## 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; dataunintentional 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**

000



## **Description of Respondents**

100,0

0.0

What	most accurately deso	cribes your job title / pro	fessional 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**

100,0

000

How large is your company?													
					Frequency		Percent Valid Pe			Valid Perc	cent Cumulative Perc		lative Percent
Annual sales between \$100 million -\$1 billion									14.4	14.4			14.4
Annual sale	s between \$2	0-\$50 million							18.1	18.1			32.5
Annual sale	s between \$5	0-\$100 millio	า			11			6.9		6.9		39.4
Annual sale	s greater thar	n \$1 billion				40			25.0		25.0		64.4
Annual sale	s less than \$2	0 million				57			35.6		35.6		100.0
Total					:			100.0		100.0	00.0		
	Are you a P	Parent or Subs	idiary comp	bany?				D	pes your company provide Hardware?				
					Cumulative								Cumulative
	Frequency	Percent	Valid Perc	ent	Percent			Frequ	iency	Percent	Valid Pe	ercent	Percent
Parent	139	86.9	8	36.9	86.9	No	)		118	73.8		73.8	73.8
Subsidiary	21	13.1	1	13.1	100.0	Ye	S		42	26.3		26.3	100.0
Total	160	100.0	10	0.00		То	tal		160	100.0		100.0	
					Are your ne	two	rks/IT syste	ems:					
				Frequency Percent Valid Percent Cumulative P							e Percent		
Primarily m	anaged by yo	ur own unit			75			46.9		46.9		46.9	
Primarily m	anaged by yo	ur parent orga	anization		85		53.1		53.1	53.1		100.0	
Total					160			100.0		100.0			



### **Description of Respondents**

1005

Does yo	ur company p	rovide Telecom	/Data Network Pr	Does your company provide Hosted/Cloud Applications?					
	Frequency	Percent	Valid Percent	Cumulative Percent		Frequency	Percent	Valid Percent	Cumulative Percent
No	124	77.5	77.5	77.5	No	106	66.3	66.3	66.3
Yes	36	22.5	22.5	100.0	Yes	54	33.8	33.8	100.0
Total	160	100.0	100.0		Total	160	100.0	100.0	

	Does your company cu	irrently supply IT products/se	ervices to the federal governm	ient?
	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 Cybers	nework for Pla	nning and Mana	agement	6.2 NIST SP 800-161, Supply Chain Risk Management Practices for						
					Federal Information Systems and Organizations					
				Cumulative					Cumulative	
	Frequency	Percent	Valid Percent	Percent		Frequency	Percent	Valid Percent	Percent	
Not Used	13	8.1	16.7	16.7	Not Used	35	21.9	45.5	45.5	
Intermittent Use	13	8.1	16.7	33.3	Intermittent Use	11	6.9	14.3	59.7	
Moderate Use	15	9.4	19.2	52.6	Moderate Use	12	7.5	15.6	75.3	
Frequent Use	22	13.8	28.2	80.8	Frequent Use	10	6.3	13.0	88.3	
Extensive Use	15	9.4	19.2	100.0	Extensive Use	9	5.6	11.7	100.0	
Total	78	48.8	100.0		Total	77	48.1	100.0		
Missing	82	51.2			Missing	83	51.9			
Total	160	100.0			Total	160	100.0			



### **Performance Assessment Characteristics**

6.3 ISO IEC 27001/27002 for 3rd Party Cybersecurity Management					6.4 ISO 20244 Trusted Technology Provider Standard					
				Cumulative					Cumulative	
	Frequency	Percent	Valid Percent	Percent		Frequency	Percent	Valid Percent	Percent	
Not Used	33	20.6	42.9	42.9	Not Used	50	31.3	64.9	64.9	
Intermittent Use	8	5.0	10.4	53.2	Intermittent Use	2	1.3	2.6	67.5	
Moderate Use	11	6.9	14.3	67.5	Moderate Use	13	8.1	16.9	84.4	
Frequent Use	11	6.9	14.3	81.8	Frequent Use	5	3.1	6.5	90.9	
Extensive Use	14	8.8	18.2	100.0	Extensive Use	7	4.4	9.1	100.0	
Total	77	48.1	100.0		Total	77	48.1	100.0		
Missing	83	51.9			Missing	83	51.9			
Total	160	100.0			Total	160	100.0			
	6.6 SA	E AS649 Avoid	ance, Detections	, Mitigation, and	Disposition of Frau	dulent/Count	terfeit Electron	ic Parts		
	Frequency Perce		nt	Valid Per	cent	Cumulativ	e 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				
Frequent Use			3		1.9	3.8		91		
Extensive Use			7		4.4		9.0		100.0	
Total			78		48.8		100.0			
Missing			82		51.2					
Total			160		100.0					



© All rights reserved Supply Chain Management Center 2017, do not reproduce without authorization

## **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







#### > 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%



#### 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?
  - Breach categories: 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?
  - Breach categories: Total; Deficient Access; Technical Exploits; and Behavioral
  - Respondent Adoption Rate 52%
- Does your risk dashboard/registry do the following: Defines key cyber risks?
  - Breach categories: Total; Deficient Access Control; and Theft
  - Respondent Adoption Rate 77%



#### 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%



#### **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





#### 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?
  - Breach categories: 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%



#### Protect continued:

- In addition to data being protected at rest and in transit, are the encryption keys securely managed?
  - <u>Breach categories:</u> Total; Deficient Access Control; Technical Exploits; and Theft
  - Respondent Adoption Rate 83%
- Are the encryption keys stored separately from the data on a keymanagement 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%



#### 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?
  - > <u>Breach categories:</u> 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%



#### 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%



#### **Detect:**

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





#### > **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%



#### 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 3<sup>rd</sup> party forensics specialist).





#### **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%

#### **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.







- 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





#### **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.





#### **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.





#### **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".





#### **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.





#### **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 3<sup>rd</sup> 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.



#### **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?



#### **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 guarantine non-conforming products until they can be verified through inspection/testing? 6. Do you guarantine 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?



#### **Tech Exploit Breaches**

<ul> <li>2.1 Tai day security company with ongoing relation?</li> <li>2.5 Doy have an orient divert response tain that diverses system details and procedures for reportage and managing a suspected midde.</li> <li>8. Bo construct and section of the diverse standard configuration?</li> <li>6. A rest tained is outdross in place to enforce standard configuration?</li> <li>7.1 Faiffer from systems on the DMC cannot directly reach the internal network, but only through a middle-ware layer, etc.?</li> <li>10. Bo you analysis outdross cances config diverse standard configuration standards in unclus on trading on the same system?</li> <li>11. Do you analysis outdross cances config diverse standard configuration and diverse you and diverse you and diverse you and diverse standard configuration through but deliverse?</li> <li>11. A vasi a cancel diverse standard configuration through but deliverse?</li> <li>12. A read acad standard and trading are test and an insuit on through but deliverse?</li> <li>13. A read acad standard tain trading are test and an insuit on through but deliverse?</li> <li>14. A read acad standard tain trading are test and an insuit on through but deliverse?</li> <li>13. Do you analysis of Naviane and standard trading are test and an insuit on through but deliverse?</li> <li>14. So you analysis of Naviane and standard trading are diverse contrasting.</li> <li>15. So you analysis of Naviane and trading are diverse contrasting are relation trading are are relation trading are proceed at relation trading are are relation to a standard to relation trading are are relation to a standard to relation trading are are relation to a standard to relation trading are are relation trading are are relation to a standard to relation trading are are relation to a standard to relation trading are are relation trading are relation trading are are relation trading are are relation trading are are relatis and trading are relation trading are relation trading are re</li></ul>	1.3 Notifications to third party insurer of loss of revenue?
<ul> <li>B. Dy was an incident response plan that addresses system details adprocedures for reporting and managing a suspected incide.</li> <li>B. Is the organizational policy for encouncils media enforcedures for reporting and managing a suspected incide.</li> <li>B. Is the organizational policy for encouncils media enforcedures for report in enforced and setting?</li> <li>A tre think ad build in plant the order is standard configurations?</li> <li>D. Su engloy network access control (IAC) for encote connections?</li> <li>T. Arffer form systems on the DMC connections of the same system?</li> <li>D. Su engloy network access control (IAC) for encote connections?</li> <li>D. Are data classified as critical plants the encryptical encote set canning engline at the supplier site to monitor work in progress?</li> <li>Are data classified as critical plants the encryptical deliver?</li> <li>A fare data scitical plants the encryptical deliver?</li> <li>A fare data scitical plants due to the order plant being scitical plants due to the plant basing scitical plants due to the order plant basing scitical plant basing scitical plants due to the order plant basing sciti</li></ul>	2.2 Third party security company with ongoing retainer?
8. bk genizitional policy removable media metriced <sup>2</sup> 9. Track changes to software and setting <sup>2</sup> 9. Jack changes to software and setting <sup>2</sup> 0. Poyue and/point week access control (ReX) for reacts does network, but only through a middle-ware layer, etc. <sup>2</sup> 1.2. Infecting the software and setting the software layer, etc. <sup>2</sup> 1.0. Information of inferent sensity through setting and the software layer, etc. <sup>2</sup> 1.0. Information of inferent sensity through setting and the software layer, etc. <sup>2</sup> 1.0. Information of inferent sensity through setting and the software layer, etc. <sup>2</sup> 1.0. Information of inferent sensity through setting and the software layer, etc. <sup>2</sup> 1.0. Information of inferent sensity through setting and through setting and the software and soft	3. Do you have an incident response plan that addresses system details and procedures for reporting and managing a suspected incide
<ul> <li>1.1 Tack hanges to software and setting<sup>2</sup></li> <li>5.4 reterinal solutions in place to enforce standard configurations?</li> <li>6.0 you enploy network acces control (NAC) for renote connections?</li> <li>7.2 traffic from yours on the DMZ connections on the same system?</li> <li>1.1 For formation of different sectivity levels prolibiled from residue on the same system?</li> <li>1.2 hours catability formation and directivity residue methods: e.g. acces canning engles at the supplier site to monitor work in progress?</li> <li>1.2 hours catability former add some and the same methods: e.g. acces canning engles at the supplier site to monitor work in progress?</li> <li>2.3 hours catability former add some and the same methods: e.g. acces canning engles at the supplier site to monitor work in progress?</li> <li>3.4 hours catability former add some and the same methods: e.g. acces canning engles at the supplier site to monitor work in progress?</li> <li>4.6 hours catability former ded some and the same methods: e.g. acces catability for the destant and monitor throughout delivery?</li> <li>4.6 hours catability former ded some and the same progress?</li> <li>6.8 hours catability former ded some and the same methods: e.g. access catability for the destant and the same same and the same same same same same same same sam</li></ul>	8. Is the organizational policy for removable media enforced?
<ul> <li>5. Are technical solutions in place to enforce standard configurations?</li> <li>6. Joy our endpy network acces control (RAG) for ensolution enters any stem?</li> <li>7. Tenffer form systems on the DMZ cannot directly reach the internal network, but only through a middle-ware layer, etc.?</li> <li>10. Is our establish renotes tec continuous auding/surveillance methods: e.g. a code scanning engine at the supplier site to monitor work in progress?</li> <li>11. Are dua cassified a critical/sentitive encryted at rest and in moniton throughout deliver?</li> <li>12. Are dua cassified as critical/sentitive encryted at rest and in moniton throughout deliver?</li> <li>13. Are dua cassified as critical/sentitive encryted at rest and in moniton throughout deliver?</li> <li>14. Indiation to dua being protected at rest and in moniton systems scence?</li> <li>15. Are ten comptiton keys stored separately from ted ato a sey -management server?</li> <li>16. Securyted data in transit carefully planed so as not to hind/induce transitive technologies?</li> <li>10. Do you use plate loss Proteention [DP] software for data in use, in motion, and at rest?</li> <li>10. Do you use plate loss Proteention [DP] software for data in use, in motion, and at rest?</li> <li>10. Do you use plate loss Proteention [DP] software for data in use, in motion, and at rest?</li> <li>10. Do you use plate loss Proteention [DP] software for data in use, in motion, and at rest?</li> <li>10. Do you use plate loss Proteention [DP] software for data in use, in motion, and at rest?</li> <li>10. Do you use plate loss proteention [DP] software for data in use, in motion, and at rest?</li> <li>10. Do you here at roces in transiticant (MP) reproteention [DP] software for data in use, in motion, and at rest?</li> <li>10. Do you here at proteents in balancement organization data rest?</li> <li>10. Do you here at proteents in balancement data in group contain at adatat for all duries</li></ul>	3.1 Track changes to software and settings?
<ul> <li>4. Do yue neploy network ascs control (MAC) for renote connections?</li> <li>7. Straffic from yeaking on the DAX connections?</li> <li>8. Straffic from yeaking on the DAX connections?</li> <li>9. Straffic from yeaking on the DAX connections?</li> <li>9. Straffic from yeaking on the DAX connection?</li> <li>9</li></ul>	5. Are technical solutions in place to enforce standard configurations?
2.1 rank from systems on the DMZ cannot directly reach the internal network, but only through a middle ware layer, etc.?         10. is information of different sensity levels prohibed from reading on the same system?         11. Do yue stabilish remote site continuous audiffug/survellance methods: e.g. a code scanning engine at the supplier site to monitor work in progress?         11. Do yue stabilish remote site continuous audiffug/survellance methods: e.g. a code scanning engine at the supplier site to monitor work in progress?         12. No us carryst offware and software patches at rest and in mation throughout deliver?         13. do yue carryst offware and software patches at rest and in mation throughout deliver?         15. do yue carryst offware and software patches and software patches activity technologies?         15. do yue us patch in the stand and varvesine, including audi destruction of tampering is detected?         15. Do yue us bat loss Prevention (DIP) software for data in use, in motion, and at rest?         15. Do yue us bat loss prevention (CIP) software for data in use, in motion, and at rest?         15. Do yue us bat loss prevention (CIP) software for data in use, in motion, and at rest?         16. Do yue use bat loss prevention (CIP) software for data in use, in motion, and at rest?         17. Is production data only located in the production environment?         18. Do yue loas a process in place to manage trutted vedors         19. Jo yue loas a process in place to manage trutted vedors         20. Jo yue loas at place torin cognizational factual twith traporting r	4. Do you employ network access control (NAC) for remote connections?
10. Is information of different sensitivity levels prohibited from residing on the same system?         11. Or you stability increds site contributes activity is excerpted at rest?         12. Are datasified as critical/sensitive encrypted at rest?         13. Or you encrypted vitable encrypted is trans, are the encryption key securely managed?         54. Are the encryption keys stored separately from the data on a key management server?         65. Is encrypted data in transit, are the encryption key securely managed?         75. Are the encryption keys stored separately from the data in use, in motion, and segarately sequence signatures?         76. Do you encrypti Nervaldated or Manidal Security Ageneratory hou indigement signatures?         76. Do you encrypti Nervaldated or Manidal Security Ageneratory hou indigement signatures?         76. Do you encrypti Nervaldated or Manidal Security Ageneratory hou indigement signatures?         76. Do you have a fortarence identified and dealy documented?         76. Broapmatation's risk to learner data theff and subscine context on the corporate network         77. Broapmatation is application standards for all divises connected to the corporate network         78. Do you have a process in place to manage trusted view monage?         79. Do you have a process in place to manage trusted view monage?         70. Do you have a process in place to manage trusted view monage?         70. Do you have a process in place to manage trusted view monage?         70. Do you have a process in place to manage trust	7.2 Traffic from systems on the DMZ cannot directly reach the internal network, but only through a middle-ware layer, etc.?
<ol> <li>De you establish remote site continuous autifung/surveillance methods: e.g. a code scanning engine at the surplier site to monitor work in progress?</li> <li>De you encrypt software and software patches at rest and in motion throughout delivery?</li> <li>An addition to deal being protected at rest and in rains, are the encryption key stored yeaparately from the data on a key-management server?</li> <li>So you employ FIPs-validated or National Security Agency-approved cryptography to implement signatures?</li> <li>Do you employ FIPs-validated or National Security Agency-approved cryptography to implement signatures?</li> <li>Do you us antist amper mechanism to conter data theft and subversion, including auto-destruction if tampering is detected?</li> <li>Do you us antist amper mechanism to conter data theft and subversion, including auto-destruction if tampering is detected?</li> <li>Do you us antist amper mechanism to conter data theft and subversion, including auto-destruction if tampering is detected?</li> <li>Do you us antist amper mechanism to conter data theft and subversion, including auto-destruction if tampering is detected?</li> <li>Do you us antist amper mechanism to conter data theft and subversion, including auto-destruction if tampering is detected?</li> <li>Do you have a loss Prevention (UI) software of controment?</li> <li>Is broy ou have a prote sing into the production enviry documented?</li> <li>Do you have a cyber risk management organizations is delivered?</li> <li>Do you have a cyber risk management organizations is delivered?</li> <li>Do you have a cyber risk management organizations is delivered?</li> <li>Do you have a cyber risk management organizations is delivered?</li> <li>Do you have a cyber risk management organizations is delivered?</li> <li>Do you have a cyber risk management organizations is delivered?</li> <li>Do you have a cyber risk manage methorganizations is delivered?</li> <li>Do you ha</li></ol>	10. Is information of different sensitivity levels prohibited from residing on the same system?
<ol> <li>Are tackas/field as cirkia/sensitive encrypted at rest?</li> <li>Do you encrypt software and software patches at rest and in nation throughout deliver?</li> <li>Is encrypted data in transit, are the encryption key score separately from the date and a ky-managenent serve?</li> <li>Is encrypted data in transit carefully planned so as not to blind/hinder the organization's score separately from the date and a ky-managenent serve?</li> <li>Do you use plat lass Prevention (DUP) software for data in use, in motion, and at rest?</li> <li>Do you use bata loss Prevention (DUP) software for data in use, in motion, and at rest?</li> <li>Do you use bata loss Prevention (DUP) software for data in use, in motion, and at rest?</li> <li>Do you use bata loss Prevention (DUP) software for data in use, in motion, and at rest?</li> <li>Do you use bata loss Prevention (DUP) software for data in use, in motion, and at rest?</li> <li>Do you use bata loss Prevention (DUP) software for data in use, in motion, and at rest?</li> <li>Do you use bata loss Prevention (DUP) software for data in use, in motion, and at rest?</li> <li>Do you use bata loss Prevention (DUP) software for data in use, in motion, and at rest?</li> <li>Do you use bata loss Prevention (DUP) software for data in use, in motion, and at rest?</li> <li>Do you use bata loss Prevention (DUP) software for data in use; in motion, and at rest?</li> <li>Do you use bata loss Prevention (DUP) software for data in use; in motion, and at rest?</li> <li>Do you use bata prevention (DUP) software for data in use; in motion, and at rest?</li> <li>Do you use bata loss Prevention (DUP) software for data in use; in motion, and at rest?</li> <li>Do you use bata in the rest prevention (DUP) software for data in use; in motion, and at rest?</li> <li>Do you use bata prevention (DUP) software for data in use; in motion at tracter data data data date data data data data</li></ol>	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?
<ol> <li>Do you encrypt software and software patches at rest and in mution throughout delivery?</li> <li>In addition to data being protected at rest and in statis, are the encryption keys scurely managed?</li> <li>Se the encryption keys stored separately from the data on a key-management server?</li> <li>Is encrypted data in transt carefully planned so as not to blind/hinder the organization's security technologies?</li> <li>Do you use milly PiPs-validated or National Security technologies?</li> <li>Do you use bait intranst carefully planned so as not to blind/hinder the organization's security technologies?</li> <li>Do you use bait intranst carefully calefully also destruction if tampering is detected?</li> <li>Do you use bait in store corefully also destruction if tampering is detected?</li> <li>Do you use bait also spectruction to your cyber security risk management program?</li> <li>Is broy out have a documented baseline configuration standards for all devices connected to the corporate network.</li> <li>Is production firsk tolerance distingt and devices connected to the corporate network.</li> <li>Is broy out have a documented baseline configuration standards for all devices connected to the corporate network.</li> <li>Is production firsk tolerance distingt and devices connected to the corporate network.</li> <li>Is broy out have a proces in place to manage trusted workment.</li> <li>Do you have a cyber risk management organizational chart with reporting relationships delineated?</li> <li>Do you have a cyber risk management organization all chart with reporting relationships delineated?</li> <li>Do you have a cyber risk management organization all chart with reporting relationships delineated?</li> <li>Do you have a manage trusted versors.</li> <li>So you have a cyber risk management organization all chart with reporting relationships delineated?</li> <li>Do you have a dip joint risk cornols?</li> <li>Do you have a dip joi</li></ol>	1. Are data classified as critical/sensitive encrypted at rest?
4. In addition to data being protected at rest and in transit, are the encryption keys securely paralety from the dato an key-management serve? 5. Are the encryption keys stored separately from the dato an key-management serve? 5. Do you use poly Physialidated on National Security Appropriately in Security technologies? 7. Do you use poly of Physialidated on National Security Appropriately in Security technologies? 7. Do you use poly contra data thet and subversion, including auto destruction if tampering is detected? 7. Do you use poly contra data thet and subversion, including auto destruction if tampering is detected? 7. Do you use poly contra data thet and subversion, including auto destruction if tampering is detected? 7. Do you use poly contra data on the yoroduction environment? 7. Do you have a process in place to manage trusted vendors contra data the? 7. Do you have a process in place to manage trusted vendors 7. Do you have a process in place to manage trusted vendors 7. Do you have a process in place to manage trusted vendors 7. Do you have a process in place to manage trusted vendors 7. Do you have a process in place to manage trusted vendors 7. Do you have a process in place to manage trusted vendors 7. Do you have a process in place to manage trusted vendors 7. Do you have a process in place to manage trusted vendors 7. Do you have a process in place to manage trusted vendors 7. Do you have a process in place to manage trusted vendors 7. Do you have a process in place to manage trusted vendors 7. Do you have a process in place to manage trusted vendors 7. Do you have a process in place to manage trusted vendors 7. Do you have a process in place to manage trusted vendors 7. Do you have a process in place to manage trusted vendors 7. Do you have a process in place to manage trusted vendors 7. Do you have a place to the produktion developed to the you visualize the IT supply chain? 7. Do you have a place to the produktion materit and you have and montrel tablet you visualiz	3. Do you encrypt software and software patches at rest and in motion throughout delivery?
<ul> <li>5. Are the encryption keys stored separately from the date on a key-management server?</li> <li>6. Is encrypted tail in transic arefully planned so as not to bink/nhomes the organization's security technologies?</li> <li>7. Do you employ FIP-suldiated or National Security Agency-approved cryptography to implement signatures?</li> <li>8. Do you use anti-tamper mechanism to counter data thet and subversion, incluing auto-destruction if tampering is detected?</li> <li>10. Do you use anti-tamper mechanism to counter data thet and subversion, incluing auto-destruction if tampering is detected?</li> <li>10. Do you aba's a counter data to key contend to the corporate network</li> <li>17. Is production data only located in the production environment?</li> <li>18. Do you have a coher risk management program?</li> <li>19. Do you have a cyber risk management program?</li> <li>20. Jou have a cyber risk management granizational chart with reporting relationships delineated?</li> <li>20. Do you have a cyber risk management granizational chart with reporting relationships delineated?</li> <li>20. Jou have a cyber risk management granizational chart with reporting relationships delineated?</li> <li>30. Do you have a cyber risk management granizational chart with reporting relationships delineated?</li> <li>31. If securits be diffed and duction data on located and you cannot data</li></ul>	4. In addition to data being protected at rest and in transit, are the encryption keys securely managed?
<ul> <li>6. Is encryted data in transic carefully planned so as not to biln/hinder the organization's security technologies?</li> <li>7. Do you engb Piesvalidated or National Security Agency-approved crytography to linghement signatures?</li> <li>8. Do you use anti-tamper mechanisms to counter data thet and subversion, including auto-destruction if tampering is detected?</li> <li>10. Do you use Data Loss Prevention (DIP) software for data in use, in motion, and at rest?</li> <li>10. Do you have data countented baseline configuration standrafs for all devices connected to the corporate network.</li> <li>17. Is production data only located in the production environment?</li> <li>10. Do you have a cyber risk management torganizational chart with reporting relationships delineated?</li> <li>20. Do you have a cyber risk management program?</li> <li>21. Or Sou have a cyber risk management program?</li> <li>21. Or Sou have a cyber risk management program?</li> <li>23. Do you have a cyber risk management program?</li> <li>24. Chief Security standrads?</li> <li>24. Chief Security standrads?</li> <li>24. Chief Security standrads?</li> <li>25. Do you have a ryber risk controls?</li> <li>27. Sou and Risk/Audit Committee?</li> <li>27. Sou and Risk/Audit Committee?</li> <li>29. Do you se not an environ the source of the restruction of</li></ul>	5. Are the encryption keys stored separately from the data on a key-management server?
<ul> <li>7. Do you employ FIPs-validated or National Security Agency-approved cryptography to implement signatures?</li> <li>8. Do you exent champer mechanisms to counter date that eff and subversion, including sub-destruction if tampering is detected?</li> <li>10. Do you use Data Loss Prevention (DLP) software for data in use, in motion, and at rest?</li> <li>12. Do you have documented baseline configuration standards for all devices connected to the corporate network.</li> <li>13. Is production data only located networment?</li> <li>14. Do you have a mission statement for your cyber security risk management program?</li> <li>2. Is the organization's risk tolerance identified and clearly documented?</li> <li>3. Do you have a cyber risk management organizational chart with reporting relationships delineated?</li> <li>3. Do you have a cyber risk management organizational chart with reporting relationships delineated?</li> <li>3. Do you have a cyber risk management organizational chart with reporting relationships delineated?</li> <li>3. Do you have a cyber risk management organizational chart with reporting relationships delineated?</li> <li>3. Do you have a process in place to manage trusted vendors</li> <li>3. Collical complications?</li> <li>3. A Chief Compliance Officer</li> <li>3. Board Risk/Audit Committee?</li> <li>3. Do so you any with critical supply, distribution &amp; service hubs/ nodes and inter-related flows to help you visualize the T supply chain?</li> <li>3. Do so you and motions external supplier cybersecurity standards?</li> <li>5. 2. Estabilishes and motions external supplier cybersecurity standards?</li> <li>5. Do so you assee according to risk/criticality?</li> <li>4. Solwar evensioning and patching history recorde for all applicabel T asset?</li> <li>5. Does your asset management program identify and classify data, systems and processes according to risk/criticality?</li> <li>4. Solwar evensioning and patching history recorder or all applicabel T asset?</li> <li>5. Does your asset management p</li></ul>	6. Is encrypted data in transit carefully planned so as not to blind/hinder the organization's security technologies?
8. Do you use anti-tamper mechanisms to counter data theff and subversion, including auto-destruction if tampering is detected?         10. Do you use bat Loss Prevention (DIP) 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         12. Do you have documented baseline configuration environment?         12. Do you have a mission statement for your cybes excurity risk management program?         2. Is the organization's risk tolerance identified and clearly documented?         3. Do you have a process in place to manage trusted vendors         2. J To Scurity standards?         3. A chief Execurity standards?         3. A chief Execurity configuration firsk Management program?         3. Do you have a process in place to manage trusted vendors         3. Do you have a process in place to manage trusted vendors         3. A chief Execurity standards?         3. A chief Execurity configuration have and power have many and the ritical supply, distribution & service hubs/ nodes and inter-related flows to help you visualize the IT supply chain?         3. Do so you approachization have a may with critical supply chistribution & service hubs/ nodes and inter-related flows to help you visualize the IT supply chain?         3. Do so you approachization have may with critical supply chistindurina Systems and Organization have a truste with related flows to help you visualize the IT supply chain?         3. Do so you approparization have a may with critical supply c	7. Do you employ FIPs-validated or National Security Agency-approved cryptography to implement signatures?
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         12. By poduated and 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?         3. Do you have a cyber risk management organizational chart with reporting relationships delineated?         3. Do you have a cyber risk management organizational chart with reporting relationships delineated?         3. Do you have a cyber risk management organizational chart with reporting relationships delineated?         3. Do you have a cyber risk management organization six tolerance officer         3.1 Ti Security Standards?         3. Da organization have a map with critical supply, distribution & service hubs/ nodes and inter-related flows to help you visualize the IT supply chain?         3. Does you organization have a map with critical supply, distribution & service hubs/ nodes and lorganizations         5. Zistabilishes and monitors esternal supplice rybersecurity standards?         6. Supply Chain Risk Management Practices for Federal Information Systems and Organizations         6. Systeme este management forgram identify and classify data systems and Processe according to risk/criticality?	8. Do you use anti-tamper mechanisms to counter data theft and subversion, including auto-destruction if tampering is detected?
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 oyber security risk management program?         2. Is the organization's risk tolerance identified and clearly documented?         3. Do you have a process in place to manage trusted vendors         3. Do you have a process in place to manage trusted vendors         2.1 If Security standards?         3.4 Chief Security Standards?         3.6 Chief Compliance Officer         3.7 Board Risk/Audit Committee         7.2 Dual or joint risk controls?         7.3 Board Risk/Audit Committee         3.0 Do you set objectives for time to recovery for critical T supply chain nodes/locations?         3.2 Establishes and monitors external supplier cybersecurity standards?         3.2 Nost Risk/Audit Committee?         3.2 Dosey set objectives for time to recovery for critical T supply chain nodes/locations?         3.2 Establishes and monitors external supplier cybersecurity standards?         3.2 Nost Risk Management Practices for Federal Information Systems and Organizations         4. Dos you are set management program identify and casify data, systems and processes according to risk/criticality?         4. Dos you are set management program identify and casify data, systems and processes according to risk/criticality?         5. Dos your area ta	10. Do you use Data Loss Prevention (DLP) software for data in use, in motion, and at rest?
<ol> <li>P. Eproduction data only located in the production environment?</li> <li>Do you have a mission statement for your cybe security risk management program?</li> <li>Do you have a cyber risk management organizational chart with reporting relationships delineated?</li> <li>Do you have a cyber risk management organizational chart with reporting relationships delineated?</li> <li>Do you have a cyber risk management organizational chart with reporting relationships delineated?</li> <li>Do you have a cyber risk management organizational chart with reporting relationships delineated?</li> <li>Do you have a cyber risk management organizational chart with reporting relationships delineated?</li> <li>Do you have a cyber risk management program identify studied.</li> <li>A Chief Security Studied Committee</li> <li>J. Board Risk/Audit Committee?</li> <li>Ja board Risk/Audit Committee?</li> <li>Joos you set objectives for tite to recovery for critical T supply distribution &amp; service hubs/ nodes and inter-related flows to help you visualize the IT supply chain?</li> <li>J boas you set objectives for tite to recovery for critical T supply chain nodes/locations?</li> <li>S tabalishes and monitors external supplier cybersecurity standards?</li> <li>Do you set objectives for tite to recovery for critical T supply chain nodes/locations?</li> <li>S boas relax(Statian Charter) and Disposition of Fraudulent/Counterfeit Electronic Parts</li> <li>Does you set management program identify and classify data, systems and programs acording to risk/criticality?</li> <li>Do you know the largest number of confidential records in any segregated database?</li> <li>Do you extrat and analyze all anomalies from audit logs, access reports, and security incident tracking reports?</li> <li>Has an organization for suduli logs, access reports, and security incident tracking reports?</li> </ol>	12. Do you have documented baseline configuration standards for all devices connected to the corporate network
<ol> <li>Do you have a mission statement for your cyber security risk management program?</li> <li>Is the organization's risk tolerance identified an clearly documented?</li> <li>Do you have a cyber risk management rganizational chart with reporting relationships delineated?</li> <li>Do you have a process in place to manage trusted vendors</li> <li>II T Security standards?</li> <li>At Chief Executive Officer</li> <li>Go field Compilance Officer</li> <li>T Board Risk/Audit Committee</li> <li>T Board Risk/Audit Committee?</li> <li>Do you have a may with critical supply, distribution &amp; service hubs/ nodes and inter-related flows to help you visualize the IT supply chain?</li> <li>Do sou have a mangement program identify and classify data, systems and Organizations?</li> <li>Establishes and monitors external supplier cybersecurity standards?</li> <li>Does your asset management program identify and classify data, systems and processes according to risk/criticality?</li> <li>Does your asset management program identify and classify data, systems and processes according to risk/criticality?</li> <li>Does your were ioning and patching history recorded for all applicable IT assets?</li> <li>Does your were ioning and patching history recorded for all applicable IT assets?</li> <li>Do you were were ioning and patching history recorded for all applicable IT assets?</li> <li>Do you were related for an analyze all anomalies from audit logs, access reports, and security incident tracking reports?</li> <li>Do you were are ioning and patching history recorded for all applicable IT assets?</li> <li>Do you were and analyze all anomalies from audit logs, access reports, and security incident tracking reports?</li> <li>Has an orcarizational baseling of an analyze and mapped?</li> <li>Has an orcarizational baseling of a management program identify and classify data, systems and processes according to risk/criticality?</li> </ol>	17. Is production data only located in the production environment?
<ol> <li>Is the organization's risk tolerance identified and clearly documented?</li> <li>Do you have a cyber risk management organizational chart with reporting relationships delineated?</li> <li>Do you have a process in place to manage trusted vendors</li> <li>TSecurity standards?</li> <li>A Chief Executive Officer</li> <li>A Chief Executive Officer</li> <li>Jo a poard Risk/Audit Committee</li> <li>Jo a poard Risk/Audit Committee?</li> <li>Do so you roganization have a map with critical supply, distribution &amp; service hubs/ nodes and inter-related flows to help you visualize the IT supply chain?</li> <li>Do so you external supplier cybersecurity standards?</li> <li>Stastis and montors external supplier cybersecurity standards?</li> <li>Dous you asset management program identify and classify data, systems and prograziations</li> <li>Sa Soxf Risk/Audit Committee for unsuber of confidentify and classify data, systems and prograziation?</li> <li>Does you asset management program identify and classify data, systems and prograziation?</li> <li>Does you maset management program identify and classify data, systems and processe according to risk/criticality?</li> <li>Is poor we be larger to remour of for all applicable IT assets?</li> <li>Doy ou work he largers number of confidential records in any segregated database?</li> <li>Doy ou work he largers number of confidential records in any segregated database?</li> <li>Are all network/application communication flows documented and mapped?</li> <li>Has an organization and analyze all anomalies from audit logs, access reports, and secretly incident tracking reports?</li> <li>Has an organizational base is established?</li> </ol>	1. Do you have a mission statement for your cyber security risk management program?
<ul> <li>3. Do you have a cyber risk management organizational chart with reporting relationships delineated?</li> <li>5. Do you have a process in place to manage trusted vendors</li> <li>2.1. IT security standards?</li> <li>3. A Chief Executive Officer</li> <li>3.4 Chief Executive Officer</li> <li>3.6 Chief Compliance Officer</li> <li>3.7 Board Risk/Audit Committee</li> <li>7.2 Dual or joint risk controls?</li> <li>7.3 Board Risk/Audit Committee?</li> <li>3.0 Does your aset objectives for time to recovery for critical IT supply, distribution &amp; service hubs/ nodes and inter-related flows to help you visualize the IT supply chain?</li> <li>4. Do you set objectives for time to recovery for critical IT supply chain nodes/locations?</li> <li>5.2 Itabilishes and monitors external supplier cybersecurity standards?</li> <li>6.2 NIST SP 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations</li> <li>6.5 AFA EAG4 Avoidance, Detections, Mitigation, and Disposition of Fraudulent/Counterfeit Electronic Parts</li> <li>2. Does your asset management program identify and classify data, systems and processes according to risk/criticality?</li> <li>4. Is software versioning and patching history recorded for all applicable IT assets?</li> <li>6. Doy ou know the largest number of confidential records in any segregated database?</li> <li>1. Are all network/application communication flows documented and mapped?</li> <li>8. Doy ou extract and analyze all anomalies from audit logs, access reports, and security incident tracking reports?</li> <li>1. Has an organizational baseline of exocet data flows been established?</li> </ul>	2. Is the organization's risk tolerance identified and clearly documented?
<ul> <li>5. Do you have a process in place to manage trusted vendors</li> <li>2.1 IT Security standards?</li> <li>3.4 Chief Executive Officer</li> <li>3.6 Chief Compliance Officer</li> <li>3.7 Board Risk/Audit Committee</li> <li>7.2 Dual or joint risk controls?</li> <li>7.3 Board Risk/Audit Committee?</li> <li>3. Does your organization have a map with critical supply, distribution &amp; service hubs/ nodes and inter-related flows to help you visualize the IT supply chain?</li> <li>4. Do you set objectives for time to recovery for critical IT supply chain nodes/locations?</li> <li>5.2 Establishes and monitors external supplier cybersecurity standards?</li> <li>6.6 SAE AS649 Avoidance, Detections, Mitigation, and Disposition of Fraudulent/Counterfeit Electronic Parts</li> <li>2. Does your asset management program identify and classify data, systems and processes according to risk/criticality?</li> <li>4. Is software versioning and patching history recorded for any segregated database?</li> <li>1. Are all network/application communication flows documented and mapped?</li> <li>8. Do you suck and analyze all anomalies from audit logs, access reports, and security incident tracking reports?</li> <li>1. Has an organizational baseline of expected data flows teen established?</li> </ul>	3. Do you have a cyber risk management organizational chart with reporting relationships delineated?
2.1 If Security standards?         3.4 Chief Executive Officer         3.6 Chief Compliance Officer         3.7 Board Risk/Audit Committee         7.3 Daard Risk/Audit Committee?         3.0 cov or oganization have a map with critical supply, distribution & service hubs/ nodes and inter-related flows to help you visualize the IT supply chain?         3.0 pour organization have a map with critical supply, distribution & service hubs/ nodes and inter-related flows to help you visualize the IT supply chain?         3.0 pour organization have a map with critical supply, distribution & service hubs/ nodes/locations?         5.2 Establishes and monitors external supplier cybersecurity standards?         6.3 ND 5.10, 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 maped?         8. Do you extract and analyze all anomalies from audit logs, access reports, and security incident tracking reports?         1. Has an organizational baseline of exocet data flows been estabilished?	5. Do you have a process in place to manage trusted vendors
<ul> <li>3.4 Chief Executive Officer</li> <li>3.6 Chief Compliance Officer</li> <li>3.7 Board Risk/Audit Committee</li> <li>3.7 Daard Risk/Audit Committee?</li> <li>3.8 Daard Risk/Audit Committee?</li> <li>3.9 Daes your organization have a map with critical supply, distribution &amp; service hubs/ nodes and inter-related flows to help you visualize the IT supply chain?</li> <li>4. Do you set objectives for time to recovery for critical T supply chain nodes/locations?</li> <li>5. Establishes and monitors external supplier cybersecurity standards?</li> <li>6.2 NIST SP 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations</li> <li>6.5 SAE AS649 Avoidance, Detections, Mitigation, and Disposition of Fraudulent/Counterfiet Electronic Parts</li> <li>2. Does your asset management program identify and classify data, systems and processes according to risk/criticality?</li> <li>4. Is software versioning and patching history recorded for all applicable IT assets?</li> <li>6. Do you know the largest number of confidential records in any segregated database?</li> <li>1. Are all network/application communication flows documented and mapped?</li> <li>8. Do you extract and analyze all anomalies from audit logs, access reports, and security incident tracking reports?</li> <li>1. Has an organizational baseline of exoceted data flows been established?</li> </ul>	2.1 IT Security standards?
3.6 Chief Compliance Officer         3.7 Board Risk/Audit Committee         7.2 Dual or joint risk controls?         7.3 Board Risk/Audit Committee?         3.0 boes 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 SITS TP 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?	3.4 Chief Executive Officer
<ul> <li>3.7 Board Risk/Audit Committee</li> <li>7.2 Dual or joint risk controls?</li> <li>7.3 Board Risk/Audit Committee?</li> <li>3. Does your organization have a map with critical supply, distribution &amp; service hubs/ nodes and inter-related flows to help you visualize the IT supply chain?</li> <li>4. Do you set objectives for time to recovery for critical IT supply chain nodes/locations?</li> <li>5.2 Establishes and monitors external supplier cybersecurity standards?</li> <li>6.2 SNTS SP 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations</li> <li>6.6 SAE AS649 Avoidance, Detections, Mitigation, and Disposition of Fraudulent/Counterfeit Electronic Parts</li> <li>2. Does your asset management program identify and classify data, systems and processes according to risk/criticality?</li> <li>4. Is software versioning and patching history recorded for all applicable IT assets?</li> <li>6. Do you know the largest number of confidential records in any segregated database?</li> <li>1. Are all network/application communication flows documented and mapped?</li> <li>8. Do you ext and analyze all anomalies from audit logs, access reports, and security incident tracking reports?</li> <li>1. Has an organizational baseline of expected data flows ben established?</li> </ul>	3.6 Chief Compliance Officer
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         6.5 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?	3.7 Board Risk/Audit Committee
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         6.5 SAE AS649 Avoidance, Detections, Mitigation, and Disposition of Fraduelent/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?	7.2 Dual or joint risk controls?
<ul> <li>3. Does your organization have a map with critical supply, distribution &amp; service hubs/ nodes and inter-related flows to help you visualize the IT supply chain?</li> <li>4. Do you set objectives for time to recovery for critical IT supply chain nodes/locations?</li> <li>5.2 Establishes and monitors external supplier cybersecurity standards?</li> <li>6.2 NIST SP 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations</li> <li>6.6 SAE AS649 Avoidance, Detections, Mitigation, and Disposition of Fraudulent/Counterfeit Electronic Parts</li> <li>2. Does your asset management program identify and classify data, systems and processes according to risk/criticality?</li> <li>4. Is software versioning and patching history recorded for all applicable IT assets?</li> <li>6. Do you know the largest number of confidential records in any segregated database?</li> <li>11. Are all network/application communication flows documented and mapped?</li> <li>8. Do you exact and analyze all anomalies from audit logs, access reports, and security incident tracking reports?</li> <li>1. Has an organizational baseline of expected data flows been established?</li> </ul>	7.3 Board Risk/Audit Committee?
<ul> <li>4. Do you set objectives for time to recovery for critical IT supply chain nodes/locations?</li> <li>5.2 Establishes and monitors external supplier cybersecurity standards?</li> <li>6.2 NIST SP 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations</li> <li>6.6 SAE AS649 Avoidance, Detections, Mitigation, and Disposition of Fraudulent/Counterfeit Electronic Parts</li> <li>2. Does your asset management program identify and classify data, systems and processes according to risk/criticality?</li> <li>4. Is software versioning and patching history recorded for all applicable IT assets?</li> <li>6. Do you know the largest number of confidential records in any segregated database?</li> <li>11. Are all network/application communication flows documented and mapped?</li> <li>8. Do you extact and analyze all anomalies from audit logs, access reports, and security incident tracking reports?</li> <li>1. Has an organizational baseline of exoceted data flows been established?</li> </ul>	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?
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. Dees 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 ben established?	4. Do you set objectives for time to recovery for critical IT supply chain nodes/locations?
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?	5.2 Establishes and monitors external supplier cybersecurity standards?
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?	6.2 NIST SP 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations
<ol> <li>Does your asset management program identify and classify data, systems and processes according to risk/criticality?</li> <li>Is software versioning and patching history recorded for all applicable IT assets?</li> <li>Do you know the largest number of confidential records in any segregated database?</li> <li>Are all network/application communication flows documented and mapped?</li> <li>Do you extract and analyze all anomalies from audit logs, access reports, and security incident tracking reports?</li> <li>Has an organizational baseline of expected data flows been established?</li> </ol>	6.6 SAE AS649 Avoidance, Detections, Mitigation, and Disposition of Fraudulent/Counterfeit Electronic Parts
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 exoceted data flows been established?	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? 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 exoceted data flows been established?	4. Is software versioning and patching history recorded for all applicable IT assets?
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?	6. Do you know the largest number of confidential records in any segregated database?
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?	11. Are all network/application communication flows documented and mapped?
1. Has an organizational baseline of expected data flows been established?	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?



#### **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?



#### **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
5.3 ISO IEC 27001/27002 for 3rd Party Cybersecurity Management
5.6 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?

