The Cyber Risk Predictive Analytics Project

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

1. Introduction & Acknowledgements

This two-year project in building the foundations for predictive cyber analytics was sponsored by the National Institute of Standards and Technology NIST (Project Leads: Mr. Jon Boyens; and Ms. Celia Paulsen); and the General Services Administration (Project Leads: Ms. Angela Smith and Mr. 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, University Of Maryland
-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

Zurich Insurance (Project Leads: Mr. Gerry Kane, Mr. John Soughan and Ms. Linda Conrad); and Beecher Carlson (Project Lead; Mr. Chris Keegan) partnered with UMD and provided insurance industry inputs on risk assessment methods and communications/ outreach.

The authors would like to acknowledge the University of Maryland's institutional support provided by Ms. Lisa Fall, Ms. Monique Anderson, and Mr. Eric Chapman; and the MITRE program support provided by Robert Martin and his team in Phase 1 of this project.

2. Major Research Objectives

Based on a series of consultations with NIST, GSA, and key industry stakeholders, our project's major research objectives were defined and refined as follows:

- Developing and deploying a secure, fully automated organizational self-assessment tool based on the Cybersecurity Framework.

- Comparing respondents' cyber security performance profiles (adoption of Framework policies and actions) with their total number and specific types of cyber breaches.

- Assessing efficacy of Cybersecurity Framework policies and actions in limiting total number and specific types of cyber breaches, and using this analysis to establish a foundation for the development of evidence-based cyber risk predictive analytics.

3. Uniqueness of This Research

Our team conducted an extensive literature review of cybersecurity predictive analytics. We reviewed 789 journal articles and conference papers. See profiles of some sample research efforts in the chart below. 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' cyber capabilities, that pulled breach data from multiple sources, or that used econometric analysis to understand which of a broad portfolio of cyber protection methods would be most effective against cyber breaches.

Examples Of Recent Cyber Risk Research Findings

Title	Year of Publication	Author	Description
User Compensation as a Data Breach Recovery Action: An Investigation of the Sony PlayStation Network Breach	2016	Sigi Goode, Hartmut Hoehle, Viswanath Venkatesh, and Susan A. Brown	Developed a hypothesis regarding the effect of compensation on key customer outcomes following major data breaches and service recovery efforts. Successfully demonstrated the impacts of compensation on customer outcomes with both theoretical and practical implications
Fear Appeals and Information Security Behaviors: An Empirical Study	2010	Allen C. Johnston and Merrill Warkentin	Study focused on the fear appeal that ultimately impacts the actions of end users. These fear inducing arguments were investigated as well as their influence on the compliance of end users with recommendations to enact security measures to mitigate threats.
Growth and Sustainability of Managed Security Services Networks (MSSN): An Economic Perspective	2012	Alok Gupta and Dmitry Zhdanov	Examined the reason why firms join MSSN in order to pool risks and access more security enabling resources and expertise.
Insiders' Protection of Organizational Information Assets: Development of a Systematics-Based Taxonomy and Theory of Diversity for Protection-Motivated Behaviors (PMB)	2013	Clay Posey, Tom L. Roberts, Paul Benjamin Lowry, Rebecca J. Bennett, and James F. Courtney	Research focused on PMBs which protected information and information systems. Proposed a six step methodology of qualitatively and quantitatively approaching a taxonomy and theory of diversity for PMBs.
Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness	2010	Burcu Bulgurcu, Hasan Cavusoglu, Izak Benbasat	Study focused on employee efforts to reduce the risks related to information security. It identified the employee compliance with information security policy and investigated the rationality based factors that drive an employee to comply with the norms of the ISP. Results show an employee's intention to comply with ISP is significantly influenced by attitude and belief and the self-efficacy to comply.

Market Value of Voluntary Disclosures Concerning Information Security	2010	Lawrence A. Gordon, Martin P. Loeb, and Tashfeen Sohail	Study focused on whether there is any value in voluntarily disclosing concerns pertaining to a company's information security. The paper empirically studied relevance models as well as a bid-ask spread analysis. Findings provide some insight into strategic choices that firms make regarding voluntary disclosures about information security
Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study	2010	Petri Puhakainen and Mikko Siponen	Study proposed a training program on two theories: the universal constructive instructional theory and elaboration likelihood model. Achieved positive results that provide insights into how training content should utilize methods that activate and motivate systematic cognitive processing of information
An Enhanced Fear Appeal Rhetorical Framework: Leveraging Threats to the Human Asset Through Sanctioning Rhetoric	2015	Allen C. Johnston, Merrill Warkentin, and Mikko Siponen	Research was based on protection motivation theory (PMT) and its application to study the information security phenomena. Validated the efficacy of the enhanced fear appeal model and determined that informal sanctions effectively enhance conventional fear appeals thus positively influencing compliance intentions

4. Study Challenges

Our rigorous econometric analysis applied to a limited number of self-assessment participants ensures reliability of the results, but limits their generalizability. Our detailed 175-question self-assessment tool went well beyond the depth of usual surveys and required substantial organizational interest/effort to complete.

Clearly, the target audience of cyber security professionals had concerns about the security of their proprietary data on corporate practices. To address these concerns, we used pre-registration IP and email screening to validate the identity of potential respondents. Furthermore, we required two factor authentication for approved registrants to access the portal. With these protections in place, we had a total of 153 respondents, with an average of 40-100 responses per question. Thus, respondents were selective in responding to the detailed questionnaire.

Breach data on our sample of survey respondents was extremely difficult to compile. Fragmentation of available cyber breach data across multiple data sets was very high: **Of the 414 total breaches collected on our sample organizations across the four large scale data sets we procured from external vendors and utilized, 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 the above limitations.

5. Assessment Tools/Technology

To securely scale the Cyber Risk Portal, we added new user features and security enhancements. These included transitioning to Amazon Web Hosting and installing provider-recommended security/encryption controls. Furthermore, we implemented both user pre-registration screening and DUO Two Factor Authentication upon registration.

We also worked closely with NIST to complete the Cyber Risk Self-Assessment Form, with questions fully aligned with the category/sub-category levels of the Cybersecurity Framework.

Finally, we developed advanced business visualization technology to display layered assessment results.

These advancements led to our Cyber Risk Portal winning the 2017 IEEE (Institute of Electrical and Electronics Engineers) Cyber Security Practice Innovation of the year award.

6. The Cyber Breach Database

We created a master data set of breaches composed of four large scale breach data sets: Advisen (commercial), Risk Based Security (commercial), Identity Theft Resource Center (non-profit), C-BERC (university).

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

These meta-categories are defined below:

7. Cyber Breach Meta-Categories

7.1. 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

7.2. Deficient Access Controls

- Definition: Inadequate assignment and management of system roles and user privileges/ permissions
- Examples: Fraud; identity-fraudulent use; privacy-unauthorized data collection; data-unintentional disclosure

7.3. Behavioral Vulnerabilities

- Definition: Social engineering, behavior-based intrusions
- Examples: Phishing/spoofing/social engineering

7.4. 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

8. 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.

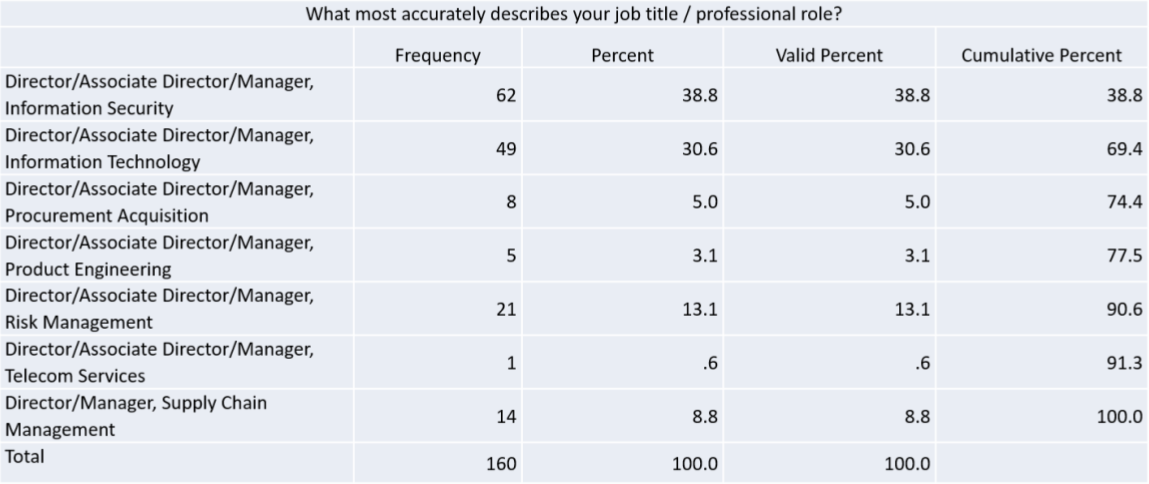
For the 2014- 2017 analysis period, there were 163 breaches directly associated with our sample of respondents. 57 breaches (or 35% of total) were categorized as access control deficiencies or administrative/network management deficiencies. Only 17 (10.4%) were behavioral or user-driven breaches.

9. Results of Statistical Analysis – Overview

Below we present the findings of our statistical analysis. First, we present the profile of our respondents through descriptive statistics; then, we map the statistically significant relationships between respondent Cybersecurity Framework policies/actions and breach frequency/types that our analysis uncovered.

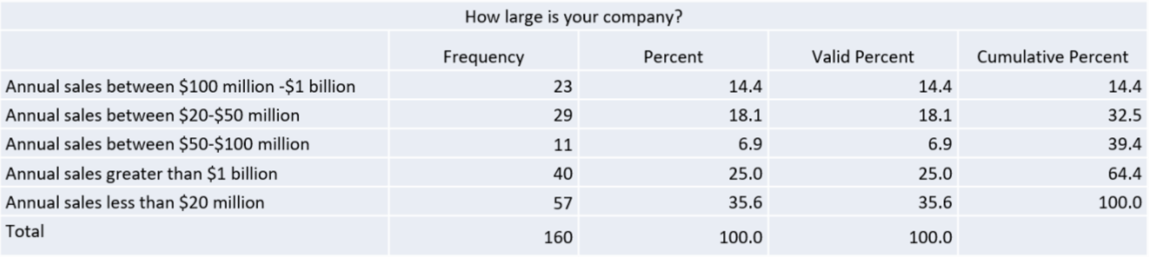
10. Description of Respondents

As seen in the table below, 69.4% of our respondents were largely IT and Information Security senior executives; and another 13.1% were Risk Management senior executives.

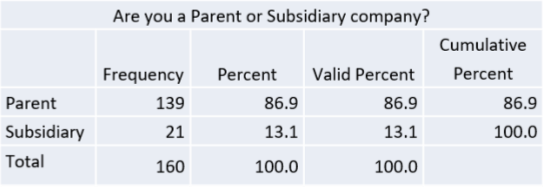


What most accurately describes your job title / professional role?				
	Frequency	Percent	Valid Percent	Cumulative Percent
Director/Associate Director/Manager, Information Security	62	38.8	38.8	38.8
Director/Associate Director/Manager, Information Technology	49	30.6	30.6	69.4
Director/Associate Director/Manager, 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	

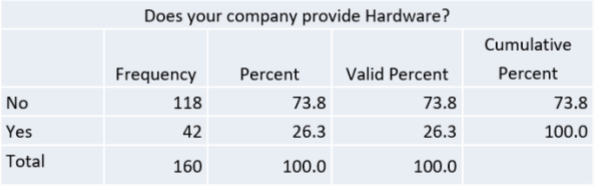
The respondent sample was well balanced, with 35.6% of respondents reporting annual sales less than $50 million; and 25% reporting annual sales of $1 billion, as shown below:



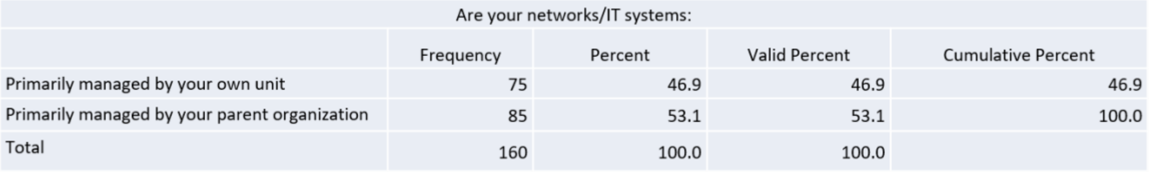
How large is your company?				
	Frequency	Percent	Valid Percent	Cumulative Percent
Annual sales between $100 million -$1 billion	23	14.4	14.4	14.4
Annual sales between $20-$50 million	29	18.1	18.1	32.5
Annual sales between $50-$100 million	11	6.9	6.9	39.4
Annual sales greater than $1 billion	40	25.0	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	

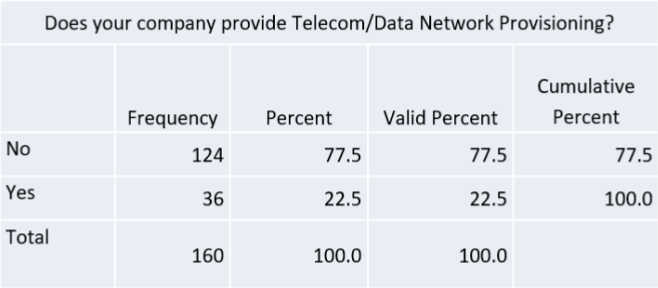


Does your company provide Hardware?				
	Frequency	Percent	Valid Percent	Cumulative Percent
No	118	73.8	73.8	73.8
Yes	42	26.3	26.3	100.0
Total	160	100.0	100.0	

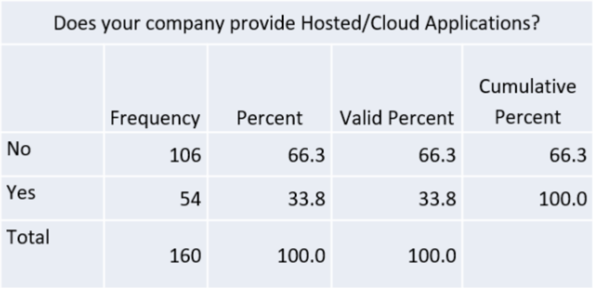


Are your networks/IT systems:				
	Frequency	Percent	Valid Percent	Cumulative Percent
Primarily managed by your own unit	75	46.9	46.9	46.9
Primarily managed by your parent organization	85	53.1	53.1	100.0
Total	160	100.0	100.0	

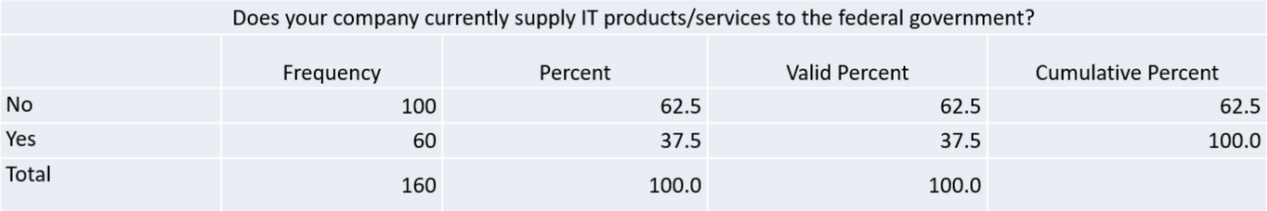
Respondents largely managed their own IT resources and did not provide IT services to others:



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	

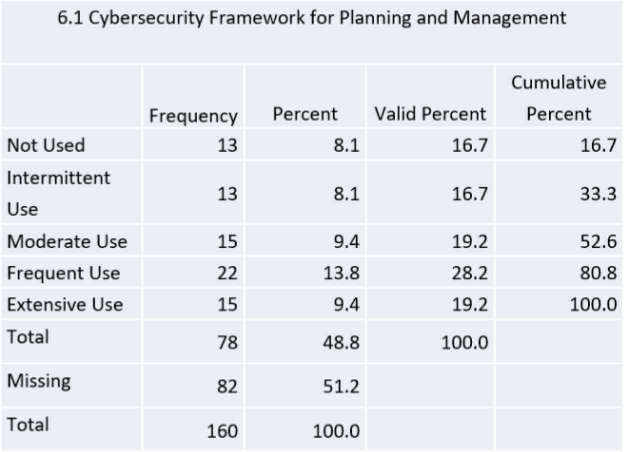


Does your company provide Hosted/Cloud Applications?				
	Frequency	Percent	Valid Percent	Cumulative Percent
No	106	66.3	66.3	66.3
Yes	54	33.8	33.8	100.0
Total	160	100.0	100.0	

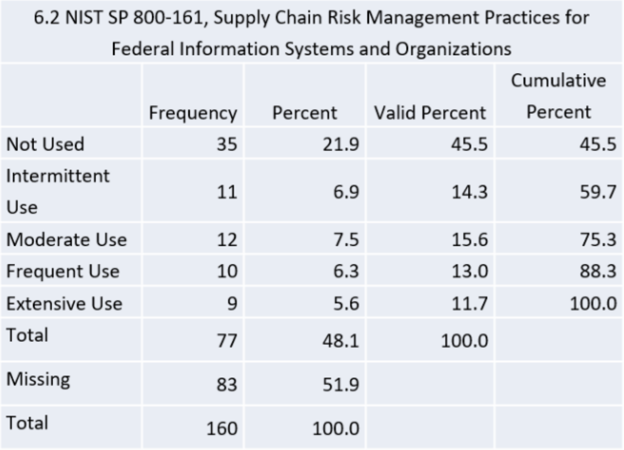


Does your company currently supply IT products/services to the federal government?				
	Frequency	Percent	Valid Percent	Cumulative Percent
No	100	62.5	62.5	62.5
Yes	60	37.5	37.5	100.0
Total	160	100.0	100.0	

Respondents adopted a range of cyber security standards. 47.4% of the respondents made frequent or extensive use of the Cybersecurity Framework for planning and management; systems; 24.7% made frequent or extensive use of NIST SP-800-161 Supply Chain Risk Management Practices.

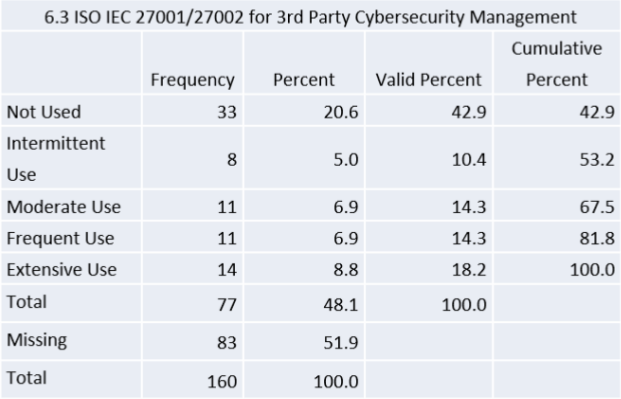


6.1 Cybersecurity Framework for Planning and Management				
	Frequency	Percent	Valid Percent	Cumulative Percent
Not Used	13	8.1	16.7	16.7
Intermittent Use	13	8.1	16.7	33.3
Moderate Use	15	9.4	19.2	52.6
Frequent Use	22	13.8	28.2	80.8
Extensive Use	15	9.4	19.2	100.0
Total	78	48.8	100.0	
Missing	82	51.2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



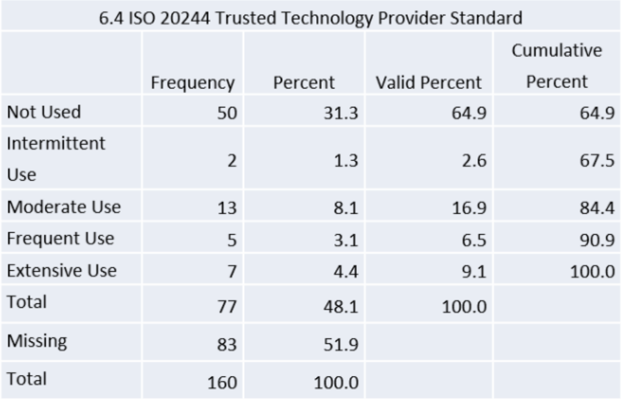
6.2 NIST SP 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations				
	Frequency	Percent	Valid Percent	Cumulative Percent
Not Used	35	21.9	45.5	45.5
Intermittent Use	11	6.9	14.3	59.7
Moderate Use	12	7.5	15.6	75.3
Frequent Use	10	6.3	13.0	88.3
Extensive Use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

Another standard that seemed to have gained traction among respondents was ISO's IEC 27001/27002 standard for 3rd party cyber security management**.**



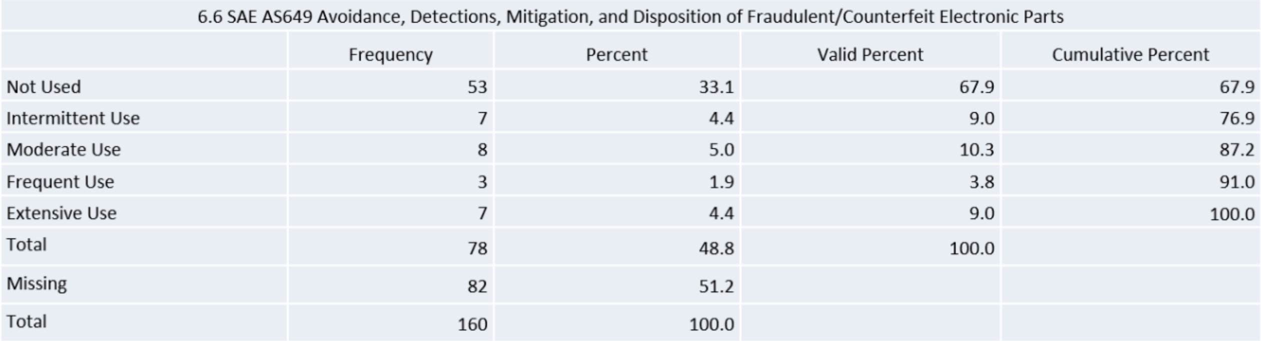
6.3 ISO IEC 27001/27002 for 3rd Party Cybersecurity Management

	Frequency	Percent	Valid Percent	Cumulative 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

	Frequency	Percent	Valid Percent	Cumulative 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		

11. Analytical Methodology

Once our research team combined both respondent performance profile data and breach profile data into a single spreadsheet, over a thousand runs were performed on the data universe to look for statistically significant relationships.

We used the negative binomial panel regression technique. This is the appropriate multiple regression technique based on a distribution of a dependent variable with the following characteristics: a skewed distribution and a count variable that is heavily weighted with zeros. The panel approach is necessitated since our data spans multiple years and industries. Specifically, our dependent variable is a 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). The independent variables used included the following: the respondent's response to each of the questions and a set of control variables (year, industry, and firm). Control variables are year, industry, firm. It is important to note that we ran a separate negative binomial panel regression for each question in the survey as well as for all breaches summed together as well as a separate analysis for each breach type. Our objective was to determine the extent to which a respondent's use of a particular action/policy was, in fact, related to the number of breaches the respondent's firm experienced (in total and for each of the individual breach categories).

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

Our statistical analysis was able to pinpoint policies and actions within each Framework category that appeared to reduce the total number or specific type of cyber breaches. These are discussed below in detail by Framework category.

I. **Identify**: Specific policies/actions in this category result in building ***better foundational understanding*** of patterns of network configuration (hubs and nodes); communications/data flows; and states of external network supplier cybersecurity.
Identify: A list of the specific policies/actions in the Identify Framework Category that are Most Significant in Leading to Fewer Breaches (in Total and by Category). These policies/actions are Statistically Significant in at Least 3 of the 5 Breach Categories (Total; Deficient Access Control; Technical Exploits; Theft; and Behavioral)

	Critical Policies	Respondent Positive Response Rate
Identify	1. Does your asset management program identify and classify data, systems and processes according to risk/criticality?	78%
	2. Do you know the largest number of confidential records in any segregated database?	51%
	3. Are all network/application communication flows documented and mapped?	51%
	4. Does your organization have a map with critical physical supply, distribution & service hubs/ nodes and inter-related flows to help you visualize the IT supply chain?	40%
	5. Do you have a supplier management program that: Establishes and monitors external supplier cybersecurity standards?	52%
	6. Does your risk dashboard/registry do the following: Defines key cyber risks?	77%
	7. 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	25%
	8. SAE AS649 Avoidance, Detection, Mitigation, and Disposition of Fraudulent/Counterfeit Electronic Parts	13%

II. **Protect:** Policies/actions cited in this category are technical risk management procedures that seek to establish **better ongoing situational awareness by** shielding sensitive network segments and information flows, assure secure communications through encryption and separate storage of encryption keys;

closely track changes in software and settings, and use supply chain quarantines to isolate code or hardware.

Protect: A list of the specific policies/actions in the Protect Framework Category that are Most Significant in Leading to Fewer Breaches (in Total and by Category). These policies/actions are Statistically Significant in at Least 3 of the 5 Breach Categories (Total; Deficient Access Control; Technical Exploits; Theft; and Behavioral)

Critical Policies		Respondent Positive Response Rate
Protect	1. Do you employ network access control (NAC) for remote connections?	75%
	2. Do you physically and logically segregate your sensitive network segments?	78%
	3. Is information of different sensitivity levels prohibited from residing on the same system?	45%
	4. In addition to data being protected at rest and in transit, are the encryption keys securely managed?	83%
	5. Are the encryption keys stored separately from the data on a key-management server?	80%
	6. Do you employ FIPS-validated or National Security Agency-approved cryptography to implement signatures?	67%
	7. Do you have documented baseline configuration standards for all devices connected to the corporate network?	60%
	8. Is the production environment separate from development and testing environments?	87%
	9. Is production data only located in the production environment?	80%
	10. Do you use end to end Configuration Management (CM) systems to track changes to software and settings?	65%
	11. Do you quarantine non-conforming products until they can be verified through inspection/testing?	55%
	12. Do you quarantine code from outside suppliers in proxy servers to undergo virus scanning and authentication procedures?	64%

III. **Detect:** All policies/actions in this category enable organizations to quickly find cyber anomalies and escalate response activities to manage them.

Detect: A list of the specific policies/actions Most Significant in Leading to Fewer Breaches (in Total and by Category). These policies/actions are Statistically Significant in at Least 2 of the 5 Breach Categories (Total; Deficient Access Control; Technical Exploits; Theft; and Behavioral)

Critical Policies		Respondent Positive Response Rate
Detect	1.Has an organizational baseline of expected data flows been established?	51%
	2.Does your SIEM dashboard display event information for units managed by external service provider?	56%
	3.Is anti-virus software deployed on endpoints to detect malicious code?	97%
	4.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?	77%

IV. **Respond:** All policies/actions in this category enable organizations to build effective response capabilities: 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).

Respond: A list of the specific policies/actions Most Significant in Leading to Fewer Breaches (in Total and by Category). These policies/actions are Statistically Significant in at Least 2 of the 5 Breach Categories (Total; Deficient Access Control; Technical Exploits; Theft; and Behavioral)

Critical Policies		Respondent Positive Response Rate
Respond	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?	32%
	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?	69%
	3.Do you have an incident response plan that addresses system details and procedures for reporting and managing a suspected incident?	72%
	4.Does your forensics capability rely on a third party security company with ongoing retainer?	50%

V. **Recover:** All policies/actions in this category build effective recovery capabilities that 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: The policies/actions Most Significant in Leading to Fewer Theft Breaches

Critical Policies		Respondent Positive Response Rate
Recover	1.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	93%
	2.Do you think your company is positioned to file and settle cyber insurance claims faster than your competitors?	50%
	3.Do you have cyber risk communications mechanisms in place to communicate recovery status with your employees and/or shareholders?	75%

13. Critical policies/actions that reduced Specific Breach Types

We were able to identify actions and policies in the Cybersecurity Framework that, if implemented, appear to reduce the frequency of overall breaches and /or target specific types of breaches. We categorized Framework policies and actions according to their impacts on overall breaches and four specific breach types. See Appendix for details.

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 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 and 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 3rd Party Standard enables high performing organizations to more systematically select vendors whose cyber security cultures mirror their own.

14. Project Lessons Learned

A. An Evidence-Based Cyber Risk Predictive Analytics Approach Is Achievable

This research has been pioneering in its fundamental approach and findings:

> "There are many cybersecurity guidelines and practices out there, but empirical evidence about what's actually effective in practice has been scarce. This is the first time such evidence has been gained".
>
> Jon Boyens, NIST Manager for Security Engineering and Risk Management

An evidence-based approach can enable study respondents to take away valuable insights from their cyber security performance profiles and help them better target where they need to bolster cyber defenses. Additionally, we hope the methodological approach we pursued in our econometric modeling will help lay the groundwork for an enhanced, more mature discipline of cyber-risk predictive analytics.

All companies can ultimately benefit from an evidence-based set of cyber security practices that have compelling operational effectiveness against specific breaches and attacks. In the future, companies will in fact probably demand more proofs of effectiveness for their investments in cyber security solutions. Think of the company in this case as a well-informed patient who will likely pay a premium to be able to use in confidence a clinically-tested product.

B. Need For Faster Diffusion Of The Cybersecurity Framework Automated Self-Assessment Tool

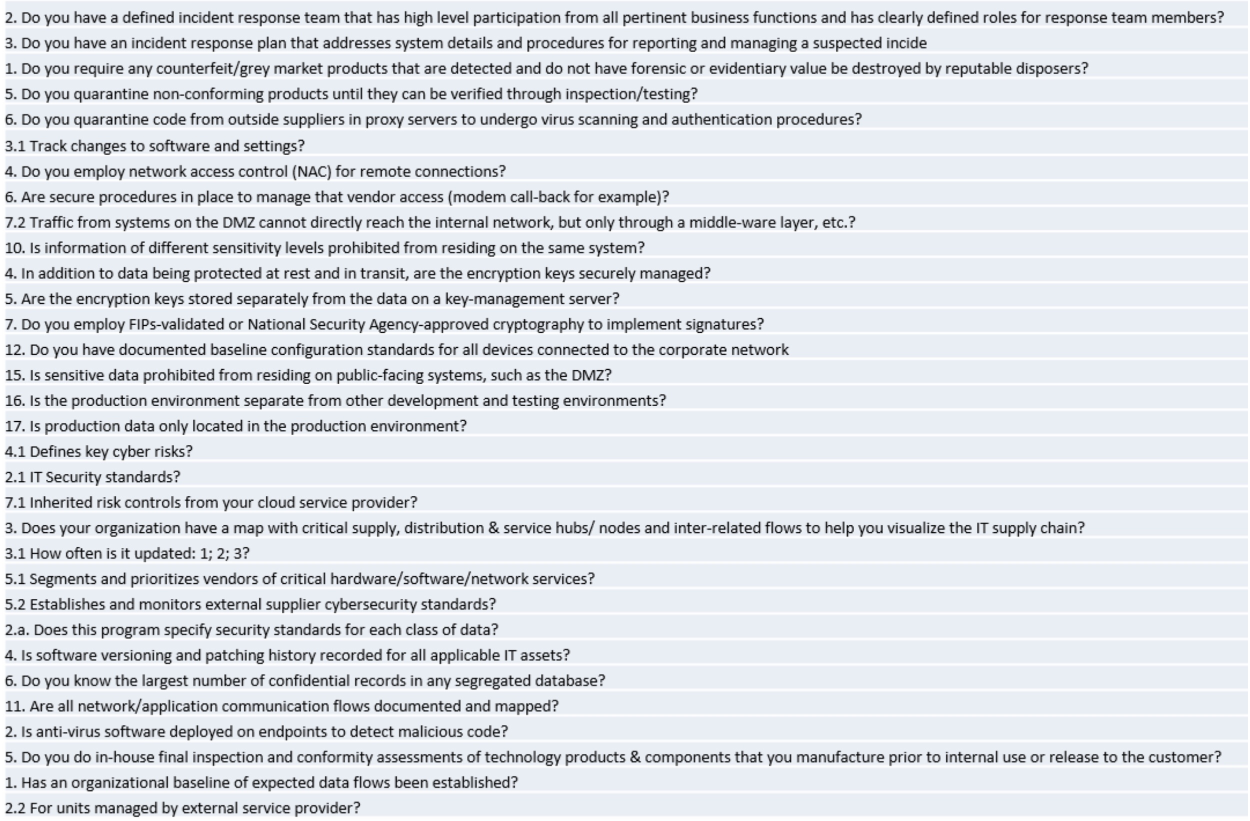
Given the comprehensive and sensitive nature of the self-assessment tool, a supply chain "driver" organization (e.g. a large global high-tech company) with the economic leverage to mandate adoption across its internal supply chain and external vendor base should be a primary vehicle of distribution.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

C. Deficiencies In Cyber Breach Data Are Persistent and Require Workarounds

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, marketplace risks and legal/financial liabilities force cyber breach disclosure, or when there is a legislative or regulatory-driven cyber breach disclosure mandate. The current, fragmented nature of cyber breach data means that analysts must use multiple sources to build complete & accurate cyber breach data repositories.

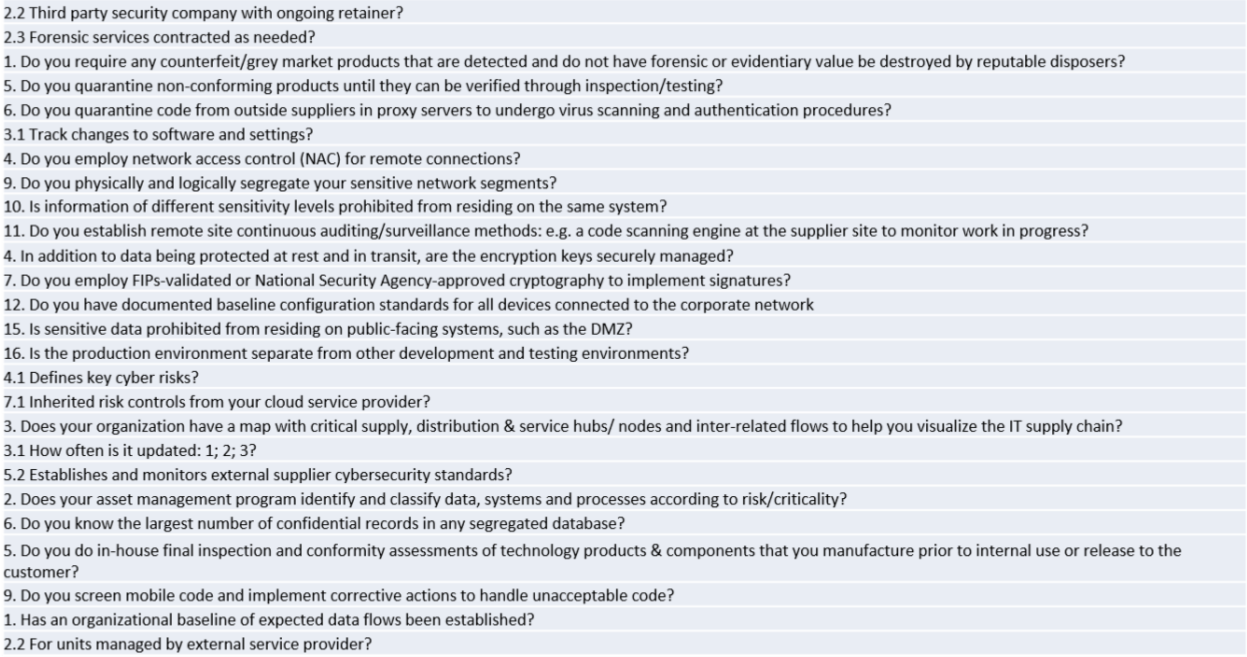
Appendix – Impactful policies & actions

Framework Policies/Actions That Reduce The 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?

Framework Policies/Actions That Reduce The Number Of 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?

Framework Policies/Actions That Reduce The Number Of 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?

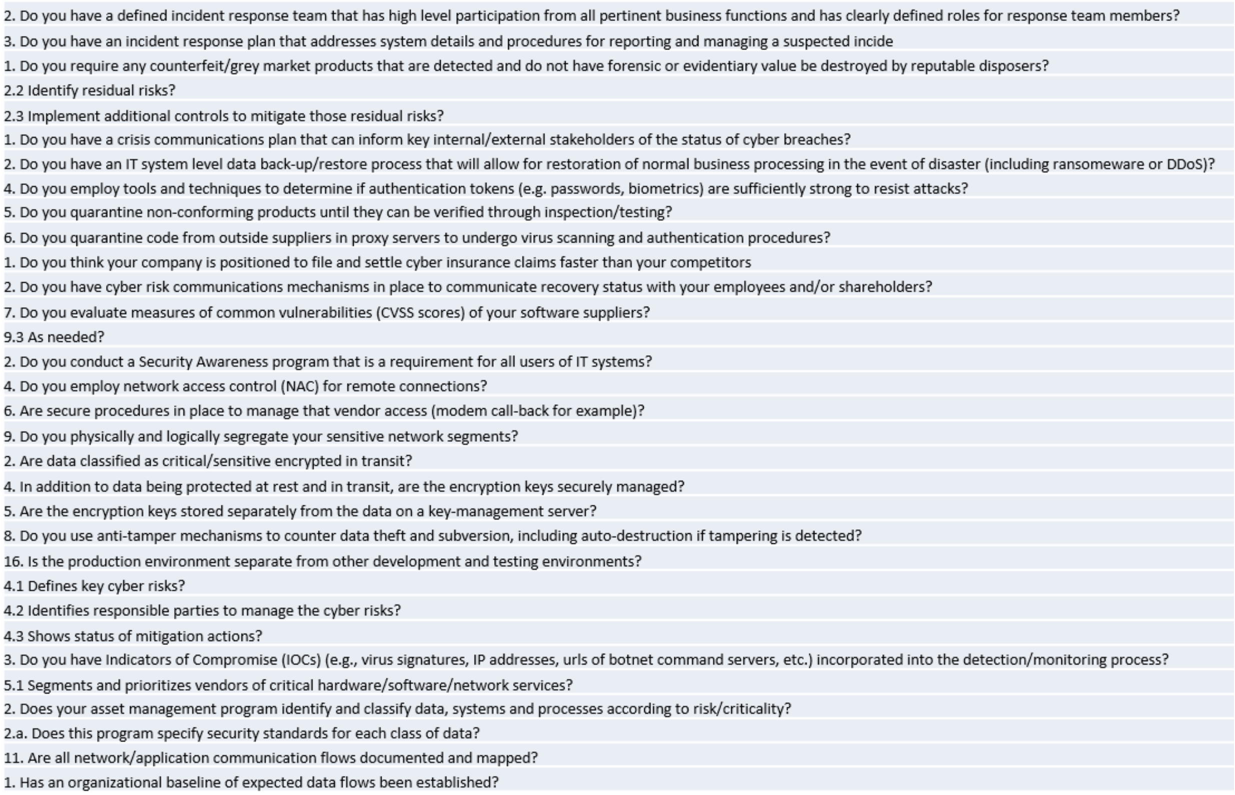
6. Do you know the largest number of confidential records in any segregated database?

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?

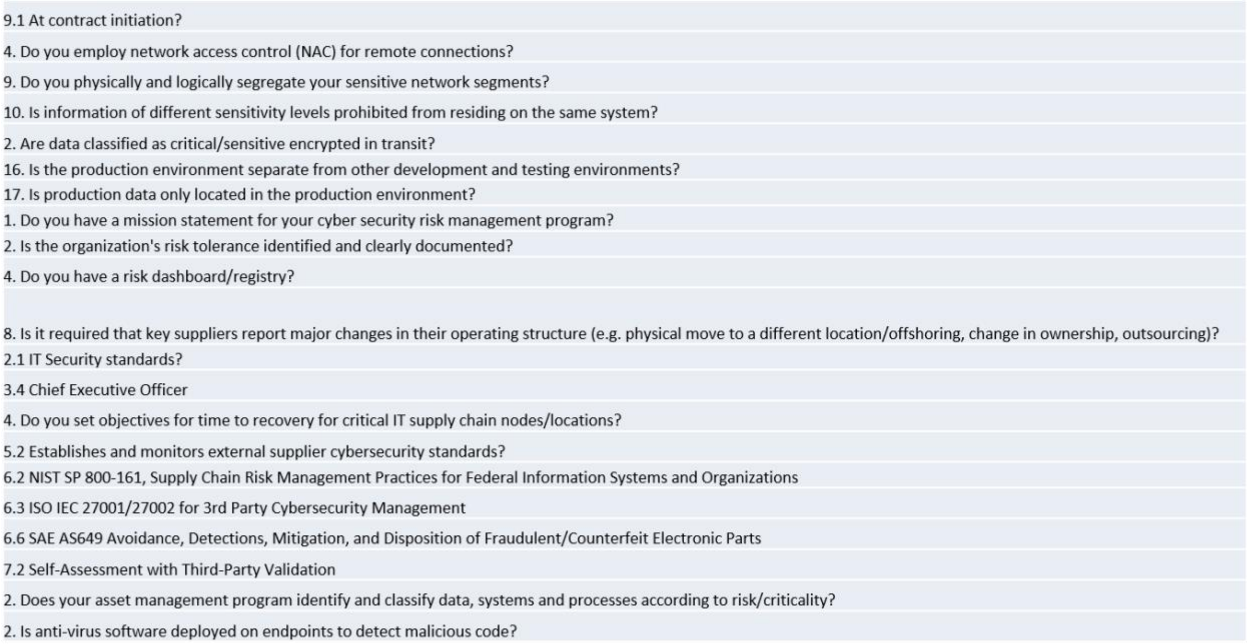
1. Has an organizational baseline of expected data flows been established?

Framework Policies/Actions That Reduce The Number Of 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?

Framework Policies/Actions That Reduce The Number Of 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?