https://cyberchain-dev.rhsmith.umd.edu/assessments/3

Welcome, han Account settings Logout | Home Resources Alerts & News Contact

CYBERCHAIN Guidelines to measure and assess cyber supply chain risk

Assessments Tools Why Use CyberChain

Instructions

Respondent Profile

Assessment Questions

Results

Step Two: How to Successfully Complete the Assessment

Each NIST category has its own set of questions you will need to answer. You might need to consult with others in your organization to answer some of these questions. Typically, the perspectives of colleagues from different functional areas are needed such as subject matter experts from IT security, supply chain and risk management. Your team can go back or forward through the assessments and save drafts before finalizing and submitting the completed survey. Once you have completed all assessments, you will be able to view your results in the Results menu.

This collection of information contains Paperwork Reduction Act (PRA) requirements approved by the Office of Management and Budget (OMB). Notwithstanding any other provisions of the law, no person is required to respond to, nor shall any person be subject to a penalty for failure to comply with, a collection of information subject to the requirements of the PRA unless that collection of information displays a currently valid OMB control number. Public reporting burden for this collection is estimated to be 90 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed and completing and reviewing the collection of information. Send comments regarding this burden estimate or any aspect of this collection of information, including suggestions for reducing this burden, to the:

National Institute of Standards and Technology
Attn: Jon Boyens.
(301) 975-5549.
jon.boyens@nist.gov
OMB Control No. 0693-0043
Expiration Date: 12/31/2018

CYBERCHAIN Guidelines to measure and assess cyber supply chain risk

Detect: Anomalies and Events

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

- Yes
- No
- Not Applicable

2. Do you use a Security Information and Event Management (SIEM) platform to aggregate and correlate security event information? *

- Yes
- No
- Not Applicable

Does your SIEM dashboard display event information:

2.1 For in-house units? *

- Yes
- No
- Not Applicable

2.2 For units managed by external service provider? *

- Yes
- No
- Not Applicable

3. Do you receive current threat information from external industry/government/commercial sources? *

- Yes
- No
- Not Applicable

4. Do you participate in Industry Specific Information Sharing and Analysis Centers (ISACs) for the purpose of sharing threat information? *

- Yes
- No
- Not Applicable

CYBERCHAIN Guidelines to measure and assess cyber supply chain risk

Detect: Detection Processes

1. Is there a centralized corporate IT Incident Database that enables your organization to track the effectiveness of operational risk controls in place across your critical IT systems?

- Yes
- No
- Not Applicable

2. Do your detection and information sharing processes extend to suppliers?

- Yes
- No
- Not Applicable

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?

- Yes
- No
- Not Applicable

Save Draft Submit

CyberChain
Supply Chain Center, Robert H. Smith School of Business
College Park, MD 20742
USA

cyberchainadmin@rhsmith.umd.edu

CYBERCHAIN Guidelines to measure and assess cyber supply chain risk

Detect: Security and Continuous Monitoring

1. Is a network-based IDS deployed, configured, and continuously monitored to detect security incidents? *

- Yes
- No
- Not Applicable

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

- Yes
- No
- Not Applicable

3. How often do you use penetration testing on your operational systems to detect vulnerabilities? *

- Always
- Often
- Sometimes
- Seldom
- Never

4. Do you have testing/inspection processes for handling the receipt of electronic products, components and spare parts that you purchase / acquire? *

- Yes
- No
- Not Applicable

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? *

- Yes
- No
- Not Applicable

6. Do you use external evaluation labs (eg Common Criteria Certified Labs) to conduct conformity assessments of hardware and software prior to internal use or release to customer? *

- Yes
- No
- Not Applicable

7. Is acceptance testing of software built into contracts, with payments to suppliers withheld until test results are positive? *

- ◯ Yes
- ◯ No
- ◯ Not Applicable

8. Do you extract and analyze all anomalies from audit logs, access reports, and security incident tracking reports? *

- ◯ Yes
- ◯ No
- ◯ Not Applicable

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

- ◯ Yes
- ◯ No
- ◯ Not Applicable

Save Draft Submit

CyberChain
Supply Chain Center, Robert H. Smith School of Business
College Park, MD 20742
USA

cyberchainadmin@rhsmith.umd.edu

CYBERCHAIN Guidelines to measure and assess cyber supply chain risk

Identify: Asset Management

Identify: Asset Management

1. Do you have an accounting or inventory of assets related to protected data? (Assets include: network devices, servers, desktops, registers, operating systems, database software, and applications.) *

- ◯ Yes
- ◯ No
- ◯ Not Applicable

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

- ◯ Yes, for ALL classes of data
- ◯ Yes, for SOME classes of data
- ◯ No, not for any class of data
- ◯ Not Applicable

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

- ◯ Yes, for ALL classes of data
- ◯ Yes, for SOME classes of data
- ◯ No, not for any class of data
- ◯ Not Applicable

3. Do you have a process for regularly and frequently identifying vulnerabilities associated with assets related to protected data? *

- ◯ Yes, regularly and frequently
- ◯ Yes, but irregularly and infrequently
- ◯ No process
- ◯ Not Applicable

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

- ◯ Yes, for ALL applicable IT assets
- ◯ Yes, for SOME applicable IT assets
- ◯ Not for any IT assets
- ◯ Not Applicable

5. Do you know how many personal confidential records (PII, PHI or other similar) you hold on your systems? *

- ◯ Yes
- ◯ No
- ◯ Not Applicable

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

- ◯ Yes
- ◯ No
- ◯ Not Applicable

7. Do you use embedded digital signatures in hardware or software to uniquely identify and authenticate supply chain elements, processes, and actors? *

- ◯ Yes, for hardware and software
- ◯ Yes, for either hardware or software
- ◯ No, for neither hardware or software
- ◯ Not Applicable

8. Do you have an Information Lifecycle Management plan that incorporates best practices for record retention, awareness and training and database storage and destruction? *

- ◯ Yes, for all three
- ◯ Yes, for at least one of the three
- ◯ No Lifecycle Management Plan
- ◯ Not Applicable

9. Have you completed as Business Impact Analysis for all enterprise applications to prioritize business continuity actions? *

- ◯ Yes, for ALL applications
- ◯ Yes, for SOME applications
- ◯ No Business Impact Analysis
- ◯ Not Applicable

10. Do you have an accurate, up-to-date network diagram? *

- ◯ Yes
- ◯ No
- ◯ Not Applicable

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

- ◯ Yes
- ◯ No
- ◯ Not Applicable

Save Draft Submit

Supply Chain Center, Robert H. Smith School of Business
College Park, MD 20742
USA

cyberchainadmin@rhsmith.umd.edu

CYBERCHAIN Guidelines to measure and assess cyber supply chain risk

Identify: Business Environment

Identify: Business Environment

1. Are your organization's business mission and objectives prioritized and communicated to stakeholders? *

- Yes
- No
- Not Applicable

2. Have you identified supply chain dependencies for these organizational mission priorities? *

- Yes
- No
- Not Applicable

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? *

- Yes
- No
- Not Applicable

3.1 How often is it updated: every few years; annually; every few months? *

- Every few months
- Annually
- Every few years
- Not Applicable

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

- Yes
- No
- Not Applicable

5. Do you have a supplier management program that:

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

- Yes
- No
- Not Applicable

5.2 Establishes and monitors external supplier cybersecurity standards? *

- ◯ Yes
- ◯ No
- ◯ Not Applicable

6. Which of the following standards / practice guidelines does your organization currently use?

6.1 National Institute of Standards and Technology Cybersecurity Framework for Planning and Management *

- ◯ Extremely Used
- ◯ Frequently Used
- ◯ Moderately Used
- ◯ Occassionally Used
- ◯ Never Used

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

- ◯ Extremely Used
- ◯ Frequently Used
- ◯ Moderately Used
- ◯ Occassionally Used
- ◯ Never Used

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

- ◯ Extremely Used
- ◯ Frequently Used
- ◯ Moderately Used
- ◯ Occassionally Used
- ◯ Never Used

6.4 ISO 20244 Trusted Technology Provider Standard *

- ◯ Extremely Used
- ◯ Frequently Used
- ◯ Moderately Used
- ◯ Occassionally Used
- ◯ Never Used

6.5 ISO/IEC 27036 Guidelines for Information Security and Supplier Relationships *

- ◯ Extremely Used
- ◯ Frequently Used
- ◯ Moderately Used
- ◯ Occassionally Used
- ◯ Never Used

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

- ◯ Extremely Used
- ◯ Frequently Used
- ◯ Moderately Used
- ◯ Occassionally Used
- ◯ Never Used

6.7 Other Standard

7. Do you verify and validate the use of these standards by any or all of the following means:

7.1 Self-Assessment *

- ◯ Yes
- ◯ No
- ◯ Not Applicable

7.2 Self-Assessment with Third-Party Validation *

- ◯ Yes
- ◯ No
- ◯ Not Applicable

7.3 Third-Party Assessment and Validation *

- ◯ Yes
- ◯ No
- ◯ Not Applicable

Save Draft Submit

CyberChain
Supply Chain Center, Robert H. Smith School of Business
College Park, MD 20742
USA

cyberchain-admin@rhsmith.umd.edu

CYBERCHAIN Guidelines to measure and assess cyber supply chain risk

Identify: Governance

1. Do you have one person who manages Information Security as a full time responsibility? *

- Yes
- No
- Not Applicable

1.1 What is this person's estimated years of information security experience? *

- 20 or more
- 10 to 19
- 4 to 9
- 1 to 3
- Not Applicable

2. Are c-suite/executive managers involved with the Information Security Officer in setting and communicating:

2.1 IT Security standards? *

- Yes
- No
- Not Applicable

2.2 Control structures? *

- Yes
- No
- Not Applicable

2.3 Roles and responsibilities? *

- Yes
- No
- Not Applicable

3. To what degree does the CIO/CSO organization coordinate actions with the following enterprise actors to manage cyber risk:

3.1 VP of Operations/Supply Chain *

- Always
- Often

- ◯ Sometimes
- ◯ Seldom
- ◯ Never

3.2 Chief Risk Officer *

- ◯ Always
- ◯ Often
- ◯ Sometimes
- ◯ Seldom
- ◯ Never

3.3 Chief Financial Officer *

- ◯ Always
- ◯ Often
- ◯ Sometimes
- ◯ Seldom
- ◯ Never

3.4 Chief Executive Officer *

- ◯ Always
- ◯ Often
- ◯ Sometimes
- ◯ Seldom
- ◯ Never

3.5 Chief Legal Officer *

- ◯ Always
- ◯ Often
- ◯ Sometimes
- ◯ Seldom
- ◯ Never

3.6 Chief Compliance Officer *

- ◯ Always
- ◯ Often
- ◯ Sometimes
- ◯ Seldom
- ◯ Never

3.7 Board Risk/Audit Committee *

- ◯ Always
- ◯ Often
- ◯ Sometimes
- ◯ Seldom
- ◯ Never

4. Are your organization's legal and regulatory requirements understood and used to prioritize cybersecurity risk management activities? *

- ◯ Yes
- ◯ No
- ◯ Not Applicable

5. Is an organizational information security policy documented? *

- ◯ Yes
- ◯ No
- ◯ Not Applicable

6. Is the Board of Directors (BoD) (or equivalent governing body) regularly apprised of cyber risk conditions and defenses? *

- ◯ Yes
- ◯ No
- ◯ Not Applicable

7. Do you have a cloud services controls matrix documenting:

7.1 Inherited risk controls from your cloud service provider? *

- ◯ Yes
- ◯ No
- ◯ Not Applicable

7.2 Dual or joint risk controls? *

- ◯ Yes
- ◯ No
- ◯ Not Applicable

7.3 Board Risk/Audit Committee? *

- ◯ Yes
- ◯ No
- ◯ Not Applicable

Save Draft Submit

CyberChain
Supply Chain Center, Robert H. Smith School of Business
College Park, MD 20742
USA

cyberchainadmin@rhsmith.umd.edu

[redacted]

CYBERCHAIN Guidelines to measure and assess cyber supply chain risk

Identify: Risk Assessment

1. Is risk assessment a required component of your cyber system development life cycle (SDLC) plan? *

- Yes
- No
- Not Applicable

2. Do you have a data-gathering mechanism to capture and consolidate information on risk events and exposures? *

- Yes
- No
- Not Applicable

3. Do you have a formal methodology to evaluate risk information based on probability of occurrence and severity of risks to your cyber systems? *

- Yes
- No
- Not Applicable

4. Are identified risks prioritized in order to inform risk management decisions? *

- Yes
- No
- Not Applicable

5. How often do you employ war gaming or other threat modeling exercises to identify the spectrum of potential attack vectors for your internal network and technology? *

- Frequently
- Often
- Sometimes
- Rarely
- Never

6. Are you able to identify critical data that needs extra protection and more investment because of business and regulatory compliance, e.g. health profile data for HIPAA compliance? *

- Yes
- No
- Not Applicable

7. Can you calculate the direct/indirect value of your company's critical data e.g. the revenue it generates, the market share it contributes toward? *

- ◯ Yes
- ◯ No
- ◯ Not Applicable

8. Can you calculate the upper boundaries or maximum probable losses from critical IT system incidents or data breaches? *

- ◯ Yes
- ◯ No
- ◯ Not Applicable

9. Are your critical vendors identified and prioritized based upon:

9.1 Access to sensitive data? *

- ◯ Yes
- ◯ No
- ◯ Not Applicable

9.3 Do you assess the cyber risks of your critical suppliers? *

- ◯ Yes
- ◯ No
- ◯ Not Applicable

9.2 Criticality in maintaining continuity of the business? *

- ◯ Yes
- ◯ No
- ◯ Not Applicable

Save Draft Submit

CyberChain
Supply Chain Center, Robert H. Smith School of Business
College Park, MD 20742
USA

cyberchain-dmin@rhsmith.umd.edu

CYBERCHAIN Guidelines to measure and assess cyber supply chain risk

Identify: Risk Management

1. Do you have a mission statement for your cyber security risk management program? *
- Yes
- No
- Not Applicable

2. Is the organization's risk tolerance identified and clearly documented? *
- Yes
- No
- Not Applicable

3. Do you have a cyber risk management organizational chart with reporting relationships delineated? *
- Yes
- No
- Not Applicable

4. Do you have a risk dashboard/registry? *
- Yes
- No
- Not Applicable

Does your risk dashboard/registry do the following:

4.1 Defines key cyber risks? *
- Yes
- No
- Not Applicable

4.2 Identifies responsible parties to manage the cyber risks? *
- Yes
- No
- Not Applicable

4.3 Shows status of mitigation actions? *
- Yes

- ◯ No
- ◯ Not Applicable

5. Do you have a process in place to manage trusted vendors *

- ◯ Yes
- ◯ No
- ◯ Not Applicable

6. Do you evaluate the previous performance of IT vendors, including on-time delivery, and product quality? *

- ◯ Yes
- ◯ No
- ◯ Not Applicable

7. As an acquirer/purchaser of vendor services, do you have contractually-mandated daisy chained risk management processes for your supply base? *

- ◯ Yes
- ◯ No
- ◯ Not Applicable

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)? *

- ◯ Yes
- ◯ No
- ◯ Not Applicable

9. Do you use trusted carriers (e.g. DHS Known Carriers) to handle your shipment and tracking of deliveries? *

- ◯ Yes
- ◯ No
- ◯ Not Applicable

Save Draft Submit

CyberChain
Supply Chain Center, Robert H. Smith School of Business
College Park, MD 20742
USA

cyberchainadmin@rhsmith.umd.edu

CYBERCHAIN Guidelines to measure and assess cyber supply chain risk

Protect: Access Control

1. Do you assign privileges and permissions based on user roles? *
- Yes
- No
- Not Applicable

2. Do you incorporate single sign-on system for authenticating users across multiple accounts? *
- Yes
- No
- Not Applicable

3. Is there a daisy chain, an interconnected set of written agreements among actors in your supply chain that assigns access control responsibilities and methods among all parties? *
- Yes
- No
- Not Applicable

4. Do you employ network access control (NAC) for remote connections? *
- Yes
- No
- Not Applicable

5. Is the organization aware of all vendor remote access to internal devices, especially those that require a direct dial-in connection? *
- Yes
- No
- Not Applicable

6. Are secure procedures in place to manage that vendor access (modem call-back for example)? *
- Yes
- No
- Not Applicable

7. Are organizationally-defined traffic flows enforced, including:

7.1 All traffic from the internet can only reach the internet-facing DMZ? *

- ◯ Yes
- ◯ No
- ◯ Not Applicable

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

- ◯ Yes
- ◯ No
- ◯ Not Applicable

8. Do you employ multifactor authentication

8.1 For remote access to your network? *

- ◯ Yes
- ◯ No
- ◯ Not Applicable

8.4 For super-users with privileged credentials? *

- ◯ Yes
- ◯ No
- ◯ Not Applicable

8.2 For internal users? *

- ◯ Yes
- ◯ No
- ◯ Not Applicable

8.3 For vendors and third parties? *

- ◯ Yes
- ◯ No
- ◯ Not Applicable

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

- ◯ Yes
- ◯ No
- ◯ Not Applicable

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

- ◯ Yes
- ◯ No
- ◯ Not Applicable

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? *

- ◯ Yes
- ◯ No
- ◯ Not Applicable

12. Do you have in place extra physical security controls (e.g, video surveillance of public areas; and location of servers in locked, inaccessible areas) over sensitive hardware/software/networks? *

- ◯ Yes
- ◯ No
- ◯ Not Applicable

Save Draft Submit

CyberChain
Supply Chain Center, Robert H. Smith School of Business
College Park, MD 20742
USA

cyberchainadmin@rhsmith.umd.edu

CYBERCHAIN Guidelines to measure and assess cyber supply chain risk

Protect: Awareness and Training

1. Do you conduct training of receiving personnel in regards to detection of counterfeit or sub-grade hardware or software? *

- Yes
- No
- Not Application

2. Do you conduct a Security Awareness program that is a requirement for all users of IT systems? *

- Yes
- No
- Not Applicable

3. Do you conduct a formal cybersecurity training program for those who have direct cyber operations responsibilities? *

- Yes
- No
- Not Applicable

4. Are phishing tests a regular part of your awareness program? *

- Yes
- No
- Not Applicable

Save Draft Submit

CyberChain
Supply Chain Center, Robert H. Smith School of Business
College Park, MD 20742
USA

cyberchain-admin@rhsmith.umd.edu

CYBERCHAIN Guidelines to measure and assess cyber supply chain risk

Protect: Data Security

1. Are data classified as critical/sensitive encrypted at rest? *
- Yes
- No
- Not Applicable

2. Are data classified as critical/sensitive encrypted in transit? *
- Yes
- No
- Not Applicable

3. Do you encrypt software and software patches at rest and in motion throughout delivery? *
- Yes
- No
- Not Applicable

4. In addition to data being protected at rest and in transit, are the encryption keys securely managed? *
- Yes
- No
- Not Applicable

5. Are the encryption keys stored separately from the data on a key-management server? *
- Yes
- No
- Not Applicable

6. Is encrypted data in transit carefully planned so as not to blind/hinder the organization's security technologies? *
- Yes
- No
- Not Applicable

7. Do you employ FIPs-validated or National Security Agency-approved cryptography to implement signatures? *
- Yes
- No
- Not Applicable

8. Do you use anti-tamper mechanisms to counter data theft and subversion, including auto-destruction if tampering is detected? *

- Yes
- No
- Not Applicable

9. Do you use tamper-resistant product packaging and digital seals to prevent or minimize in-transit intrusion? *

- Yes
- No
- Not Applicable

10. Do you use Data Loss Prevention (DLP) software for data in use, in motion, and at rest? *

- Yes
- No
- Not Applicable

11. Is egress traffic monitored (e.g. # of connections, length of connections, amount of traffic) so as to detect outbound connections that may be exfiltrating organizational data? *

- Yes
- No
- Not Applicable

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

- Yes
- No
- Not Applicable

13. Do you follow OWASP (or similar) standards for coding of web applications? *

- Yes
- No
- Not Applicable

14. Do you have network segmentation such that very critical data are located in subnets that are protected by their own firewall and intrusion detection system (IDS)? *

- Yes
- No
- Not Applicable

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

- Yes
- No
- Not Applicable

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

- Yes
- No
- Not Applicable

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

- ◯ Yes
- ◯ No
- ◯ Not Applicable

18. Do you turn off unnecessary functions in COTs or GOTs products to reduce or eliminate unauthorized access or exposure of the system? *

- ◯ Yes
- ◯ No
- ◯ Not Applicable

19. Are your network risk management controls automated? *

- ◯ Always
- ◯ Often
- ◯ Sometimes
- ◯ Seldom
- ◯ Never

Save Draft Submit

CyberChain
Supply Chain Center, Robert H. Smith School of Business
College Park, MD 20742
USA

cyberchainadmin@rhsmith.umd.edu

CYBERCHAIN Guidelines to measure and assess cyber supply chain risk

Protect: Information Protection Processes

1. Do you conduct baseline security reviews (e.g. criminal, education, credit checks) of key IT personnel and high access users? *
- Yes
- No
- Not Applicable

2. How often do you update personnel security reviews? *
- Always
- Often
- Sometimes
- Seldom
- Never

3. Do you use end to end Configuration Management (CM) systems to:

3.1 Track changes to software and settings? *
- Yes
- No
- Not Applicable

3.2 Record geo-spatial or IP address-based location information of actors? *
- Yes
- No
- Not Applicable

4. Are all proposed configuration changes required to be reviewed by a Change Control Board? *
- Yes
- No
- Not Applicable

5. Are technical solutions in place to enforce standard configurations? *
- Yes
- No
- Not Applicable

6. Do you evaluate your suppliers' certifications in common IT standards (e.g. ISO/IEC 9001, ISO/IEC 27001, ISO 2800)? *

- Yes
- No
- Not Applicable

7. Do you evaluate measures of common vulnerabilities (CVSS scores) of your software suppliers? *

- Yes
- No
- Not Applicable

8. Is a vulnerability management plan in place to feed risk management decisions? *

- Yes
- No
- Not Applicable

9. How often is cyber response/recovery planning and testing conducted with critical suppliers :

9.1 At contract initiation? *

- Yes
- No
- Not Applicable

9.2 During ongoing performance reviews? *

- Yes
- No
- Not Applicable

9.3 As needed? *

- Yes
- No
- Not Applicable

10. Are regular backups of information conducted and tested? *

- Yes
- No
- Not Applicable

Save Draft Submit

CyberChain
Supply Chain Center, Robert H. Smith School of Business
College Park, MD 20742
USA

cyberchainadmin@rhsmith.umd.edu

CYBERCHAIN Guidelines to measure and assess cyber supply chain risk

Protect: Protective Technology

1. Do you have backup or mirror sites to ensure continuity of operations in case of an incident at a primary site? *

- Yes
- No
- Not Applicable

2. Do you routinely encrypt sensitive communications INTERNALLY using techniques such as DNSSEC, TLS, or SSL? *

- Yes
- No
- Not Applicable

3. Do you routinely encrypt sensitive communications with VENDORS OR CUSTOMERS using techniques such as DNSSEC, TLS, or SSL? *

- Yes
- No
- Not Applicable

4. Do you employ tools and techniques to determine if authentication tokens (e.g. passwords, biometrics) are sufficiently strong to resist attacks? *

- Yes
- No
- Not Applicable

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

- Yes
- No
- Not Applicable

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

- Yes
- No
- Not Applicable

7. Has an organizational policy for removable media been documented? Is it enforced? *

- Yes
- No

- ◯ Not Applicable

8. Is the organizational policy for removable media enforced? *

- ◯ Yes
- ◯ No
- ◯ Not Applicable

9. Do you use standard components and parts across you IT product lines to increase resiliency of the supply chain? *

- ◯ Yes
- ◯ No
- ◯ Not Applicable

Save Draft Submit

CyberChain
Supply Chain Center, Robert H. Smith School of Business
College Park, MD 20742
USA

cyberchainadmin@rhsmith.umd.edu

CYBERCHAIN Guidelines to measure and assess cyber supply chain risk

Recover: Communications

1. Do you think your company is positioned to file and settle cyber insurance claims faster than your competitors *

- Yes
- No
- Not Applicable

2. Do you have cyber risk communications mechanisms in place to communicate recovery status with your employees and/or shareholders? *

- Yes
- No
- Not Applicable

3. Do you have cyber risk communications mechanisms in place to communicate recovery status with external partners and customers *

- Yes
- No
- Not Applicable

Save Draft Submit

CyberChain
Supply Chain Center, Robert H. Smith School of Business
College Park, MD 20742
USA

cyberchainadmin@rhsmith.umd.edu

CYBERCHAIN Guidelines to measure and assess cyber supply chain risk

Recover: Improvements

1. Are proposed solutions to breaches and cyber events tested to assure that the same exploit or error can not happen again? *

- Yes
- No
- Not Applicable

Save Draft Submit

CyberChain
Supply Chain Center, Robert H. Smith School of Business
College Park, MD 20742
USA

cyberchainadmin@rhsmith.umd.edu

CYBERCHAIN

Guidelines to measure and assess cyber supply chain risk

Recover: Recovery Planning

1. Do you update your IT system level disaster recovery plan at least annually? *

- Yes
- No
- Not Applicable

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)? *

- Yes
- No
- Not Applicable

Save Draft Submit

CyberChain
Supply Chain Center, Robert H. Smith School of Business
College Park, MD 20742
USA

cyberchainadmin@rhsmith.umd.edu

CYBERCHAIN Guidelines to measure and assess cyber supply chain risk

Respond: Analysis

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? *

- Yes
- No
- Not Applicable

2. Does your Corporate Audit/Risk Committee:

2.1 Examine the response to an incident? *

- Yes
- No
- Not Applicable

2.2 Identify residual risks? *

- Yes
- No
- Not Applicable

2.3 Implement additional controls to mitigate those residual risks? *

- Yes
- No
- Not Applicable

Save Draft Submit

cyberchainadmin@rhsmith.umd.edu

This site was developed in partnership between the National Institute of Standards and Technology and the University of Maryland, Robert H. Smith School of Business.

CYBERCHAIN Guidelines to measure and assess cyber supply chain risk

Respond: Communications

1. Do you have a crisis communications plan that can inform key internal/external stakeholders of the status of cyber breaches? *

- ○ Yes
- ○ No
- ○ Not Applicable

Save Draft Submit

CyberChain
Supply Chain Center, Robert H. Smith School of Business
College Park, MD 20742
USA

cyberchainadmin@rhsmith.umd.edu

CYBERCHAIN Guidelines to measure and assess cyber supply chain risk

Respond: Improvements

1. Are major incident response performances debriefed with C-suite executives and the Board? *

- Yes
- No
- Not Applicable

2. Do you have a lessons learned phase in which the incident response team reviews and modifies the incident response plan (IRP)? *

- Yes
- No
- Not Applicable

3. If needed, are baseline configurations modified to prevent the same exploit or error? *

- Yes
- No
- Not Applicable

Save Draft Submit

CyberChain
Supply Chain Center, Robert H. Smith School of Business
College Park, MD 20742
USA

cyberchainadmin@rhsmith.umd.edu

CYBERCHAIN Guidelines to measure and assess cyber supply chain risk

Respond: Mitigation

1. Do you have a corporate digital forensics capacity that performs the following:

1.1 Protocols for investigation and systems traceability/auditability *
- Yes
- No
- Not Applicable

1.2 Engagement of third party law/accounting firms to determine value of claims? *
- Yes
- No
- Not Applicable

1.3 Notifications to third party insurer of loss of revenue? *
- Yes
- No
- Not Applicable

1.4 Notifications to Government Authorities (e.g., FBI) *
- Yes
- No
- Not Applicable

2. Does your forensics capability rely on:

2.3 Forensic services contracted as needed? *
- Yes
- No
- Not Applicable

2.2 Third party security company with ongoing retainer? *
- Yes
- No
- Not Applicable

2.1 In-house security staff? *

- ◯ Yes
- ◯ No
- ◯ Not Applicable

3. Does your evidence handling process establish a "chain of custody" in your forensics management program? *

- ◯ Yes
- ◯ No
- ◯ Not Applicable

4. Do you have processes in place for mitigating, disposing, and reporting fraudulent or counterfeit electronic hardware and software? *

- ◯ Yes
- ◯ No
- ◯ Not Applicable

Save Draft Submit

CyberChain
Supply Chain Center, Robert H. Smith School of Business
College Park, MD 20742
USA

cyberchainadmin@rhsmith.umd.edu

CYBERCHAIN Guidelines to measure and assess cyber supply chain risk

Respond: Response Planning

1. Do you have procedures for rating, reporting, and escalating events identified through detection/monitoring activities? *

- Yes
- No
- Not Applicable

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? *

- Yes
- No
- Not Applicable

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

- Yes
- No
- Not Applicable

Save Draft Submit

CyberChain
Supply Chain Center, Robert H. Smith School of Business
College Park, MD 20742
USA

cyberchainadmin@rhsmith.umd.edu