



Cybersecurity Lifecycle

© 2023 CyberForce|Q

25+ YEARS OF CYBERSECURITY INNOVATION



AGENDA

- Why is Cybersecurity Difficult?
- Step 1: Determine Your Risk Level
- Step 2: Inventory Application Processes for Risk Alignment
- Step 3: Inject Cybersecurity Information into Operational Processes?
- New Application/Service Walkthrough
- Questions

© 2022 CyberForce|Q

25+ YEARS OF CYBERSECURITY INNOVATION



WHO WE ARE

COLLECTIVE

Malicious actors are working together to find new ways to attack organizations. To combat these threats, we partner with our clients, sharing tactical information between entities, to break down silos and make everyone stronger.

CONTINUOUS

With cybercriminals adapting every day, cybersecurity programs need to continuously advance in order to combat threats. We focus on continuous improvement in everything we do to make our customers stronger.



EVIDENCE-BASED

We provide clients with proven results, using quantifiable measurement that demonstrates evidence-based proof of your cybersecurity progress, helping you advance your security posture.

CUSTOMIZED

We know every organization is unique, which is why our team works one-on-one with you, to determine the best solutions for your specific needs, taking into account your industry, goals, and organization's technologies and processes.

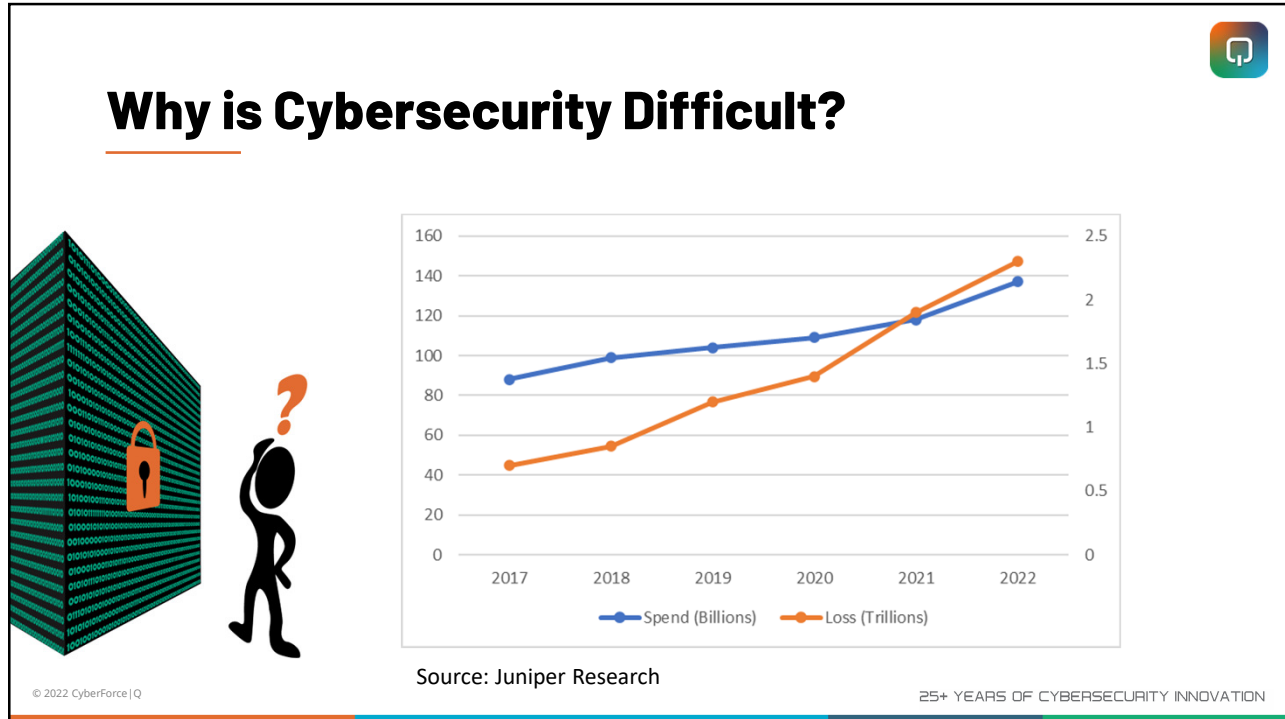


PARTNERSHIPS



Minnesota Hospital Association
Endorsed Business Partner





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

© 2022 CyberForce|Q

25+ YEARS OF CYBERSECURITY INNOVATION



Organization Considerations



MITIGATING RISK



POLICY & PROCEDURE COMPLIANCE

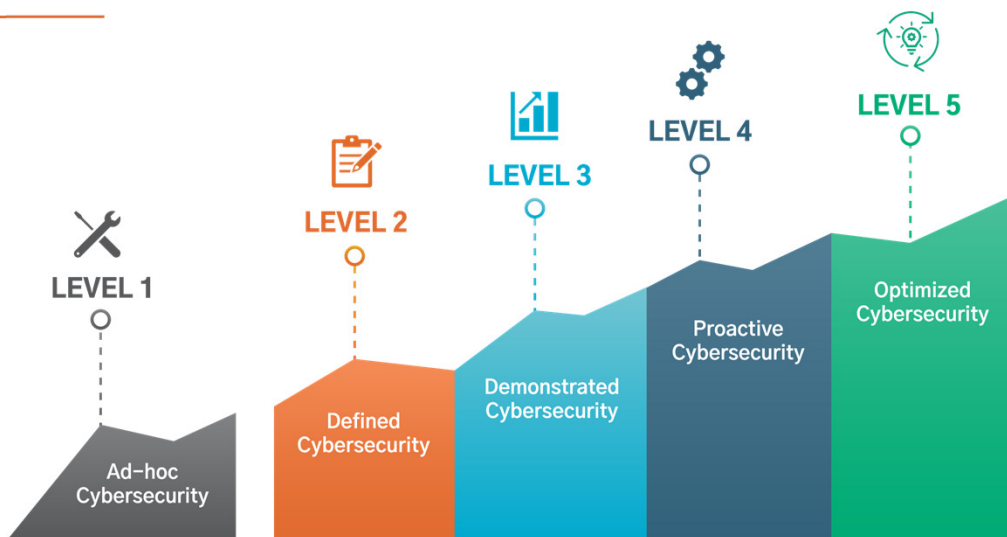


INSURANCE PREMIUMS

What is the business problem you are attempting to solve?

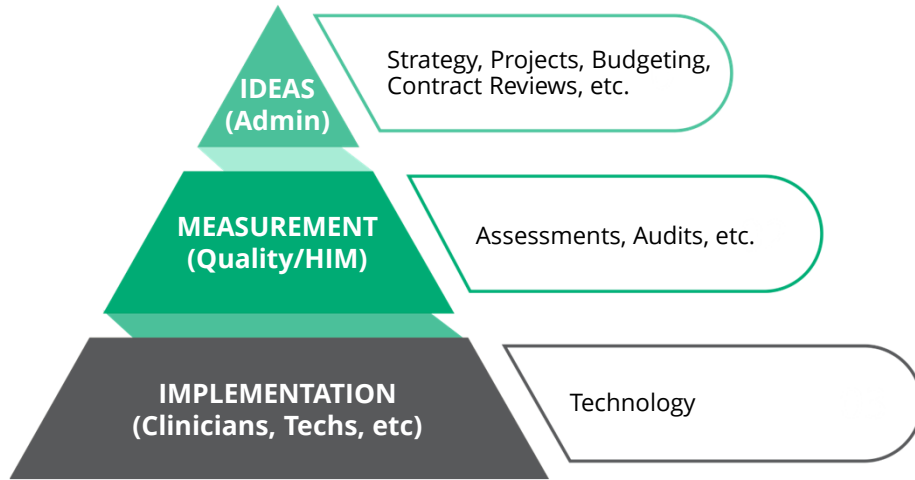


PROGRESSION TO OPTIMIZATION





Breaking Down Operational Silos



© 2022 CyberForce|Q

25+ YEARS OF CYBERSECURITY INNOVATION

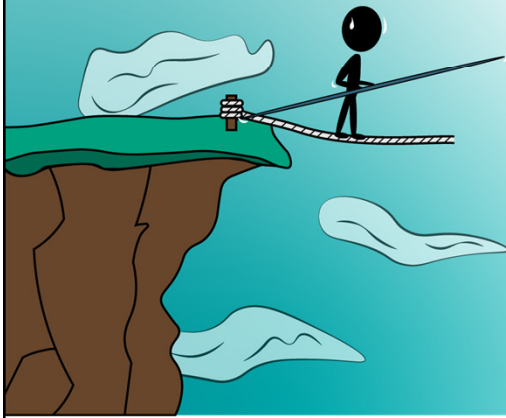


Step 1: Determine your risk tolerance



25+ YEARS OF CYBERSECURITY INNOVATION

Risk Tolerance



- Variant system and user behavior
- Pure Risk vs. Speculative Risk
- “More things can happen than will happen” -Dimson
- Probability of threat vs. probability of significant loss

25+ YEARS OF CYBERSECURITY INNOVATION

Cybersecurity Risk is Reduced by Maturity




© 2022 CyberForce|Q

25+ YEARS OF CYBERSECURITY INNOVATION



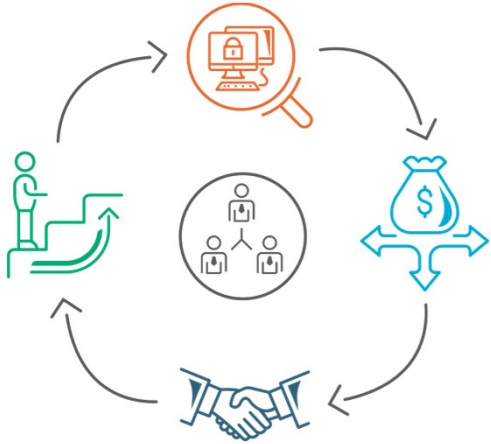
Step 2: Inventory operational processes for risk alignment

25+ YEARS OF CYBERSECURITY INNOVATION



Building Momentum & Reducing Friction

1. Evaluate and prioritize cybersecurity needs
2. Where should the next dollar of effort be spent
3. Align cybersecurity with operational processes
4. Each unit of work builds up to next unit work



© 2022 CyberForce|Q

25+ YEARS OF CYBERSECURITY INNOVATION

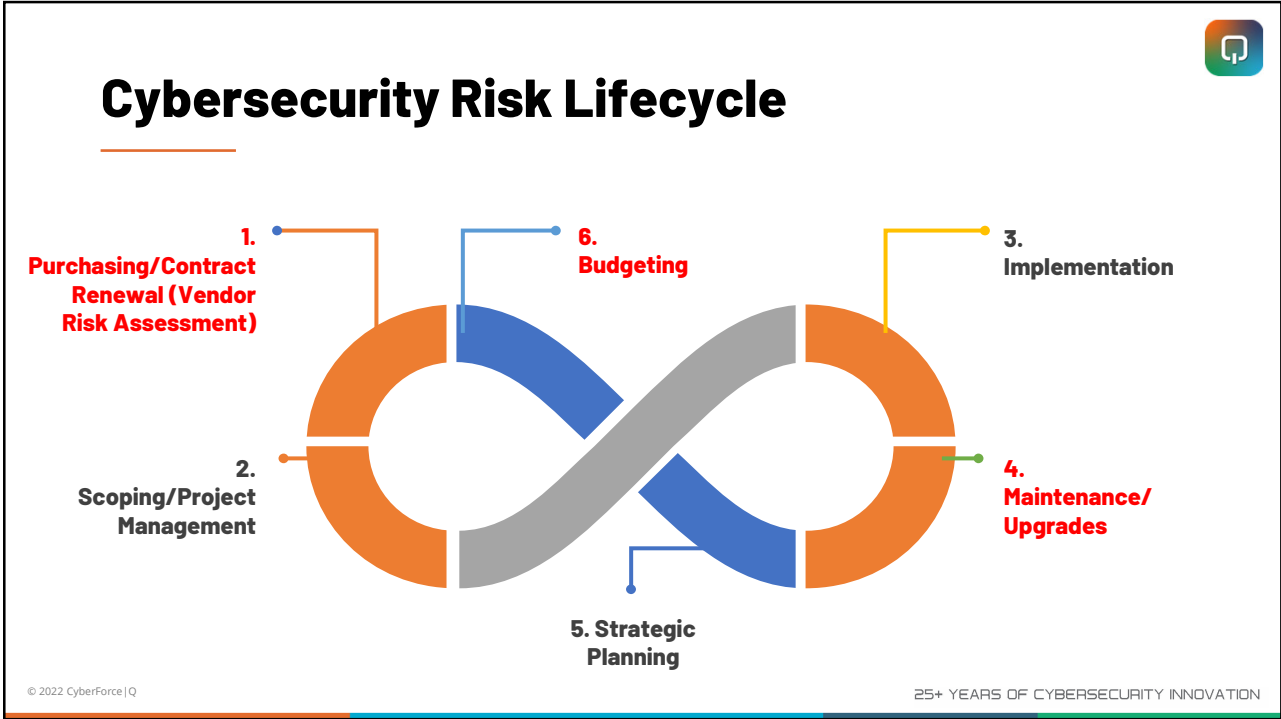
How can IT data improve operations?

- 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



Step 3: Inject cybersecurity information into operational processes

25+ YEARS OF CYBERSECURITY INNOVATION



New Application/Service Walkthrough

© 2022 CyberForce|Q 25+ YEARS OF CYBERSECURITY INNOVATION



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 Selection - Documents

- Some documents that will help with this process:
 - *Scoping Questionnaire* – Helps determine when IT needs to be engaged.
 - *Minimum Security Standards* – Core IT standards by Data Classification and System Criticality to help with scoping.
 - *3rd Party Risk Assessment* – Assessment to determine if the vendor's own environment is suitable.



Vendor Contract 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?

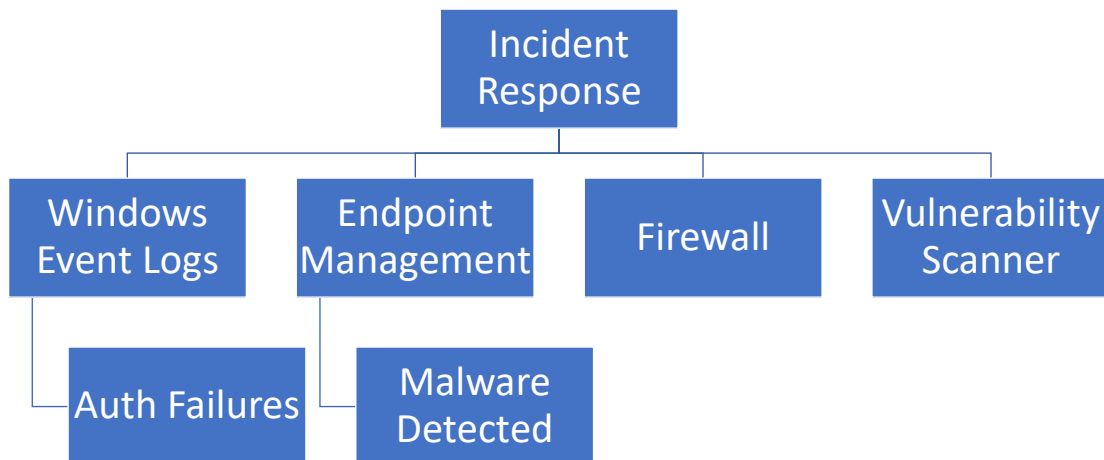


Implementation - Documents

- During the implementation phase you want to capture or update the following information:
 - *BC/DR/IRP* – How do you respond to an outage for this system?
 - *Risk Register* – Are there any accepted exceptions during the initial purchase that need to be accounted for?
 - *Alerting/Monitoring* – What logs should be monitored and alerted on?
 - *Application Datasheet* – What information is core to how this application operates, needs to be supported, or is recovered?



How does the new app fit in your audit flow?





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.



Upgrades and Maintenance - Documents

- Two important documents during upgrades and maintenance are the *Risk Register* and the *Application Datasheet*.
 - The *Risk Register* should contain all of the approved exceptions.
 - An *Application Datasheet* should contain key information for supporting this system. That includes top issues, application-level security controls, logs configured to monitor, and recovery information; among other things. Validate that these are still accurate and appropriate for the system post-upgrade.



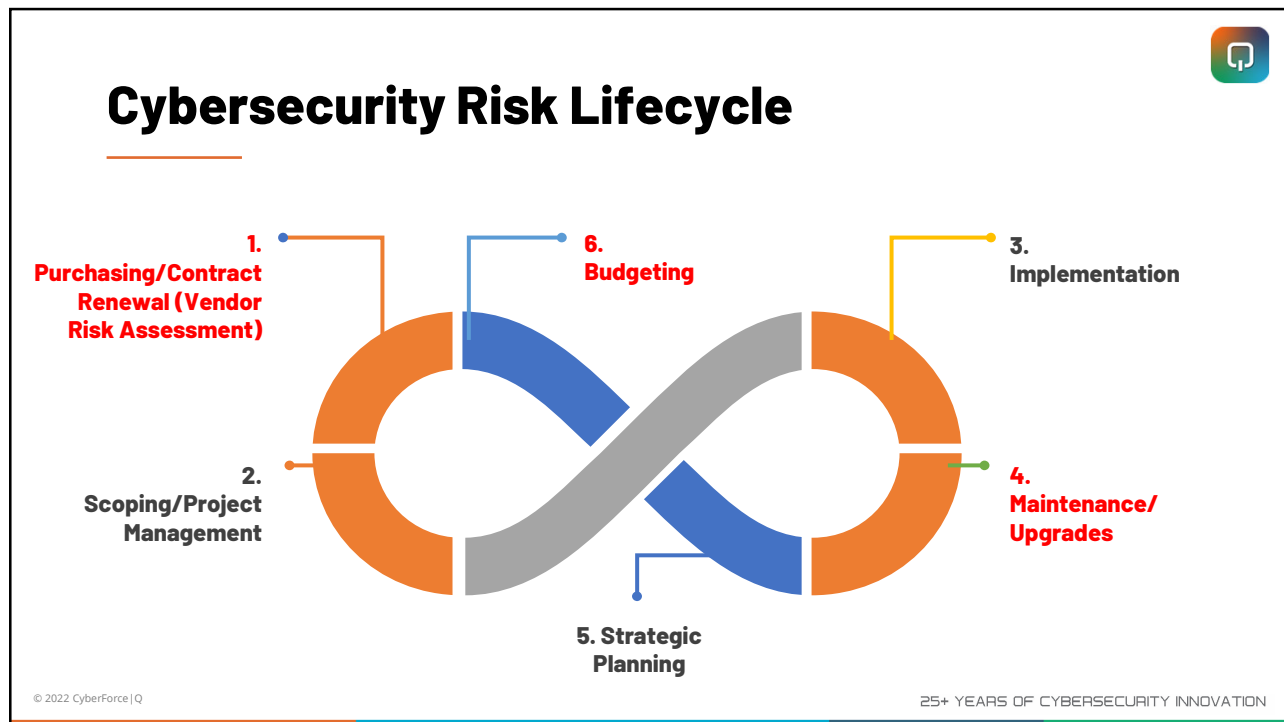
Sample Risk Register

A	B	C	D	E	F	G	H	I
ID	Date raised	Risk description	Likelihood of the risk occurring	Impact if the risk occurs	Severity <i>Rating based on impact & likelihood.</i>	Owner <i>Person who will manage the risk.</i>	Mitigating action <i>Actions to mitigate the risk e.g. reduce the likelihood.</i>	Contingent action <i>Action to be taken if happens.</i>
1	[enter date]	Project purpose and need is not well-defined.	Medium	High	High	Project Sponsor	Complete a business case if not already provided and ensure purpose is well defined on Project Charter and PID.	Escalate to the Project Sponsor with an assessment of runaway costs/ending project.



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.



How to contact us with questions

- Brad Maughan
bmaughan@cyberforceq.com - (214) 914-5185
[linkedin.com/in/bradmaughanhcispp454](https://www.linkedin.com/in/bradmaughanhcispp454)
- Wayne Pierce
wpierce@cyberforceq.com - (248) 837-1417
[linkedin.com/in/Pierce](https://www.linkedin.com/in/Pierce)

© 2022 CyberForce|Q

25+ YEARS OF CYBERSECURITY INNOVATION



Questions?