From Shoestring Budget to Unified Front:

Building cybersecurity resilience across diverse subsidiaries

By: Matthew Webster, *MA, CISSP, CISA, CRISC, etc.*

Founder / CEO / CISO

Housekeeping

- This is an advanced talk. I don't explain the ABCs of everything I am talking about.
- The generalities are true, but a great deal of data presented is fictitious.
- I encourage questions, but ask questions *only* related to the current slide. If your question is not answered, there will be time for questions later.

Agenda

- Personal Context
- Cybersecurity Context
- Backend Stakeholder Alignment
- Assessments on a Dime
- What would I improve?

3 Takeaways

1. From Boardroom to Budget: Using Cyber Insurance to Champion Security Investments

2. Bridging the Expertise Gap Aligning Security Standards Across Subsidiaries:

3. NIST CSF as a Roadmap, Not a Rulebook: Tailoring the Framework for Maximum Impact

Personal Context

Who is Matthew Webster

Who is Matthew Webster

- Over 25 years of experience
- Three-time CISO including a global CISO
- Sales: Cybersecurity Solutions Architect
- Built several cybersecurity programs from the ground up
- I've reviewed *maybe* 1000 products and services over the years
- Author

Certifications and Training

IT / Security Certifications

- Certified Information System Security Professional (CISSP)
- Certified in Risk and Information Systems Control (CRISC)
- Certified Information Systems Auditor (CISA)
- GIAC: Law of Data Security and Investigations (expired) (GLEG)
- Cisco Certified Security Professional (retired) (CCSP)
- Certified Ethical Hacker and Countermeasures (Version 7) (expired) (CEH&C)
- Holistic Information Security Practitioner (HISP)
- Information Systems Security Professional (INFOSEC)
- VMware Certified Professional (expired) (VCP4)
- Microsoft Certified Systems Engineer: Security (MCSE: Security)
- Microsoft Certified Systems Administrator: Security (MCSA: Security)
- Cisco Certified Network Professional (expired) (CCNP)
- Certified Wireless Professional (CWP)
- Cisco Wireless LAN Support Specialist (expired) (CQS-CWLSS)
- Microsoft Certified Systems Engineer (MCSE)
- Microsoft Certified Systems Administrator (MCSA)
- Cisco Certified Network Associate (expired) (CCNA)
- Microsoft Certified Professional (MCP)
- Designing Cisco Network Architecture (expired) (ARCH)
- Committee on National Security Systems 4013 (recognition) (CNSS 4013)
- Information Technology Infrastructure Library (Version 3) (ITIL v3)
- QualysGuard Certified Specialist (including DAST and Configuration Management)

Training

- SANS Track One: The Ten Domains of the CISSP 2003
- Mile2: Certified Penetration Testing Specialist 2005
- SANS Track Seven: Auditing Networks, Perimeters, and Systems 2005
- CMS: Best Practices Conferences (1 per year) 2006 - 2010
- HG64: HOW TO AUDIT MVS, RACF, ACF2, TOP SECRET, CICS, DB2, & MQ SERIES 2008
- HOLISTIC INFORMATION SECURITY PRACTITIONER 2009
- PROJECT MANAGEMENT PROFESSIONAL (PMP) 2009
- VMWARE VSPHERE: FAST TRACK [V4] 2010
- CERTIFIED ETHICAL HACKER & COUNTERMEASURES (CEH&C) 2011
- INFORMATION TECHNOLOGY INFRASTRUCTURE LIBRARY 2011
- CERTIFIED HACKER FORENSIC INVESTIGATOR 2012
- OWASP TOP 10 2012
- CLOUD SECURITY ALLIANCE (3 DAY) 2012
- FIREWALL 2.0 – DEPLOYING CISCO ASA FIREWALL 2013
- ISACA CRISC ITEM WRITING WORKSHOP 2013
- QUALYS – VULNERABILITY MANAGEMENT, POLICY COMPLIANCE & WEB APP SCANNING, PCI 2014
- SANS LEGAL 523: LAW OF DATA SECURITY AND INVESTIGATIONS 2014
- HEALTHCARE INFORMATION MANAGEMENT SYSTEMS SOCIETY 16 (HIMSS 16 & 17) 2016 - 2017
- TRIPWIRE ENTERPRISE 2016
- RSA SECURITY CONFERENCE 2018, 2019, 2021 - 2023
- BLACK HAT, DEFCON 2019
- IAPP CIPP/US 2019
- SANS 521: DRIVING CYBERSECURITY CHANGE – ESTABLISHING A CULTURE OF PROTECT, DETECT, AND RESPOND 2020
- Countless few hours to 2 day events

Range of Experiences

Vertical Experience

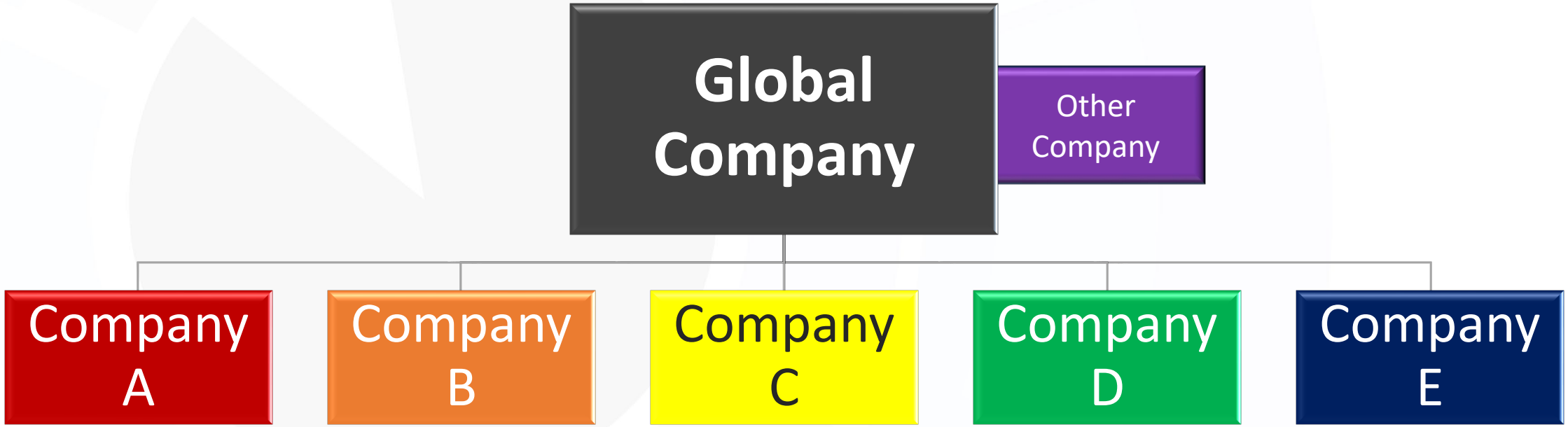
- Federal Government
- State Government
- Financial Services
- Retail
- Cyber Insurance
- Several others

Compliance Experience

- NIST 800-53 (3 variants)
- NIST CSF (1.1 and 2.0)
- HITRUST
- MARS-E
- NIST 800-171
- PCI
- HIPAA
- SOC2 (Type 1 and 2)
- ISO 27,001
- TISAX

Cybersecurity Context

Global Cybersecurity Context



Subsidiary Budgets, Maturity, Knowledge

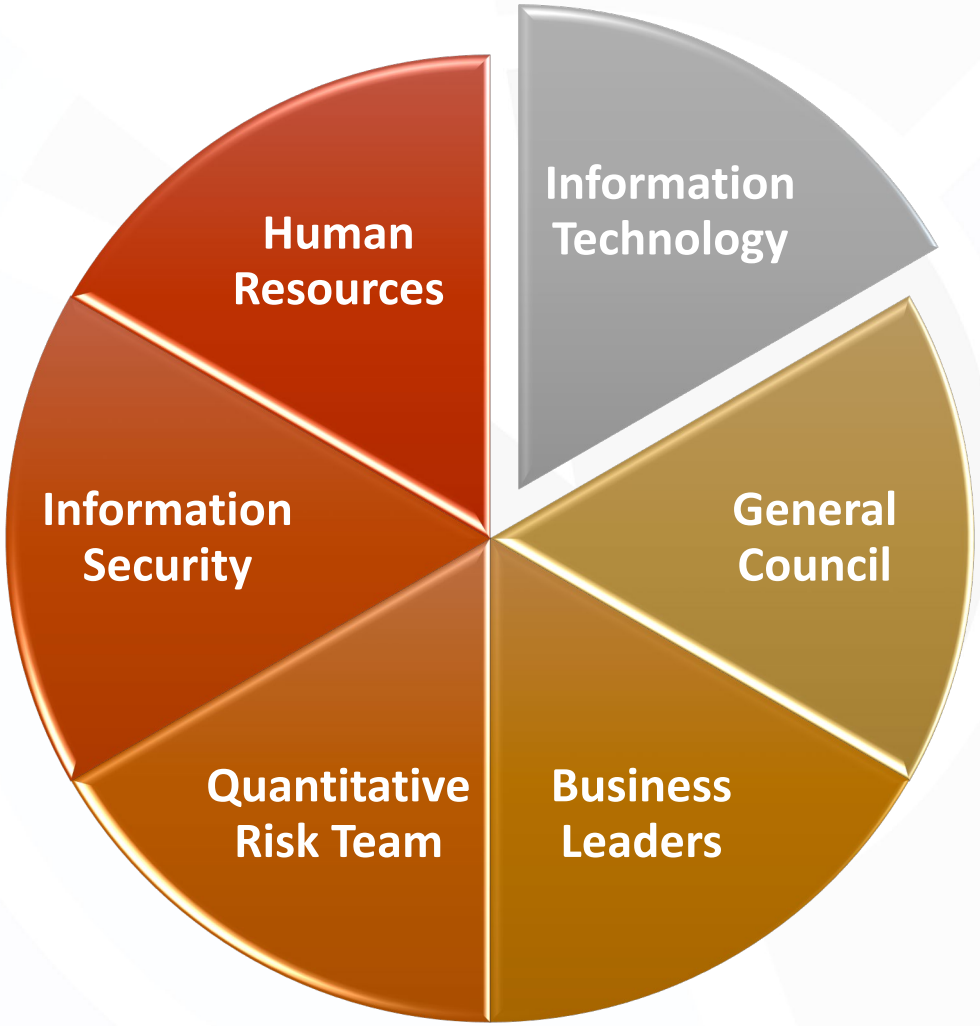
Range

My Budget

Shoestring

Backend Stakeholder Alignment

Global Cybersecurity Committee



- Key people
- Monthly meetings with minutes
- Getting buy in

Qualitative & Quantitative Alignment

- Mapping qualitative to quantitative risk levels

Qualitative	Quantitative	Description
Minimal	Up to $50,000	This has an insignificant impact to the business.
Low	$50,000 to $100,000	Minor systems were affected.
Moderate	$100,000 to $500,000	There is significant business impact.
High	$500,000 to $5,000,000	Company takes a severe hit.
Critical	Over $5,000,000	Company is at risk for going out of business.

This is entirely fictional data, but the general idea is true.

Other Risk Considerations

- Risk Tolerance and Risk Appetite mapped to CIA and Reputation
- Risk Register (mapped to business risks)

Business Led Cybersecurity Goals

- Risk reduction to an acceptable level across subsidiaries
- Return On Security Investment (ROSI) across subsidiaries
- Standardized technology, services, and processes across subsidiaries

Assessments on a Dime

Challenges & Needs

- Improve knowledge of junior leaders
- Cross organizational buy in
- Organizational visibility
- Standardized reporting
- Clear communication with senior management
- Change minds of business leaders
- Aligned risk management across organizations
- Shoestring budget
- Repeatable

Time to Make a Choice

- My choice? DIY Security
- What were my tools?
  - Cyber Insurance
  - My wits and experience (uh oh!)
- What did I choose?
  - DIY NIST CSF 1.1 (2 was not out)
  - Continual Education
  - Risk Alignment

NIST CSF

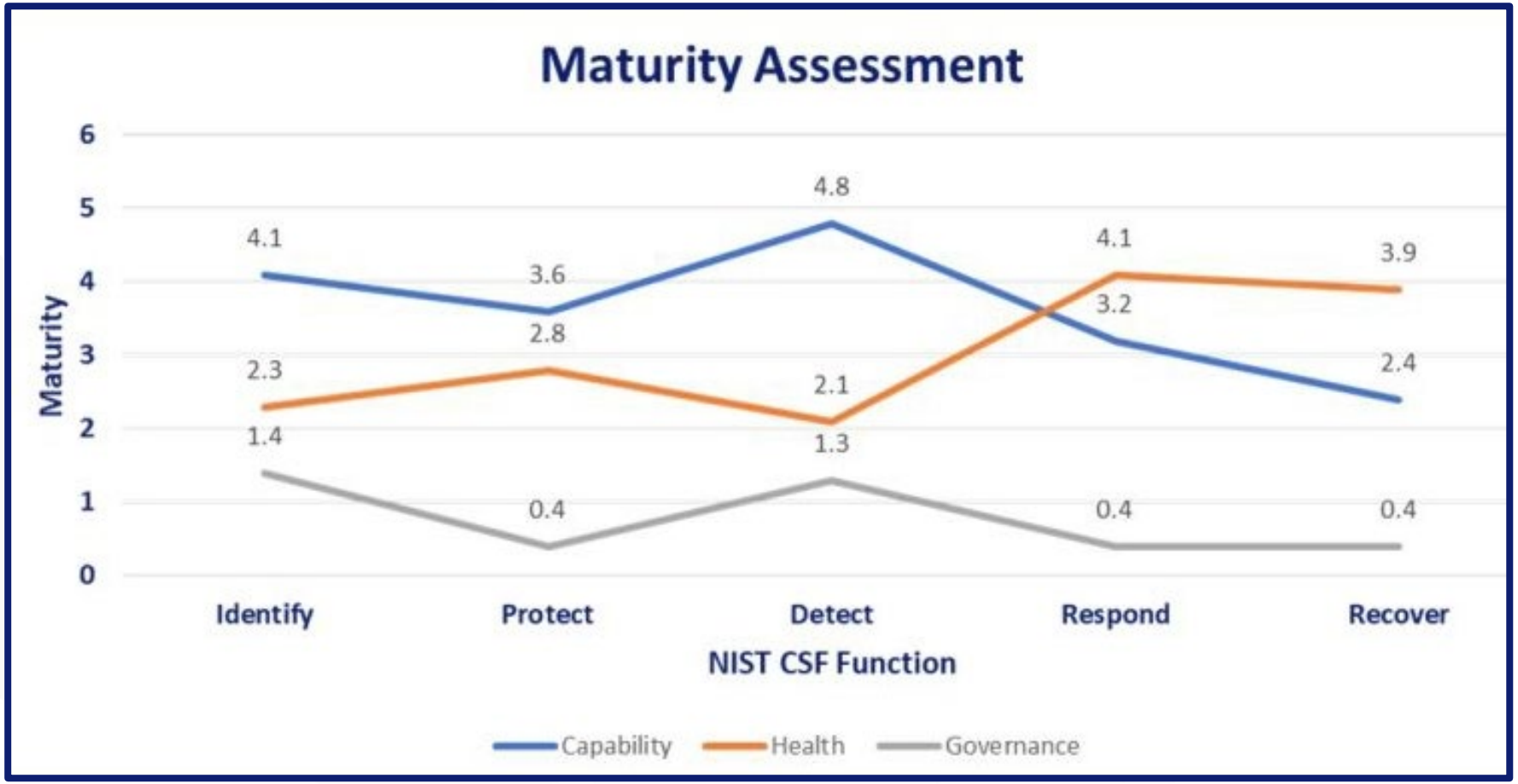
- Clear communication with senior management
- Standardized reporting
- Measurements to gain clarity across subsidiaries
- Shoestring budget
- After modifications, more complete than certifications
- Repeatable

How????

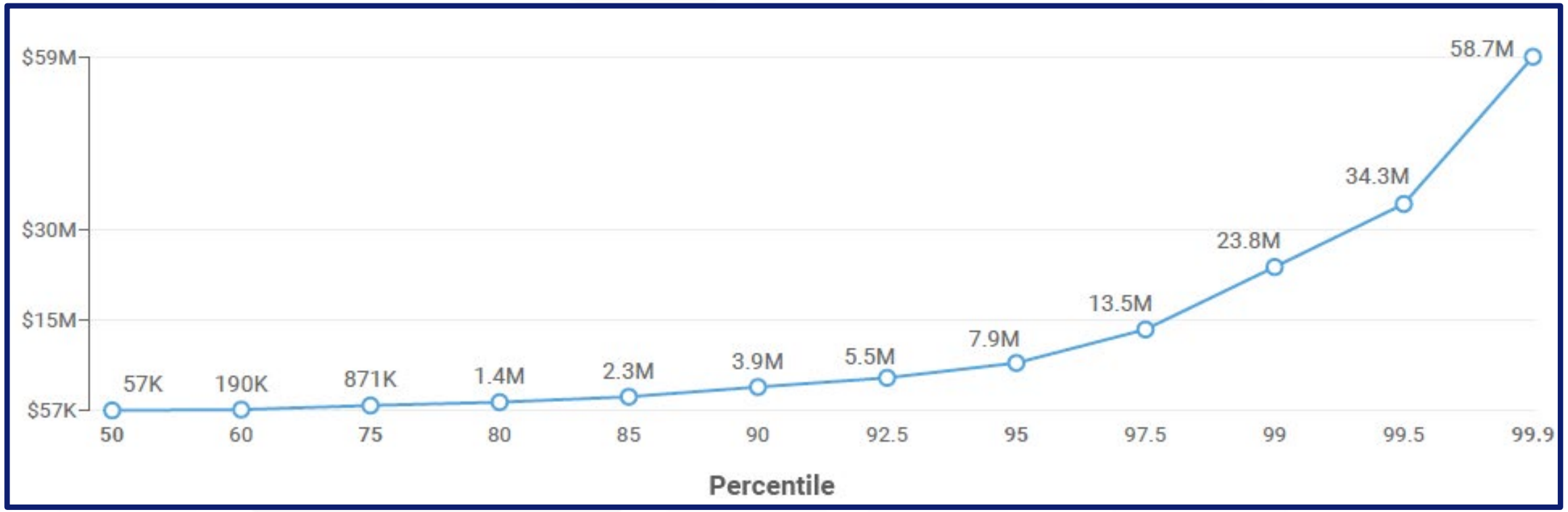
- Self assessments
- Review of key documents
  - Audits
  - Incident Response Plans
  - Disaster Recovery Plans
  - SOC reports
- Education and training on the methodology
- Q&A sessions
- One on One Meetings
- Qualitative / quantitative risk appetite and tolerance

DIY NIST CSF: A Tailored Framework

This is entirely fictional data, but the general idea is true.



Insurance: Data Breach Severity Distribution

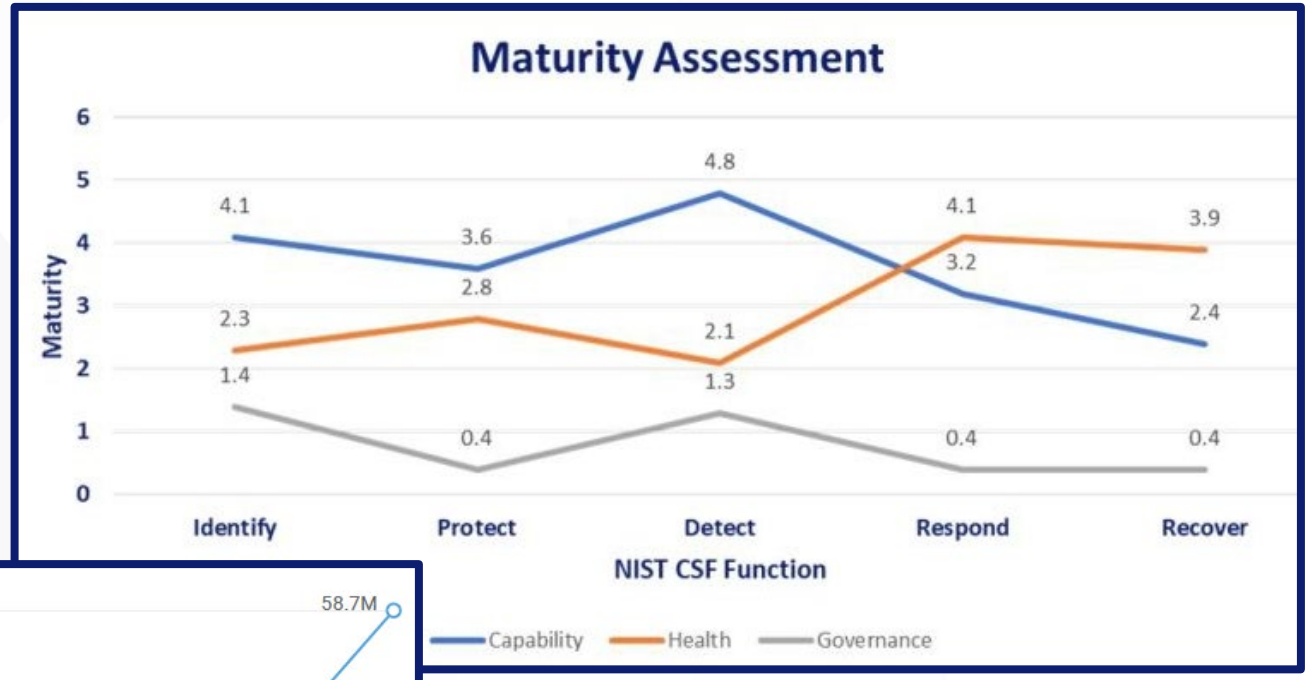


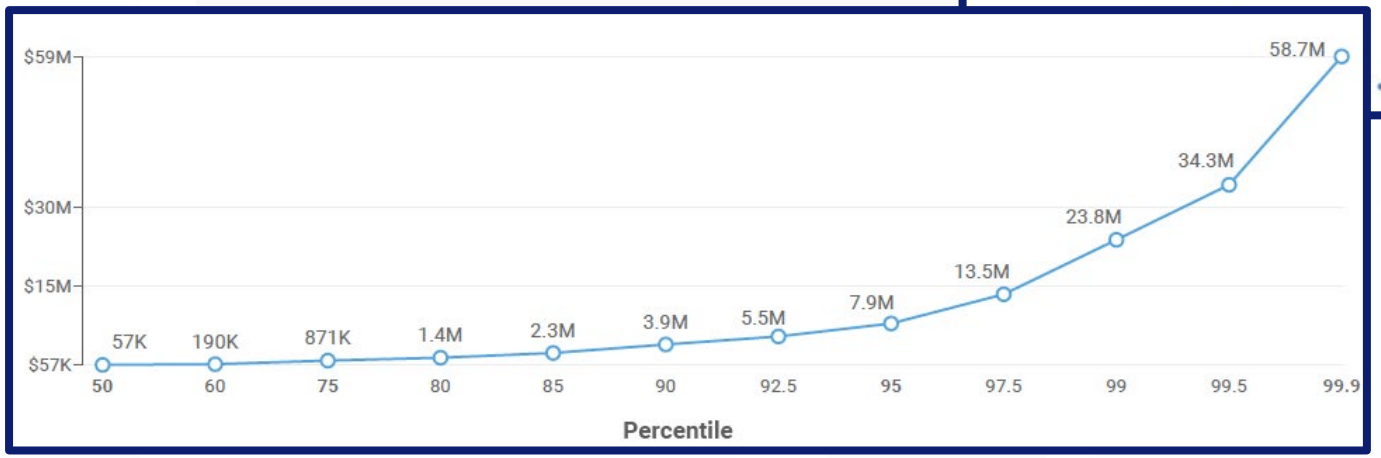
This is entirely fictional data, but the general idea is true.

Putting the Pieces Together

Risk Mapping

- Minimal: 0 to $50k
- Low: $50k to $250k
- Medium: $250k to $500k
- High: $500K to $5M
- Critical Over $5M





Risk Appetite

- Confidentiality: Accepts Medium Risk
- Integrity: Accepts High Risk
- Availability: Accepts Low Risk
- Reputation: Accepts Low Risk

CYVERGENCE

This is entirely fictional data, but the general idea is true.

Outcomes

- Clearer picture than compliance.
- As cybersecurity is put into place, cybersecurity risk is reduced.
- Hiring of CISOs.
- External programs, were easier to introduce.
- Measurable progress over time.

What Would I Improve?

What would I change now?

- Define what the risk levels mean
- Further business alignment / integration
- Cybersecurity value
  - Risk Reduction (Previously included)
  - Business Enablement
  - Operational Risk
- Better risk quantification

Return on Investment Calculation

- Inherent Cybersecurity Risk: $100 million
- Current Cybersecurity Risk: $85 million
- Potential Cybersecurity Program Risk Reduction: $45 million
- Minimum Potential Cybersecurity Risk: $55 million
- Estimated Preventative Value: $8 for every dollar spent

CYVERGENCE

This is entirely fictional data, but the general idea is true.

Thank you!

Contact

- Matthew.webster@cyvergence.biz

Follow us on

- YouTube
- LinkedIn

If you have questions, please visit our site at

www.cyvergence.biz