McGrath | North

Assessing And Addressing Cyber Risk:

Proactive Strategies For Business

Iowa Association of Corporate Counsel
Des Moines, Iowa
May 29, 2015

Amy Roland
402.633.1490
aroland@mcgrathnorth.com

Tom Kelley
402.633.9549
tkelley@mcgrathnorth.com

McGrath North Mullin & Kratz, PC LLO
www.mcgrathnorth.com

Overview

- Background
- Regulatory/Legal Landscape
- Company Approach
  - Establish/Improve Cybersecurity Program
  - Vendor Management
  - Cyber Insurance

Background

Target Cyber Incident - Timeline

- November 12 – Incident
- December 12 – DOJ Notice
- December 1 – First Announcement
- January 10 – Theft PII Announced
- CIO resigned March 5, 2013
- CEO resigned May 5, 2013

Cyber Incident Costs/Harm

- Potential First Party Costs
  - – Forensic Costs
  - – Professional Advice
  - – Notification Costs
  - – Mitigation Costs
  - – Costs of Regulatory Investigation, Fines & Penalties
  - – Reputational Harm / Lost Business

Cyber Incident Costs/Harm

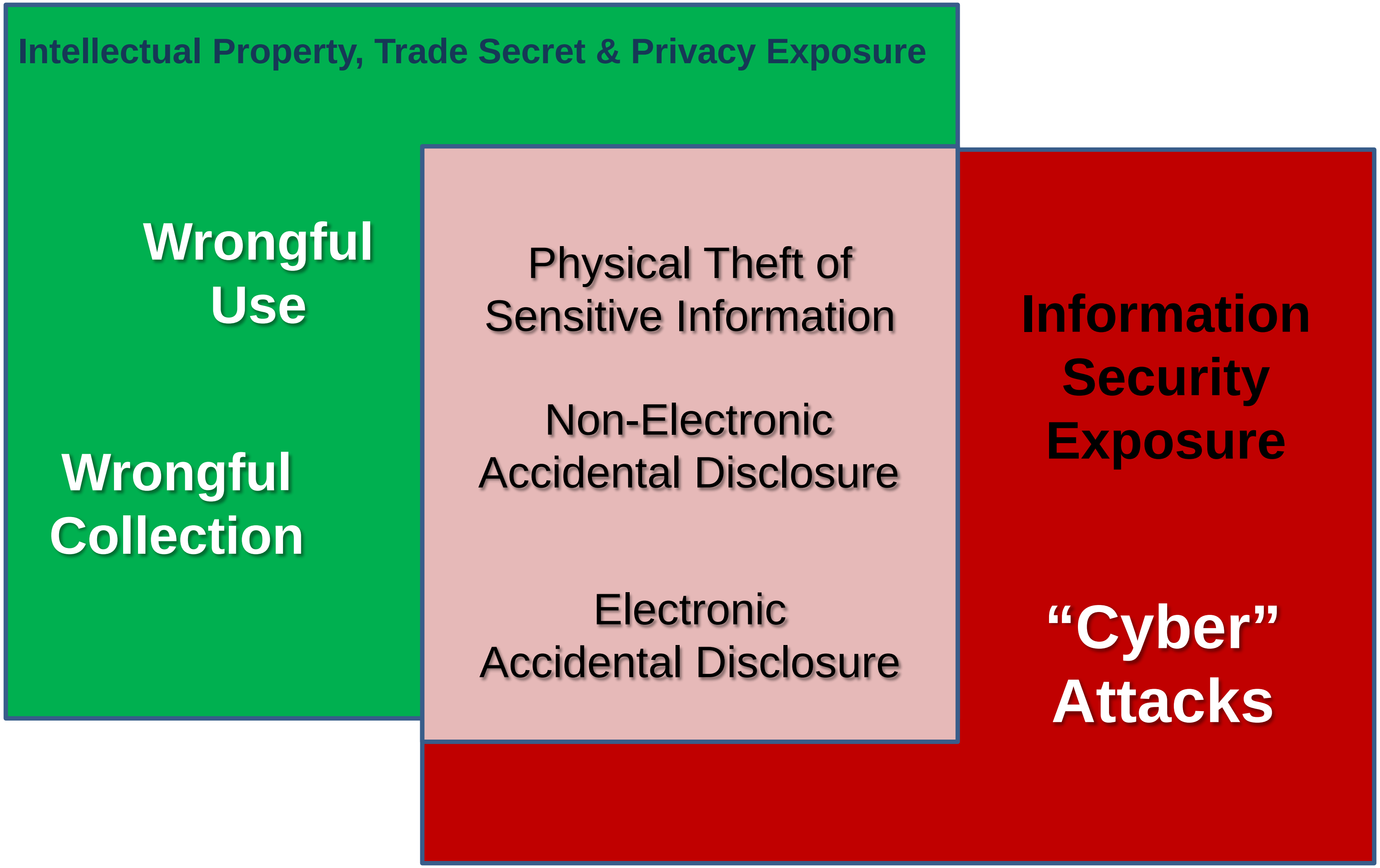
- Potential Third Party Claims
  - Class Actions by consumers (fear of identity theft generally insufficient)
  - By others with resulting losses
    - Banks, credit unions and other issuers of payment cards
    - Insurers of those who pay
    - Other merchants & third parties

What Data Is Involved?

- Personal Information For Use In Identify Theft
  - Name Plus:
    - Credit Card #
    - Social Security Number
    - Drivers License Or Government Issued ID
    - Medical Insurance ID Number
    - Financial Account Information
  - Personal Financial ***And Health*** Information
  - Electronic ***Or Paper***
- Other Confidential Information
  - Corporate Information
  - ***Trade Secrets/Intellectual Property***
  - Cyber Attacks to disrupt operations

What Data Is Involved? (cont.)

- Protected Health Information (HIPAA)
  - “Individually identifiable health information" maintained or transmitted by a CE or its BA, electronic, paper, or oral.
  - “IIHI” is information created/received by CE/employer relating to:
    - the individual’s past, present or future physical or mental health or condition,
    - the provision of health care to individual, or
    - the past, present, or future payment for the provision of health care to the individual,
  - ***AND*** that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual.
  - Common Identifiers include Name, Address, Birth Date, Social Security Number.



Intellectual Property, Trade Secret & Privacy Exposure

Wrongful Use

Wrongful Collection

Physical Theft of Sensitive Information

Non-Electronic Accidental Disclosure

Electronic Accidental Disclosure

Information Security Exposure

"Cyber" Attacks

Targeted Industries

- Financial Institutions
- Insurance Industry: Operations & Insured Exposure
- Universities
- Medical Facilities
- Retailers & Payment Processors
- Food & Beverage/Hospitality Industry
- Law firms
- Government and Defense Industry
- Employers of all kinds
- Any entity with Personal information on their systems of employees, customers/clients, third parties

The Regulatory/Legal Landscape

The Regulatory/Legal Landscape

- 47 State Laws (Data Protection & Notification)
  - Iowa Title XVI, Subtitle 1, Chapter 715C
- HIPAA
- Gramm-Leach-Bliley Act
- Sarbanes Oxley
- SEC Guidance
- Executive Order 13636 & Cybersecurity Framework
- FTC Regulations
- HHS
- Payment Card Industry Data Security Standards
- FINRA

The Regulatory/Legal Landscape (cont.)

Contractual Requirements

- Vendor Contracts
  - Some imposed by law or regulation
  - Watch for assumption of obligations beyond what is required by applicable law
- Customer Agreements
  - Privacy Policies
  - Overstated Privacy Policies can come back to haunt
  - Review policies on your website

The Regulatory/Legal Landscape (cont.)

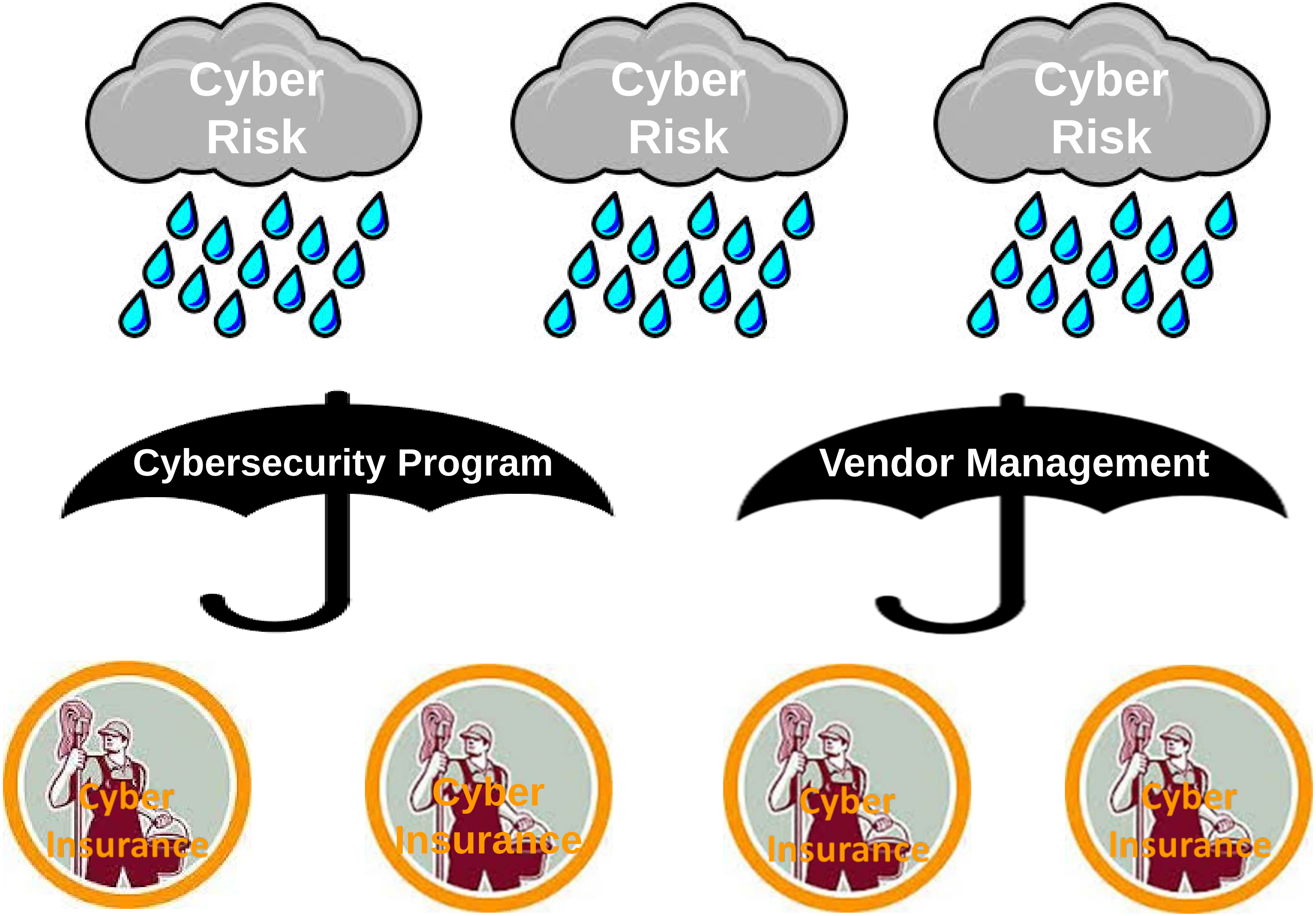
Common Law rights –

- To privacy of Personal Information
- To protection of other confidential information
- HIPAA as a standard of care in State court actions?

Policy Options

- Federal Data Security/Breach Notification Law
- Modify FTC Enforcement Powers
- Require Adoption Of More Advanced Technologies
- Create Federal Standards For Data Security, Including For Businesses
- Source: CRS Report, April 22, 2014

Company Approach



Cyber Risk

Cyber Risk

Cyber Risk

Cybersecurity Program

Vendor Management

Cyber Insurance

Cyber Insurance

Cyber Insurance

Cyber Insurance

Company Approach

First Line of Defense:

- **Establish/improve cybersecurity program by assessing cyber risk & cyber policies, including review of:**
  - Information governance
  - Employee education and training (human firewall)
  - Incident response plans
  - Board and/or executive support
- **Vendor Management**
  - Due Diligence
  - Recommended Contract Provisions

Cyber insurance as a second layer of risk financing

Cybersecurity

Program

U.S. Cybersecurity Framework

- Executive Order 13636 (February 19, 2013)
  - Develop voluntary risk-based Cybersecurity Framework
  - Industry standards and best practices to help organizations manage cybersecurity risks.
- National Institute of Standards and Technology (NIST) U.S. Cybersecurity Framework (February 12, 2014)

Establishing or Improving a Cybersecurity Program

- **Step 1: Prioritize and Scope** *(identify business mission objectives and high level organizational priorities)*
- **Step 2: Orient** *(identify related systems & assets, regulatory requirements, overall risk approach & threats to/vulnerabilities of identified systems and assets)*
- **Step 3: Create Current Profile** *(utilizing framework core)*
- **Step 4: Conduct a Risk Assessment** *(assign actual ratings ("tiers") to framework core)*
- **Step 5: Create Target Profile** *(assign desired tiers to framework core)*
- **Step 6: Determine, Analyze, and Prioritize Gaps** *(Current vs. Target)*
- **Step 7: Implement Action Plan**

U.S. Cybersecurity Framework

- ***Framework Core*** - Set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors
- **Framework Implementation Ratings or “Tiers”** - Provide context on how an organization views cybersecurity risk and the processes in place to manage that risk based on the Framework Core.
- ***Framework Profile*** - Represents the outcomes based on business needs that an organization has selected from the Framework Core.

U.S. Cybersecurity Framework Core

IDENTIFY

(Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities)

PROTECT

(Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services)

DETECT

(Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event)

RESPOND

(Develop and implement the appropriate activities to take action regarding a detected cybersecurity event)

RECOVER

(Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event)

U.S. Cybersecurity Framework Core

Function	Category	Subcategories	Informative References
IDENTIFY			
PROTECT			
DETECT			
RESPOND			
RECOVER			

U.S. Cybersecurity Framework Core

Function	Category
IDENTIFY	Asset Management
	Business Environment
	Governance
	Risk Assessment
	Risk Management Strategy
PROTECT	Access Control
	Awareness and Training
	Data Security
	Information Protection Processes and
	Maintenance
	Protective Technology
DETECT	Anomalies and Events
	Security Continuous Monitoring
	Detection Processes
RESPOND	Response Planning
	Analysis
	Mitigation
	Improvements
RECOVER	Recovery Planning
	Improvements
	Communications

U.S. Cybersecurity Framework Core

Function	Category	Subcategory
IDENTIFY	**Asset Management:** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**Physical devices and systems within the organization are inventoried**
		Software platforms and applications within the organization are inventoried
		Organizational communication and data flows are mapped
		External information systems are catalogued
		Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value
		Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established
	Business Environment: The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	The organization's role in the supply chain is identified and communicated
		The organization's place in critical infrastructure and its industry sector is identified and communicated
		Priorities for organizational mission, objectives, and activities are established and communicated
		Dependencies and critical functions for delivery of critical services are established
		Resilience requirements to support delivery of critical services are established
	Governance: The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	Organizational information security policy is established
		Information security roles & responsibilities are coordinated and aligned with internal roles and external partners
		Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed
		Governance and risk management processes address cybersecurity risks
	Risk Assessment: The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	Asset vulnerabilities are identified and documented
		Threat and vulnerability information is received from information sharing forums and sources
		Threats, both internal and external, are identified and documented
		Potential business impacts and likelihoods are identified
		Threats, vulnerabilities, likelihoods, and impacts are used to determine risk
		Risk responses are identified and prioritized
	Risk Management Strategy: The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	Risk management processes are established, managed, and agreed to by organizational stakeholders
		Organizational risk tolerance is determined and clearly expressed
		The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis

Identify→Asset Management→Subcategory
Physical devices and systems within the organization are inventoried
Software platforms and applications within the organization are inventoried
Organizational communication and data flows are mapped
External information systems are catalogued
Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value
Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established

U.S. Cybersecurity Framework Core

Function	Category	Subcategory
PROTECT	**Access Control:** Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	Identities and credentials are managed for authorized devices and users
		Physical access to assets is managed and protected / Remote access is managed
		Access permissions managed, incorporating the principles of least privilege & separation of duties
		Network integrity is protected, incorporating network segregation where appropriate
	Awareness and Training: The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	All users are informed and trained / Privileged users understand roles & responsibilities
		Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities
		Senior executives understand roles & responsibilities
		Physical and information security personnel understand roles & responsibilities
	Data Security: Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	Data-at-rest is protected / Data-in-transit is protected
		Assets are formally managed throughout removal, transfers, and disposition
		Adequate capacity to ensure availability is maintained / Protections against data leaks are implemented
		Integrity checking mechanisms are used to verify software, firmware, and information integrity
	Information Protection Processes and Procedures: Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	The development and testing environment(s) are separate from the production environment
		A baseline configuration of info. technology/industrial control systems is created and maintained
		A System Development Life Cycle to manage systems is implemented
		Configuration change control processes are in place / Backups of info. are conducted, maintained & tested periodically
		Policy & regulations regarding the physical operating environment for organizational assets are met
		Data is destroyed according to policy / Protection processes are continuously improved
		Effectiveness of protection technologies is shared with appropriate parties
		Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed / Response and recovery plans are tested
		Cybersecurity included in human resources practices (e.g., deprovisioning, personnel screening)
		A vulnerability management plan is developed and implemented
	Maintenance: Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.	Maintenance and repair of org. assets is performed & logged in a timely manner, with approved and controlled tools
		Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access
	Protective Technology: Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	Audit/log records determined, documented, implemented, and reviewed in accordance with policy
		Removable media is protected and its use restricted according to policy
		Access to systems and assets is controlled, incorporating the principle of least functionality
		Communications and control networks are protected

U.S. Cybersecurity Framework Core

Function	Category	Subcategory
DETECT	**Anomalies and Events:** Anomalous activity is detected in a timely manner and the potential impact of events is understood.	A baseline of network operations and expected data flows for users and systems is established and managed
		Detected events are analyzed to understand attack targets and methods
		Event data are aggregated and correlated from multiple sources and sensors
		Impact of events is determined
		Incident alert thresholds are established
	Security Continuous Monitoring: The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	The network is monitored to detect potential cybersecurity events
		The physical environment is monitored to detect potential cybersecurity events
		Personnel activity is monitored to detect potential cybersecurity events
		Malicious code is detected
		Unauthorized mobile code is detected
		External service provider activity is monitored to detect potential cybersecurity events
		Monitoring for unauthorized personnel, connections, devices, and software is performed
		Vulnerability scans are performed
	Detection Processes: Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	Roles and responsibilities for detection are well defined to ensure accountability
		Detection activities comply with all applicable requirements
		Detection processes are tested
		Event detection information is communicated to appropriate parties
		Detection processes are continuously improved

U.S. Cybersecurity Framework Core

Function	Category	Subcategory
RESPOND	**Response Planning:** Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.	Response plan is executed during or after an event
	Communications: Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	**Personnel know their roles and order of operations when a response is needed**
		Events are reported consistent with established criteria
		Information is shared consistent with response plans
		Coordination with stakeholders occurs consistent with response plans
		Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness
	Analysis: Analysis is conducted to ensure adequate response and support recovery activities.	Notifications from detection systems are investigated
		The impact of the incident is understood
		Forensics are performed
		Incidents are categorized consistent with response plans
	Mitigation: Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.	Incidents are contained
		Incidents are mitigated
		Newly identified vulnerabilities are mitigated or documented as accepted risks
	Improvements: Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	Response plans incorporate lessons learned
		Response strategies are updated

Respond→Communications→Subcategory
Personnel know their roles and order of operations when a response is needed
Events are reported consistent with established criteria
Information is shared consistent with response plans
Coordination with stakeholders occurs consistent with response plans
Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness

U.S. Cybersecurity Framework Core		
Function	**Category**	**Subcategory**
RECOVER	**Recovery Planning:** Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.	Recovery plan is executed during or after an event
	Improvements: Recovery planning and processes are improved by incorporating lessons learned into future activities.	Recovery plans incorporate lessons learned
		Recovery strategies are updated
	Communications: Restoration activities are coordinated with internal & external parties, such as coordinating centers, ISPs, owners of attacking systems, victims, other Computer Security Incident Response Teams & vendors.	Public relations are managed
		Reputation after an event is repaired
		Recovery activities are communicated to internal stakeholders and executive and management teams

U.S. Cybersecurity Framework Ratings or "Tiers"

Tier 1: Partial - Organizational cybersecurity risk management practices are not formalized, and risk is managed in an ad hoc and sometimes reactive manner ….

Tier 2: Risk Informed (Goal) - Risk management practices are approved by management but may not be established as organizational-wide policy …

Tier 3: Repeatable - The organization's risk management practices are formally approved and expressed as policy and are regularly updated ….

Tier 4: Adaptive - The organization adapts its cybersecurity practices based on lessons learned and predictive indicators derived from previous and current cybersecurity activities…

U.S. Cybersecurity Framework Profile

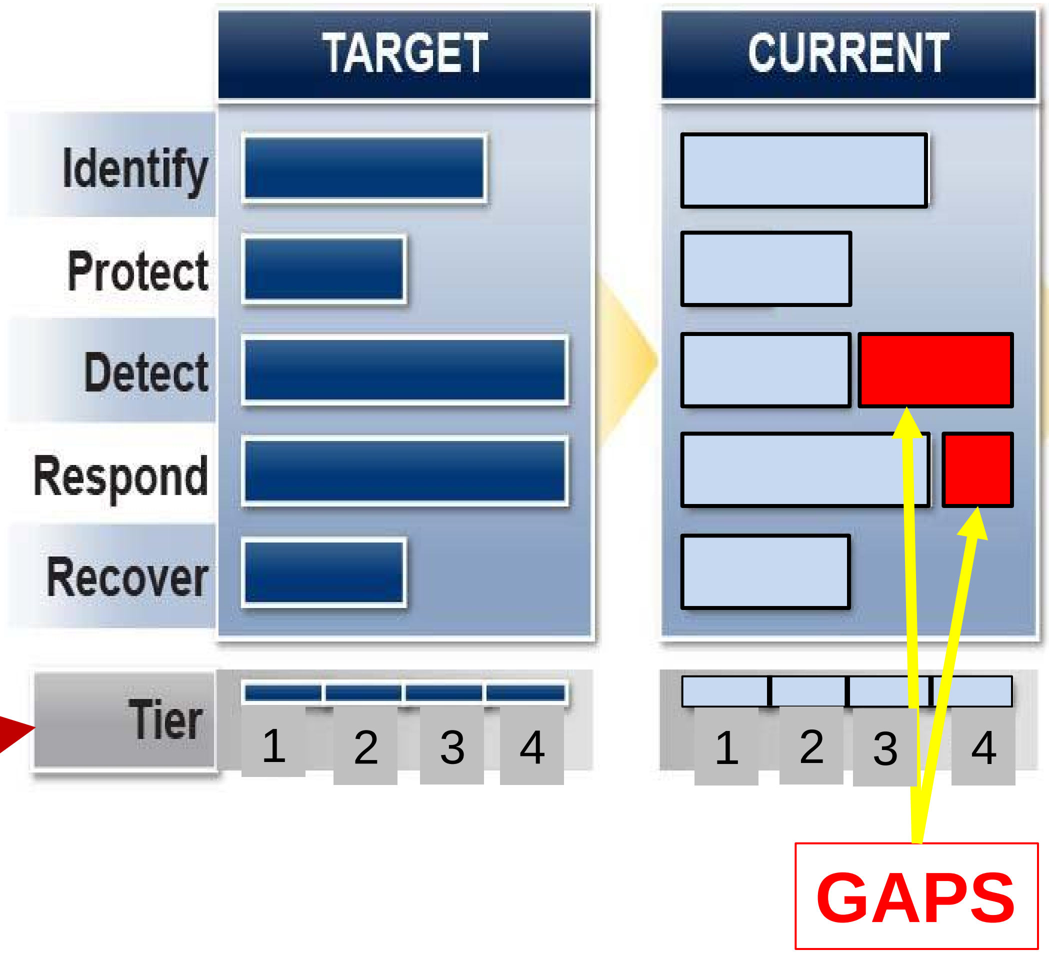
Tiers

Tier 4: *Adaptive*

Tier 3: *Repeatable*

Tier 2: *Risk-Informed*

Tier 1: *Partial*



From Cyber Security Framework: Intel's Implementation Pilot, Tim Casey, CISSP Senior Strategic Risk Analyst, ISSA Presentation, January 12, 2015.

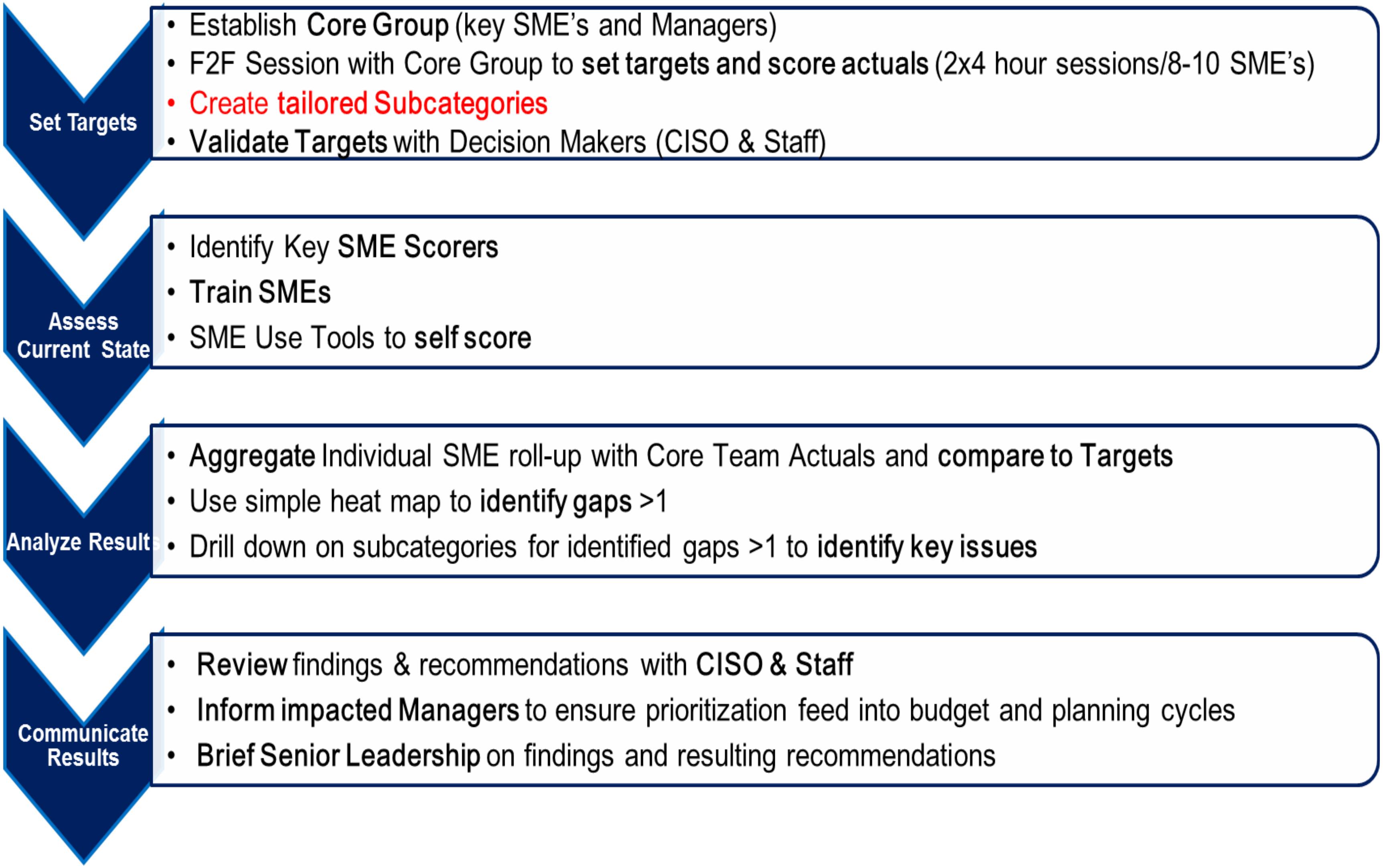
The Intel Pilot

Use U.S. Cybersecurity Framework on subset of Company to:

- Establish alignment on risk tolerance
- Inform budget planning for 2015
- Communicate risk “heat map” to Senior Leadership
- Use Framework as a risk management approach NOT a compliance checklist

Intel Pilot information from Cyber Security Framework: Intel’s Implementation Pilot, Tim Casey, CISSP Senior Strategic Risk Analyst, ISSA Presentation, January 12, 2015.

The Intel Pilot



Set Targets

- Establish **Core Group** (key SME's and Managers)
- F2F Session with Core Group to **set targets and score actuals** (2x4 hour sessions/8-10 SME's)
- Create **tailored Subcategories**
- **Validate Targets** with Decision Makers (CISO & Staff)

Assess Current State

- Identify Key **SME Scorers**
- **Train SMEs**
- SME Use Tools to **self score**

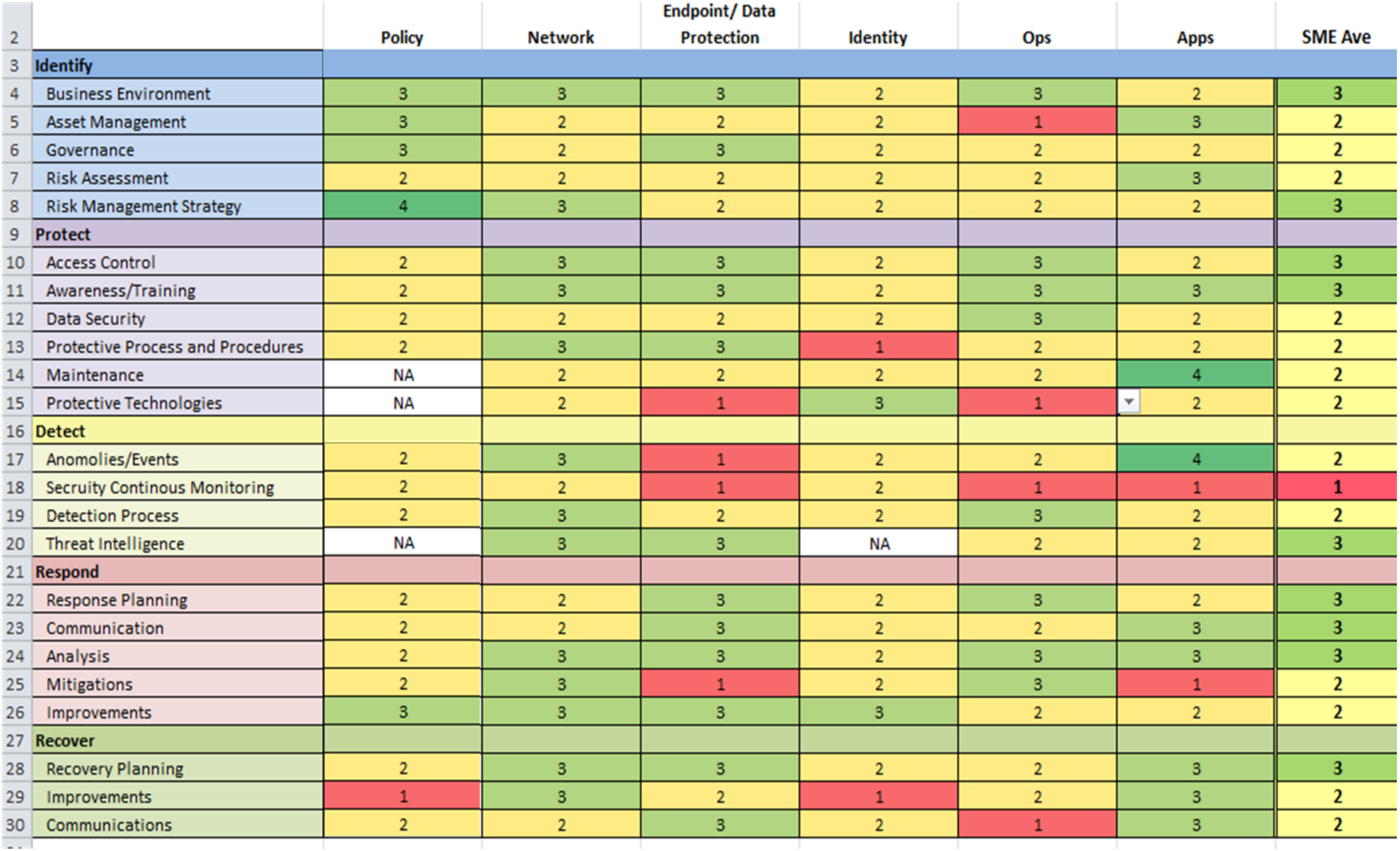
Analyze Results

- **Aggregate** Individual SME roll-up with Core Team Actuals and **compare to Targets**
- Use simple heat map to **identify gaps** >1
- Drill down on subcategories for identified gaps >1 to **identify key issues**

Communicate Results

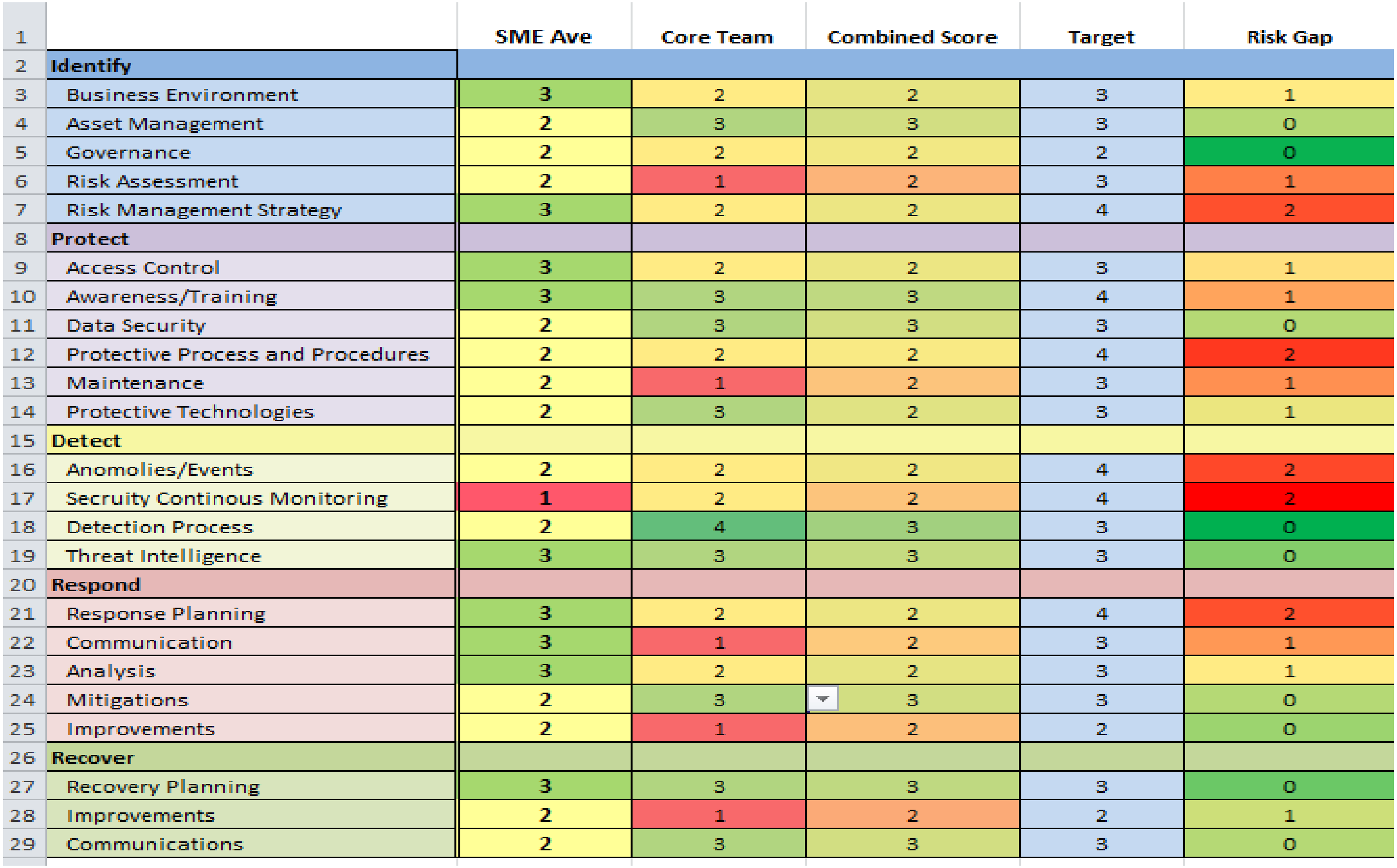
- **Review** findings & recommendations with **CISO & Staff**
- **Inform impacted Managers** to ensure prioritization feed into budget and planning cycles
- **Brief Senior Leadership** on findings and resulting recommendations

The Intel Pilot – Use of “Heat Map”



	Policy	Network	Endpoint/ Data Protection	Identity	Ops	Apps	SME Ave
Identify							
Business Environment	3	3	3	2	3	2	3
Asset Management	3	2	2	2	1	3	2
Governance	3	2	3	2	2	2	2
Risk Assessment	2	2	2	2	2	3	2
Risk Management Strategy	4	3	2	2	2	2	3
Protect							
Access Control	2	3	3	2	3	2	3
Awareness/Training	2	3	3	2	3	3	3
Data Security	2	2	2	2	3	2	2
Protective Process and Procedures	2	3	3	1	2	2	2
Maintenance	NA	2	2	2	2	4	2
Protective Technologies	NA	2	1	3	1	2	2
Detect							
Anomolies/Events	2	3	1	2	2	4	2
Secruity Continous Monitoring	2	2	1	2	1	1	1
Detection Process	2	3	2	2	3	2	2
Threat Intelligence	NA	3	3	NA	2	2	3
Respond							
Response Planning	2	2	3	2	3	2	3
Communication	2	2	3	2	2	3	3
Analysis	2	3	3	2	3	3	3
Mitigations	2	3	1	2	3	1	2
Improvements	3	3	3	3	2	2	2
Recover							
Recovery Planning	2	3	3	2	2	3	3
Improvements	1	3	2	1	2	3	2
Communications	2	2	3	2	1	3	2

The Intel Pilot



1		SME Ave	Core Team	Combined Score	Target	Risk Gap
2	**Identify**					
3	Business Environment	3	2	2	3	1
4	Asset Management	2	3	3	3	0
5	Governance	2	2	2	2	0
6	Risk Assessment	2	1	2	3	1
7	Risk Management Strategy	3	2	2	4	2
8	**Protect**					
9	Access Control	3	2	2	3	1
10	Awareness/Training	3	3	3	4	1
11	Data Security	2	3	3	3	0
12	Protective Process and Procedures	2	2	2	4	2
13	Maintenance	2	1	2	3	1
14	Protective Technologies	2	3	2	3	1
15	**Detect**					
16	Anomolies/Events	2	2	2	4	2
17	Secruity Continous Monitoring	1	2	2	4	2
18	Detection Process	2	4	3	3	0
19	Threat Intelligence	3	3	3	3	0
20	**Respond**					
21	Response Planning	3	2	2	4	2
22	Communication	3	1	2	3	1
23	Analysis	3	2	2	3	1
24	Mitigations	2	3	3	3	0
25	Improvements	2	1	2	2	0
26	**Recover**					
27	Recovery Planning	3	3	3	3	0
28	Improvements	2	1	2	2	1
29	Communications	2	3	3	3	0

Vendor

Management

Vendor Management

- Note vendor involvement in numerous cyber incidents (e.g., Target)
- Analyze type of data involved, not just size of vendor
- Mitigate risk by conducting due diligence and including recommended contract provisions

Vendor Management

Due Diligence:

- Background check
- Is entity well capitalized?
- Review vendor privacy and security policies
- On-site visit
- Where will data be accessed and stored?
- Will any data be accessed or stored offshore?

Vendor Management

Additional Due Diligence Related to Offshore Access:

- Where is the contracting entity incorporated or organized and where is it available for service of process? U.S. entity with offshore location would mitigate risk of enforceability of contract.

- Does the host nation have a legal infrastructure that will allow meaningful enforcement of data protection obligations in the contract?

- Examination of customer contracts regarding prohibitions or other requirements regarding offshore outsourcing.

- Examination of privacy and security laws and regulations in general because such laws and regulations are constantly in flux.

Vendor Management

Vendor contracts that include vendor access to customer or company data should specify the following:

- Location(s) where data will be stored and accessed and a prohibition on changing such location(s) without company's consent.
- Vendor should be required to do background checks on its personnel.
- Portable devices that store company confidential information should be encrypted.
- Vendor should be required to abide by agreed-upon security policies and procedures to maintain safeguards against unauthorized access, destruction, loss or alteration of company confidential information.

Vendor Management

- Establish incident response plan for addressing security and privacy breaches.
- Confidentiality obligations apply to company and customer data.
- Obligation to comply with applicable law and a mechanism to address changes in the law, including responsibility for monitoring changes and responsibility for costs to implement such changes.
- Immediate right to terminate and/or withhold payments upon discovery of a significant security breach.
- An ongoing and immediate right to retrieve data.
- Indemnification for breaches of confidentiality, privacy and security obligations, failures to comply with the law or standby letters of credit.

Vendor Management

- Damages for breaches of confidentiality obligations, security obligations and failures to comply with the law or standby letters of credit should be excluded from limitations of liability.
- Audit rights, including on-site audits, and audit of vendor’s and its subcontractors’ privacy and security policies and procedures and compliance with such policies and procedures.
- Annual SSAE 16 audit or its equivalent and provide results of such audit to company.
- Prohibition on subcontracting without consent, together with obligation that vendor remains fully responsible for all acts and omissions of its subcontractors.
- Insurance

Vendor Management

Additional Contract Requirements for Offshore Outsourcing:

- Specify what law governs the interpretation of the agreement and disputes arising under the agreement.
- Specify the venue for resolving disputes.
- Specify how to enforce judgments and arbitration decisions.

Vendor Management

Reminder: The contract with the vendor is the tool to manage the relationship. It is not enough to have contract provisions in place. Company should actively monitor vendor’s performance and compliance with the agreement, enforce the terms of the agreement and use the tools contracted for (i.e. audit rights).

Cyber Insurance

Cyber Insurance Coverage

Third-Party Coverage

Insures for the liability of the policyholder to third parties — including clients and governmental entities — arising from a data breach or cyber attack.

Cyber Insurance Coverage

Third-party coverages include:

- Litigation And Regulatory. Covers the legal, technical or forensic costs associated coverage for civil lawsuits, judgments, settlements and vendor proceedings (e.g., credit card issuers / PCI-DSS) resulting from a cyber event, as well as the judgments, settlements, vendor fines and vendor penalties themselves. *(Selection of counsel and other advisors should be addressed.)*

Cyber Insurance Coverage

Third-party coverages include (cont.):

- Regulatory Response. Covers the legal, technical or forensic services necessary to assist the policyholder in responding to federal or state governmental inquiries relating to a cyber attack, and provides coverage for fines, penalties, investigations or other regulatory actions. *(Selection of counsel and other advisors should be addressed.)*

- Notification Costs. Covers the costs to notify customers, employees or other victims affected by a cyber event, including notice required by law.

Cyber Insurance Coverage

Third-party coverages include (cont.):

- Crisis Management And Public Relations. Covers crisis management and public relations expenses incurred to educate customers concerning a cyber event and the policyholder’s response, including the cost of advertising for this purpose.
- Credit Monitoring. Covers the costs of credit monitoring, fraud monitoring or other related services to customers or employees affected by a cyber event.
- Privacy Liability. Provides coverage for liability to employees or customers for a breach of privacy.
- Media Liability. Coverage for claims against, and damages to, your company arising from certain personal injury torts, dissemination of information through a website, and certain types of intellectual property infringement.

Cyber Insurance Coverage

First-Party Coverage

Insures for losses to the policyholder’s own data or lost income or for other harm to the policyholder’s business resulting from a data breach or cyber attack.

Cyber Insurance Coverage

First-party coverages include:

- Theft And Fraud. Covers destruction or loss of the policyholder’s data as the result of a criminal or fraudulent cyber event, including theft and transfer of funds. Cover both “loss” and “theft”.
- Forensic Investigation. Covers the legal, technical or forensic services necessary to assess whether a cyber attack has occurred, to assess the impact of the attack and to stop an attack.
- Business Interruption. Covers lost income and related costs where a policyholder is unable to conduct business due to a cyber event or data loss.

Cyber Insurance Coverage

First-party coverages include (cont.):

- Extortion. Provides coverage for the costs associated with the investigation of threats to commit cyber attacks against the policyholder's systems and for payments to extortionists who threaten to obtain and disclose sensitive information.
- Computer Data Loss And Restoration. Covers physical damage to, or loss of use of, computer-related assets, including the costs of retrieving and restoring data, hardware, software or other information destroyed or damaged as the result of a cyber attack.

Cyber Insurance Checklist

- ❑ Identify Your Unique Risks.
- ❑ Understand Your Existing Coverage.
- ❑ Buy What You Need.
- ❑ Secure Appropriate Limits And Sublimits.
- ❑ Beware of Exclusions.
- ❑ Consider Retroactive Coverage.
- ❑ Consider Coverage For Acts And Omissions By Third Parties.
- ❑ Evaluate Coverage For Data Restoration Costs.
- ❑ Involve All Stakeholders.

Cyber Insurance Checklist

- □ Take Advantage Of Risk Management Services.
- □ Dovetail Cyber Insurance With Indemnity Agreements.
- □ Understand The “Triggers”.
- □ Consider Coverage For Loss Of Information On Unencrypted Mobile And Other Remote Devices.
- □ Consider Coverage For Regulatory Actions.
- □ Consider A Partial Subrogation Waiver.
- □ Selection Of Counsel And Other Professionals.
- □ Be Wary Of Warranty Statements On Applications.

Finis

McGrath | North

Amy Roland
402.633.1490
aroland@mcgrathnorth.com

Tom Kelley
402.633.9549
tkelley@mcgrathnorth.com