

ICT 공급망 보안위협 및 국내·외 정책 현황

2020. 7. 16

한국인터넷진흥원 이향진

jiinii@kisa.or.kr



Contents

I : ICT 공급망 보안

II : ICT 공급망 보안 위협

III : 국내외 ICT 공급망 보안정책 현황



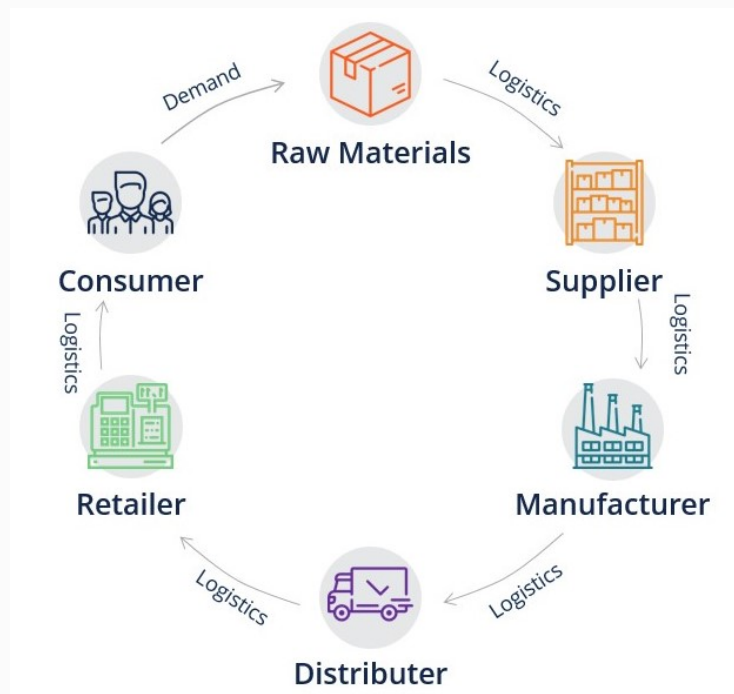
I

ICT 공급망 보안



공급망 관리

- 부품 제공업체부터 생산자, 배포자, 고객에 이르는 물류의 흐름을 하나의 가치사슬 관점에서 파악하고 필요한 정보가 원활히 흐르도록 (구글)
- 제품, 정보가 생산자에게서 사용자에게 전달되는 일련의 과정을 감독, 효율적으로 처리 .. (네이버)



ICT 공급망 보안 관리

- ICT 제품(HW, SW, 서비스)의 생산자, 배포자, 고객에 이르는 ICT공급망 전 단계에 걸쳐 보안성(Security)을 관리



ICT 공급망 보안 관리의 어려움, but...

- 다양한 형태의 생산자, 배포자, 고객
- 글로벌 이슈화
- 불분명한 계약관계
- 사고발생 시 책임소재 불분명
- 보안관리를 위한 기술적 한계
- 보안성 관리를 위한 기존 관련 제도의 한계

 그럼에도 ICT 공급망 보안관리는 핫이슈!!

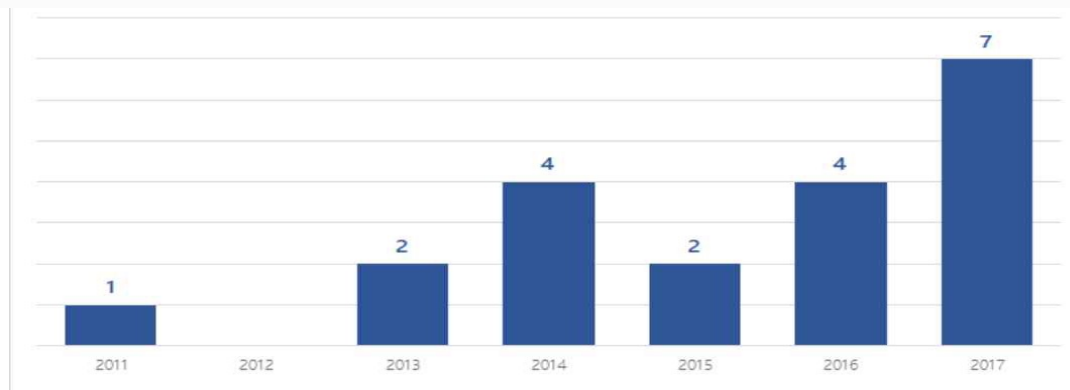
II

ICT 공급망 보안 위협



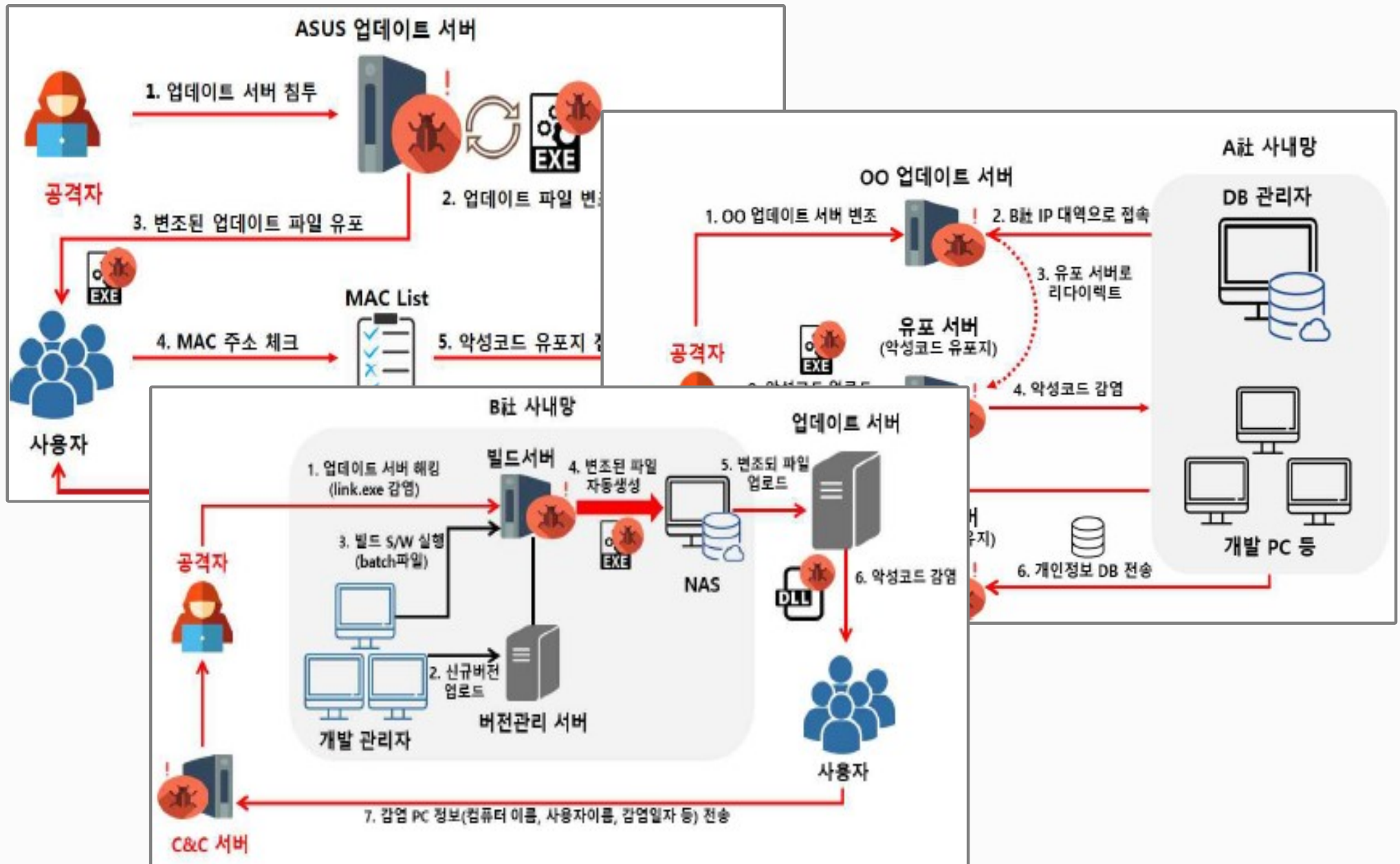
SW 공급망 공격 증가, 주로 SW개발환경 침투 및 업데이트서버 해킹 형태

▪ RSA 컨퍼런스 발표('18)




▪ 공급망 공격 사례 분석 및 대응 방안(KISA, '19.2)





보다 손쉽게, 보다 많은 대상을 상대로, 은밀하고 지속적인 공격 가능

- 최종 공격 대상보다, 상대적으로 허술한 보안 관리 악용
- 잠재적으로 여러 고객사에 대한 공격 가능
- 고도의 기술과 상당한 시간이 소요되지만 공격 성공 시, 은밀하고 지속적인 공격 가능
- 제조 단계 등에서 악성코드 삽입 시, 폐쇄망 환경에서도 손쉽게 공격 가능

 선제적 대응이 어려움에 따라,
ICT공급망 전반에 대한 보안관리 및 지속적 모니터링 필요



국내외 ICT공급망 보안 정책 현황



2010

- Cybersecurity 강화를 위한 조직 설립(Comprehensive National Cybersecurity Initiatives)

2011

- National Defense Authorization Act 제정

2012

- NIST IR 7622 - Supply Chain Risk Management Practices 발표

2013

- 오바마 대통령 행정명령(주요기반시설 보안 및 레질리언스 강화)

2014

- Cyber Supply Chain Management and Transparency Act 제정 실패(민간업계 및 계약자들의 반대)

2015

- NIST SP 800-161 - ICT Supply Chain Risk Management 발표

2016

- 국방 관련 공급망 보안을 위한 Defense Federal Acquisition Regulations Supplement 발표

2017

- 사이버 위협국가 지정(중국, 이란, 북한, 러시아) 및 주요 ICT 제조사와의 공급망 상관관계 조사

2018 ~

- Securing Homeland Security Supply Chain Act 발표 및 공급망 보안 태스크 포스 구성
- 공급망 퓨전센터(인증/평가, 위협정보 공유 등) 설립, 민간 파트너십 및 역량 강화 프로그램 운영 중

CISA의 C-SCRM 프로그램

- HR 6430(Securing Homeland Security Supply Chain Act, '18.9) 의회 통과 후, DHS에 공급망 위험 관련 정보를 정부로 부터 제공받을 권한 부여
- DHS의 사이버 공급망 위험관리 향후 추진계획 발표('18.12)

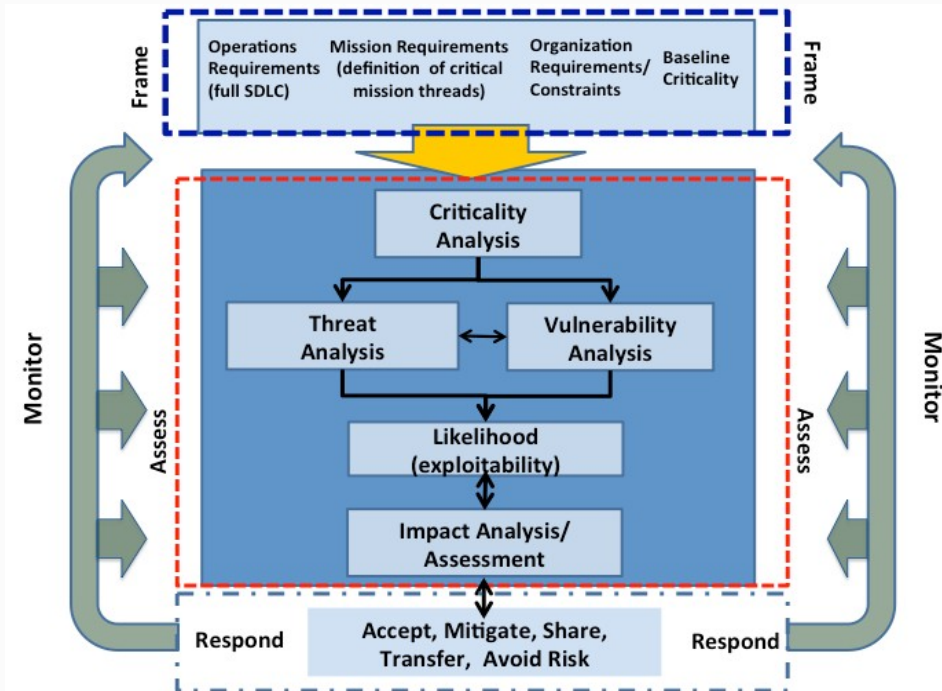
| 공급망 퓨전 센터 | 민관 파트너십 | 역량 강화 |
|--|---|--|
| <ul style="list-style-type: none"> 공급망 평가 서비스 공급망 위협 정보 공유 검증된 입찰자 및 제조자 목록 | <ul style="list-style-type: none"> ICT 공급망 위험관리 대책 위원회 | <ul style="list-style-type: none"> 조직의 역량 평가 훈련, 교육 및 가이드 제공 등 |

☞ 구성 : 국토안보부, 국방부, 상무부 등 8개 부처 및 AT&T, CISCO, FireEye, MS, 삼성 등 26개 민간 사업자

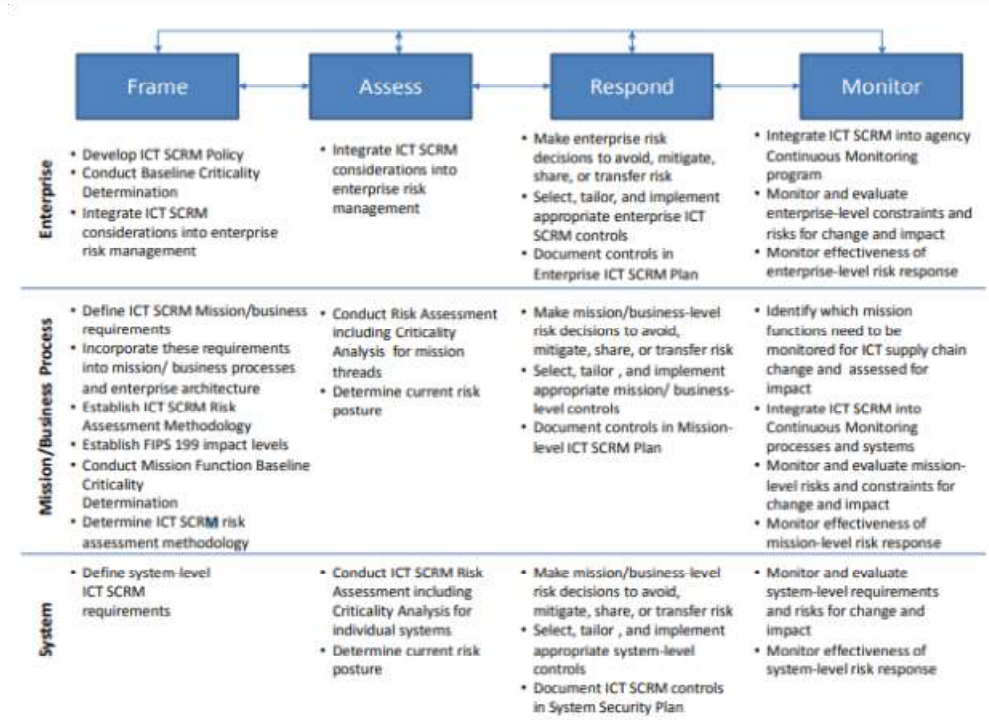
- ICT 공급망 위험관리 대책 위원회 업무 착수('19.2)
 - 정부와 산업의 양방향 정보 공유 및 공유 프레임워크 개발
 - ICT 제품 및 서비스에 대한 위협 평가 절차 및 기준 개발
 - 검증된 입찰자와 우선 구매 제조업체 목록 평가기준 마련
 - 검증된 제조업체와 판매자로 부터의 ICT 제품 및 서비스 구매에 대한 인센티브 제공 정책 마련

NIST, ICT 공급망 보안관리 지침(SP 800-161)('15.4)

- 연방기관 정보시스템과 조직의 ICT 공급망 위험관리를 위한 지침 개발
 - NIST SP 800-39의 위험관리 프로세스 + NIST SP 800-53 R4의 보안통제 항목
- ICT SCRM 관점에서 조직 전체 위험관리 활동 통합 권고, 19가지 대분류 통제 항목 추가/개선



ICT SCRM Risk Management



ICT SCRM Activities in Risk Management Process

NIST IR 7622_National SCRM Practices for Federal IS

10 Practices

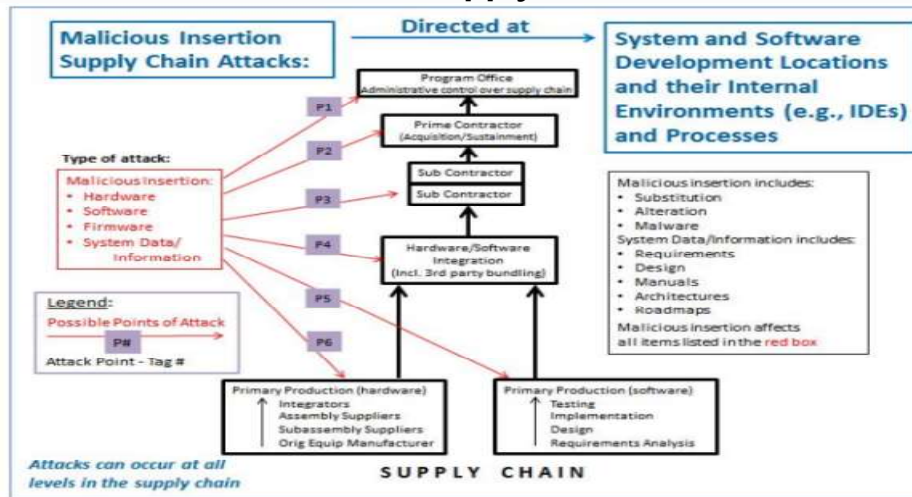
- 4.1 Uniquely Identify Supply Chain Elements, Processes, and Actors
- 4.2 Limit Access and Exposure within the Supply Chain
- 4.3 Establish and Maintain the Provenance of Elements, Processes, Tools, and Data
- 4.4 Share Information within Strict Limits
- 4.5 Perform SCRM Awareness and Training
- 4.6 Use Defensive Design for Systems, Elements, and Processes
- 4.7 Perform Continuous Integrator Review
- 4.8 Strengthen Delivery Mechanisms
- 4.9 Assure Sustainment Activities and Processes
- 4.10 Manage Disposal and Final Disposition Activities throughout the System or Element Life Cycle

4 Type of Actions

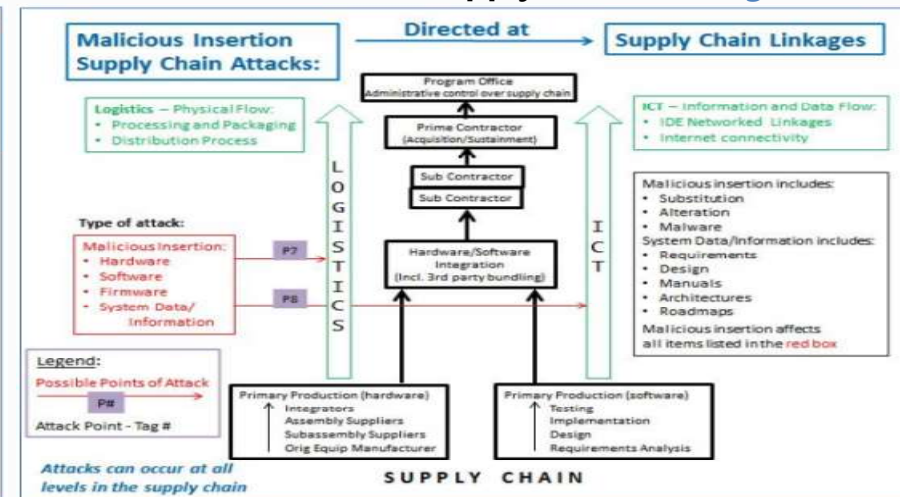
| Type of Action | Role | Description of Action |
|--|------------|--|
| Programmatic Activities | Acquirer | Practices that a federal department and agency acquirer will undertake within their programs, including requirements to be included in contractual documents, as well as internal policies and procedures. |
| General Requirements | Integrator | General practices that an integrator will implement within programs that are either in response to contractual requirements or to document existence of programmatic activities that reduce ICT supply chain risk. |
| | Supplier | General practices that a supplier will implement within programs to document existence of programmatic activities that reduce ICT supply chain risk. |
| Technical Implementation Requirements | Integrator | Detailed technical practices that an integrator will implement within programs to document technical capabilities to manage ICT supply chain risk. |
| | Supplier | Detailed technical practices that a supplier will implement within programs to document technical capabilities to manage ICT supply chain risk. |
| Verification and Validation Activities | Acquirer | Suggestions for how a federal agency acquirer can ascertain that integrators have implemented ICT SCRM in compliance with contract requirements. |
| | Integrator | Suggestions on how an integrator can demonstrate that they have implemented ICT SCRM. |
| | Supplier | Suggestions on how a supplier can demonstrate that they have implemented ICT SCRM. |

MITRE, ICT 공급망 유형에 따른 위협, 공격 패턴 및 사이버보안 관련 지침

< Points of Attack – Supply Chain Locations >



< Points of Attack – Supply Chain Linkages >



| MSA Phase 3 Attacks | TD Phase 12 Attacks | EMD Phase 28 Attacks | P&D Phase 24 Attacks | O&S Phase 22 Attacks |
|------------------------|------------------------|-------------------------|-------------------------|-------------------------|
| Mal. Insertion of: | Mal. Insertion of: | Mal. Insertion of: | Mal. Insertion of: | Mal. Insertion of: |
| - Hardware | - Hardware (5) | - Hardware (13) | - Hardware (12) | - Hardware (10) |
| - Software | - Software (5) | - Software (15) | - Software (9) | - Software (11) |
| - Firmware | - Firmware (1) | - Firmware (8) | - Firmware (8) | - Firmware (6) |
| - Sys Info/Data (3) | - Sys Info/Data (4) | - Sys Info/Data (3) | - Sys Info/Data (3) | - Sys Info/Data (2) |

< 41 Attack Patterns >

- Elevate Security as a Primary Metric in DoD Acquisition and Sustainment
- Form a Whole-of-Government National Supply Chain Intelligence Center (NSIC)
- Execute a Campaign for Education, Awareness, and Ownership of Supply Chain and Digital Risk
- Identify and Empower a Chain of Command for Supply Chain with Accountability for Integrity to DEPSECDEF
- Centralize SCRM-TAC under DSS and Extend DSS Authority
- Increase DoD Leadership Recognition and Awareness of Asymmetric Warfare via Blended Operations
- Establish Independently Implemented Automated Assessment and Continuous Monitoring of DIB Software
- Advocate for Litigation Reform and Liability Protection
- Ensure Supplier Security and Use Contract Terms
- Extend the 2015 National Defense Authorization Act (NDAA) Section 841 Authorities for "Never Contract with the Enemy"
- Institute Innovative Protection of DoD System Design and Operational Information
- Institute Industry-Standard IT Practices in all Software Developments
- Require Vulnerability Monitoring, Coordinating, and Sharing across the Chain of Command for Supply Chain
- Advocate for Tax Incentives and Private Insurance Initiatives
- For Resilience, Employ Failsafe Mechanisms to Backstop Mission Assurance

< 공급망 및 사이버보안 관련 지침 >

2011

- (UK) NCSS는 사이버 보안 인식제고, 민간부문 파트너십 강화를 위한 Natioanl Cyber security programme 수립

2012

- (UK) Defence Cyber Protection Partnership (DCPP) 설립
- (UK) Industrial Security Working Group(ISWG)이 Cabinet Office에 공급망 보안의 위험 및 중요성 보고

2013

- (UK) Cabinet Office, Supplier Assurance Framework 발표 (2018 개정)

2014

- (UK) 공급망 보안 인증제도 시작(Cyber Essential)
- (UK) NCSS는 MoD 등 주요 기관에 ICT 제품 및 서비스를 제공하는 공급자는 Cyber Essential 인증 획득 의무화
- (ENISA) Secure ICT Procurement in Electronic Communications 발표
- (ENISA) Security Guide for ICT Procurement 발표

2015

- (UK) MOD DEFSTAN(Defence Standard) 05-138에서 Cyber security model 소개

2017

- (UK) MOD DEFCON(Defence Condition) 658 발표(MOD Identifiable Information 포함 계약 시 Cyber security model 적용 의무화)

2018

- (UK) CPNI(Centre for Protection of National Infrastructure)는 공급망 사이버 공격 대응을 위한 12개 원칙 발표
- (EU) 유럽의회, 유럽연합 이사회, 유럽위원회가 Cybersecurity Act 합의

2019

- (EU) Cybersecurity Act ICT 장비/서비스 사용에 따른 위험, 잠재적인 공격에 따른 영향도를 고려할 것을 명시

UK, Supplier Assurance Framework

- 조직 및 공급자의 자체 위험평가 결과를 분석하여 사업자 선정 및 계약 관련 보안대책 수립에 활용, 총 8개 항목으로 구성

| 구분 | 주요 내용 |
|-----------------------|--|
| 사전 준비 | <ul style="list-style-type: none"> • 조직의 정보자산, 보안 위험, 위험성향, 위험관리 절차 등 분석 |
| 공급업체와의 계약 식별 | <ul style="list-style-type: none"> • 개별 팀에 산재되어 있는 계약현황 파악 및 리스트 작성 |
| 위험평가가 필요한 계약 식별 | <ul style="list-style-type: none"> • 개인정보, 기밀정보 취급 계약, 과거 사고 사례 등 분석 • 계약의 종류 무관, 종료 임박 계약 및 재계약 철회 건 제외 |
| 위험평가의 수행주체 식별 | <ul style="list-style-type: none"> • 정보자산 및 시스템 소유자, 계약 주관부서, 보안 부서 참여 |
| 위험관리 전략 수립 | <ul style="list-style-type: none"> • CIA 관점에서 비즈니스 영향도 평가 • 전략 수립 시 조직의 위험성향 고려, 현업의 참여 |
| 위험평가 대응 및 조정 | <ul style="list-style-type: none"> • 공급자의 CCfAR(Common Criteria for Assessing Risk) 검토 • 검토결과를 조직의 위험허용 수준 및 위험성향과 매핑 |
| 결과 정리 및 요약 | <ul style="list-style-type: none"> • 계약 관련 위험 및 공급업체에 대한 위험의 우선순위 선정 • 상위 20% 위험에 대한 우선적인 대책수립 방향 제시 |
| 보증(Assurance) 프로그램 수행 | <ul style="list-style-type: none"> • 위험수준 상 계약: 공급자 자체평가 및 SoA(Statement of Assurance) 제출, 증빙 검토, 감사 • 위험수준 중 계약: 공급자 자체평가 및 SoA 제출, 증빙 검토, 정의된 기간 내 재평가 • 위험수준 하 계약: 공급자 자체평가 및 SoA 제출 |
| 프로세스 검토 | <ul style="list-style-type: none"> • 잔여위험 및 공급자의 보안대책 검토 및 보안책임자에게 보고 • 조직차원의 보안대책 수립 및 개선계획 수립 |

UK, Cyber Essential Scheme

- 사이버 위협 대응, 조직의 사이버 보안 역량 강화를 위한 Cyber Essential 인증체계 수립('14.5)
 - 주요 조직의 민감 정보, 개인정보 등 기밀정보를 취급하는 계약과 관련된 공급자에게 Cyber Essential 인증 취득을 의무화('14.10)
- Cyber Essential Scheme의 구성

| UK - DCP | N/A | VL | L | M | H |
|---------------------------|----------|-----------|-----------|-----------|-----------|
| Technology | | 1* | 5 | 7 | 10 |
| Governance | | | 2 | 1 | |
| Culture & Awareness | | | 3 | 2 | |
| Personnel | | | 3 | 3 | |
| Risk Management | | | | 1 | |
| Info Management | | | 2 | 3 | |
| Incident Management | | | 1 | | 1 |
| Total Requirements | 0 | 1* | 17 | 33 | 44 |

*This Requirement, Cyber Essentials Scheme, comprises 26 controls.

| Cyber Risk Profile | Not Applicable | Very Low | Low | Moderate | High |
|--------------------|------------------------------|------------------|--|---------------------|---------------------|
| | | | | | Additional controls |
| | | | | Additional controls | |
| | | | Cyber Essentials +, plus additional controls | | |
| | Cyber Essentials recommended | Cyber Essentials | | | |

ENSIA, Security Guide for ICT Procurement ('14.12)

- ICT 제품을 조달하거나 주요 ICT 서비스를 제3자에게 아웃소싱할 때 보안 위험을 관리하기 위한 보안 요구사항 제시

- 7가지 보안 도메인

- Governance and risk management
- Human resources security
- Security of systems and facilities
- Operations management
- Incident management
- Business continuity management
- Monitoring, auditing and testing

2.1 Governance and risk management

SO1: Information security policy/ SO2: Governance and risk management

Security Risks

Vendor's failure to align its security practises to the provider's security objectives.

Security requirements

- ✓ The provider's security objectives should be fully understood and integrated by the vendor.
- ✓ The vendor selected should have an information security policy ensuring the security and resilience of its products and services, and aligned with the provider's high level security objectives.
- ✓ The vendor should provide evidence of its relevant internal information security policy ensuring the security and resilience of its products and services for provider's analysis.

일본 - 정부 주도로 추진, Society 5.0 환경에서의 보안 프레임워크 발표('19.4)

- Society 5.0을 지원하기 위한 Connected Industry 프로그램과 함께, 증가하는 사이버 위험 (공급망 보안 위험 포함)에 대응하기 위한 Cyber/Physical Security Framework 발표
 - 단일 기업 단위의 보안 대책만으로는 공급망 보안 보장이 어려우므로 공급망에 참여하는 모든 주체가 적용 대상
 - 각 공급망 참가자들의 Security by Design 채택 및 공유 데이터의 보안을 보장, 전체 공급망 시스템에 대한 Resilience 내장을 요구

중국 - 종합적 공급망 보안 정책은 확인되지 않으나, 네트워크 안전법 시행

- 네트워크 안전법(Cyber Security Law) 시행에 따라 중국 내에서 사용되는 네트워크 제품 및 서비스에 대한 보안인증 의무화
- 다양한 필수 인증제도(CCC, NAL, CC-IS 등) 를 통해 정보통신기기, SW 등에 대한 인증을 실시

4 시사점



- 기반시설 등 **주요기관 대상** ICT 공급망 보안강화 정책 수립
- **위험관리 기반**의 접근방법 채택
- **정부 주도**의 공급망 퓨전센터 설립, 인증제도 시행 예정
- 검증된 기업에 대한 **인센티브** 제공



- 공급자 위험 평가를 통해 별도의 **보증** 프로세스 요구
- **공급자에 대한 평가**를 위한 **인증제도**
- 정부 주도의 정책 시행



- **변화하는 미래 융합 환경을 대비한** 보안 프레임워크 개발
- 정부 주도의 정책 시행



- 국가 차원에서 중요 기관의 장비 및 보안제품에 대한 보안인증 강제화

5 국내 정책 수립 방향

- 정부 주도의 정책 수립/추진
- 공급자에 대한 보안관리 강화
- 기존 제도의 사각지대 보완, 국내외 관련 지침, 표준 등과 일관성 있는 기준 제시
- 대상/범위 구체화를 통해 단계적 추진
- 기존 인증제도 등을 활용, 자율적 관리체계 구축
- 관리체계 운영의 실효성 향상을 위한 공급업체 대상 인센티브 방안 마련

감사합니다

