR service
- IF you're successful, you've basically built an MSSP with a customer base of 1.

Figure 1: building your own SOC

Selecting an MSSP/MDR

- With great power comes great responsibility

- Onboarding
- Leveraging existing technology
- Supporting your cloud initiatives
- Understanding what they're actually doing
- Making less work for you, not more (or different) work

Life hacks

- You don’t need an dedicated asset management program (you get one for free in several places)
- Build your own profile opportunistically as you do your reviews
- Your supply chain/third party assessment process can be VERY simple to have value

More life hacks

- Going cloud native shifts risks
- Developing an IR plan scratches a lot of Recover/Response itches
- Bring in an external auditor to serve as a backstop
- Your CIO should report to your CISO

So what?

- Risk management should only be as complicated as you need it to be
- Focus on thinking early to facilitate doing more later
- As you go from a 2 to a 3, think about what moving from a 3 to a 4 looks like

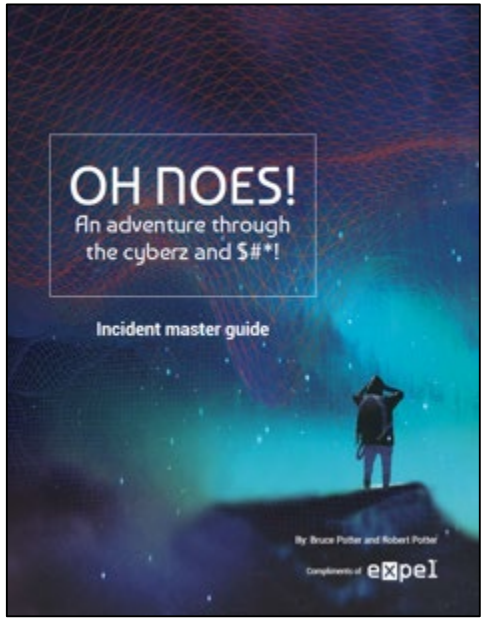
Resources available at **expel.io/blog**

Bruce Potter

@gdead

bruce.potter@expel.io

443-538-4125



Third-party assessments