Texas Association for
Home Care & Hospice
Leading ★ Advancing ★ Advocating

56th Annual Meeting
Tuesday, August 26, 2025
3:15pm-4:15pm

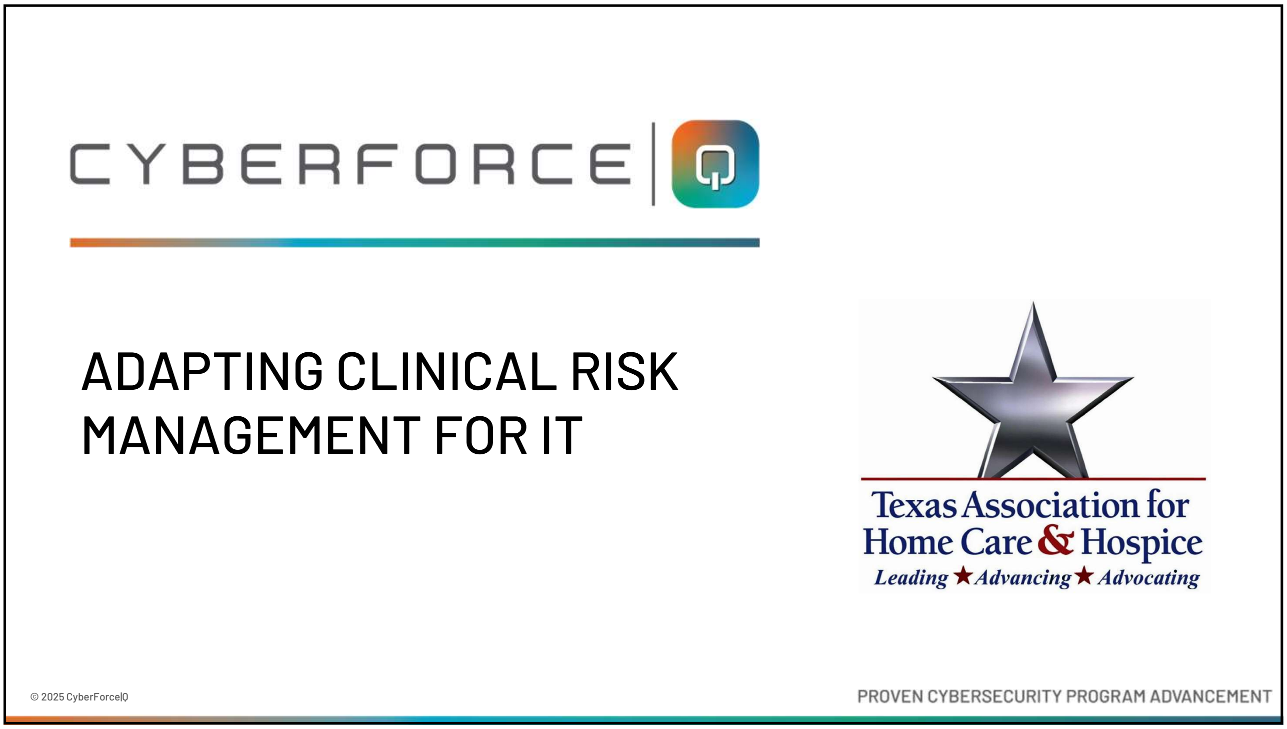
PC3a. Population Adapting Clinical Risk Management for IT/Cybersecurity

Presented by:

Brad Maughan, HCISPP, Regional Sales Director, CyberForce |Q
Wayne Pierce, Cybersecurity Program Advisor, CyberForce |Q

Thank you to our Sponsors:

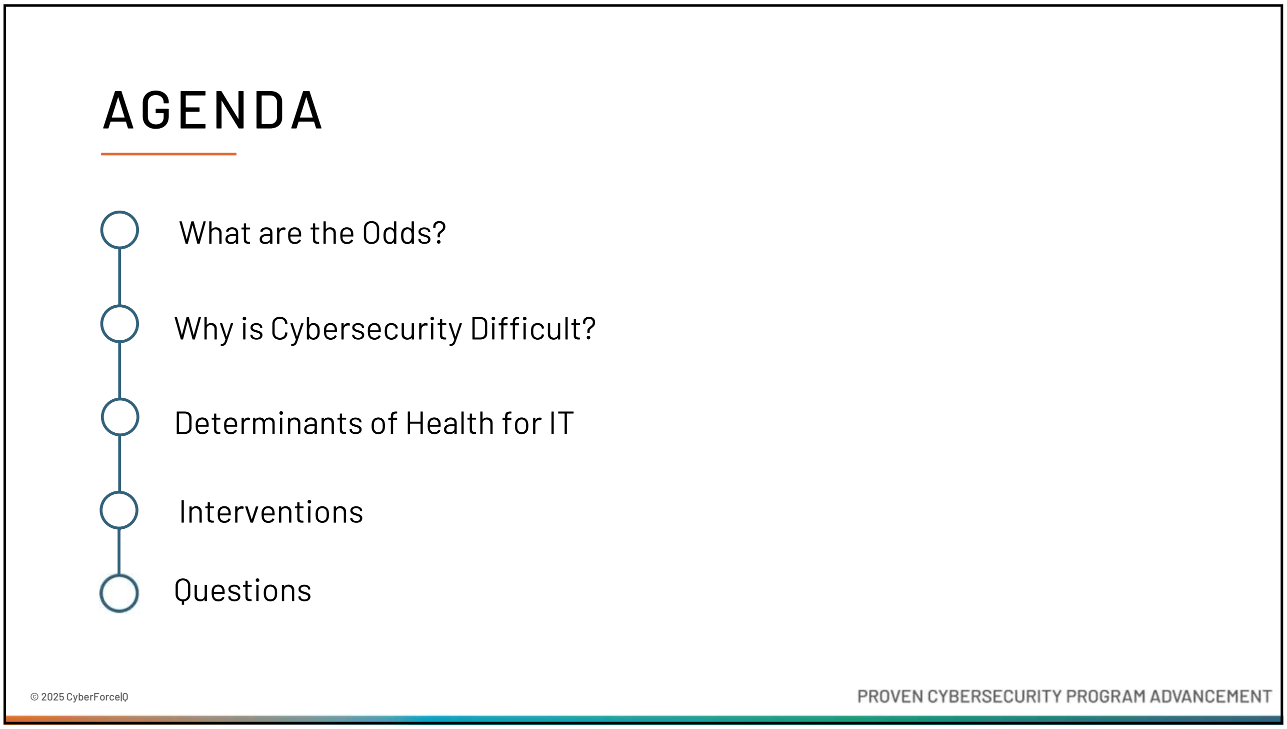
AXXESS Vesta® HHAeXchange



CYBERFORCE|Q

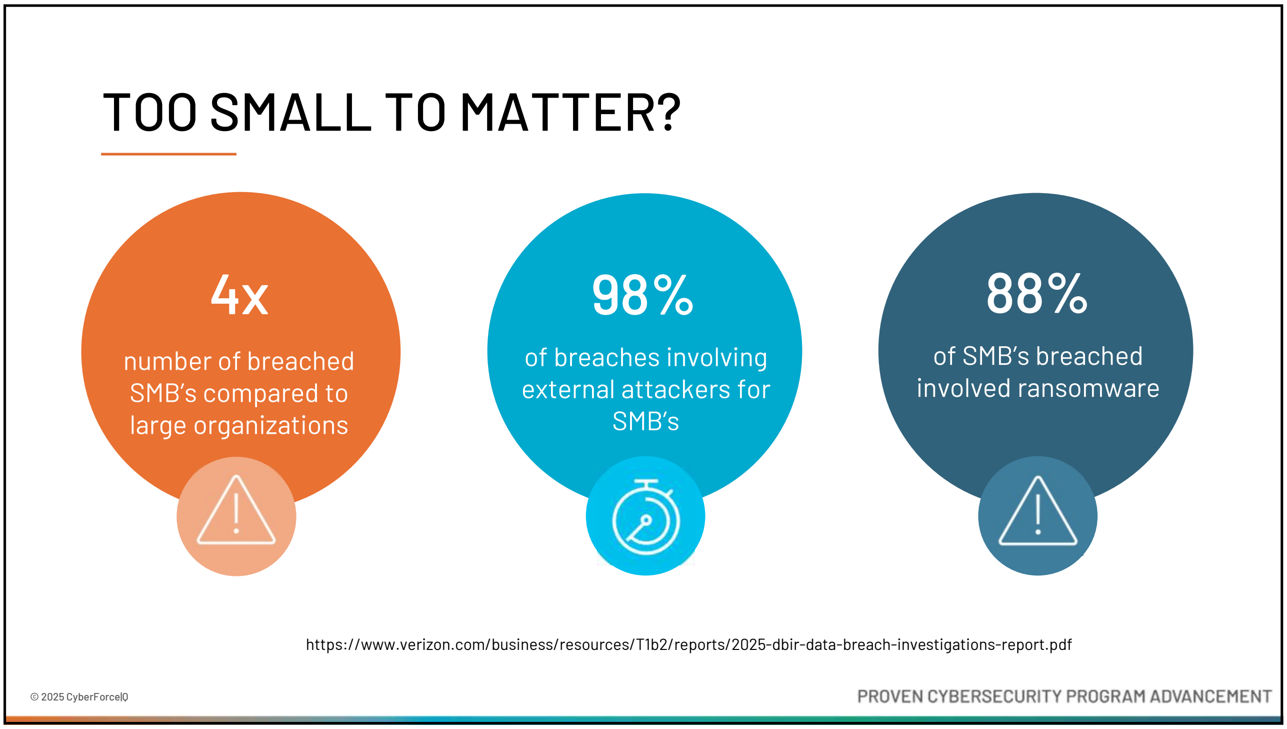
ADAPTING CLINICAL RISK MANAGEMENT FOR IT

Texas Association for Home Care & Hospice
Leading ★ Advancing ★ Advocating



AGENDA

- What are the Odds?
- Why is Cybersecurity Difficult?
- Determinants of Health for IT
- Interventions
- Questions



TOO SMALL TO MATTER?

4x

number of breached SMB's compared to large organizations

98%

of breaches involving external attackers for SMB's

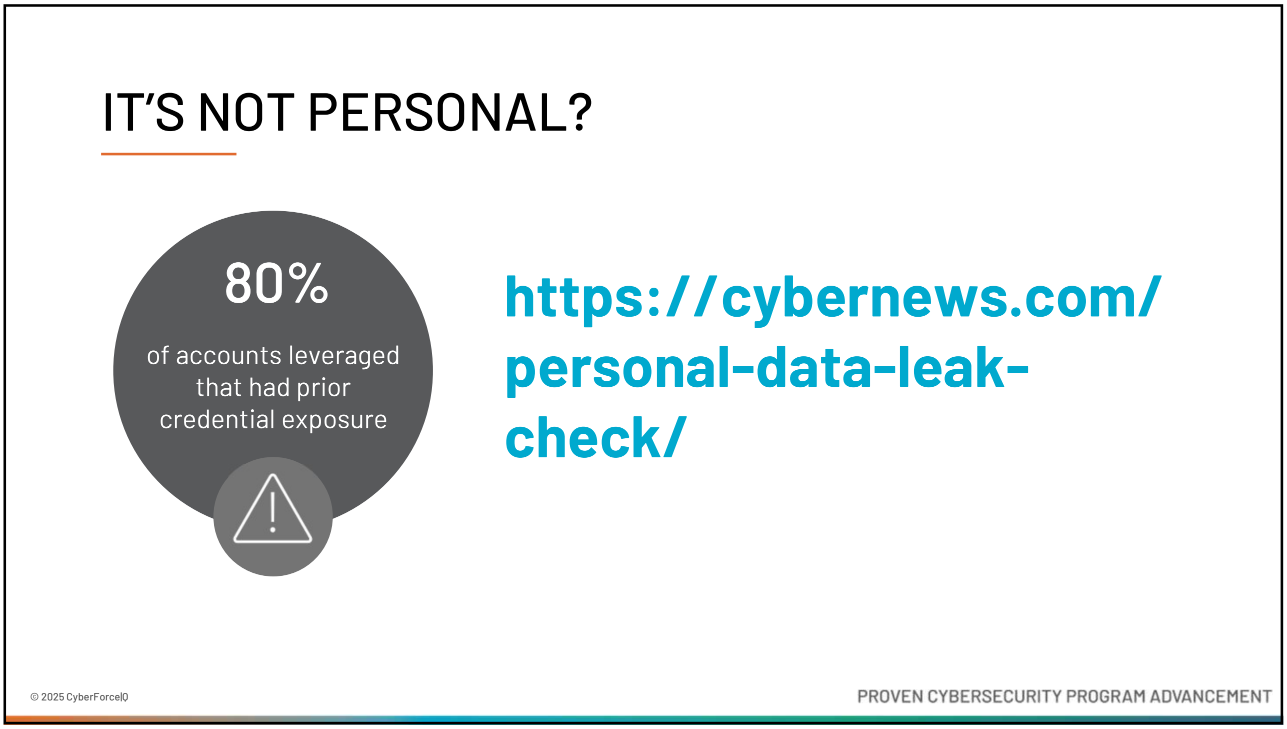
88%

of SMB's breached involved ransomware

https://www.verizon.com/business/resources/T1b2/reports/2025-dbir-data-breach-investigations-report.pdf

PROVEN CYBERSECURITY PROGRAM ADVANCEMENT

3



IT'S NOT PERSONAL?

80%

of accounts leveraged that had prior credential exposure

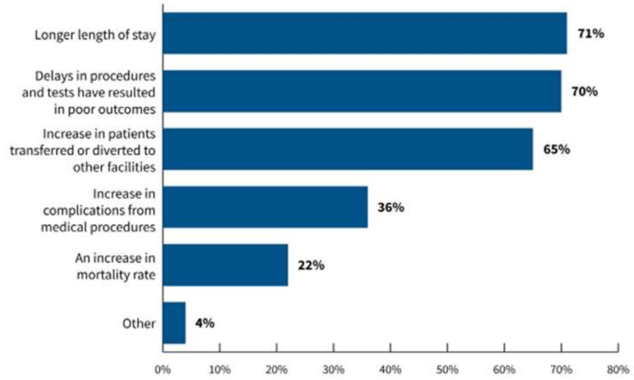
https://cybernews.com/personal-data-leak-check/

PROVEN CYBERSECURITY PROGRAM ADVANCEMENT

4

THE REAL IMPACT OF RANSOMWARE

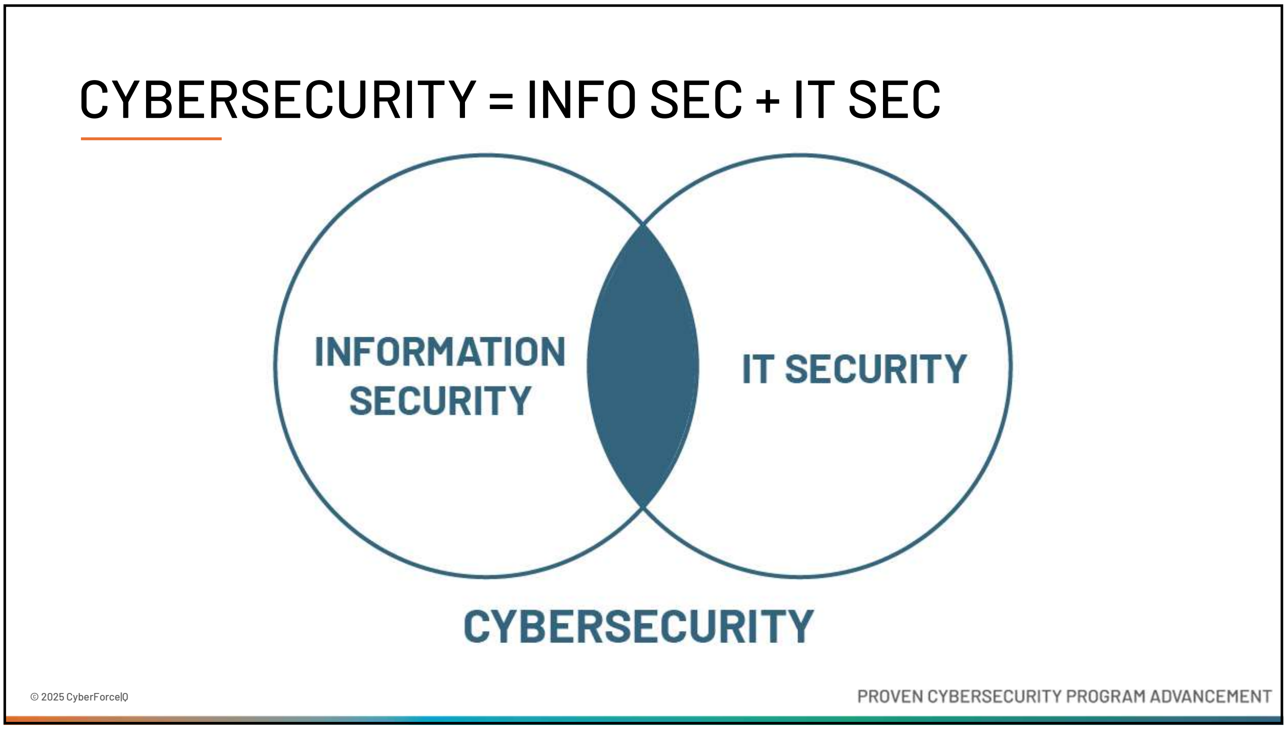
Figure 1. What impact does ransomware have on patient care?
More than one response from the 43 percent of respondents in HDOs that had a ransomware attack.



> *"The silver lining here is sometimes you have to hit rock bottom. If we're still talking about this as fines or records and not as human life and adverse patient outcomes, then we won't bring the right tools to fix this."*
>
> - **Joshua Corman**

The 405(d) Post, Volume XV (hhs.gov)

WHY IS CYBERSECURITY DIFFICULT?



CYBERSECURITY = INFO SEC + IT SEC

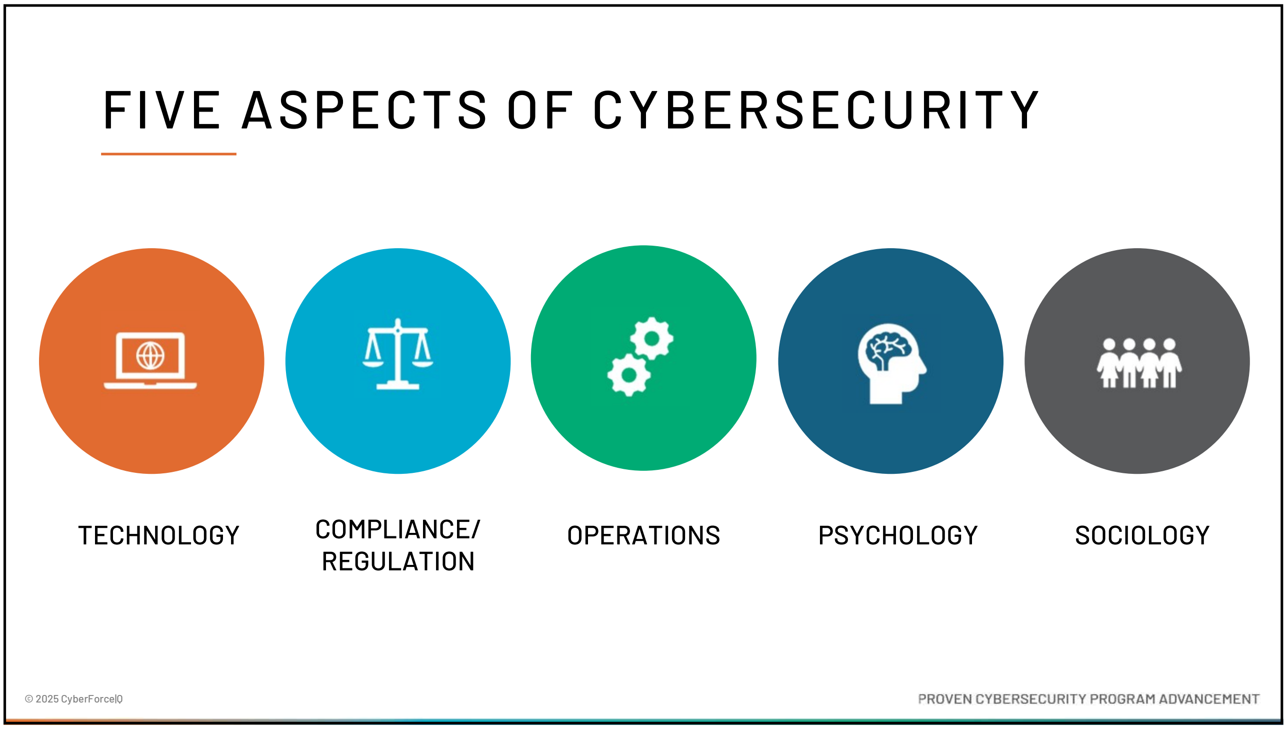
INFORMATION SECURITY

IT SECURITY

CYBERSECURITY

PROVEN CYBERSECURITY PROGRAM ADVANCEMENT

7



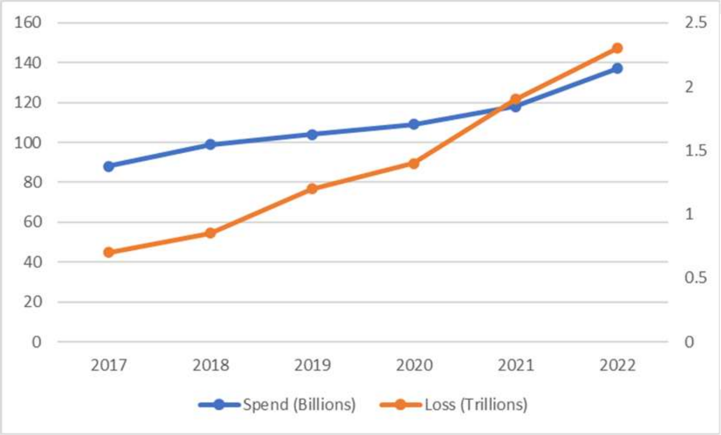
FIVE ASPECTS OF CYBERSECURITY

- TECHNOLOGY
- COMPLIANCE/ REGULATION
- OPERATIONS
- PSYCHOLOGY
- SOCIOLOGY

PROVEN CYBERSECURITY PROGRAM ADVANCEMENT

8

WHAT IF THIS WAS CLINICAL RISK?

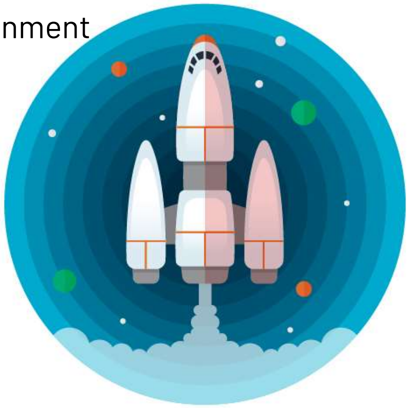


Source: Juniper Research

9

COMPLICATED VS COMPLEX SYSTEMS

- **Complicated**
  - Space Launch – 5 computer systems in closed environment
  - Structured data
- **Complex**
  - Interconnected applications
  - Open environment
  - Dynamic data
  - 3rd party integration / Semantic integration
  - Globalization
  - Hosted regionally, on-prem, and Cloud

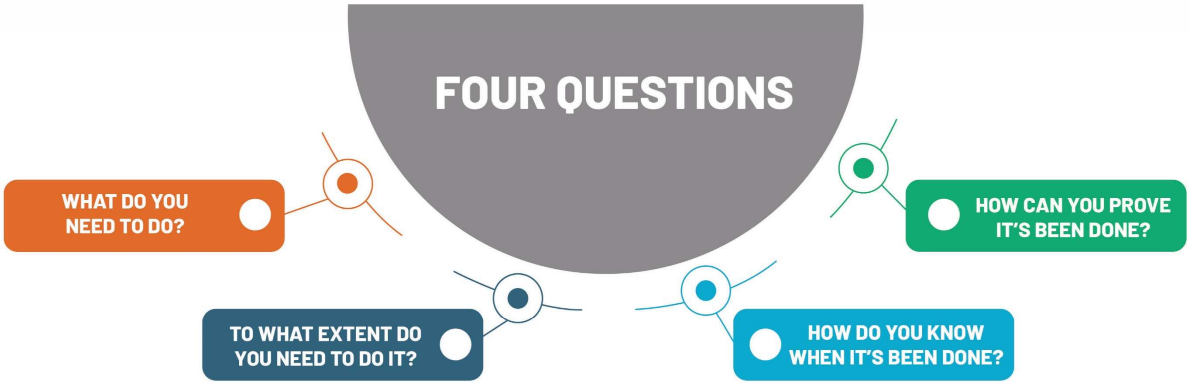


10

WHY DOES CLINICAL RISK MANAGEMENT SCALE?

11

CYBERSECURITY'S FOUR QUESTIONS



FOUR QUESTIONS

WHAT DO YOU NEED TO DO?

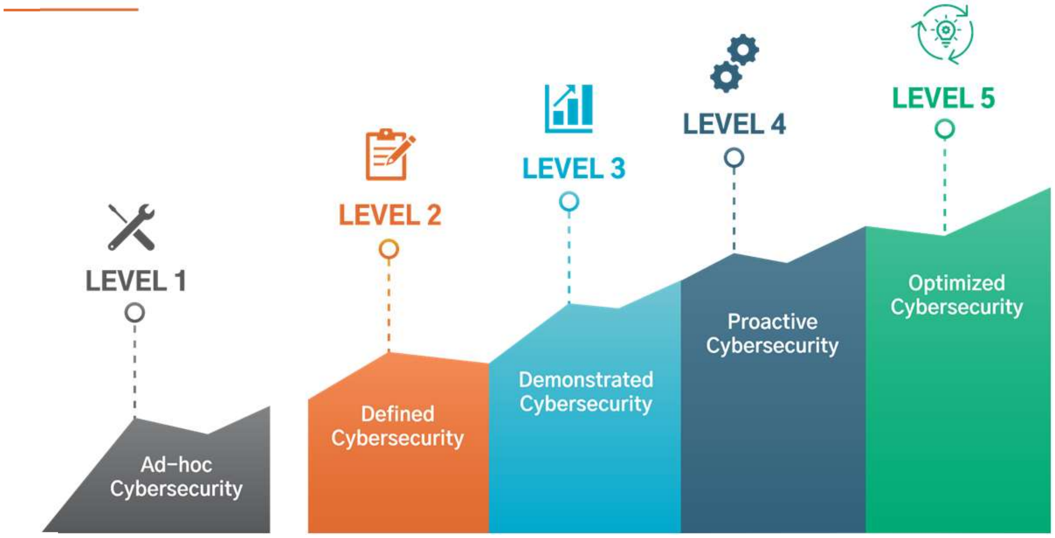
TO WHAT EXTENT DO YOU NEED TO DO IT?

HOW DO YOU KNOW WHEN IT'S BEEN DONE?

HOW CAN YOU PROVE IT'S BEEN DONE?

12

RISK IS REDUCED BY MATURITY



LEVEL 1

Ad-hoc Cybersecurity

LEVEL 2

Defined Cybersecurity

LEVEL 3

Demonstrated Cybersecurity

LEVEL 4

Proactive Cybersecurity

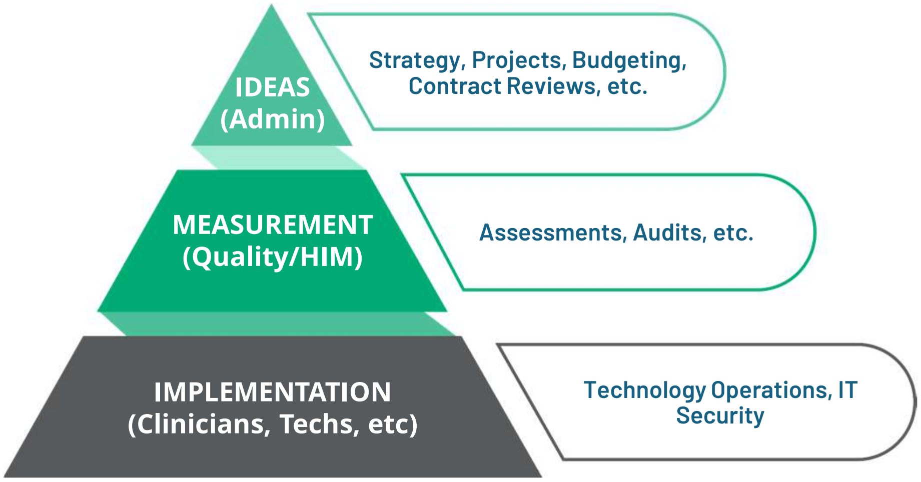
LEVEL 5

Optimized Cybersecurity

PROVEN CYBERSECURITY PROGRAM ADVANCEMENT

13

BREAKING DOWN OPERATIONAL SILOS



IDEAS (Admin)

Strategy, Projects, Budgeting, Contract Reviews, etc.

MEASUREMENT (Quality/HIM)

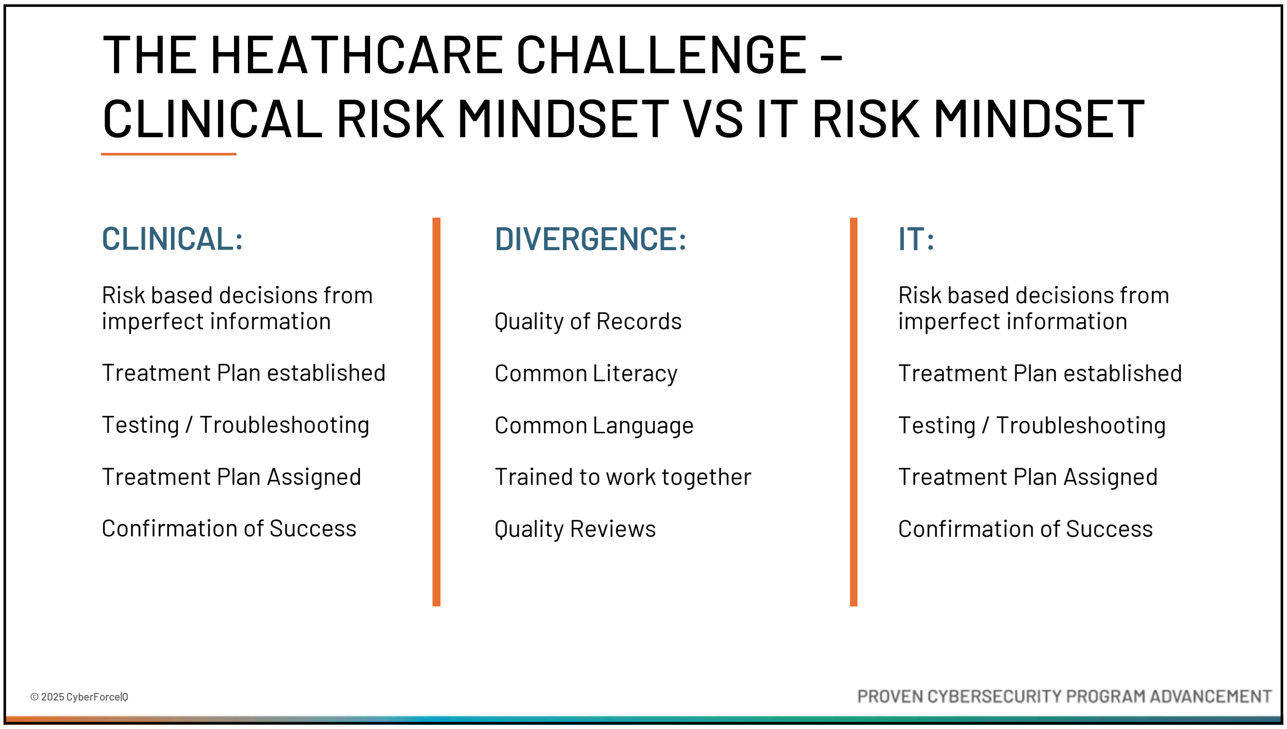
Assessments, Audits, etc.

IMPLEMENTATION (Clinicians, Techs, etc)

Technology Operations, IT Security

PROVEN CYBERSECURITY PROGRAM ADVANCEMENT

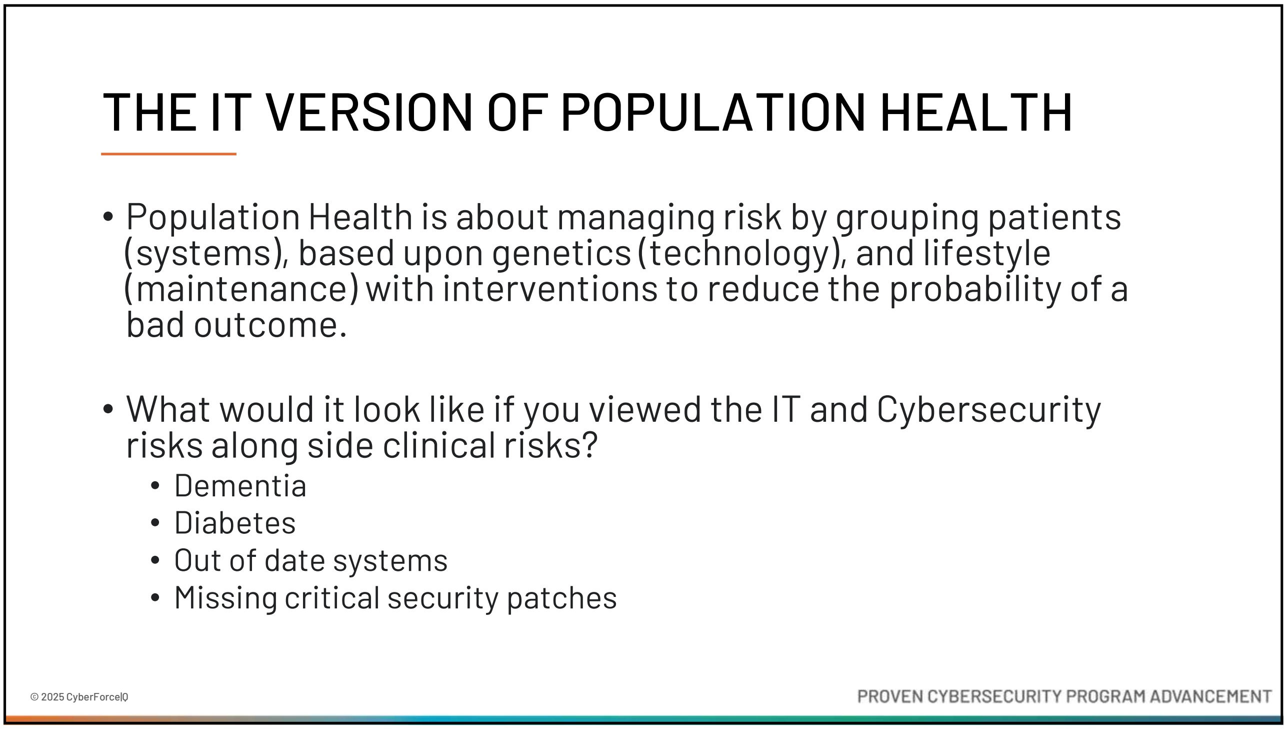
14



THE HEATHCARE CHALLENGE – CLINICAL RISK MINDSET VS IT RISK MINDSET

CLINICAL:	DIVERGENCE:	IT:
Risk based decisions from imperfect information	Quality of Records	Risk based decisions from imperfect information
Treatment Plan established	Common Literacy	Treatment Plan established
Testing / Troubleshooting	Common Language	Testing / Troubleshooting
Treatment Plan Assigned	Trained to work together	Treatment Plan Assigned
Confirmation of Success	Quality Reviews	Confirmation of Success

15



THE IT VERSION OF POPULATION HEALTH

- Population Health is about managing risk by grouping patients (systems), based upon genetics (technology), and lifestyle (maintenance) with interventions to reduce the probability of a bad outcome.
- What would it look like if you viewed the IT and Cybersecurity risks along side clinical risks?
  - Dementia
  - Diabetes
  - Out of date systems
  - Missing critical security patches

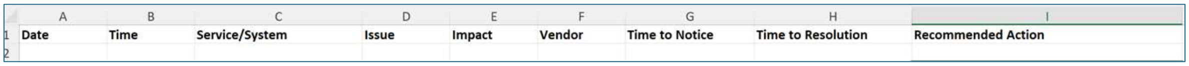
16

DETERMINANTS OF HEALTH FOR IT

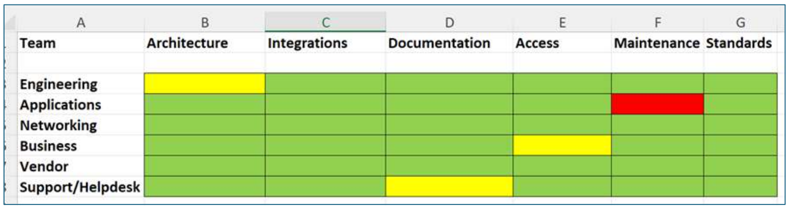
- The determinants of health are the economic and social conditions that influence individual and group differences in health status.

- Some of the IT Social Determinants of Health include:
  - The Department involved
  - The people involved
  - The technology used
  - Who manages the system

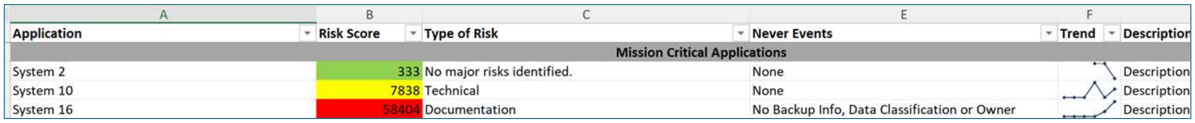
SCORECARD SAMPLES



Date	Time	Service/System	Issue	Impact	Vendor	Time to Notice	Time to Resolution	Recommended Action



Team	Architecture	Integrations	Documentation	Access	Maintenance	Standards
Engineering	🟨	🟩	🟩	🟩	🟩	🟩
Applications	🟩	🟩	🟩	🟩	🟥	🟩
Networking	🟩	🟩	🟩	🟩	🟩	🟩
Business	🟩	🟩	🟩	🟨	🟩	🟩
Vendor	🟩	🟩	🟩	🟩	🟩	🟩
Support/Helpdesk	🟩	🟩	🟨	🟩	🟩	🟩



Application	Risk Score	Type of Risk	Never Events	Trend	Description
Mission Critical Applications					
System 2	333	No major risks identified.	None		Description
System 10	7838	Technical	None		Description
System 16	58404	Documentation	No Backup Info, Data Classification or Owner		Description

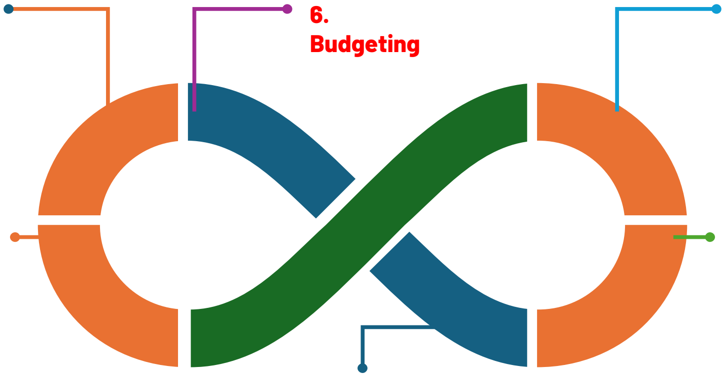
WHEN TO HAVE AN INTERVENTION?

- There are six common points where an intervention can organically happen. Any of these are good places to start:
  - Contract purchase or renewal
  - Scoping or Project implementation/management
  - Implementation
  - Maintenance or Upgrades
  - Strategic Planning
  - Budgeting

PROVEN CYBERSECURITY PROGRAM ADVANCEMENT

19

COMMON INTERVENTION OPPORTUNITIES



1. Purchasing/Contract Renewal (Vendor Risk Assessment)

6. Budgeting

3. Implementation

2. Scoping/Project Management

4. Maintenance/ Upgrades

5. Strategic Planning

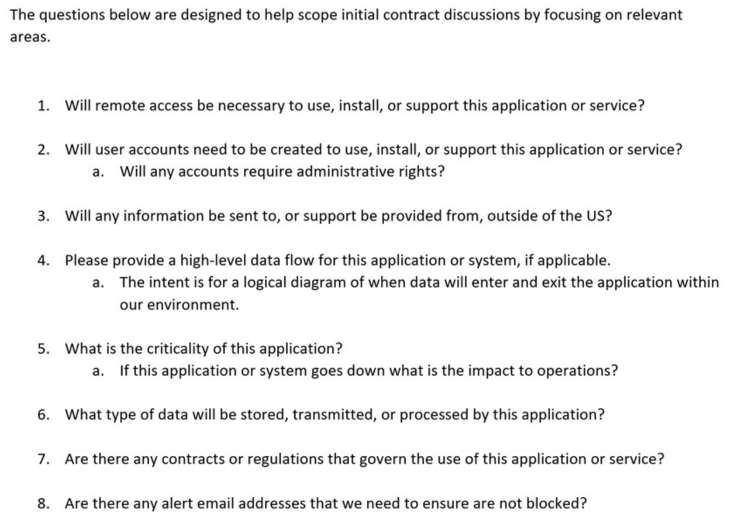
PROVEN CYBERSECURITY PROGRAM ADVANCEMENT

20

VENDOR SELECTION

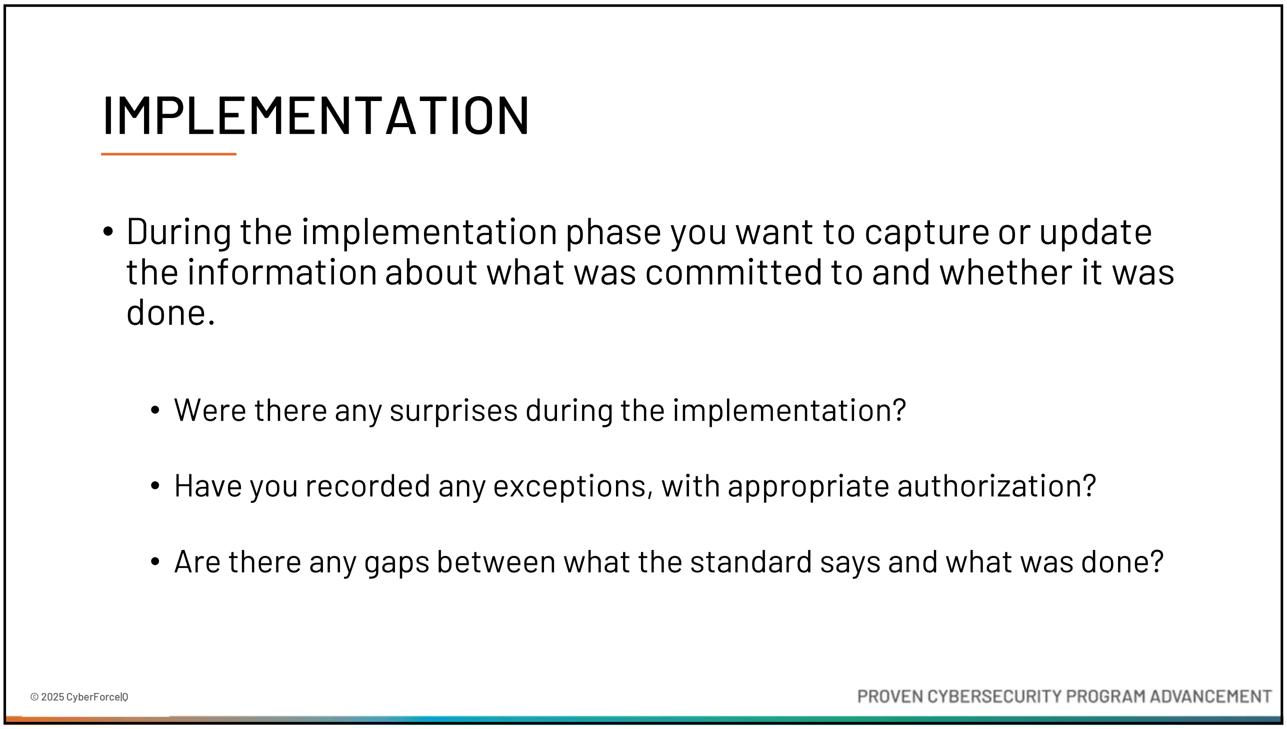
- The first part to a new system is finding suitable vendors. Some things to consider during this step are:
  - What are the standards a vendor, service, or tool must meet?
    - Do they need to integrate with AD Auth? What redundancy is required?
  - When should IT be involved with contract reviews?
  - How can you empower the contracting/supply chain group to take more ownership of this?

VENDOR SCOPING QUESTIONS



The questions below are designed to help scope initial contract discussions by focusing on relevant areas.

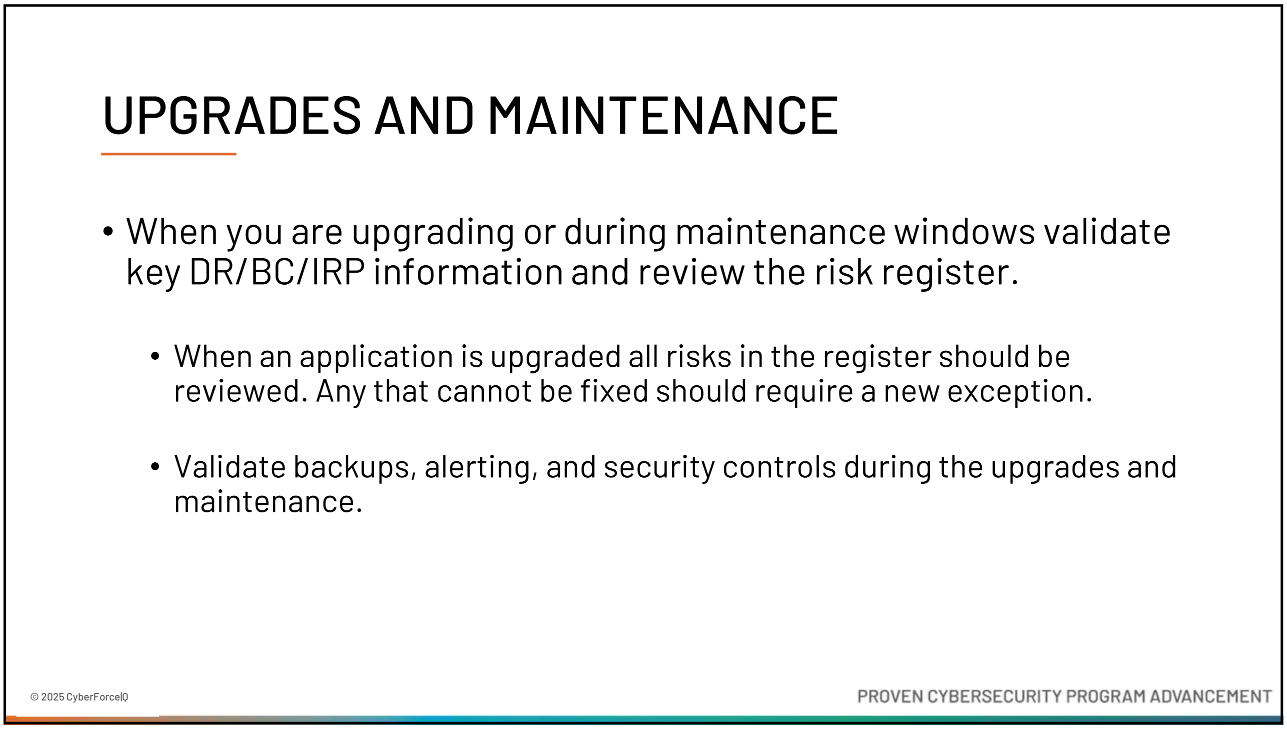
1. Will remote access be necessary to use, install, or support this application or service?
2. Will user accounts need to be created to use, install, or support this application or service?
   a. Will any accounts require administrative rights?
3. Will any information be sent to, or support be provided from, outside of the US?
4. Please provide a high-level data flow for this application or system, if applicable.
   a. The intent is for a logical diagram of when data will enter and exit the application within our environment.
5. What is the criticality of this application?
   a. If this application or system goes down what is the impact to operations?
6. What type of data will be stored, transmitted, or processed by this application?
7. Are there any contracts or regulations that govern the use of this application or service?
8. Are there any alert email addresses that we need to ensure are not blocked?



IMPLEMENTATION

- During the implementation phase you want to capture or update the information about what was committed to and whether it was done.
  - Were there any surprises during the implementation?
  - Have you recorded any exceptions, with appropriate authorization?
  - Are there any gaps between what the standard says and what was done?

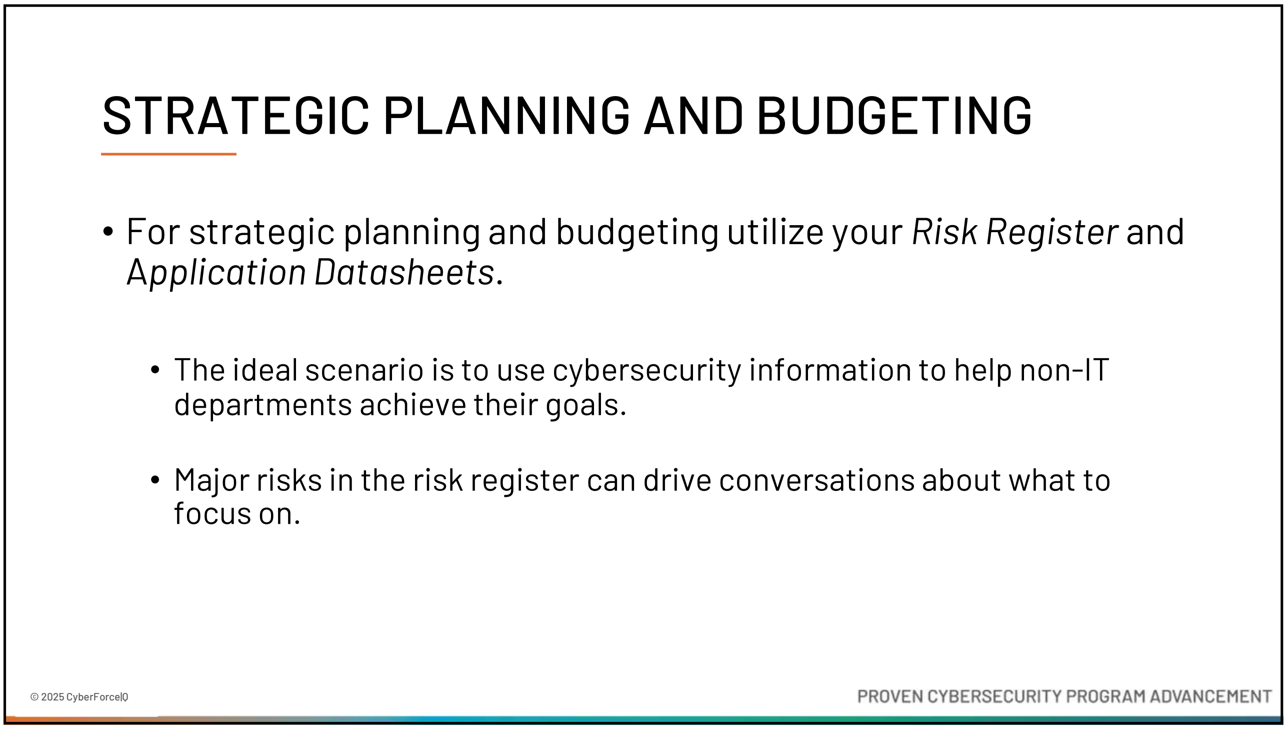
23



UPGRADES AND MAINTENANCE

- When you are upgrading or during maintenance windows validate key DR/BC/IRP information and review the risk register.
  - When an application is upgraded all risks in the register should be reviewed. Any that cannot be fixed should require a new exception.
  - Validate backups, alerting, and security controls during the upgrades and maintenance.

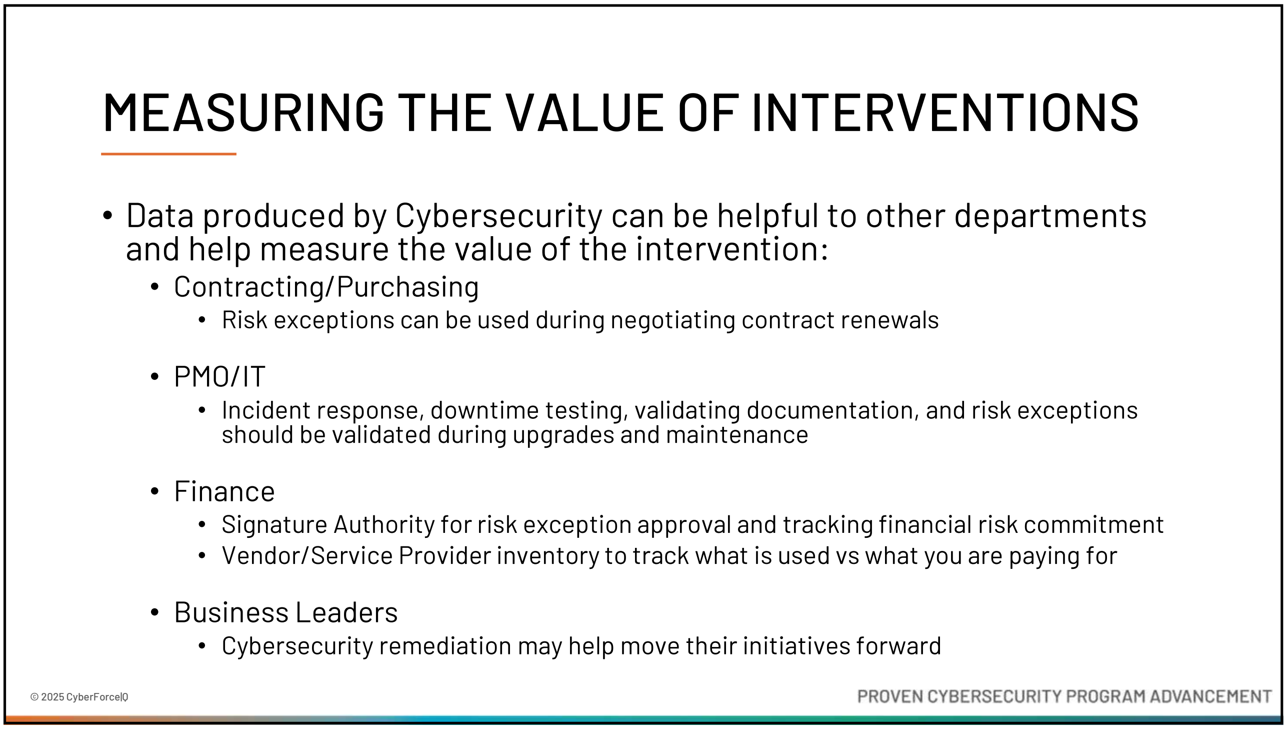
24



STRATEGIC PLANNING AND BUDGETING

- For strategic planning and budgeting utilize your *Risk Register* and *Application Datasheets*.
  - The ideal scenario is to use cybersecurity information to help non-IT departments achieve their goals.
  - Major risks in the risk register can drive conversations about what to focus on.

PROVEN CYBERSECURITY PROGRAM ADVANCEMENT



MEASURING THE VALUE OF INTERVENTIONS

- Data produced by Cybersecurity can be helpful to other departments and help measure the value of the intervention:
  - Contracting/Purchasing
    - Risk exceptions can be used during negotiating contract renewals
  - PMO/IT
    - Incident response, downtime testing, validating documentation, and risk exceptions should be validated during upgrades and maintenance
  - Finance
    - Signature Authority for risk exception approval and tracking financial risk commitment
    - Vendor/Service Provider inventory to track what is used vs what you are paying for
  - Business Leaders
    - Cybersecurity remediation may help move their initiatives forward

PROVEN CYBERSECURITY PROGRAM ADVANCEMENT

HOW TO CONTACT US WITH QUESTIONS

- Wayne Pierce
  wpierce@cyberforceq.com – (248) 837–1417
  linkedin.com/in/Pierce

- Brad Maughan
  bmaughan@cyberforceq.com - (214) 914-5183
  linkedin.com/in/bradmaughanhcispp454

QUESTIONS?