Building a Cyber Intelligence Driven Risk (CI-DR) Program

HOW TO INCORPORATE CYBER INTO RISK MANAGEMENT PROGRAMS

Why are we here today?

Building a Cyber Intelligence-Driven Risk Program

- Why do organizations fail to respond and react appropriately to emerging cyber threats?
- What is missing for many small-to-midsized organizations, and why is a Cyber Intelligence driven risk program valuable?
- How can Managed Service Providers, Technology, and Information Security leaders within SMB markets build a program that can quickly recapture costs and poor decisions?

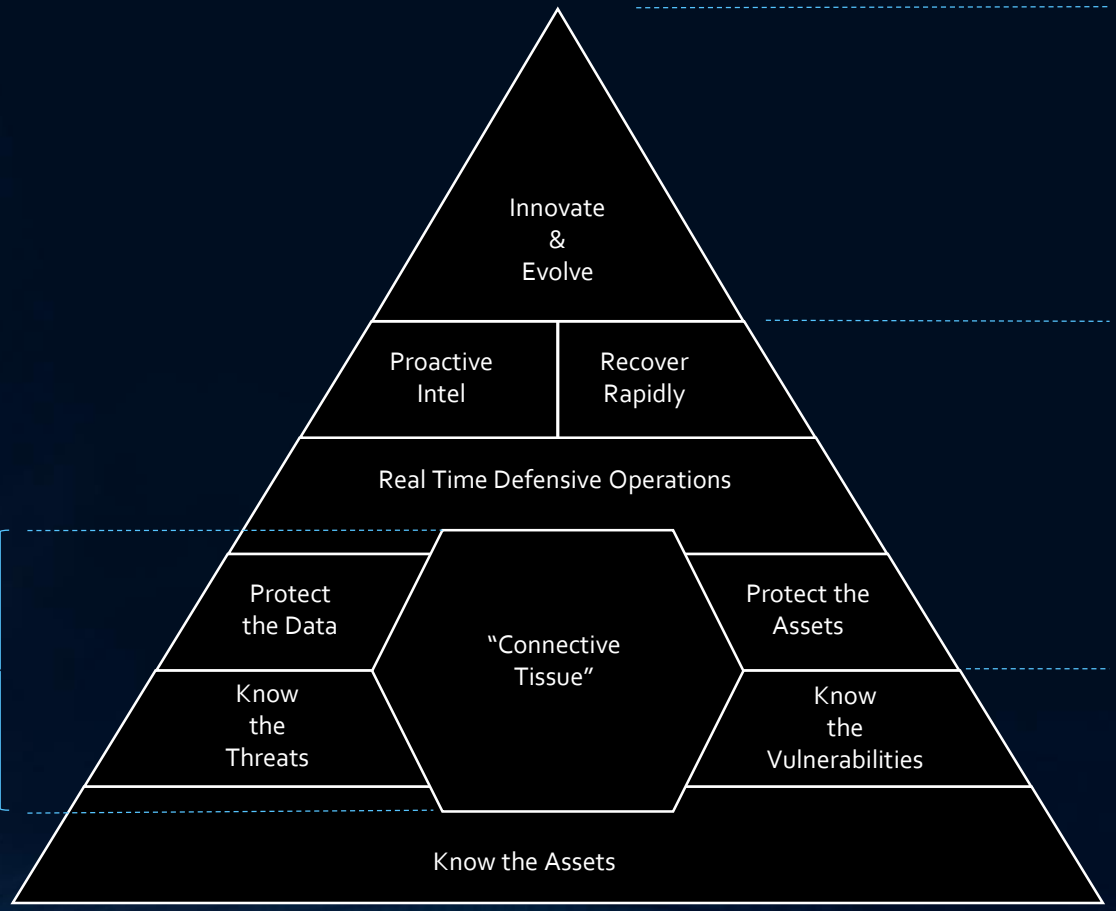
What can a CI-DR program do?

- Provides business and technology leaders with better decisions
  - *Breach Discovery resulted in a $350 million reduction in the purchase price paid by Verizon, with Yahoo! required to pay a $35 million penalty to settle securities fraud charges alleged by the U.S. Securities and Exchange Commission (SEC) and an additional $80 million to settle securities lawsuits brought by unhappy shareholders. - Forbes*
- Provides Risk Management functions with data points
  - *"Operational risk" related to cybersecurity is elevated due to sophistication of cyber threats, and pervasive technology vulnerabilities. - OCC National Risk Committee*
- Provides the organization decision points in meeting strategic business objectives
  - *"The consumer does not care how much you know, just tell them what is important." – Frank Watanabe, 15 Intelligence Axioms*
- Reduces overall risks and directs technology and human resources
  - *Google Cloud vs Azure vs AWS, etc. What is the cost in fines will we have to pay if there is an event?*

CTIP vs CI-DR

- Cyber Threat Intelligence program is tactical level, focused on technology, TTPs, and IOCs
- Cyber Intelligence Driven Risk is a strategic level, focused on business outcomes, reducing organizational risks, and generating decision support structures

Maslow's Hierarchy of CI-DR



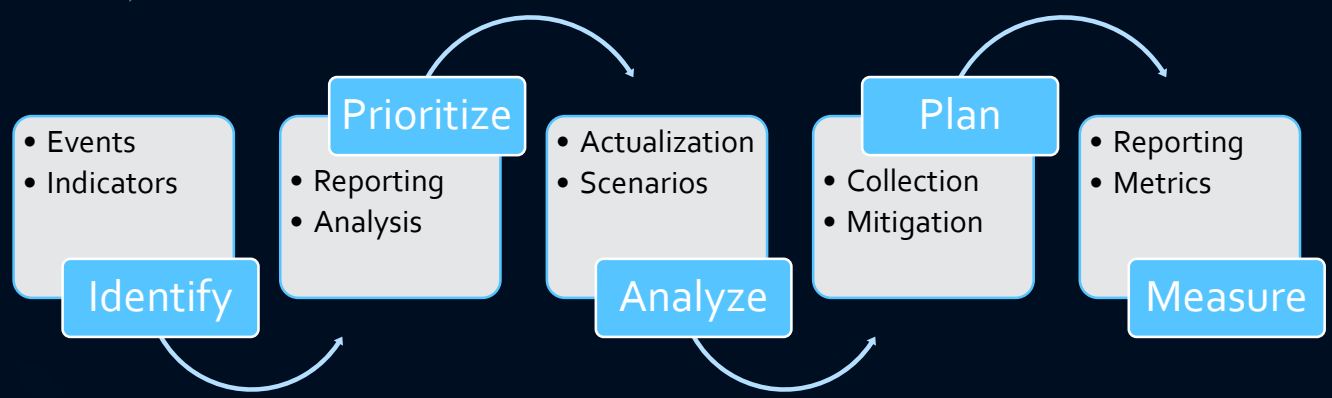
Advanced Mechanisms to Ensure Continued Relevance of Program

Enhanced Capabilities Needed to Reduce Risk (Residual Risk?)

Foundational Capabilities Needed to Measure Risk (Inherent Risk?)

Management & Execution of Overall Program

Intelligence Workflow



Overall functional design aligned to NICE

Governance
Strategy & Operating Model
Policies & Procedures
Training & Awareness
Metrics & Reporting

Information Risk Management
Asset Risk Assessment
Third Party Risk Assessment
Policy Exception & Change Management
Audit & Compliance Interaction
Independent Risk Assessment

Security Assurance
Vulnerability Management
Standard & Architecture
Application Security
Secure Coding & Development
Data Risk Assessment
Data Loss Prevention Oversight

Security Operations Oversight
Identity & Access Management Oversight
SOC/SIEM Oversight
Infrastructure Security Operations
Security Testing
Physical & Environmental Security
Digital Continuity of Operations

Intelligence & Response
Incident & Crisis Management
Coordination & Intelligence
Cyber & Behavioral Analytics
Forensics
eDiscovery

Cyber functional Capabilities for CI-DR

Governance
Strategy & Operating Model
Policies & Procedures
Training & Awareness
Metrics & Reporting

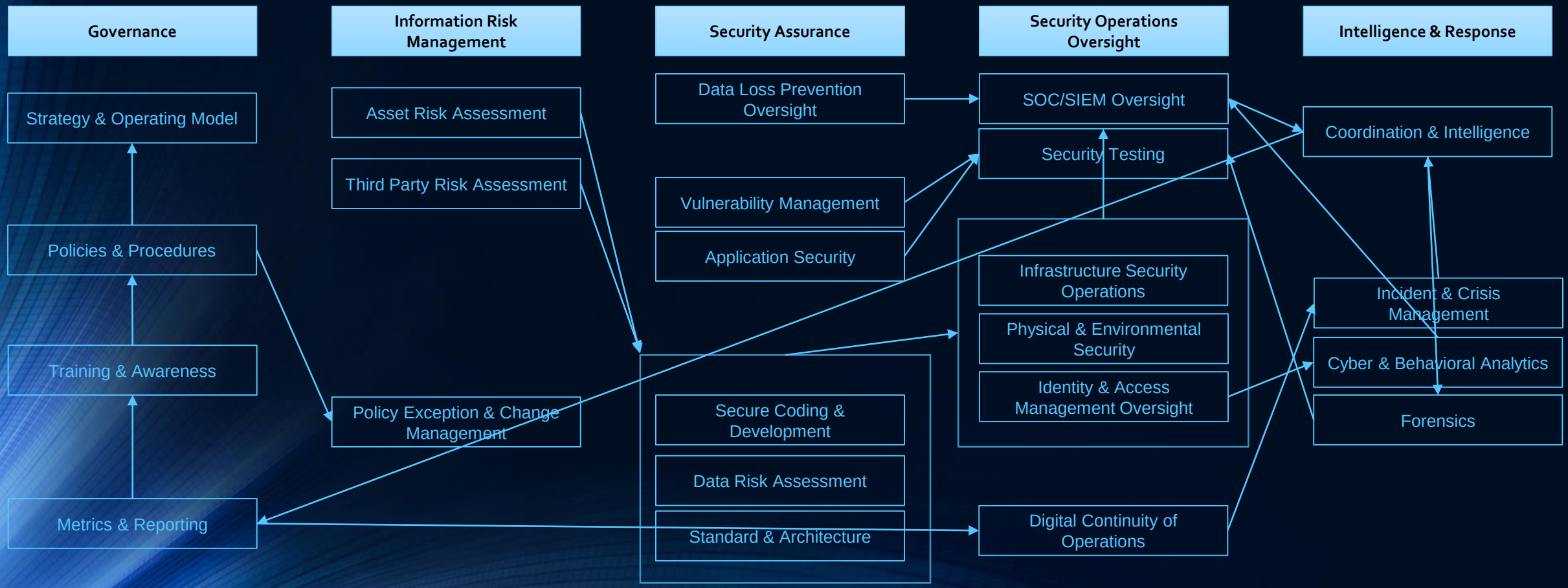
Information Risk Management
Asset Risk Assessment
Third Party Risk Assessment
Policy Exception & Change Management

Security Assurance
Vulnerability Management
Standard & Architecture
Application Security
Secure Coding & Development
Data Risk Assessment
Data Loss Prevention Oversight

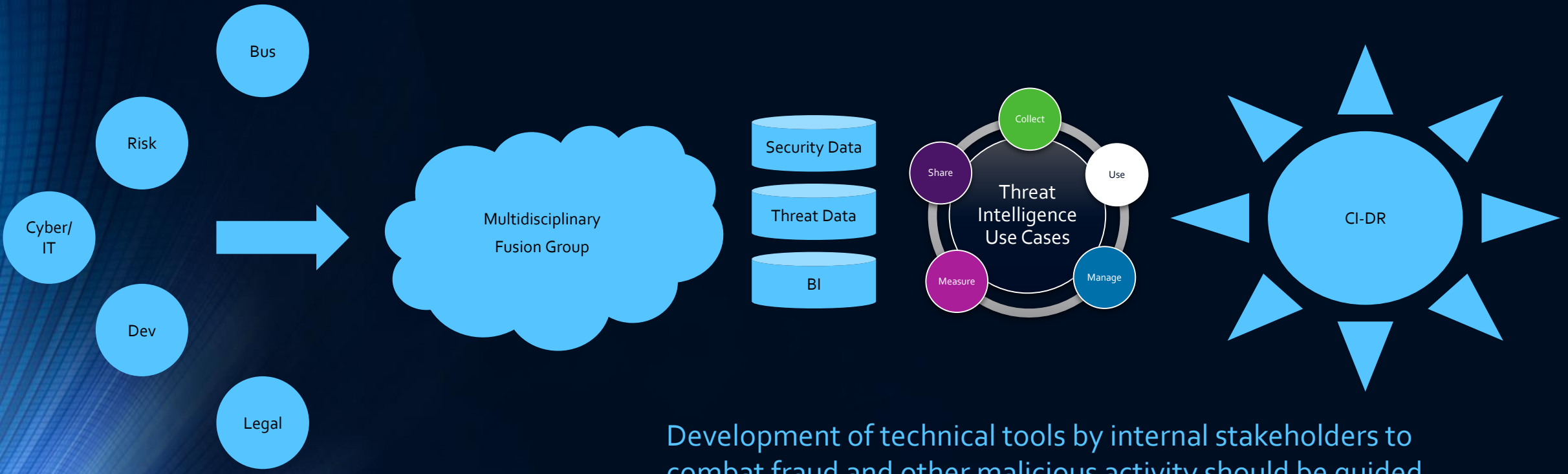
Security Operations Oversight
Identity & Access Management Oversight
SOC/SIEM Oversight
Infrastructure Security Operations
Security Testing
Physical & Environmental Security
Digital Continuity of Operations

Intelligence & Response
Incident & Crisis Management
Coordination & Intelligence
Cyber & Behavioral Analytics
Forensics

Cyber Program of CI-DR Connective Tissue

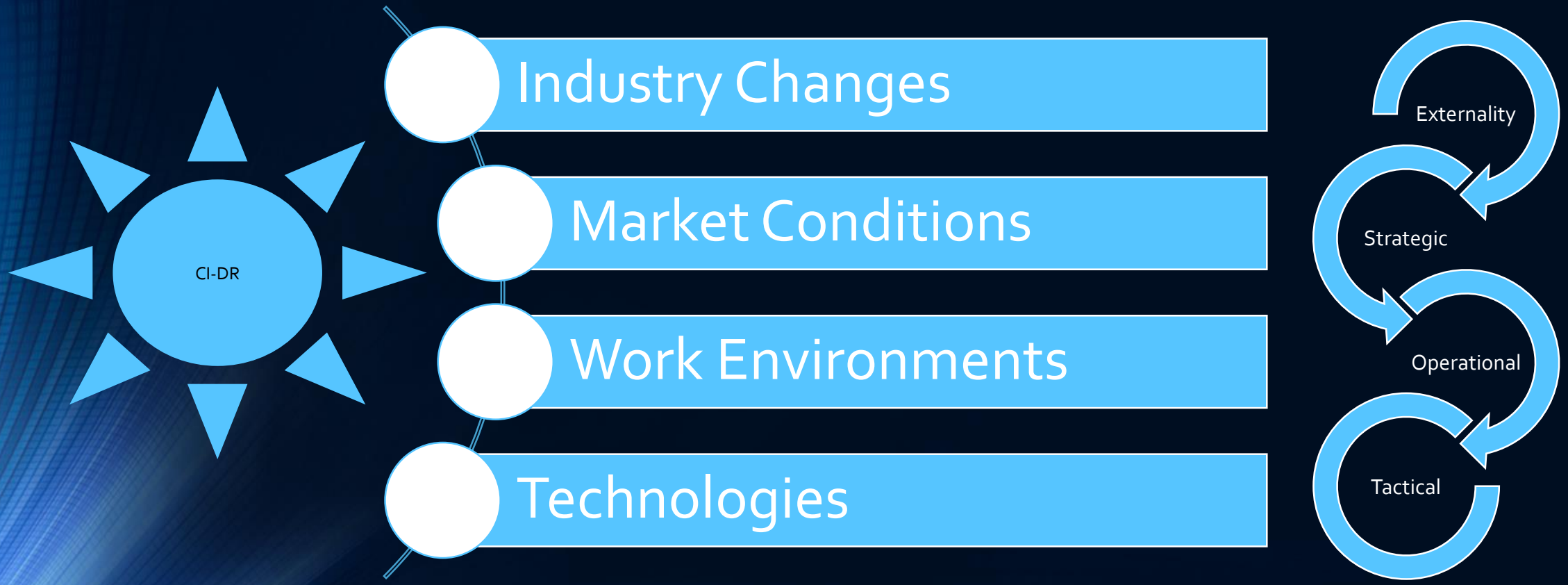


Fusion Groups can coordinate and focus threat collection, analysis, and subsequent interdiction efforts within their ecosystem.



Development of technical tools by internal stakeholders to combat fraud and other malicious activity should be guided and focused by relevant intelligence products

Focus on RCA for C-Suite Disrupters



Lessons Learned

HOW TO EFFECTIVELY USE A CI-DR PROGRAM

Previous Experience

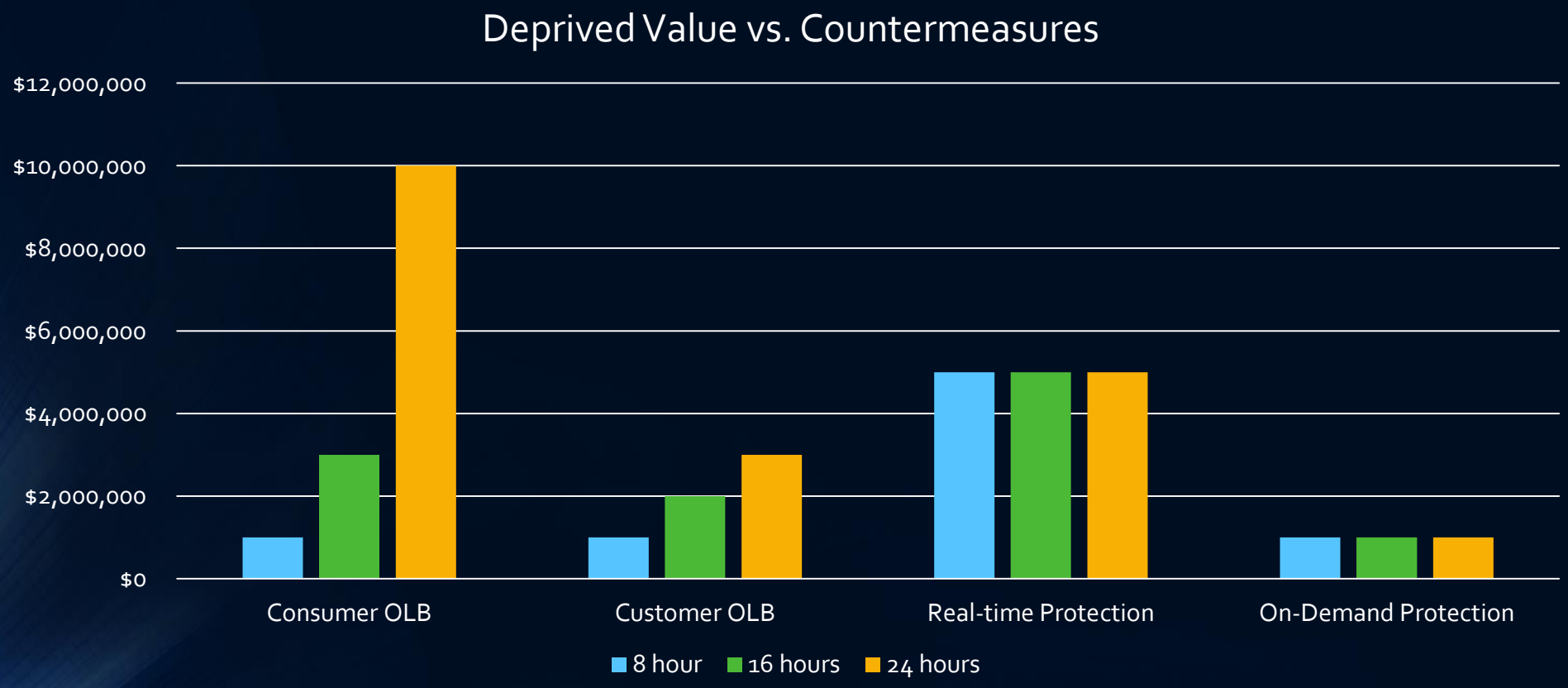
25 FINANCIAL INSTITUTIONS

- DDoS attack 2012
- 25 Banks under attack from QCF
- Does the bank deploy $$ of tech? Or something radical
- Who is involved?

CYBER IN 1 FINANCIAL INSTITUTION

- Collected revenue of critical assets "Crown Jewels"
- Collected all available Intelligence (OSINT, FSISAC, Peer Orgs, Deep/Dark Web)
- Expected loss by 8 / 16/ 24 hours. ~$10MM to include fees

Cost Benefit Analysis for technology



What did we do?

- The cyber intelligence team predicted from collected intelligence that an attack would be imminent during first week of January from the hours of 14:00 – 16:00.
- Presented findings and intelligence to the Board and C-Suite
- CFO acknowledged the deprived value financials
- Was agreed to take the hit, go off-line for 8 hours not to employ technology mitigations.
- Next attack we purchased on-demand DDoS mitigation. Maintained 1 hour of Deprived value

Preparation

- What is deprived value and how did we obtain those numbers?
  - Simple formula – We did not use ALE (Annual Loss Expectancy) or SLE (Single Loss Occurrence), we used actual revenue numbers for a year and put that into business time, off-hours, and weekends. We had statistics available for online activities.
- We built a cyber playbook.
  - The playbook was owned by the Cyber Intelligence team working with the Fusion Team from Corporate Communications, Finance, Technology, General Council, Privacy, and Governmental Affairs.
    - It was who will do what during an attack, what will be communicated to customers and consumers, Treasury, peer institutions, and to the Shareholders and stakeholders.

Examples of Corporate Comms and Legal Playbook Check lists

6.1 LEGAL RESPONSE PROCEDURES

The corporate legal response and advisement to senior executives should be considered as one of the most critical elements of the executive cyber response team. Corporate counsel's primary duties during a cyber-incident include but are not limited to working with outside regulators, ensuring response actions are in accordance with applicable laws and federal guidance and protecting the company against possible liabilities resulting from actual or perceived causes. Corporate counsel's input is required for any external communications to assure that such communication is in accordance to company policy and supports any statutory or regulatory requirements. In addition to the aforementioned, legal counsel should consider the following actions that will help organization navigate through the complexities of a cyber-related incident.

6.1.3 LEGAL RESPONSE FOR CATEGORY 3 INCIDENTS – MINOR IMPACT

- Work with the executive response team lead to determine what legal procedures to follow
- Advises Human Resources on identifying, securing, and distributing remedy/compensation for employees, as applicable due to data breaches
- Assist Human Resources in managing communications to investor relations and inquiries from the workforce
- Advise the board regarding corporate governance and regulatory issues

6.1.4 LEGAL RESPONSE FOR CATEGORY 4 INCIDENTS – CLEAR IMPACT

- Review contracts / commitments and determine disclosures required for employees or other 3rd parties (Customers, Suppliers, etc.)
- Determine outside regulatory disclosures required (SEC, Form 8-K,)
- Coordinates disciplinary action if needed (incidents caused by employee or employee failure to follow procedures)

6.1.5 LEGAL RESPONSE FOR CATEGORY 5 INCIDENTS – SIGNIFICANT IMPACT

6.2 CORPORATE COMMUNICATIONS RESPONSE PROCEDURES

Organization has a 'single voice' policy for responding to media inquiries meaning that ONLY THOSE designated by the CEO to speak on behalf of Company shall be permitted to provide information to media outlets. To that end:

- Corporate Communications shall review and coordinate on all media requests
- No external media personnel shall be permitted at any impacted location without clearance from local authorities and/or Corporate representatives.

6.2.3 CORP COMM RESPONSE FOR CATEGORY 3 INCIDENTS – MINOR IMPACT

- Coordinate with IT Service Desk to distribute initial informational email for awareness only (no specifics)
- Prepare for internal communications to affected Function(s) / Site(s)
-

6.2.4 CORP COMM RESPONSE FOR CATEGORY 4 INCIDENTS – CLEAR IMPACT

- Inform Leadership of impact to normal Operations
- Prepare external communication to specific (impacted) Customers / stakeholders
-

6.2.5 CORP COMM RESPONSE FOR CATEGORY 5 INCIDENTS – SIGNIFICANT IMPACT

- Engage external Marketing expertise to craft messages for external stakeholders
- Prepare communications for internal/external/Media sources – pending Executive approval
- Prepare communications to regulatory agencies – pending approval from Legal and Executive
- Prepare for rebuttal comments and notifications based on stakeholder receipt of primary communications
- Prepare communication to Board members for CEO

Proactive Intelligence Monitoring

- Chose the right tools for your environment. You don't have to go out and "follow the heard." Forget the Axiom, "I can't get fired by buying IBM."
- Fit those tools to meet your business objectives
- Create a cyber intelligence or Information Security Steering Committee, and by all means bring external guests from peer organizations to talk about what they are doing in cyber.
- Create weekly, monthly, and quarterly cyber intelligence meetings about business objectives and provide the facts.

Be on the look out in Summer 2020

Cyber Intelligence Driven Risk:
How to Build, Deploy, and Use Cyber Intelligence for Improved Business Risk Decisions – by Richard Moore

Available from Wiley & Sons

Contact me here!