CYBERSECURITY FOR PROCUREMENT

STANDARD

The significance of cybersecurity has grown in recent years as a result of the increased frequency, size, and visibility of breaches in the realms of business and politics. Even as the importance of strong passwords, multi-factor authentication, and phishing awareness have become common knowledge, threats and their associated risks continue to evolve.

The guidance in this document is offered to counter the cybersecurity risk faced by procurement professionals, who must collaborate with the entity's Information Technology Department (IT) to safeguard procurement operations. This practice focuses on Procurement's role in identifying, assessing, and addressing cybersecurity risk.

Definition

Cybersecurity:

Cybersecurity: Prevention of damage to and protection and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.
— The National Institute of Standards and Technology

Element 1: Cyber risks

The procurement professional should work with IT and other stakeholders to identify cyber risks pertaining to procurement operations and functions. The global best practice "The Place of Public Procurement within the Entity" describes Procurement as a liaison to all other departments. Procurement should first identify its operations and functions and then collaborate with IT and other stakeholders to determine the types and levels of cyber risk pertaining to procurement.

Procurement professionals may encounter cyber risk in areas such as:

- People
  - Rigor and frequency of staff training
  - Individual security practices
  - Number of stakeholders
  - Contractors, sub-contractors, and other third parties
    - Location, e.g., parties outside the U.S.
    - Authorization, e.g., federally banned parties
    - Level of access to system
    - Training and practices
- Process
  - Solicitation
    - Scope of work
    - Evaluation of responses
    - Contract terms and conditions
    - Vetting and onboarding of suppliers

Public Procurement Practice

CYBERSECURITY FOR PROCUREMENT

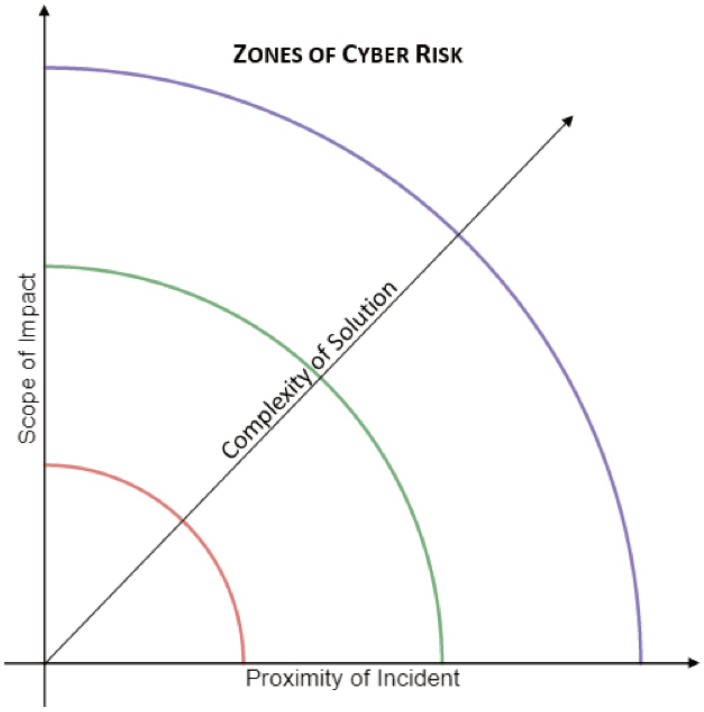
(Cont'd)

- Outsourcing of procurement functions, e.g., payment processing
- Identification of and response to security incidents
- Reporting and accountability
- Handling of sensitive or confidential information

- Technology
  - Network security
    - Configuration, e.g., on-premise vs. remote access
    - Internet of Things (IoT), e.g., HVAC, CCTV, public transit, police cars
  - Hardware and software
    - Compatibility and level of integration
    - Authenticity
    - Reliability, e.g., frequency of testing
    - Age and currency, e.g., updates and patches

The graphic below illustrates how cyber risk levels are affected by factors such as:

- Proximity: origin of incident, i.e., internal vs. external
- Scope:
  - Size of impact, e.g., individual, department, entity, nation
  - Nature of impact, e.g., financial, brand/reputation, privacy/security
- Complexity: requirements for resolution, e.g., training, software patches, litigation



Cyber risk continues to evolve as a result of technological innovation, compromise of sensitive information from cyber attacks, and availability of information, e.g., system manuals. Just as the procurement process may help to mitigate vulnerabilities, there is also the potential to introduce them. Procurement professionals should consult with IT when planning to procure products with embedded technology and services that may require direct or indirect connection with technology systems. Procurement must perform its due diligence in accordance with each unique contract by providing clearly-written scopes of work, minimum qualifications, and contract terms and conditions, as well as ensuring thorough supplier vetting and onboarding.

(Cont'd)

As noted in Information Technology (IT) Procurement Series — No. 2, procurement professionals function as liaisons to other departments and must understand the concepts, unique attributes, and language of IT. Terms with which public procurement professionals should be familiar include:

- Cyber risk
- Cyber liability
- Cyber liability insurance, cyber risk insurance, cyber breach insurance
- Technology Professional Liability
- Data breach
- Security incident
- Control system
- Privacy
- Phishing
- Ransomware
- Blockchain

Element 2: Policies to address identified cybersecurity risk

Procurement professionals must work with IT to ensure appropriate cybersecurity policies are established for procurement operations and functions. These policies provide the authority for daily due diligence and training.

Procurement expertise and collaboration with IT is essential. Policies should be regularly updated and consistent with the entity's cybersecurity plan. Additionally, rigorous training in cybersecurity best practices should be regular and mandatory.

Policies should address:

- Roles and responsibilities
  - Accountability and reporting
  - Redundancy
  - Points-of-contact for cybersecurity incidents
- Compliance with state or federal requirements for privacy and security, such as:
  - Health Insurance Portability and Accountability Act (HIPAA)
  - Family Educational Rights and Privacy Act (FERPA)
  - 2 CFR § 200.79 - Personally Identifiable Information (PII)
    - Limited and monitored access
    - Encryption
- Solicitation and contract development
  - Clear, specific language
  - Unique to procurement
- Hardware and software
  - System monitoring
  - Penetration testing
  - Updates and maintenance
  - Replacement

CYBERSECURITY FOR PROCUREMENT

(Cont'd)

- Supplier management, i.e., vetting, onboarding, and monitoring
  - Compliance and training practices
  - Performance standards and certifications
  - Debarments, suspensions, or corporate convictions
  - Cybersecurity insurance
  - Alternate/backup contractors

Standards are essential in developing solicitations that produce relevant responses without burdening proposers and evaluators. Independently audited certifications can provide assurance that suppliers meet general industry standards, but each solicitation should include minimum requirements specific to the services the entity intends to contract. An entity may decide to develop its own evaluation tool or utilize standards created and maintained by global experts. Examples of widely known, reputable cybersecurity standards include:

- **ISO 27001:** A certification covering an ISMS (Information Security Management System) framework, including a requirement for detailed documentation of IT policies and procedures; Compliance with ISO 27001 indicates a strong foundation and implementation of information security principles.
- **ISAE 3000 / SOC 2:** An independent, in-depth audit resulting in a report on the effectiveness of the actual operations managing specific risks; ISO 27001 and ISAE 3000 are complementary.
- **FISMA and FedRAMP:** Security controls and risk assessment for contracts involving U.S. federal agencies.
- **NIST SP 800-53:** Security controls and test cases for federal information systems; NIST SP 800-53 serves as the basis for FISMA and FedRAMP.
- **CMMC:** The Department of Defense's verification mechanism for cybersecurity controls.
- **GDPR (EU):** The General Data Protection Regulation Law concerning the protection of personal data.

Increasingly, entities are hiring independent auditors, e.g., universities, consulting firms to assess cybersecurity surrounding systems and processes. Similarly, insurance companies are increasingly requiring suppliers to verify and maintain certifications pertaining to cybersecurity. As with evaluating quality or delivery performance, if a supplier fails to meet or maintain minimum requirements, Procurement should be empowered to end the relationship.

Element 3: Cybersecurity plan

The entity should develop and maintain a cybersecurity plan alongside business continuity and disaster recovery plans. IT holds primary responsibility for the entity's cybersecurity posture, but all departments must coordinate to ensure that their roles, policies, and practices are aligned with the entity's cybersecurity plan. For example, procurement-specific content should incorporate the types and levels of risk defined with IT as well as policies and best practices for preventing, mitigating, and responding to cyber risk in the procurement cycle and supply chain.

CYBERSECURITY FOR PROCUREMENT

(Cont'd)

In general, a cybersecurity plan should:

- Be regularly updated.
- Be readily available as a single comprehensive document with department-specific subsections, as needed.
- Use consistent language, e.g., terminology adopted from NIST to facilitate effective communication and coordination.
- Establish the entity's incident reporting hierarchy, e.g., points of contact, emergency responders, incident response team, backups, based on authority and expertise.
- Detail protocols for reporting, escalation, and response.
- Contain checklists with actionable steps based on the nature of an incident.
- Provide a framework for continuous improvement, e.g., benchmarking, compliance monitoring, incident and response analysis, training.

> *The Federal Communications Commission's (FCC) "Cyber Security Planning Guide" is one of many resources available for developing a cybersecurity plan. For more information, visit https://transition.fcc.gov/cyber/cyberplanner.pdf*

Resources

- "Christchurch Call | to Eliminate Terrorist and Violent Extremist Content Online." Accessed January 24, 2020. https://www.christchurchcall.com/.
- "Cybersecurity & Supply Chain Risk Management | FAI.gov." Accessed January 24, 2020. https://www.fai.gov/topics/cybersecurity-supply-chain-risk-management.
- "Cybersecurity." CSRC.NIST.gov. Accessed February 12, 2020. https://csrc.nist.gov/glossary/term/cybersecurity
- "Cybersecurity – What Does It Mean For Procurement In 2019? - Blog | Procurious." Accessed January 24, 2020. https://www.procurious.com/procurement-news/cybersecurity-what-does-it-mean-for-procurement-in-2019.
- Editor, CSRC Content. "Home | CSRC." Accessed January 24, 2020. https://csrc.nist.gov/.
- "Enterprise Security Policies and Standards." Accessed January 24, 2020. https://www.its.ms.gov/Services/Pages/ENTERPRISE-SECURITY-POLICY.aspx.
- Financial Services Sector Coordinating Council. "Purchaser's Guide to Cyber Insurance Products," 2016. https://fsscc.org/files/galleries/FSSCC_Cyber_Insurance_Purchasers_Guide_FINAL-TLP_White.pdf.
- Foxman, Stephen. "Sample Contract Clauses." Eckert Seamans, n.d. https://www.eckertseamans.com/app/uploads/Steve-Foxman_Eckert-Seamans_DATA-PROTECTION-CLAUSES-101016-M1566466xA35AF.pdf.
- "How Good Is Your Cyberincident-Response Plan? | McKinsey." Accessed January 28, 2020. https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/how-good-is-your-cyberincident-response-plan.
- "Information Technology Series No. 2 - IT Procurement," n.d. https://www.nigp.org/docs/default-source/new-site/global-best-practices/it-procurement-software.pdf?sfvrsn=8a56917a_0.
- "Information Technology Series No. 3 Hardware," n.d. https://www.nigp.org/docs/default-source/new-site/global-best-practices/it-procurement-series-3-hardware-final-2.pdf?sfvrsn=9a56917a_0.

CYBERSECURITY FOR PROCUREMENT

(Cont'd)

- "Information Technology Series No. 4 Services," n.d. https://www.nigp.org/docs/default-source/new-site/global-best-practices/it-procurement-series-no-4---services-non-professional-support-and-maintenance-cloud.pdf?sfvrsn=f3911b76_0.
- JMark Business Solutions, Inc. "Your Cybersecurity Checklist," n.d. https://www.jmark.com/wp-content/uploads/2018/10/Cybersecurity-Checklist.pdf.
- "Mississippi Enterprise Security Program Provides Framework for Agency Partnerships." Accessed January 24, 2020. https://www.govtech.com/security/Mississippi-Enterprise-Security-Program-Provides-Framework-for-Agency-Partnerships.html.
- "National Cybersecurity Awareness Month Resources | CISA." Accessed January 24, 2020. https://www.cisa.gov/publication/national-cyber-security-awareness-month-resources.
- NASPO.org. "Cyber Liability Insurance 101." Accessed January 24, 2020. https://www.naspo.org/Publications/ArtMID/8806/ArticleID/3403.
- National Institute of Standards and Technology. Accessed February 24, 2020. https://www.nist.gov.
- NIGP: The Institute for Public Procurement. "Information Technology Series No. 1," n.d. https://www.nigp.org/docs/default-source/new-site/global-best-practices/it-procurement-practice---series-1.pdf?sfvrsn=7132917a_0.
- "Pennsylvania Specialists Share Cybersecurity Tips." Accessed January 24, 2020. https://www.govtech.com/security/Pennsylvania-Specialists-Share-Cybersecurity-Tips.html.
- Rogers, Zac, and Thomas Y. Choi. "Purchasing Managers Have a Lead Role to Play in Cyber Defense." *Harvard Business Review*, July 10, 2018. https://hbr.org/2018/07/purchasing-managers-have-a-lead-role-to-play-in-cyber-defense.
- "Texas Towns Slammed in 'Coordinated' Ransomware Attack." Accessed January 24, 2020. https://www.govtech.com/security/Texas-Towns-Slammed-in-Coordinated-Ransomware-Attack.html.

Resources for Standards

- 2020. *NVLpubs.NIST.gov.* https://nvlpubs.nist.gov/NISTpubs/SpecialPublications/NIST.SP.800-53r4.pdf.
- "DOD To Require Cybersecurity Certification In Some Contract Bids". 2020. *U.S. DEPARTMENT OF DEFENSE.* https://www.defense.gov/Explore/News/Article/Article/2071434/dod-to-require-cybersecurity-certification-in-some-contract-bids/.
- "EUR-Lex - 32016R0679 - EN - EUR-Lex". 2020. *EUR-Lex.EUROPA.eu.* https://eur-lex.europa.eu/eli/reg/2016/679/oj.
- "Federal Information Security Modernization Act | CISA". 2020. *CISA.gov.* https://www.cisa.gov/federal-information-security-modernization-act.
- "FedRAMP.gov | FedRAMP.gov". 2020. *FedRAMP.gov.* https://www.fedramp.gov/.
- "Home | ISAE 3000". 2020. *ISAE3000.com.* http://www.isae3000.com/.
- "ISO/IEC 27001:2013". 2020. *ISO.* https://www.iso.org/standard/54534.html.