RSAConference2022
San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **TECH-T08**

Know Your Environment…Better Than The Enemy

Paul Suarez, VP & CISO, Casey's General Stores

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA® Conference, RSA Security LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

Do you know your unknowns?

"…we know there are known knowns…things we know we know. We also know there are known unknowns…that is to say *we know there are some things we do not know*. But there are also unknown unknowns—the ones we don't know we don't know. And if one looks throughout the history of our country and other free countries, it is the latter category that tend to be the difficult ones".

Donald Rumsfeld

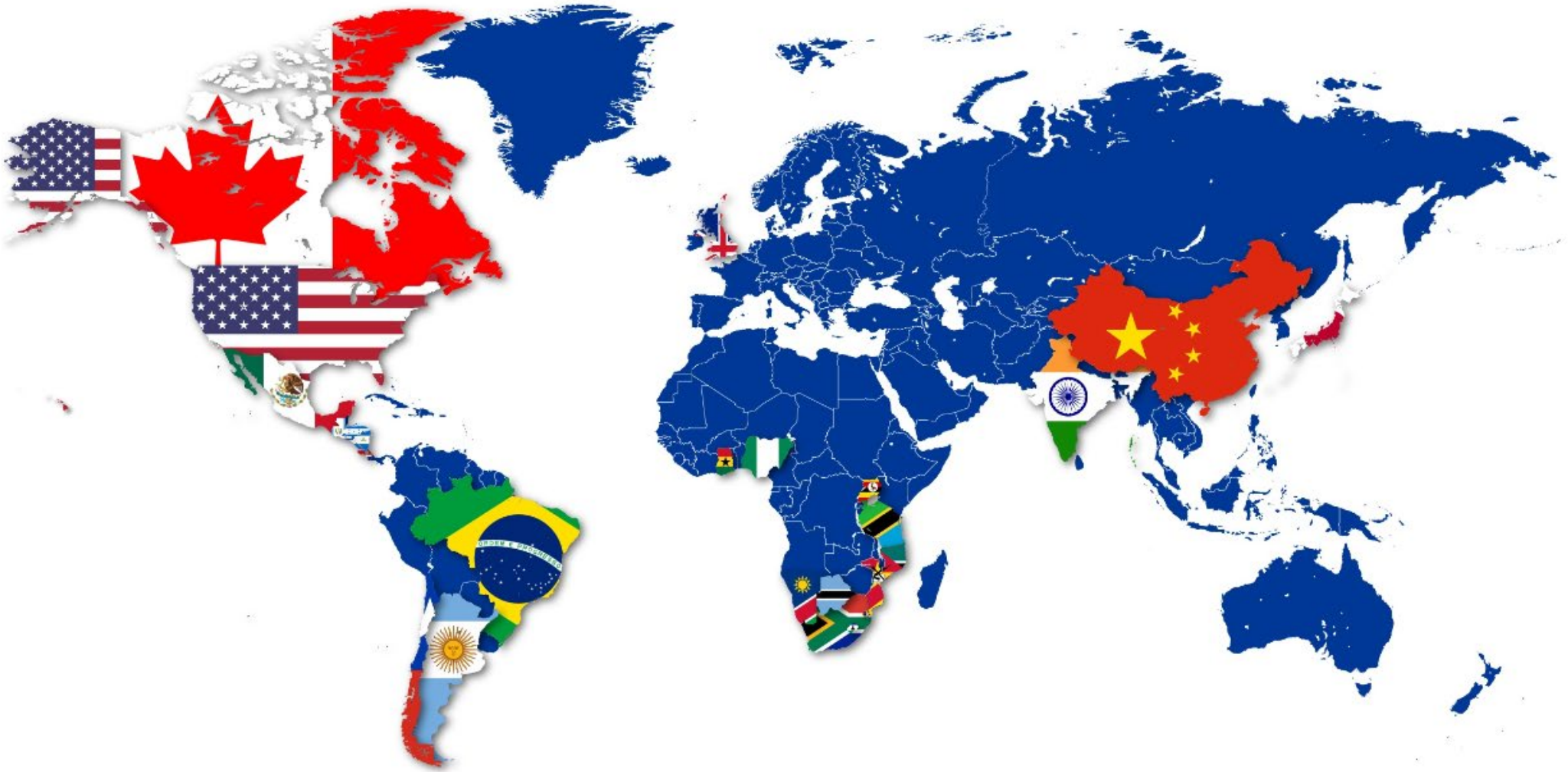
US Secretary of Defense

Why should you care?

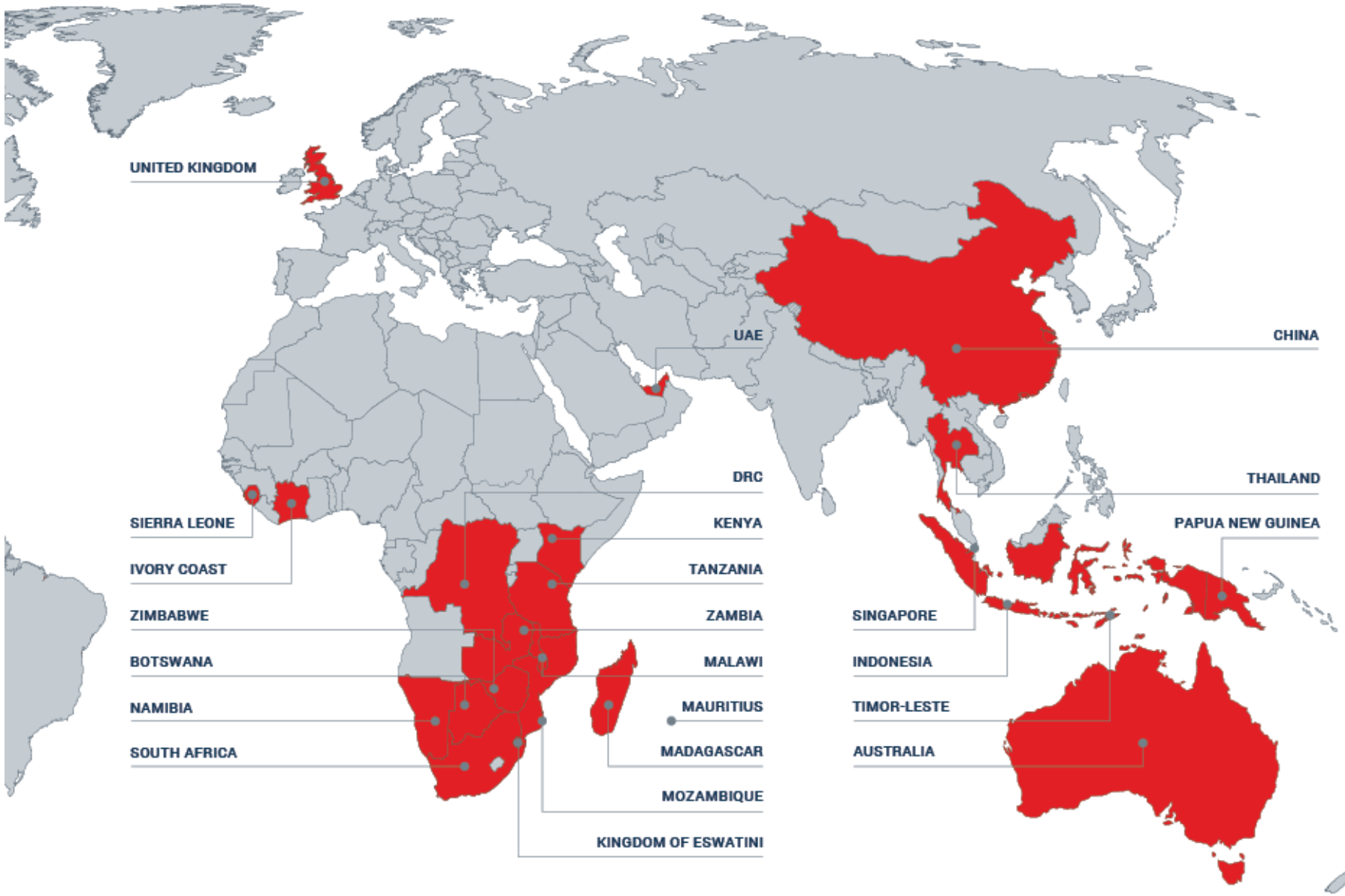
Cybersecurity Ventures expects global cybercrime costs to grow by 15 percent per year over the next five years, reaching $10.5 trillion USD annually by 2025, up from $3 trillion USD in 2015. This represents *the greatest transfer of economic wealth in history*…

Cybercrime Magazine

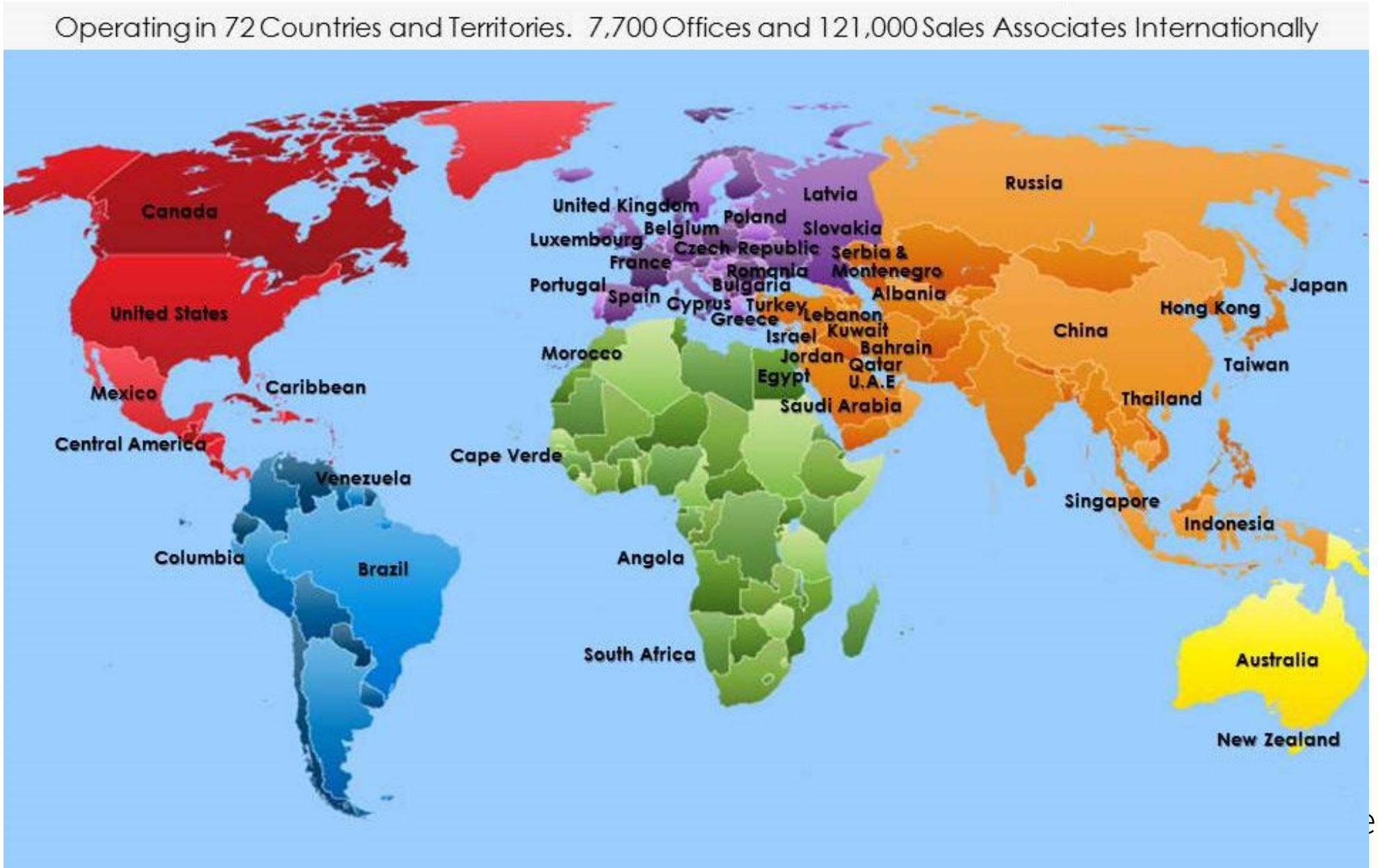
Do you have a global footprint?



Or a regional one?



Does it span all time zones?



Or spread across multiple geographies?

America♦	Europe♦	ROW♦ (Rest of the World)	India♦
Chicago, IL (3)	Basel, Switzerland	Beijing, China	Bengaluru (2)*
Cleveland, OH	Diegem, Belgium	Dubai, UAE	Bhubaneswar
Dallas, TX	Cologne, Germany	Kuala Lumpur,	Chennai (2)
Gainesville, FL	Dublin, Ireland	Malaysia (2)	Hyderabad
Burbank, CA	London, UK (3)	Selangor, Malaysia	Pune
Minneapolis, MN (2)	Munich, Germany	Melbourne, Australia	
New York, NY	Paris, France	Singapore (2)	*Company HQ
San Joe, CA	Stockholm, Sweden	Sydney, Australia	
Scottsdale, AZ	Utrecht, Netherlands	Shanghai, China	
Toronto, Canada	Warszawa, Poland	Tokyo, Japan	
Redmond, WA			
Warren, NJ*			

♦Customer base spread across the above 4 geographies.

Do you have multiple brands? Banners?

In multiple countries? Under different formats?

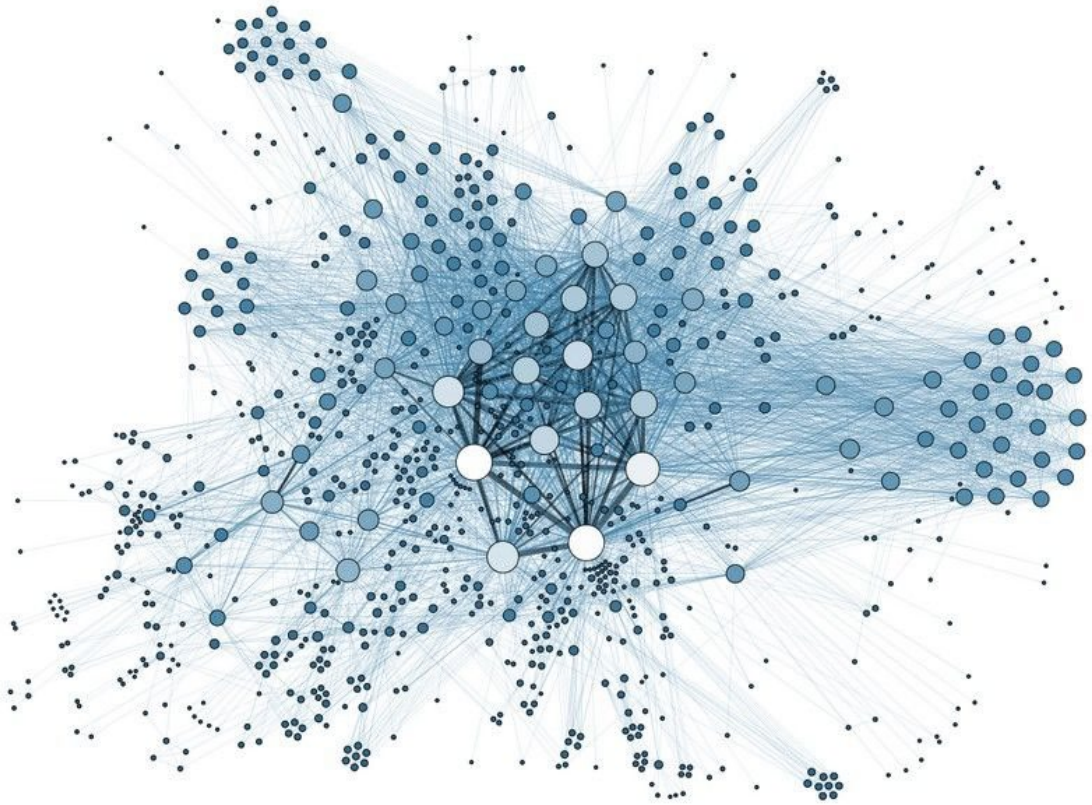
Do you collect lots of data?

# Trillion Cyber Events	**##.# Billion** Blocked Cyber Attacks	**# Billion** Blocked Spam Emails	**### Million** Malware Alerts
### Security Products Supported	**###,000** Endpoints Protected	**#.# Billion** Lines of Code Reviewed	**#.# Million** User Accounts Managed
#.# Million Vulnerabilities Remediated	**#.# Million** Certificates Issued	**#.# Million** Unwanted/Malicious Blocked Web Requests	**## Million** 2-Step Authentications

Or, how about in an average minute at “Yourco”

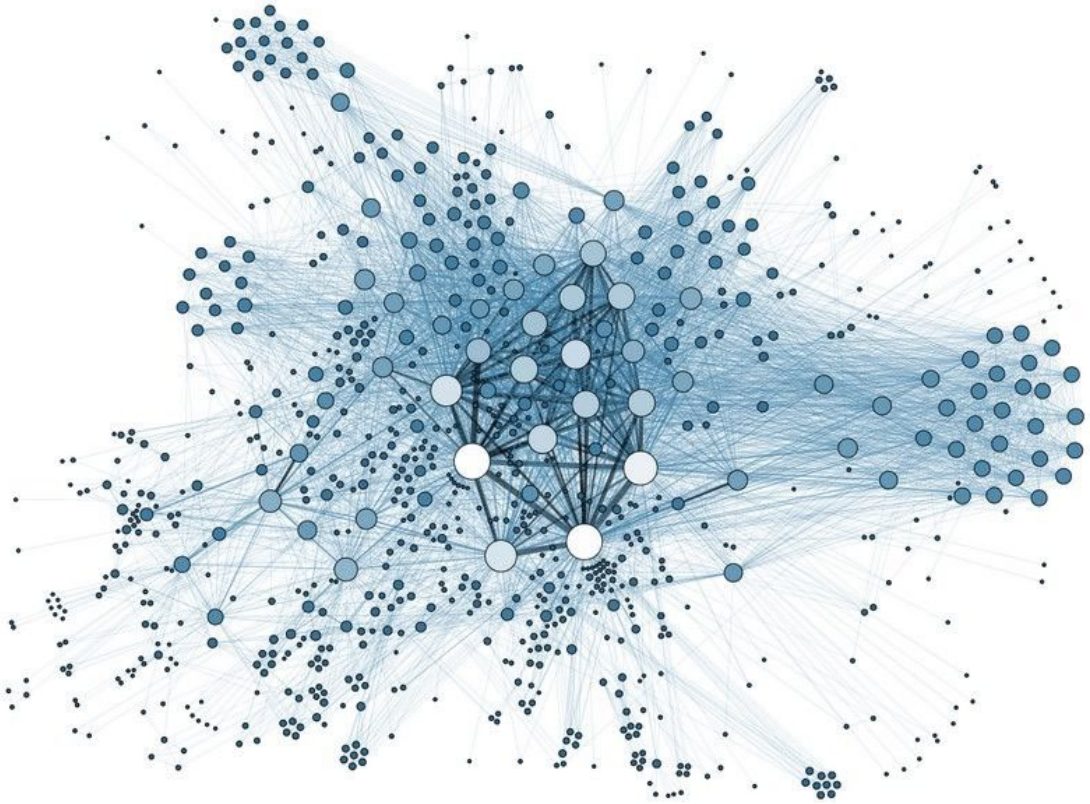
How do you make sense of it?

This?

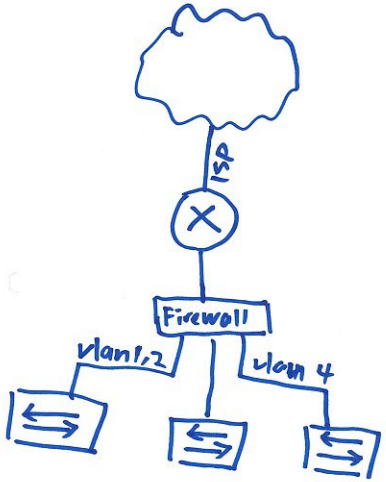


How do you make sense of it?

This?



Or this?




where do I start?

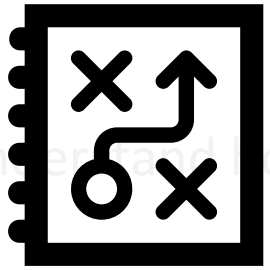
A 3-step process to discover your environment:

1. What's out there?
2. How mature is it?
3. How does it compare vs. standards?

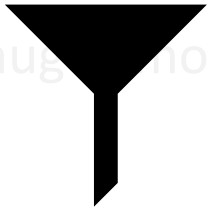
What you'll learn

- Understand how to approach the challenge of knowing your environment.
- Learn how to filter huge amounts of data in complex networks.
- See how to present it in a digestible, easy-to-read format for analysts…and execs.
- Gain ideas on how to rate maturity in order to address "first things first"

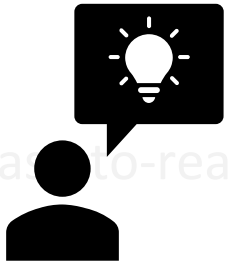
What you'll learn (in pictures!)



- Understand how to approach the challenge of knowing your environment.



- Learn how to filter huge amounts of data in complex networks.



- See how to present it in a digestible, easy-to-read format for analysts…and execs.

- Gain ideas on how to rate maturity in order to address "first things first"

Step #1: What's out there?

1. What's out there?

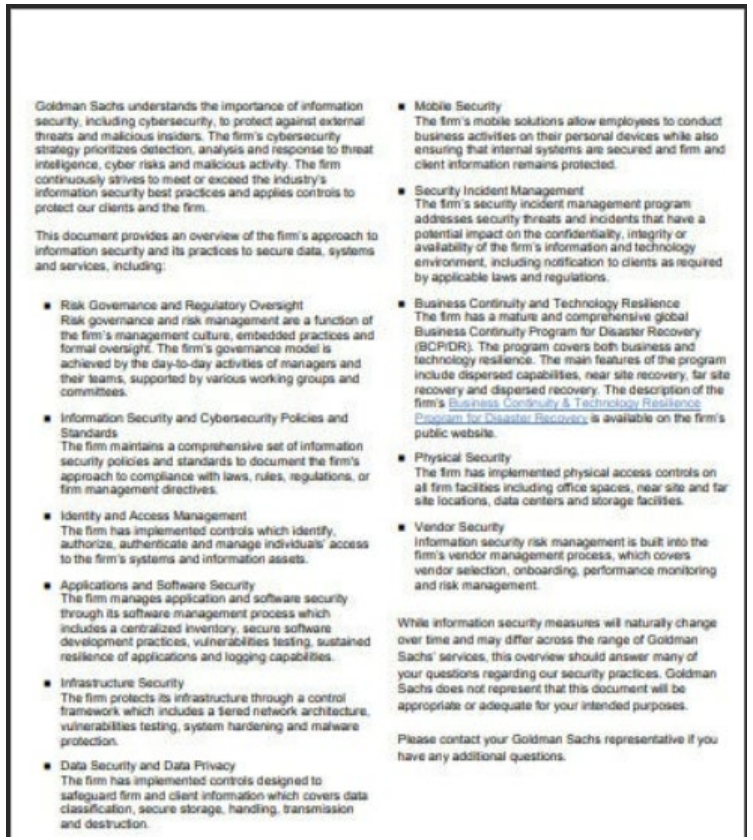
Start by surveying your teams

Tip: be sure to group core services

- Examples
  - Incident Management
  - Identity and Access Management
  - Security Infrastructure Controls
  - Risk, Management and Compliance
- Remember to involve product owners
  - Allows for better validation…and understanding

And how do you want to present it?

Textually?



Goldman Sachs understands the importance of information security, including cybersecurity, to protect against external threats and malicious insiders. The firm's cybersecurity strategy prioritizes detection, analysis and response to threat intelligence, cyber risks and malicious activity. The firm continuously strives to meet or exceed the industry's information security best practices and applies controls to protect our clients and the firm.

This document provides an overview of the firm's approach to information security and its practices to secure data, systems and services, including:

- Risk Governance and Regulatory Oversight
  Risk governance and risk management are a function of the firm's management culture, embedded practices and formal oversight. The firm's governance model is achieved by the day-to-day activities of managers and their teams, supported by various working groups and committees.
- Information Security and Cybersecurity Policies and Standards
  The firm maintains a comprehensive set of information security policies and standards to document the firm's approach to compliance with laws, rules, regulations, or firm management directives.
- Identity and Access Management
  The firm has implemented controls which identify, authorize, authenticate and manage individuals' access to the firm's systems and information assets.
- Applications and Software Security
  The firm manages application and software security through its software management process which includes a centralized inventory, secure software development practices, vulnerabilities testing, sustained resilience of applications and logging capabilities.
- Infrastructure Security
  The firm protects its infrastructure through a control framework which includes a tiered network architecture, vulnerabilities testing, system hardening and malware protection.
- Data Security and Data Privacy
  The firm has implemented controls designed to safeguard firm and client information which covers data classification, secure storage, handling, transmission and destruction.
- Mobile Security
  The firm's mobile solutions allow employees to conduct business activities on their personal devices while also ensuring that internal systems are secured and firm and client information remains protected.
- Security Incident Management
  The firm's security incident management program addresses security threats and incidents that have a potential impact on the confidentiality, integrity or availability of the firm's information and technology environment, including notification to clients as required by applicable laws and regulations.
- Business Continuity and Technology Resilience
  The firm has a mature and comprehensive global Business Continuity Program for Disaster Recovery (BCP/DR). The program covers both business and technology resilience. The main features of the program include dispersed capabilities, near site recovery, far site recovery and dispersed recovery. The description of the firm's Business Continuity & Technology Resilience Program for Disaster Recovery is available on the firm's public website.
- Physical Security
  The firm has implemented physical access controls on all firm facilities including office spaces, near site and far site locations, data centers and storage facilities.
- Vendor Security
  Information security risk management is built into the firm's vendor management process, which covers vendor selection, onboarding, performance monitoring and risk management.

While information security measures will naturally change over time and may differ across the range of Goldman Sachs' services, this overview should answer many of your questions regarding our security practices. Goldman Sachs does not represent that this document will be appropriate or adequate for your intended purposes.

Please contact your Goldman Sachs representative if you have any additional questions.

Tabular…ly?

2015 SEC OCIE Areas of Focus for Cybersecurity Examinations

Cybersecurity Policy Documentation Provided by NES Cyber Team	Security Governance & Risk Mgmt	Access Rights & Controls	Data Loss Prevention	Vendor Management	Training	Incident Response
Vulnerability Scan & Analysis	✓	✓	✓	✓		
Employee Cyber Training Guide	✓	✓	✓	✓	✓	✓
3rd Party Cyber Training Guide	✓	✓	✓	✓	✓	✓
Security Provisions for 3rd Party Contracts	✓	✓	✓	✓		
Cyber Health Assessment Questionnaire	✓	✓	✓	✓	✓	✓
Asset Management Policy & Asset Log	✓	✓	✓		✓	✓
Information Security Policy	✓	✓	✓	✓	✓	✓
Cyber Roles & Responsibilities Policy	✓	✓	✓		✓	✓
Business Continuity Policy (COOP)	✓		✓	✓	✓	✓
Insider Threat Awareness Policy	✓	✓	✓		✓	
Data Management & Data Destruction Policy	✓	✓	✓		✓	
Mobile & BYOD Policy	✓	✓	✓		✓	✓
Incident Response Policy and Logs	✓		✓	✓	✓	✓
System Maintenance Log	✓	✓	✓		✓	
Access Controls & User Privileges Policy	✓	✓	✓	✓	✓	
Network Segmentation Procedures	✓	✓	✓	✓	✓	
3rd Party Security Verification Policy	✓	✓	✓	✓	✓	✓
Encryption Policy	✓	✓	✓	✓	✓	
Database Hardening Procedures	✓	✓	✓	✓		
Password Management Policies	✓	✓	✓	✓	✓	
Configuration Management Policy	✓	✓	✓		✓	✓

Negative, you want to “catch their eye”

Like a “heads up display”

Key elements to consider:

- Keep it concise
- Use plain language
- Make it “filterable”
- Let it speak for itself

Step #2: How mature is it?

2. How mature is it?

Start with your product owners

- Assess each capability individually, whether deployed from your core or procured locally
- Utilize technical means, such as:
  - Network scans
  - Vulnerability scans
  - Penetration tests
  - Red teams
- Focus on the configuration and not just the *presence* of your security hardware and software

Sample Maturity Legend

For assessing capabilities

Title	Description
Mature Core Provider	Capability is provided by the Core Capability Owner. Capability exists and is considered mature for its context.
Mature Other	Capability exists and is considered at least as mature as the comparable capability that could be consumed from Core Capability Owner.
Evolving	Capability exists, but is not considered mature or does not have majority/complete coverage within its context. This is a flag and the details should be captured in the notes.
Undeveloped	Capability does not exist. This is a flag and the details should be captured in the notes.
Consumed	Capability is provided by somebody other than the Capability owner (i.e. a 3rd Party). This is a flag and the details should be captured in the notes.
Unknown	Capability is unknown or has not been completely assessed.
N/A	Only use "Not Applicable" IF the capability is truly not applicable - blank is better than an incorrect answer.

Sample Segment "Heat Map"*

Security capability	Category	Non-Networked Entity	Networked Entity
Centralized Identity Storage	Identity & Access Management	Consumed	Mature Core
Federated Identity Provider	Identity & Access Management	Evolving	Undeveloped
Identity Lifecycle Management - internal	Identity & Access Management	Consumed	Evolving
Identity Lifecycle Management – partners	Identity & Access Management	Consumed	N/A
Privileged Access Management	Identity & Access Management	Evolving	Mature Core
Two-Factor Authentication	Identity & Access Management	Consumed	Mature Core
Data Loss Prevention	Incident Management	Consumed	Undeveloped
Forensics and Legal Discovery	Incident Management	Consumed	Mature Core
Incident Response	Incident Management	Consumed	Unknown
Red Team - Adversary Simulation	Incident Management	Consumed	Evolving
Security Operations Center	Incident Management	Evolving	Consumed
Anti-Virus and Whitelisting	Infrastructure Controls	Consumed	Mature Core
DMARC for Mail	Infrastructure Controls	Consumed	Undeveloped
Domain Name Search Filtering	Infrastructure Controls	Consumed	Evolving
eCommerce and Website Protection	Infrastructure Controls	Consumed	N/A
Email Filtering	Infrastructure Controls	Evolving	Evolving
Encryption at Rest	Infrastructure Controls	Consumed	Mature Core
Firewall and Network ACLs	Infrastructure Controls	Consumed	Evolving
Intrusion Prevention	Infrastructure Controls	Evolving	Mature Core
Laptop Encryption	Infrastructure Controls	Consumed	Undeveloped
Mobile Device Management	Infrastructure Controls	Consumed	Unknown
Remote Access	Infrastructure Controls	Consumed	Mature Core
Web Gateway or Proxy	Infrastructure Controls	Consumed	Mature Core
Wireless Intrusion Detection and Prevention	Infrastructure Controls	Evolving	Mature Core
Awareness	Risk Management	Consumed	Unknown
Code Scanning and Analysis	Risk Management	Consumed	Evolving

*notional & not representative

How does it compare vs. standards?

ISO

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

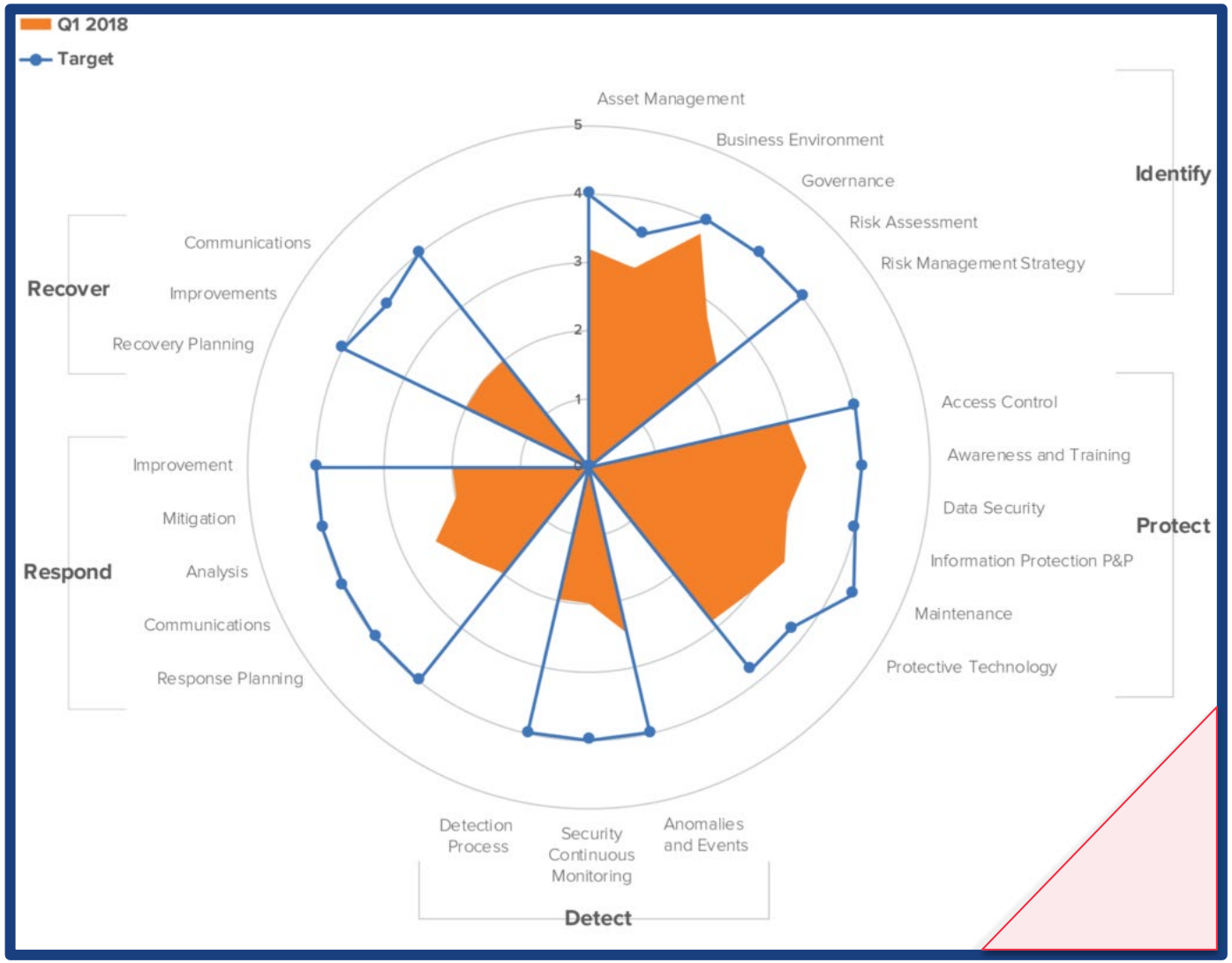
Casey's

3. How does it compare vs. your standards?

- Again, your product owners should know this, but may need your help to establish/document
- Decide early which framework you intend to follow
  - US NIST? ISO? COBIT? OEM?
    - Cybersecurity (CSF)? Risk (RMF)? Privacy? Big Data Interoperability?
  - Regardless, it should help answer:
    - Where are you strongest?
    - Where are you weakest?
    - Where are your biggest gaps (vs. target)?
  - And then repeat it…

NIST CSF Matrix Example*

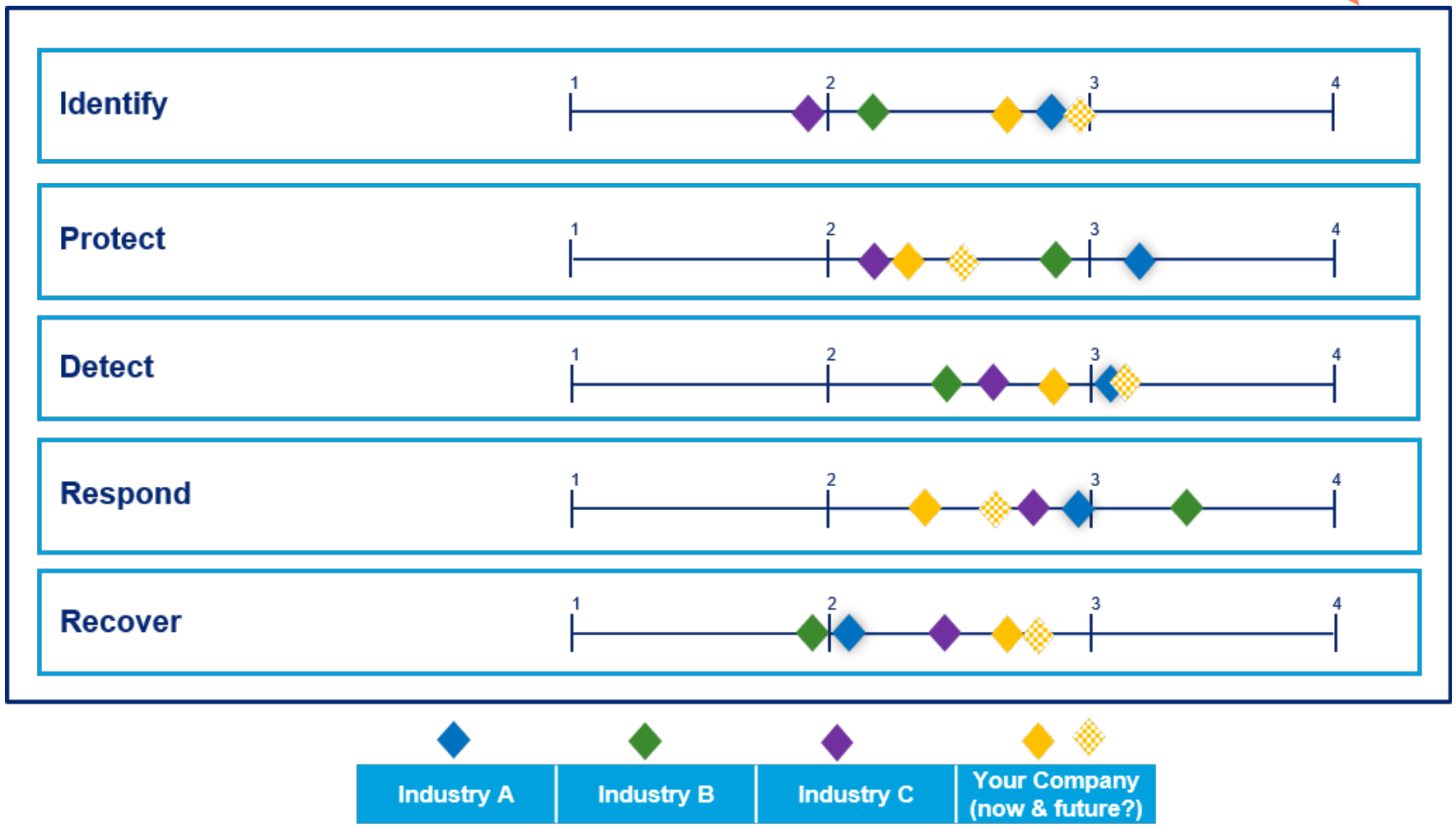
Where do you want to expand into?



* matrix is notional & not representative

NIST CSF Graph Example*

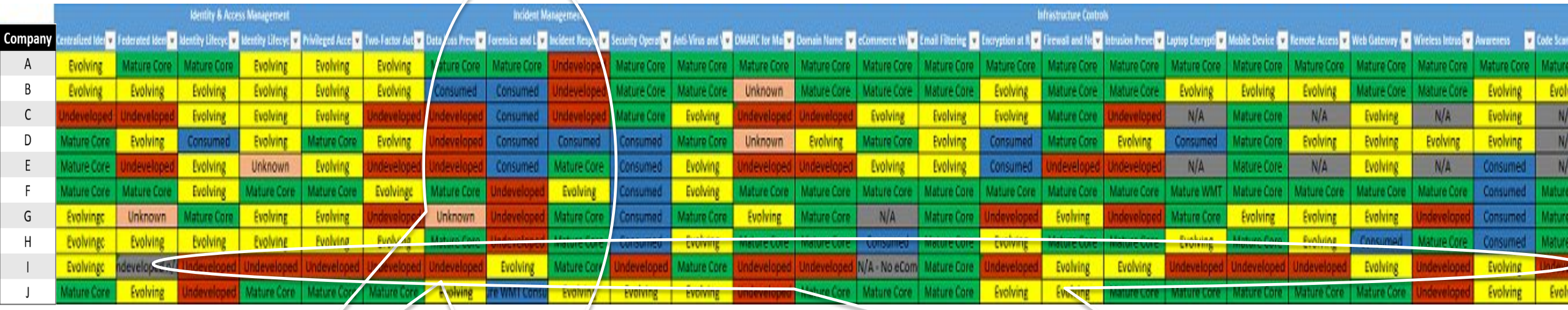
Where do you want to be?



* graph is notional & not representative

What priorities should we focus on?

Put it all together with a Heat Map



Company	Identity & Access Management						Incident Management			Infrastructure Controls																
	Centralized Ide	Federated Ider	Identity Lifecyc	Identity Lifecyc	Privileged Acce	Two-Factor Aut	Data Loss Prev	Forensics and L	Incident Resp	Security Operat	Anti-Virus and	DMARC for Ma	Domain Name	eCommerce We	Email Filtering	Encryption at R	Firewall and Ne	Intrusion Preve	Laptop Encrypti	Mobile Device	Remote Access	Web Gateway	Wireless Intrus	Awareness	Code Scan
A	Evolving	Mature Core	Mature Core	Evolving	Evolving	Evolving	Mature Core	Mature Core	Undeveloped	Mature Core	Mature Core	Mature Core	Mature Core	Mature Core	Mature Core	Mature Core	Mature Core	Mature Core	Mature Core	Mature Core	Mature Core	Mature Core	Mature Core	Mature Core	Mature
B	Evolving	Evolving	Evolving	Evolving	Evolving	Evolving	Consumed	Consumed	Undeveloped	Mature Core	Mature Core	Unknown	Mature Core	Mature Core	Mature Core	Evolving	Mature Core	Mature Core	Evolving	Evolving	Evolving	Mature Core	Mature Core	Evolving	Evol
C	Undeveloped	Undeveloped	Evolving	Evolving	Evolving	Undeveloped	Undeveloped	Consumed	Undeveloped	Mature Core	Evolving	Undeveloped	Undeveloped	Evolving	Evolving	Evolving	Mature Core	Undeveloped	N/A	Mature Core	N/A	Evolving	N/A	Evolving	N/
D	Mature Core	Evolving	Consumed	Evolving	Mature Core	Evolving	Undeveloped	Consumed	Consumed	Consumed	Mature Core	Unknown	Evolving	Mature Core	Evolving	Consumed	Mature Core	Evolving	Consumed	Mature Core	Evolving	Evolving	Evolving	Evolving	N/
E	Mature Core	Undeveloped	Evolving	Unknown	Evolving	Undeveloped	Undeveloped	Consumed	Mature Core	Consumed	Evolving	Undeveloped	Undeveloped	Evolving	Evolving	Consumed	Undeveloped	Undeveloped	N/A	Mature Core	N/A	Evolving	N/A	Consumed	N/
F	Mature Core	Mature Core	Evolving	Mature Core	Mature Core	Evolving	Mature Core	Undeveloped	Evolving	Consumed	Evolving	Mature Core	Mature Core	Mature Core	Mature Core	Mature Core	Mature Core	Mature Core	Mature WMT	Mature Core	Mature Core	Mature Core	Mature Core	Consumed	Mature
G	Evolving	Unknown	Mature Core	Evolving	Evolving	Undeveloped	Unknown	Undeveloped	Mature Core	Consumed	Mature Core	Evolving	Mature Core	N/A	Mature Core	Undeveloped	Evolving	Undeveloped	Mature Core	Evolving	Evolving	Evolving	Undeveloped	Consumed	Mature
H	Evolving	Evolving	Evolving	Evolving	Evolving	Evolving	Mature Core	Undeveloped	Mature Core	Consumed	Evolving	Mature Core	Mature Core	Consumed	Mature Core	Evolving	Mature Core	Mature Core	Evolving	Mature Core	Evolving	Consumed	Mature Core	Consumed	Mature
I	Evolving	[illegible]	Undeveloped	Undeveloped	Undeveloped	Undeveloped	Undeveloped	Evolving	Mature Core	Undeveloped	Mature Core	Undeveloped	Undeveloped	N/A - No eCom	Mature Core	Undeveloped	Evolving	Evolving	Undeveloped	Undeveloped	Undeveloped	Evolving	Undeveloped	Evolving	[illegible]
J	Mature Core	Evolving	Undeveloped	Mature Core	Mature Core	Mature Core	Evolving	re WMT Consu	Evolving	Evolving	Evolving	Undeveloped	Mature Core	Mature Core	Mature Core	Evolving	Evolving	Mature Core	Mature Core	Mature Core	Mature Core	Mature Core	Undeveloped	Evolving	Evol

Core Service priority

(notional and not representative)

Segment priority

OK, then how can you continuously improve?

- Stick to your priorities
  - But ensure they're aligned with the business
- Revisit ratings with product owners
  - At least annually, but more frequent is preferred
- Measure, share and compare results
  - Since a little competition is a great motivator ☺
  - aka OODA/PDCA

Apply What You Have Learned Today

- Next week you should:
  - Identify data sources at your disposal to describe your environment
- In the first three months following this presentation you should:
  - Decide which framework your want to measure yourself against
  - Assemble questionnaires/guides/manuals to assess the above
  - Identify who your product owners are and socialize the process with them
- Within six months you should:
  - Begin surveying your product owners to get them involved and engaged
  - Decide on how you want to categorize the data
  - Begin plotting the data so you can begin to see your biggest areas for improvement

Then you will know your environment… better than the enemy

1. Survey your environment
2. Assess the maturity of your tools
3. Measure yourself against established standards

Questions?