Cyber Risk Analytics:
A NIST & GSA-Sponsored Project

Conducted By:

The Supply Chain Management Center,
R.H. Smith School of Business, University of Maryland College Park

Principal Investigators:

Dr. Sandor Boyson
Dr. Thomas Corsi
Ms. Holly Mann

Introduction

- Two year project sponsored by NIST (Project Lead: Mr. Jon Boyens; and Ms. Celia Paulsen); and GSA (Ms. Angela Smith and Emile Monette).
- Our R.H. Smith School of Business team included:
  - Dr. Sandor Boyson and Dr. Thomas Corsi- Faculty & Co-Directors, Supply Chain Management Center, R.H. Smith School of Business
  - Ms. Holly Mann, R.H. Smith School of Business Chief Information Officer
  - Dr. John Patrick Paraskevas, Faculty, Miami University (Ohio)
  - Mr. Hart Rossman, Senior Research Fellow, R.H. Smith School of Business
- The insurance industry -Zurich (Mr. Gerry Kane and Ms. Linda Conrad) and Beecher Carlson (Mr. Chris Keegan) partnered with UMD and provided inputs on risk assessment & industry outreach.

Major Research Objectives

- Develop & deploy a secure, organizational self-assessment tool based on the Cybersecurity Framework.
- Compare respondents' cyber performance profiles (adoption of Framework policies & actions) with their total number and specific types of cyber breaches.
- Assess efficacy of Cybersecurity Framework policies & actions in limiting total number and specific types of cyber breaches.
- Use this analysis to establish a foundation for the development of evidence-based cyber risk predictive analytics.

Uniqueness Of This Research

- Our team conducted an extensive literature review of cybersecurity predictive analytics. We reviewed 789 journal articles and conference papers. The vast majority were theory articles with no data.

- We found only 26 academic articles that used primary or secondary data, mostly in the context of individual security and as part of experiments in behavioral labs.

- We could find no research that:
  - Conducted an assessment of firms to determine their cyber capabilities.
  - Pulled breach data from multiple sources.
  - Used econometric analysis to understand which of a broad portfolio of cyber protection methods would be most effective against cyber breaches.

Study Challenges

A. Rigorous econometric analysis applied to a limited number of self-assessment participants, which ensures reliability but limits generalizability

- ➢ Detailed 175-question self-assessment tool went well beyond the depth of usual surveys and required lot of organizational interest/effort to fill in.
- ➢ Our target audience of cyber security professionals was cautious about the security of their proprietary data on corporate practices.
- ➢ To address these concerns, we used pre-registration IP & email screening to validate identity of potential respondents; plus two factor authentication for approved registrants to access the portal.
- ➢ Despite these barriers, there were 153 respondents, with 40-100 responses per question.

Study Challenges

B. Breach data on our sample of survey respondents was extremely difficult to compile

- Fragmentation of available cyber breach data across multiple data sets: of the 414 total breaches collected on our sample organizations across the four data sets, there was only a 7% duplication rate.
- Overall lack of meaningful incentives for corporate disclosure of breaches meant available breach data had real potential gaps and shortcomings.

Confidence levels in final results are constrained by above limitations

Assessment Tools/Technology

- The **Cyber Risk Portal:** new user features & security enhancements:
  - Completed Self-Assessment Form, with questions fully aligned with the category/sub-category levels of the Cyber Security Framework.
  - Developed business visualization technology to display layered assessment results.
  - Transitioned to Amazon Web Hosting and provider-recommended security/encryption controls.
  - Implemented user pre-registration screening and DUO Two Factor Authentication.
- **The Cyber Risk Portal won the 2017 IEEE (Institute Of Electrical and Electronics Engineers) Cyber Security Practice Innovation of the year.**

The Cyber Breach Database

- Created a master data set of breaches composed of four breach data sets:

  1. **Advisen**
(commercial)
  2. **Risk Based Security**
(commercial)
  3. **Identity Theft Resource Center**
(non-profit)
  4. **C-BERC**
(university)

- Developed meta-breach categories to encompass the breach categories used within the four data sets.
- Our team of faculty and students sorted each breach into one of these meta-categories: access control deficiencies; technical exploits; theft; and behavioral vulnerabilities.

Cyber Breach Data Meta-Typology

1. Technical Exploits

Definition: Exploits involving manipulation of website code, network ports, configuration or implementation errors

Examples: Hacks; snooping; IT processing errors; IT configuration errors; network/website design

2. Deficient Access Controls

Definition: Inadequate assignment and management of system roles & user privileges/ permissions

Examples: Fraud; identity-fraudulent use; privacy-unauthorized data collection; data-unintentional disclosure

3. Behavioral Vulnerabilities

Definition: Social engineering, behavior-based intrusions

Examples: Phishing/spoofing/social engineering

4. Theft

Definition: Unauthorized use of technology or data

Examples: Stolen computer; data – malicious breach; data – physically lost or stolen; privacy – unauthorized contact or disclosure; privacy – unauthorized data collection

Cyber Breach Data: Volume/Patterns

- As previously noted, 414 total breaches were collected for all years for those organizations who employed our self-assessment tool.
- However, we specifically focused our analysis on the period 2014-2017 in order to cover immediate past, present and emerging breach patterns.
- For the 2014-2017 analysis period, there were 163 breaches directly associated with our sample of respondents.
- 57 breaches (or 35% of total) were categorized as access control deficiencies or administrative/network management deficiencies. Only 17 (10.4%) were behavioral or user-driven breaches.

Results of Analysis – Overview

Description of Respondents

What most accurately describes your job title / professional role?				
	Frequency	Percent	Valid Percent	Cumulative Percent
Director/Associate Director/Manager, Information Security	62	38.8	38.8	38.8
Director/Associate Director/Manager, Information Technology	49	30.6	30.6	69.4
Director/Associate Director/Manager, Procurement Acquisition	8	5.0	5.0	74.4
Director/Associate Director/Manager, Product Engineering	5	3.1	3.1	77.5
Director/Associate Director/Manager, Risk Management	21	13.1	13.1	90.6
Director/Associate Director/Manager, Telecom Services	1	.6	.6	91.3
Director/Manager, Supply Chain Management	14	8.8	8.8	100.0
Total	160	100.0	100.0	

Description of Respondents

How large is your company?

	Frequency	Percent	Valid Percent	Cumulative Percent
Annual sales between $100 million -$1 billion	23	14.4	14.4	14.4
Annual sales between $20-$50 million	29	18.1	18.1	32.5
Annual sales between $50-$100 million	11	6.9	6.9	39.4
Annual sales greater than $1 billion	40	25.0	25.0	64.4
Annual sales less than $20 million	57	35.6	35.6	100.0
Total	160	100.0	100.0	

Are you a Parent or Subsidiary company?

	Frequency	Percent	Valid Percent	Cumulative Percent
Parent	139	86.9	86.9	86.9
Subsidiary	21	13.1	13.1	100.0
Total	160	100.0	100.0	

Does your company provide Hardware?

	Frequency	Percent	Valid Percent	Cumulative Percent
No	118	73.8	73.8	73.8
Yes	42	26.3	26.3	100.0
Total	160	100.0	100.0	

Are your networks/IT systems:

	Frequency	Percent	Valid Percent	Cumulative Percent
Primarily managed by your own unit	75	46.9	46.9	46.9
Primarily managed by your parent organization	85	53.1	53.1	100.0
Total	160	100.0	100.0	

Description of Respondents

Does your company provide Telecom/Data Network Provisioning?				
	Frequency	Percent	Valid Percent	Cumulative Percent
No	124	77.5	77.5	77.5
Yes	36	22.5	22.5	100.0
Total	160	100.0	100.0	

Does your company provide Hosted/Cloud Applications?				
	Frequency	Percent	Valid Percent	Cumulative Percent
No	106	66.3	66.3	66.3
Yes	54	33.8	33.8	100.0
Total	160	100.0	100.0	

Does your company currently supply IT products/services to the federal government?				
	Frequency	Percent	Valid Percent	Cumulative Percent
No	100	62.5	62.5	62.5
Yes	60	37.5	37.5	100.0
Total	160	100.0	100.0	

Performance Assessment Characteristics: Adoption Of Framework & Standards

6.1 Cybersecurity Framework for Planning and Management				
	Frequency	Percent	Valid Percent	Cumulative Percent
Not Used	13	8.1	16.7	16.7
Intermittent Use	13	8.1	16.7	33.3
Moderate Use	15	9.4	19.2	52.6
Frequent Use	22	13.8	28.2	80.8
Extensive Use	15	9.4	19.2	100.0
Total	78	48.8	100.0	
Missing	82	51.2		
Total	160	100.0		

6.2 NIST SP 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations				
	Frequency	Percent	Valid Percent	Cumulative Percent
Not Used	35	21.9	45.5	45.5
Intermittent Use	11	6.9	14.3	59.7
Moderate Use	12	7.5	15.6	75.3
Frequent Use	10	6.3	13.0	88.3
Extensive Use	9	5.6	11.7	100.0
Total	77	48.1	100.0	
Missing	83	51.9		
Total	160	100.0		

Performance Assessment Characteristics

6.3 ISO IEC 27001/27002 for 3rd Party Cybersecurity Management				
				Cumulative
	Frequency	Percent	Valid Percent	Percent
Not Used	33	20.6	42.9	42.9
Intermittent Use	8	5.0	10.4	53.2
Moderate Use	11	6.9	14.3	67.5
Frequent Use	11	6.9	14.3	81.8
Extensive Use	14	8.8	18.2	100.0
Total	77	48.1	100.0	
Missing	83	51.9		
Total	160	100.0		

6.4 ISO 20244 Trusted Technology Provider Standard				
				Cumulative
	Frequency	Percent	Valid Percent	Percent
Not Used	50	31.3	64.9	64.9
Intermittent Use	2	1.3	2.6	67.5
Moderate Use	13	8.1	16.9	84.4
Frequent Use	5	3.1	6.5	90.9
Extensive Use	7	4.4	9.1	100.0
Total	77	48.1	100.0	
Missing	83	51.9		
Total	160	100.0		

6.6 SAE AS649 Avoidance, Detections, Mitigation, and Disposition of Fraudulent/Counterfeit Electronic Parts				
	Frequency	Percent	Valid Percent	Cumulative Percent
Not Used	53	33.1	67.9	67.9
Intermittent Use	7	4.4	9.0	76.9
Moderate Use	8	5.0	10.3	87.2
Frequent Use	3	1.9	3.8	91.0
Extensive Use	7	4.4	9.0	100.0
Total	78	48.8	100.0	
Missing	82	51.2		
Total	160	100.0		

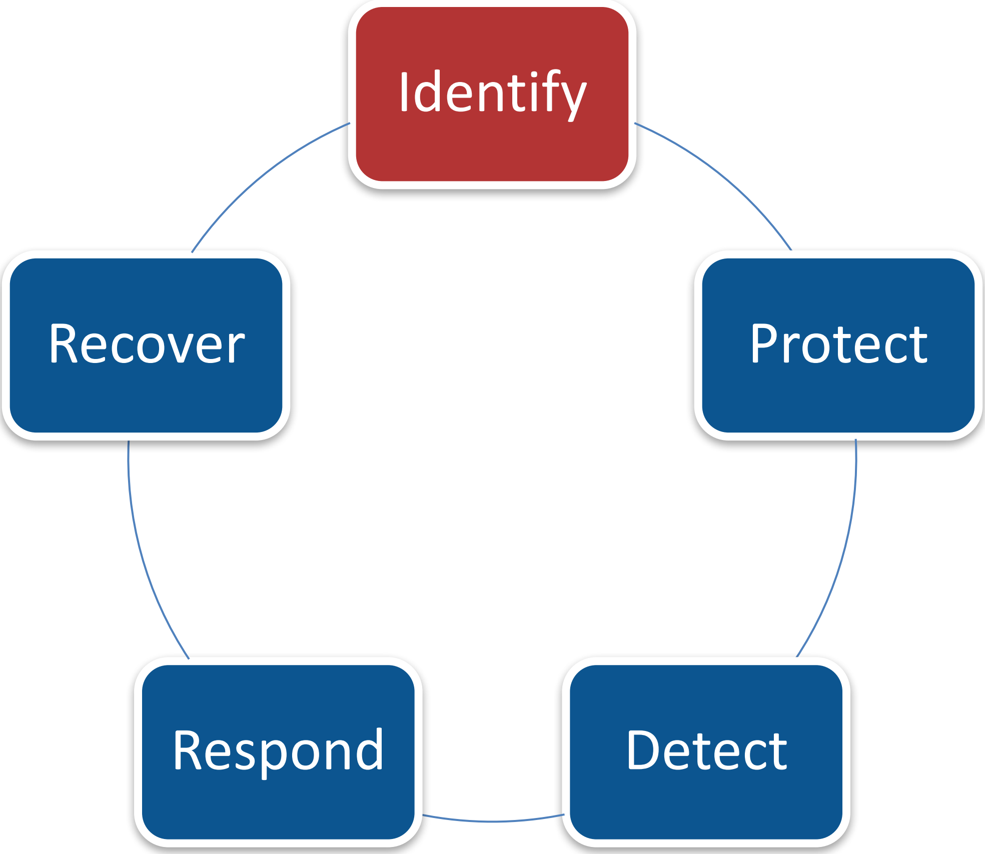
Analytical Methodology

- Negative binomial panel regression technique:
  - Appropriate multiple regression technique based on:
    - Distribution of dependent variable (i.e. skewed distribution, count variable, heavily weighted with zeros)
    - Data spanning multiple years and industries
- Dependent variable:
  - Count of total breaches for a company in a given year
    - Additional analysis was conducted with breach sub-categories (i.e. Deficient Access Breaches; Technical Exploits Breaches; Theft Breaches; and Behavioral Vulnerability Breaches)
- Independent Variables:
  - Respondent score for each survey question
- Control variables:
  - Year, industry, firm

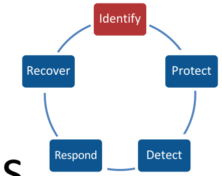
A. Critical policies/actions that reduced breaches, by Framework Category

Identify:

All actions result in building **better foundational understanding** of patterns of network configuration (hubs and nodes); communications/data flows; and states of external network supplier cybersecurity.

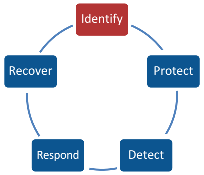


A. Critical policies/actions that reduced breaches, by Framework Category



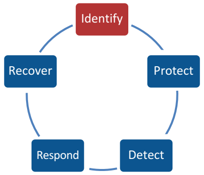
- **Identify**: Actions Most Significant in Leading to Fewer Breaches
  - (in Total and by Category); Statistically Significant in at Least 3 of the 5 Breach Categories (Total; Deficient Access Control; Technical Exploits; Theft; and Behavioral)
- Does your asset management program identify and classify data, systems and processes according to risk/criticality?
  - Breach categories: Deficient Access Control; Technical Exploits; Theft; and Behavioral
  - Respondent Positive Response Rate 78%
- Do you know the largest number of confidential records in any segregated database?
  - Breach categories: Total; Deficient Access Control; and Technical Exploits
  - Respondent Positive Response Rate 51%
- Are all network/application communication flows documented and mapped?
  - Breach categories: Total; Technical Exploits; and Theft
  - Respondent Positive Response Rate 51%

A. Critical policies/actions that reduced breaches, by Framework Category



- **Identify** continued:
  - Does your organization have a map with critical physical supply, distribution & service hubs/ nodes and interrelated flows to help you visualize the IT supply chain?
    - <u>Breach categories:</u> Total; Deficient Access Control; and Technical Exploits
    - Respondent Adoption Rate 40%
  - Do you have a supplier management program that: Establishes and monitors external supplier cybersecurity standards?
    - <u>Breach categories:</u> Total; Deficient Access; Technical Exploits; and Behavioral
    - Respondent Adoption Rate 52%
  - Does your risk dashboard/registry do the following: Defines key cyber risks?
    - <u>Breach categories:</u> Total; Deficient Access Control; and Theft
    - Respondent Adoption Rate 77%

A. Critical policies/actions that reduced breaches, by Framework Category



- **Identify** continued:
  - Note (Negative Association with 2 Breach Categories): Frequent or Extensive Use of NIST SP 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations
    - Breach categories: Technical Exploits and Behavioral
    - Respondent Frequent or Extensive Use Rate 25%
  - SAE AS649 Avoidance, Detection, Mitigation, and Disposition of Fraudulent/Counterfeit Electronic Parts
    - Breach categories: Technical Exploits and Behavioral
    - Respondent Frequent or Extensive Use Rate 13%

A. Critical policies/actions that reduced breaches, by Framework Category

Protect:

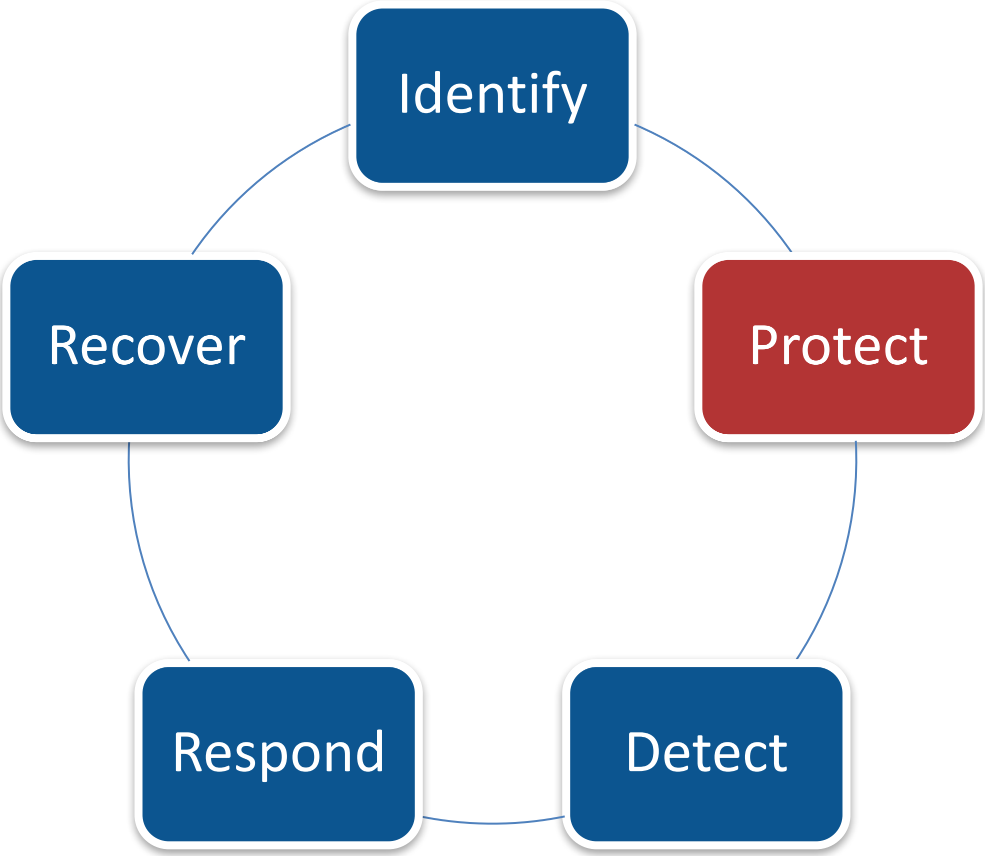
Actions below are technical risk management procedures that seek to establish **better ongoing situational awareness by**:

-Shielding sensitive network segments and information flows

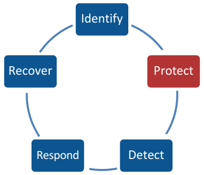
-Assuring secure communications through encryption and separate storage of encryption keys

-Closely tracking changes in software and settings

-Using supply chain quarantines to isolate code or hardware



A. Critical policies/actions that reduced breaches, by Framework Category


Identify

Protect

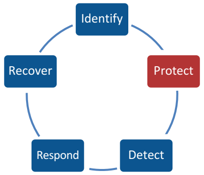
Detect

Respond

Recover

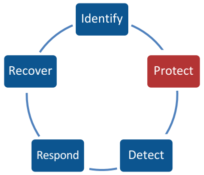
- **Protect**: Actions Most Significant in Leading to Fewer Breaches
    - (in Total and by Category); Statistically Significant in at Least 3 of the 5 Breach Categories (Total; Deficient Access Control; Technical Exploits; Theft; and Behavioral)
  - Do you employ network access control (NAC) for remote connections?
    - <u>Breach categories: </u>Total Deficient Access Control; Technical Exploits; Theft; and Behavioral
    - Respondent Adoption Rate 75%
  - Do you physically and logically segregate your sensitive network segments?
    - <u>Breach categories: </u>Deficient Access Control; Theft; and Behavioral
    - Respondent Adoption Rate 78%
  - Is information of different sensitivity levels prohibited from residing on the same system?
    - <u>Breach categories: </u>Total; Deficient Access Control; Technical Exploits; and Behavioral
    - Respondent Adoption Rate 45%

A. Critical policies/actions that reduced breaches, by Framework Category



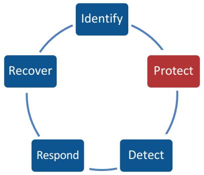
- **Protect** continued:
  - In addition to data being protected at rest and in transit, are the encryption keys securely managed?
    - Breach categories: Total; Deficient Access Control; Technical Exploits; and Theft
    - Respondent Adoption Rate 83%
  - Are the encryption keys stored separately from the data on a key-management server?
    - Breach categories: Total; Technical Exploits; and Theft
    - Respondent Adoption Rate 80%
  - Do you employ FIPS-validated or National Security Agency-approved cryptography to implement signatures?
    - Breach categories: Total; Deficient Access Control; and Technical Exploits
    - Respondent Adoption Rate 67%

A. Critical policies/actions that reduced breaches, by Framework Category



- **Protect** continued:
  - Do you have documented baseline configuration standards for all devices connected to the corporate network?
    - Breach categories: Total; Deficient Access Control; and Technical Exploits
    - Respondent Adoption Rate 60%
  - Is the production environment separate from development and testing environments?
    - Breach categories: Total; Deficient Access Control; Theft; and Behavioral
    - Respondent Adoption Rate 87%
  - Is production data only located in the production environment?
    - Breach categories: Total; Technical; and Behavioral
    - Respondent Adoption Rate 80%

A. Critical policies/actions that reduced breaches, by Framework Category

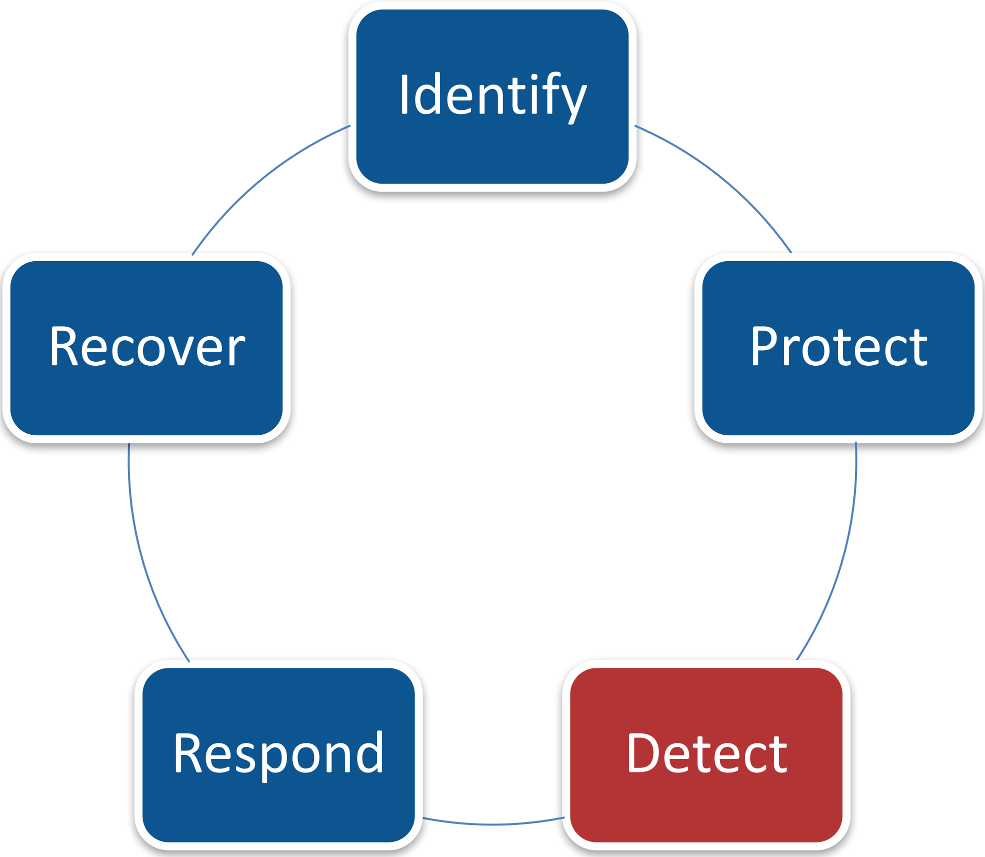


- **Protect** continued:
  - Do you use end to end Configuration Management (CM) systems to track changes to software and settings?
    - Breach categories: Total; Deficient Access Control; and Technical Exploits
    - Respondent Adoption Rate 65%
  - Do you quarantine non-conforming products until they can be verified through inspection/testing?
    - Breach categories: Total; Deficient Access Control; and Theft
    - Respondent Adoption Rate 55%
  - Do you quarantine code from outside suppliers in proxy servers to undergo virus scanning and authentication procedures?
    - Breach categories: Total; Deficient Access Control; and Theft
    - Respondent Adoption Rate 64%

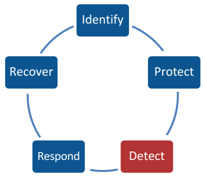
A. Critical policies/actions that reduced breaches, by Framework Category

Detect:

All actions below enable organizations to quickly find cyber anomalies and escalate response activities to manage them.



A. Critical policies/actions that reduced breaches, by Framework Category

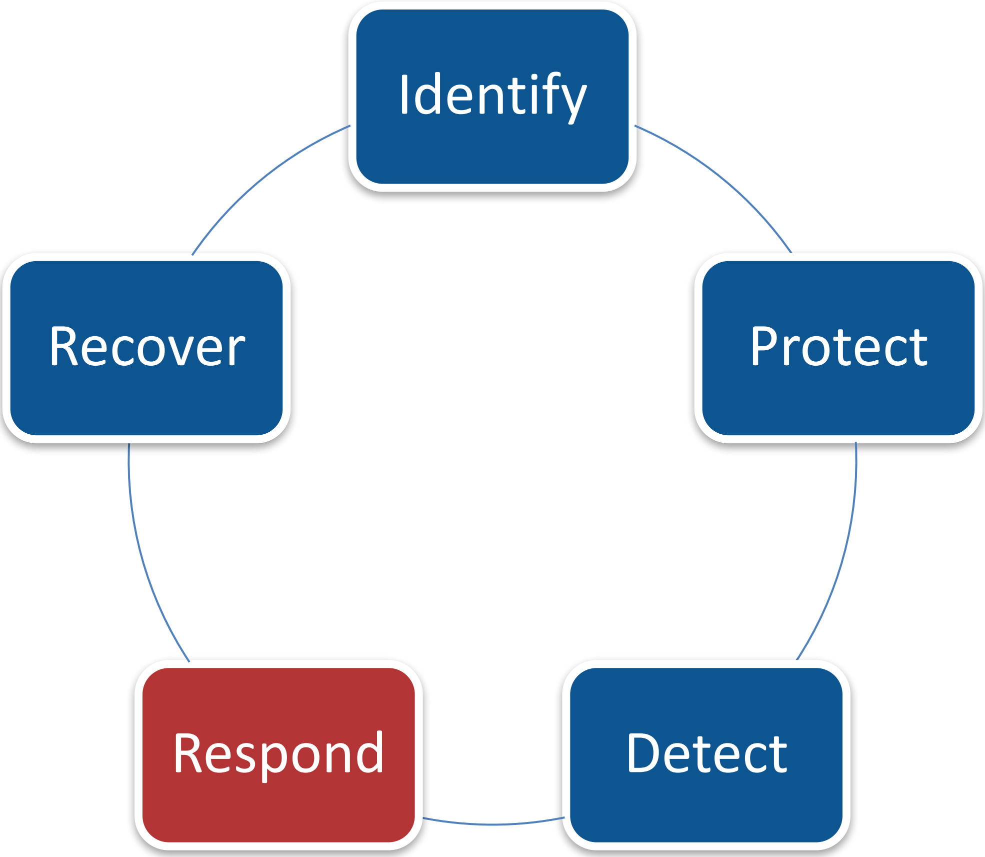


- **Detect**: Actions Most Significant in Leading to Fewer Breaches
    - (in Total and by Category); Statistically Significant in at Least 2 of the 5 Breach Categories (Total; Deficient Access Control; Technical Exploits; Theft; and Behavioral)
- Has an organizational baseline of expected data flows been established?
    - Breach categories: Total; Deficient Access Control; Technical Exploits; and Theft
    - Respondent Adoption Rate 51%
- Does your SIEM dashboard display event information for units managed by external service providers?
    - Breach categories: Total; and Deficient Access Control
    - Respondent Adoption Rate 56%
- Is anti-virus software deployed on endpoints to detect malicious code?
    - Breach categories: Total and Behavioral
    - Respondent Adoption Rate 97%
- Do you do in-house final inspection and conformity assessments of technology products & components that you manufacture prior to internal use or release to the customer?
    - Breach categories: Total; and Deficient Access Control
    - Respondent Adoption Rate 77%

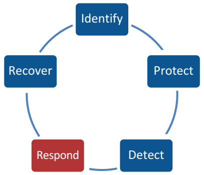
A. Critical policies/actions that reduced breaches, by Framework Category

Respond

Building effective response capabilities involve both *internal skill-building* (creation of an effective Incident Response Team and Incident Response Plan); and *external specialty skill access* (ongoing retainer with 3rd party forensics specialist).



A. Critical policies/actions that reduced breaches, by Framework Category

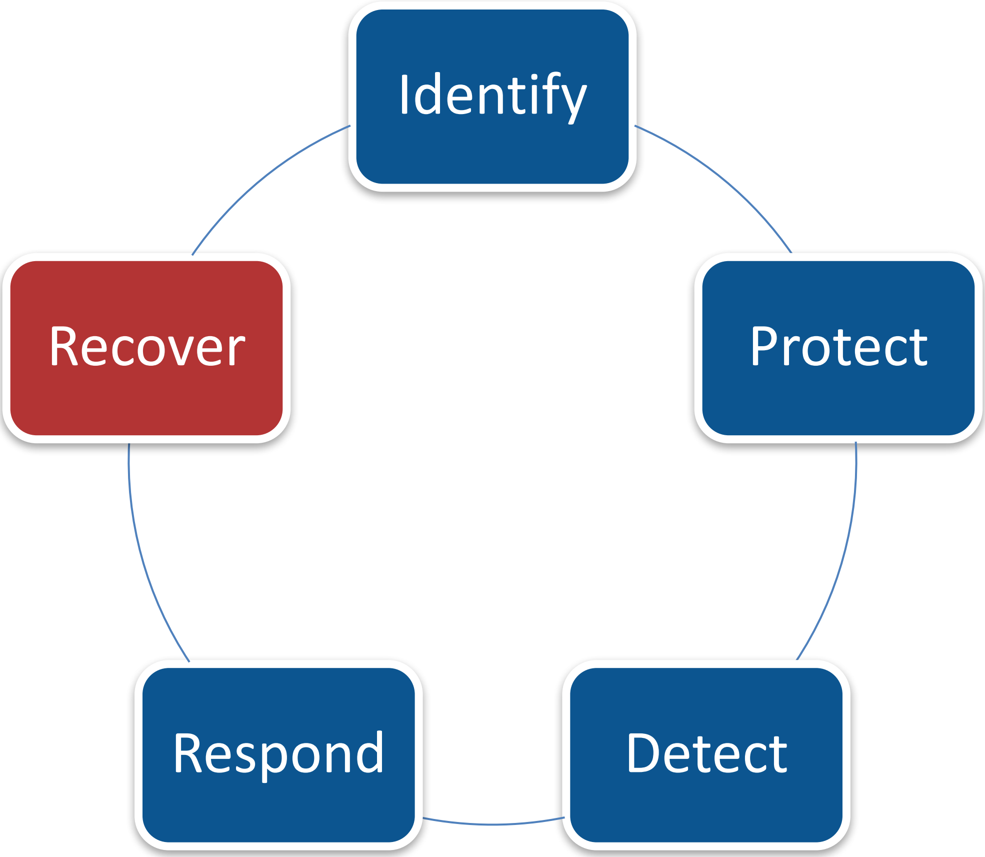

Identify
Protect
Detect
Respond
Recover

- **Respond**: Actions Most Significant in Leading to Fewer Breaches
    - (in Total and by Category); Statistically Significant in at Least 2 of the 5 Breach Categories (Total; Deficient Access Control; Technical Exploits; Theft; and Behavioral)
  - Do you require any counterfeit/grey market products that are detected and do not have forensic or evidentiary value be destroyed by reputable disposers?
    - Breach categories: Total; Deficient Access Control; and Theft
    - Respondent Adoption Rate 32%
  - Do you have a defined incident response team that has high level participation from all pertinent business functions and has clearly defined roles for response team members?
    - Breach categories: Total; and Theft
    - Respondent Adoption Rate 69%
  - Do you have an incident response plan that addresses system details and procedures for reporting and managing a suspected incident?
    - Breach categories: Technical Exploits; and Theft
    - Respondent Adoption Rate 72%
  - Does your forensics capability rely on a third party security company with ongoing retainer?
    - Breach categories: Deficient Access Control; and Technical Exploits
    - Respondent Adoption Rate 50%

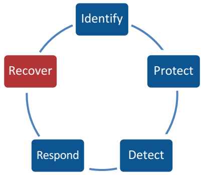
A. Critical policies/actions that reduced breaches, by Framework Category

Recover:

Building effective recovery capabilities require high levels of overall readiness/ preparedness including automated system backups; rapid damage assessment/insurance filings; and Standard Operating Procedures (SOPs) for internal/external stakeholder communications.



A. Critical policies/actions that reduced breaches, by Framework Category



- **Recover**: Actions Most Significant in Leading to Fewer Theft Breaches
  - Do you have an IT system-level data back-up/restore process that will allow for restoration of normal business processing in the event of disaster (including ransomware or DDoS)?
    - Respondent Adoption Rate 93%
  - Do you think your company is positioned to file and settle cyber insurance claims faster than your competitors?
    - Respondent Agreement Rate 50%
  - Do you have cyber risk communications mechanisms in place to communicate recovery status with your employees and/or shareholders?
    - Respondent Adoption Rate 75%

B. Critical policies/actions that reduced total breaches & specific breach types

Impactful policies & actions – Breach types

Total No.
DCA
Tech Exploit
Theft
Behavioral Vulnerability

Reducing The Total Number Of Breaches

- Strategic Cyber Policies & Actions
  - Defined Incident Response Team with high level participation from all business functions.
  - Incident Response Plan that addresses system details for managing suspected incidents.
- Cyber Hygiene/Systems Management
  - Track changes for software & settings.
  - Quarantining code from outside suppliers in proxy servers.
  - Having a supplier management program that establishes and monitors external supplier cyber-security standards.

Impactful policies & actions – Breach types

Total No.

DCA

Tech Exploit

Theft

Behavioral Vulnerability

Reducing Deficient Access Control Breaches

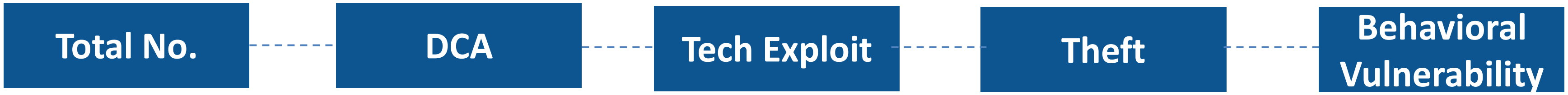
- Segmenting data systems with risk-based criticality analyses e.g. targeting systems which need to be managed more aggressively.
- Administrative consistency & vigor in applying risk controls:
  - Quarantining code and data.
  - Segregating sensitive network segments.
  - Establishing remote site continuous auditing (e.g. code scanning engine at a supplier site).
  - Managing continuously changing user roles, access levels and permissions.

Impactful policies & actions – Breach types

Reducing Technical Exploit Breaches

- Encryption keys stored separately from the data on a key management server.
- Encrypted data in transit carefully planned so as not to blind/hinder the organization’s security technologies.
- Use of these two standards appear critical in reducing technical exploit breaches: NIST’s SP 800-161, “Supply Chain Risk Management Practices For Federal Information Systems & Organizations; and SAE AS649 “Avoidance, Detection Of Fraudulent/Counterfeit Electronics Parts”.

Impactful policies & actions – Breach types


Total No.
DCA
Tech Exploit
Theft
Behavioral Vulnerability

Reducing Theft Breaches

- Conduct a Security Awareness Program that is a requirement for all users of IT systems
  - e.g. An organization launches an email phishing attack on its own employees to raise awareness of risk.
- Network Risk Management Controls & Alerts are automated, with an IT system-level data back-up/restore process that will allow for restoration of normal business processing in event of disaster or to reduce impacts of threats such as ransom ware.

Impactful policies & actions – Breach types

Total No.

DCA

Tech Exploit

Theft

Behavioral Vulnerability

Reducing Behavioral Vulnerability Breaches

- Strong Chief Executive Officer integration with IT Security Team, with CEO setting tone for whole organization, making all corporate IT users more aware of security mandate and defining/changing the culture.
- Use of ISO Standard IEC 27001/27002 For 3rd Party Cybersecurity Management was associated with lowered behavioral vulnerability breaches; and joined NIST's SP800-161 and SAE's AS649 as part of the triad of impactful practice guidelines in breach management.
- Perhaps the use of the ISO 3rd Party Standard enables high performing organizations to more systematically select vendors whose cyber security cultures mirror their own.

Project Lessons Learned

- Given the comprehensive & sensitive nature of the self-assessment tool, a supply chain "driver" organization (e.g. a large global high tech company) with the economic leverage to mandate adoption across its internal supply chain and external vendor base should be a primary vehicle of distribution.

- This distribution across the supply chain and aligned vendors of focal organizations will be the most efficient way to attain the scale of participant responses and data necessary to attain high levels of confidence in the results.

Project Lessons Learned

- The current, fragmented nature of cyber breach data means that analysts must use multiple sources to build complete & accurate cyber breach data repositories.

- The difficulty of obtaining high quality and comprehensive data will persist:
  - until such time as the insurance industry requires clients to undergo full cyber assessment and risk disclosure.
  - until marketplace risks and legal/financial liabilities force cyber breach disclosure.
  - until there is a legislative or regulatory-driven cyber breach disclosure mandate.

Appendix – Impactful policies & actions

Number of Total Breaches

2. Do you have a defined incident response team that has high level participation from all pertinent business functions and has clearly defined roles for response team members?

3. Do you have an incident response plan that addresses system details and procedures for reporting and managing a suspected incide

1. Do you require any counterfeit/grey market products that are detected and do not have forensic or evidentiary value be destroyed by reputable disposers?

5. Do you quarantine non-conforming products until they can be verified through inspection/testing?

6. Do you quarantine code from outside suppliers in proxy servers to undergo virus scanning and authentication procedures?

3.1 Track changes to software and settings?

4. Do you employ network access control (NAC) for remote connections?

6. Are secure procedures in place to manage that vendor access (modem call-back for example)?

7.2 Traffic from systems on the DMZ cannot directly reach the internal network, but only through a middle-ware layer, etc.?

10. Is information of different sensitivity levels prohibited from residing on the same system?

4. In addition to data being protected at rest and in transit, are the encryption keys securely managed?

5. Are the encryption keys stored separately from the data on a key-management server?

7. Do you employ FIPs-validated or National Security Agency-approved cryptography to implement signatures?

12. Do you have documented baseline configuration standards for all devices connected to the corporate network

15. Is sensitive data prohibited from residing on public-facing systems, such as the DMZ?

16. Is the production environment separate from other development and testing environments?

17. Is production data only located in the production environment?

4.1 Defines key cyber risks?

2.1 IT Security standards?

7.1 Inherited risk controls from your cloud service provider?

3. Does your organization have a map with critical supply, distribution & service hubs/ nodes and inter-related flows to help you visualize the IT supply chain?

3.1 How often is it updated: 1; 2; 3?

5.1 Segments and prioritizes vendors of critical hardware/software/network services?

5.2 Establishes and monitors external supplier cybersecurity standards?

2.a. Does this program specify security standards for each class of data?

4. Is software versioning and patching history recorded for all applicable IT assets?

6. Do you know the largest number of confidential records in any segregated database?

11. Are all network/application communication flows documented and mapped?

2. Is anti-virus software deployed on endpoints to detect malicious code?

5. Do you do in-house final inspection and conformity assessments of technology products & components that you manufacture prior to internal use or release to the customer?

1. Has an organizational baseline of expected data flows been established?

2.2 For units managed by external service provider?

Appendix – Impactful policies & actions

Deficient Access Control Breaches

2.2 Third party security company with ongoing retainer?

2.3 Forensic services contracted as needed?

1. Do you require any counterfeit/grey market products that are detected and do not have forensic or evidentiary value be destroyed by reputable disposers?

5. Do you quarantine non-conforming products until they can be verified through inspection/testing?

6. Do you quarantine code from outside suppliers in proxy servers to undergo virus scanning and authentication procedures?

3.1 Track changes to software and settings?

4. Do you employ network access control (NAC) for remote connections?

9. Do you physically and logically segregate your sensitive network segments?

10. Is information of different sensitivity levels prohibited from residing on the same system?

11. Do you establish remote site continuous auditing/surveillance methods: e.g. a code scanning engine at the supplier site to monitor work in progress?

4. In addition to data being protected at rest and in transit, are the encryption keys securely managed?

7. Do you employ FIPs-validated or National Security Agency-approved cryptography to implement signatures?

12. Do you have documented baseline configuration standards for all devices connected to the corporate network

15. Is sensitive data prohibited from residing on public-facing systems, such as the DMZ?

16. Is the production environment separate from other development and testing environments?

4.1 Defines key cyber risks?

7.1 Inherited risk controls from your cloud service provider?

3. Does your organization have a map with critical supply, distribution & service hubs/ nodes and inter-related flows to help you visualize the IT supply chain?

3.1 How often is it updated: 1; 2; 3?

5.2 Establishes and monitors external supplier cybersecurity standards?

2. Does your asset management program identify and classify data, systems and processes according to risk/criticality?

6. Do you know the largest number of confidential records in any segregated database?

5. Do you do in-house final inspection and conformity assessments of technology products & components that you manufacture prior to internal use or release to the customer?

9. Do you screen mobile code and implement corrective actions to handle unacceptable code?

1. Has an organizational baseline of expected data flows been established?

2.2 For units managed by external service provider?

Appendix – Impactful policies & actions

Tech Exploit Breaches

1.3 Notifications to third party insurer of loss of revenue?
2.2 Third party security company with ongoing retainer?
3. Do you have an incident response plan that addresses system details and procedures for reporting and managing a suspected incide
8. Is the organizational policy for removable media enforced?
3.1 Track changes to software and settings?
5. Are technical solutions in place to enforce standard configurations?
4. Do you employ network access control (NAC) for remote connections?
7.2 Traffic from systems on the DMZ cannot directly reach the internal network, but only through a middle-ware layer, etc.?
10. Is information of different sensitivity levels prohibited from residing on the same system?
11. Do you establish remote site continuous auditing/surveillance methods: e.g. a code scanning engine at the supplier site to monitor work in progress?
1. Are data classified as critical/sensitive encrypted at rest?
3. Do you encrypt software and software patches at rest and in motion throughout delivery?
4. In addition to data being protected at rest and in transit, are the encryption keys securely managed?
5. Are the encryption keys stored separately from the data on a key-management server?
6. Is encrypted data in transit carefully planned so as not to blind/hinder the organization's security technologies?
7. Do you employ FIPs-validated or National Security Agency-approved cryptography to implement signatures?
8. Do you use anti-tamper mechanisms to counter data theft and subversion, including auto-destruction if tampering is detected?
10. Do you use Data Loss Prevention (DLP) software for data in use, in motion, and at rest?
12. Do you have documented baseline configuration standards for all devices connected to the corporate network
17. Is production data only located in the production environment?
1. Do you have a mission statement for your cyber security risk management program?
2. Is the organization's risk tolerance identified and clearly documented?
3. Do you have a cyber risk management organizational chart with reporting relationships delineated?
5. Do you have a process in place to manage trusted vendors
2.1 IT Security standards?
3.4 Chief Executive Officer
3.6 Chief Compliance Officer
3.7 Board Risk/Audit Committee
7.2 Dual or joint risk controls?
7.3 Board Risk/Audit Committee?
3. Does your organization have a map with critical supply, distribution & service hubs/ nodes and inter-related flows to help you visualize the IT supply chain?
4. Do you set objectives for time to recovery for critical IT supply chain nodes/locations?
5.2 Establishes and monitors external supplier cybersecurity standards?
6.2 NIST SP 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations
6.6 SAE AS649 Avoidance, Detections, Mitigation, and Disposition of Fraudulent/Counterfeit Electronic Parts
2. Does your asset management program identify and classify data, systems and processes according to risk/criticality?
4. Is software versioning and patching history recorded for all applicable IT assets?
6. Do you know the largest number of confidential records in any segregated database?
11. Are all network/application communication flows documented and mapped?
8. Do you extract and analyze all anomalies from audit logs, access reports, and security incident tracking reports?
1. Has an organizational baseline of expected data flows been established?

Appendix – Impactful policies & actions

Theft Breaches

2. Do you have a defined incident response team that has high level participation from all pertinent business functions and has clearly defined roles for response team members?
3. Do you have an incident response plan that addresses system details and procedures for reporting and managing a suspected incide
1. Do you require any counterfeit/grey market products that are detected and do not have forensic or evidentiary value be destroyed by reputable disposers?
2.2 Identify residual risks?
2.3 Implement additional controls to mitigate those residual risks?
1. Do you have a crisis communications plan that can inform key internal/external stakeholders of the status of cyber breaches?
2. Do you have an IT system level data back-up/restore process that will allow for restoration of normal business processing in the event of disaster (including ransomeware or DDoS)?
4. Do you employ tools and techniques to determine if authentication tokens (e.g. passwords, biometrics) are sufficiently strong to resist attacks?
5. Do you quarantine non-conforming products until they can be verified through inspection/testing?
6. Do you quarantine code from outside suppliers in proxy servers to undergo virus scanning and authentication procedures?
1. Do you think your company is positioned to file and settle cyber insurance claims faster than your competitors
2. Do you have cyber risk communications mechanisms in place to communicate recovery status with your employees and/or shareholders?
7. Do you evaluate measures of common vulnerabilities (CVSS scores) of your software suppliers?
9.3 As needed?
2. Do you conduct a Security Awareness program that is a requirement for all users of IT systems?
4. Do you employ network access control (NAC) for remote connections?
6. Are secure procedures in place to manage that vendor access (modem call-back for example)?
9. Do you physically and logically segregate your sensitive network segments?
2. Are data classified as critical/sensitive encrypted in transit?
4. In addition to data being protected at rest and in transit, are the encryption keys securely managed?
5. Are the encryption keys stored separately from the data on a key-management server?
8. Do you use anti-tamper mechanisms to counter data theft and subversion, including auto-destruction if tampering is detected?
16. Is the production environment separate from other development and testing environments?
4.1 Defines key cyber risks?
4.2 Identifies responsible parties to manage the cyber risks?
4.3 Shows status of mitigation actions?
3. Do you have Indicators of Compromise (IOCs) (e.g., virus signatures, IP addresses, urls of botnet command servers, etc.) incorporated into the detection/monitoring process?
5.1 Segments and prioritizes vendors of critical hardware/software/network services?
2. Does your asset management program identify and classify data, systems and processes according to risk/criticality?
2.a. Does this program specify security standards for each class of data?
11. Are all network/application communication flows documented and mapped?
1. Has an organizational baseline of expected data flows been established?

Appendix – Impactful policies & actions

Behavioral Vulnerability Breaches

9.1 At contract initiation?

4. Do you employ network access control (NAC) for remote connections?

9. Do you physically and logically segregate your sensitive network segments?

10. Is information of different sensitivity levels prohibited from residing on the same system?

2. Are data classified as critical/sensitive encrypted in transit?

16. Is the production environment separate from other development and testing environments?

17. Is production data only located in the production environment?

1. Do you have a mission statement for your cyber security risk management program?

2. Is the organization's risk tolerance identified and clearly documented?

4. Do you have a risk dashboard/registry?

8. Is it required that key suppliers report major changes in their operating structure (e.g. physical move to a different location/offshoring, change in ownership, outsourcing)?

2.1 IT Security standards?

3.4 Chief Executive Officer

4. Do you set objectives for time to recovery for critical IT supply chain nodes/locations?

5.2 Establishes and monitors external supplier cybersecurity standards?

6.2 NIST SP 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations

6.3 ISO IEC 27001/27002 for 3rd Party Cybersecurity Management

6.6 SAE AS649 Avoidance, Detections, Mitigation, and Disposition of Fraudulent/Counterfeit Electronic Parts

7.2 Self-Assessment with Third-Party Validation

2. Does your asset management program identify and classify data, systems and processes according to risk/criticality?

2. Is anti-virus software deployed on endpoints to detect malicious code?