State Cybersecurity Requirements & Considerations for IT Procurement

Patti Bowers

Chief Procurement Officer

October 11, 2019

Own IT. Secure IT. Protect IT

Procurement and Cyber Security – New Best Friends?

- Cyber security has never been more in the public eye, which means it’s more important than ever for businesses and governments to be prepared.
- The cost of such breaches is also on the rise.
- For procurement professionals, this may mean the role as trusted advisor is extended further.
- Procurement is uniquely placed to ensure a solid line of defense is in place.
- It may be that online security is no longer something procurement professionals should rely on someone else to take care of.
- To be a leader in procurement, the job description may need a wider scope – trusted advisor, financial guru, and now security guard.

Spend Matters - post by Lucy Ashdown, head of network compliance for Tungsten Network, leading global eInvoicing, financing and analytics expert.

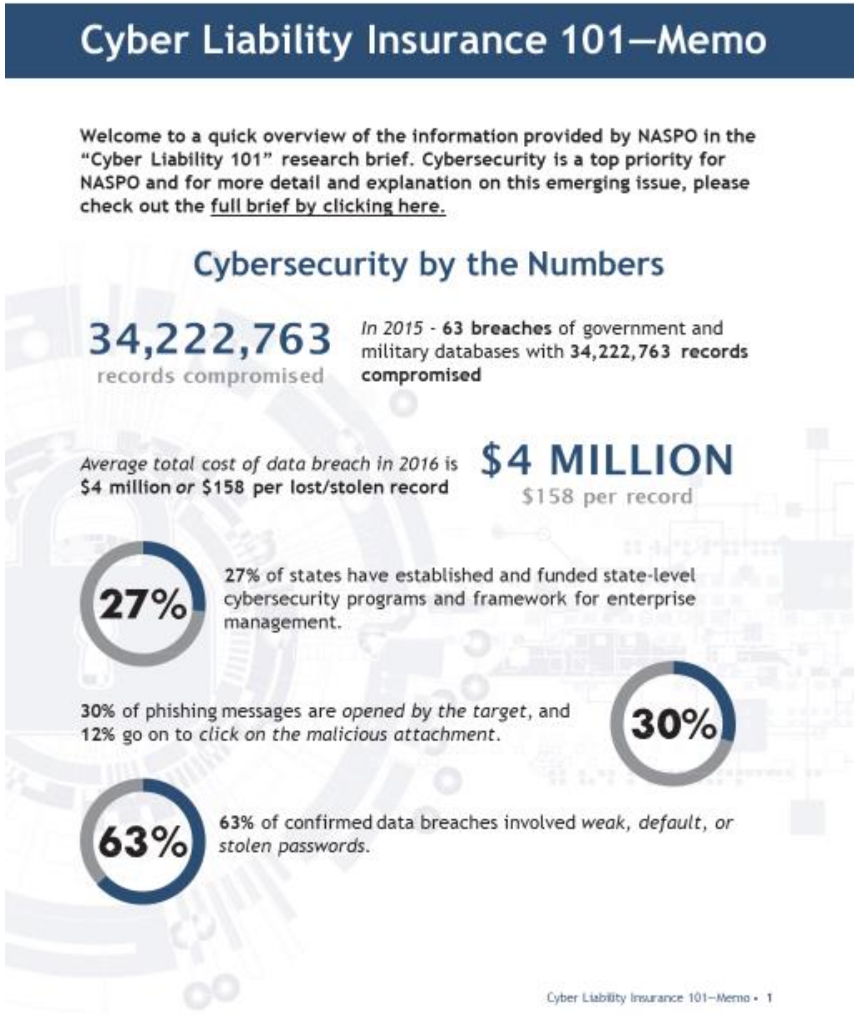
Own IT. Secure IT. Protect IT

Cyber Security: What Procurement Professionals Need to Know in 2019

- The 2014 attack on Target caused an estimated $162 million in damages. This was due to a small HVAC company, Fazio. Hackers broke through Fazio’s firewall and stole Fazio’s credentials to break into Target’s system.
- [24]7.ai, a vendor that provides customer support to clients via online chats, was breached affecting customers of Sears, Delta, and Best Buy.
- In 2015 about 1,025 Wendy’s locations were hit by a credit card breach. Wendy’s placed blame on an unnamed third-party that serves Wendy’s locations.
- The major credit bureau, Experian, suffered a major data breach in 2015. The hackers got access to the personal information of 15 million people who recently signed up for T-Mobile's service.

Own IT. Secure IT. Protect IT

NASPO Research Brief: Cyber Liability Insurance 101



Cyber Liability Insurance 101—Memo

Welcome to a quick overview of the information provided by NASPO in the "Cyber Liability 101" research brief. Cybersecurity is a top priority for NASPO and for more detail and explanation on this emerging issue, please check out the full brief by clicking here.

Cybersecurity by the Numbers

34,222,763 records compromised

In 2015 - **63 breaches** of government and military databases with **34,222,763 records compromised**

Average total cost of data breach in 2016 is **$4 million** *or* **$158 per lost/stolen record**

$4 MILLION $158 per record

27% — 27% of states have established and funded state-level cybersecurity programs and framework for enterprise management.

30% of phishing messages are *opened by the target*, and 12% go on to *click on the malicious attachment*. — **30%**

63% — 63% of confirmed data breaches involved *weak, default, or stolen passwords*.

Cyber Liability Insurance 101—Memo • 1

Own IT. Secure IT. Protect IT

Common Cyber Liability Coverage Components

- **Data Breach and Privacy Crisis Management** – Includes expenses for general management of an incident, specifically; the investigation, remediation, data subject notification, call management, and credit checking and monitoring.
- **Breach Response Coverage** – Can provide legal consultation with breach response experts, forensic investigation expenses, data restoration or replacement expenses, public relations consultant expenses; and can also include expenses involved with notifying affected parties and offering credit monitoring and repair.
- **Business Interruption Coverage** – Provides coverage for the business loss experienced during and immediately following a data breach.
- **Fiduciary Liability Coverage** – Protects in the event of a data breach that requires prompt notice of the breach, and/or comes with strict penalties if there is a violation of law involved. This policy may also include coverage for notice expenses but may not cover credit monitoring and/ or full forensic investigations.

Own IT. Secure IT. Protect IT

Common Cyber Liability Coverage Components

- **Cyber Extortion/ Ransomware Coverage** – Hackers can attempt to extort money by threatening to release the information they have obtained through a successful data breach. They can also threaten to hold a network hostage. This coverage will allow funds to pay for the money required to pay the ransom/extortion demand, the costs of a consultant or expert to help negotiate with the hackers, and/or the costs of an expert to help block the attempted intrusion and reinforce the security.
- **Media Liability Coverage** - Provides coverage for defense costs and liability arising out of claims alleging libel, slander, and/or infringement of intellectual property.
- **Professional Liability Coverage** – Provides coverage for defense costs and liability arising out of claims that allege negligence in providing a professional service such as a consultant, advertising agency, technology developer, and/ or service provider.

Own IT. Secure IT. Protect IT

Five Suggestions for Prevention

1) INVEST IN PROPER CYBERSECURITY

- The importance of having the right cybersecurity software, encryption devices, and firewalls cannot be overstated.
- Update software regularly; educate staff about why that is important.

2) EDUCATE STAFF ABOUT PHISHING

- Educate staff with about what phishing messages look like.
- Prevent phishing by using strong email filters, segmenting your networks from one another, and requiring authentication when logging onto the network.

3) EMPHASIZE PASSWORD AND AUTHENTICATION SECURITY

- Choose a strong password and change it every 30 days.
- Limit access to hard and electronic data by staff, vendors, or service providers, based on their job or task requirements and duties.

4) CREATE A "SECURITY AWARENESS CULTURE"

- Empower staff, vendors, and service providers to be on guard for cyber attacks.
- Let staff know that the firewall will not always protect them.
- Create an environment where everyone feels comfortable asking for help or advice before making a questionable move on the network.

5) KNOW THE CYBER BREACH RESPONSE PLAN

- Staff should know to immediately document any breaches they become aware of, noting the date, time, and duration (if known) of the alleged breach.
- Educate everyone on whom to contact in the event of a data breach and establish a method for reporting questionable activity or suspected breaches.
- Conduct training on your state or office's cyber breach response plan with staff at least once a year to emphasize the importance of such measures.
- Work with your state's CIO and CISO to educate everyone on your state's cyber liability policies and incident or breach response plans.

NC DIT

Own IT. Secure IT. Protect IT

What is IT?

NC G.S. 143B, Chapter 15

Distributed information technology assets:

- Hardware, software, and communications equipment not classified as traditional mainframe-based items, including personal computers, local area networks, servers, mobile computers, peripheral equipment, and other related hardware and software items.

Information technology or IT:

- Set of tools, processes, and methodologies, including, but not limited to, coding and programming; data communications, data conversion, and data analysis; architecture; planning; storage and retrieval; systems analysis and design; systems control; mobile applications; and equipment and services employed to collect, process, and present information to support the operation of an organization.
- The term also includes office automation, multimedia, telecommunications, and any personnel and support personnel required for planning and operations.

Own IT. Secure IT. Protect IT

How is IT Managed and Acquired?

The Secretary of the Department of Information Technology is responsible for:

(1) Information technology architecture.

(2) State information technology strategic plan that reflects State and agency business plans and the State information technology architecture.

(3) Information technology funding process to include standardized, transparent rates that reflect market costs for information technology requirements.

(4) Information technology personnel management.

(5) Information technology project management.

(6) Information technology procurement.

(7) Hardware configuration and management.

(8) Software acquisition and management.

(9) Data center operations.

(10)Network operations.

(11)System and data security, including disaster recovery.

Own IT. Secure IT. Protect IT

IT Procurement

- The Statewide IT Procurement Office establishes processes, specifications, and standards for IT products and services that are purchased, licensed, or leased by state agencies and educational entities.
- Develops and manages statewide contracts that can be used by all State agencies and governmental entities and approves contracts applicable to individual business needs of the State.
- Provides training to government procurement professionals on IT procurement laws and best practices to help them perform their job duties in keeping with all related rules, policies and procedures.

Own IT. Secure IT. Protect IT

Exceptions

- In cases where current or future information technology operations cannot achieve compliance with established information technology laws, policies, standards, or practices, an exception must be documented, submitted, and receive prior approval pursuant to NCGS § 143B-1320(c)-(d).
- These guiding authorities include, but are not limited to, North Carolina General Statutes, Session Laws, Executive Orders, North Carolina Administrative Code, the Statewide Information Security Manual, North Carolina Procurement Manual, Statewide IT Term Contracts, and standards set through authority granted to the SCIO.
- Form A – Procurement
- Form B – Standards
- Form C – Security
- Form D – Exception Information

Own IT. Secure IT. Protect IT

IT Procurement Forms and Templates

09 NCAC 06A .0101 - FORMS, TERMS AND CONDITIONS

In these Rules the State Chief Information Officer (State CIO) shall prescribe forms, terms and conditions and advertisement requirements for acquiring goods and services related to information technology (IT) for use by purchasing agencies. The forms, terms and conditions, and advertisement requirements shall be established taking into consideration market volatility, trends and conditions, legal requirements, and any other factors determined to be in the State's best interest. These shall be made available to all agencies via the State's designated IT procurement website.

Own IT. Secure IT. Protect IT

IT Procurement Forms and Templates

- Invitation for Bids (IFB)/Request for Quote (RFQ) Form for IT Goods and Services
- Invitation for Bids (IFB)/Request for Quote (RFQ) Form for Software and Software support
- Invitation for Bid (IFB)/Request for Quote (RFQ) Form for Software Maintenance (for existing software)
- Instructions and Optional Terms for the RFP
- Non-Disclosure Form
- Online Services Terms and Conditions
- Request for Proposal (RFP) Form
- Request for Proposal (RFP) Online Services Form
- Software as a Service (SaaS) Terms and Conditions
- Clarification of Confidential Information Form
- Best and Final Offer (BAFO) Template
- Award Recommendation Letter Template
- Statewide IT Procurement Checklist for Agencies
- Request for Information (RFI)

Own IT. Secure IT. Protect IT

Privacy Threshold Analysis

The Privacy Threshold Analysis (PTA) is a required document that serves as the official determination by the Enterprise Security and Risk Management Office (ESRMO) as to whether a State program or system has privacy implications, and if additional privacy compliance documentation is required. The PTA is built into the ESRMO processes for technology investments and security. PTAs expire and must be reviewed and re-certified every year or when a change to the environment and security posture occurs.

Own IT. Secure IT. Protect IT

Privacy Threshold Analysis

The PTA:

- Identifies programs and systems that are privacy-sensitive, i.e. Restricted or Highly Restricted data per N.C.G.S. § 132.1-6(c)
- Demonstrates the inclusion of privacy considerations during the review of a program or system
- Provides a record of the program or system and its privacy requirements to the ESRMO
- Demonstrates compliance with privacy laws and regulations

Own IT. Secure IT. Protect IT

Privacy Threshold Analysis

Generally, a PTA is required before a program or system containing Restricted or Highly Restricted data becomes operational. N.C.G.S. § 132-1.10 establishes the following reasons for conducting a privacy analysis:

- Government should collect the information only for legitimate purposes or when required by law
- Social security numbers collected by an agency must be relevant to the purpose for which collected and shall not be collected until and unless the need for social security numbers has been clearly documented.
- Restrict the use of social security numbers for any purpose other than the purpose stated

Own IT. Secure IT. Protect IT

Data Glossary

Health Insurance Portability and Accountability Act **(HIPAA)**

- Medical and substance abuse

Personally Identifiable Information **(PII)**

Public (Non-Sensitive):

- Address information, such as street address or email address
- Mail lists

Non-Public (Sensitive):

- SSN
- Driver's License or State Identification Number
- Passport Number
- Alien Registration Number
- Financial Account Number
- Medical Information
- Mother maiden name
- Biometric data

Own IT. Secure IT. Protect IT

Data Glossary

Payment Card Industry (PCI)

- Primary Account Number (PAN)
- Cardholder Name
- Expiration Date
- Service Code
- Full track data (magnetic-stripe data or equivalent on an chip)
- CAV2/CVC2/CVV2/CID
- PINs/PIN blocks
- Personal characteristics, including photographic image (especially of face or other identifying characteristic), fingerprints, handwriting, or other biometric data (e.g., retina scan, voice signature, facial geometry)

Own IT. Secure IT. Protect IT

Data Glossary

Criminal Justice Information **(CJI)**

- Biometric Data—data derived from one or more intrinsic physical or behavioral traits of humans typically for the purpose of uniquely identifying individuals from within a population. Used to identify individuals, to include: fingerprints, palm prints, iris scans, and facial recognition data.
- Identity History Data—textual data that corresponds with an individual’s biometric data, providing a history of criminal and/or civil events for the identified individual.
- Biographic Data—information about individuals associated with a unique case, and not necessarily connected to identity data. Biographic data does not provide a history of an individual, only information related to a unique case.
- Property Data—information about vehicles and property associated with crime when accompanied by any personally identifiable information (PII).
- Case/Incident History—information about the history of criminal inc

Own IT. Secure IT. Protect IT

Data Glossary

Federal Tax Information **(FTI)**

- Information, including the return, that IRS obtained from any source or developed through any means that relates to the potential liability of any person under the IRC for any tax, penalty, interest, fine, forfeiture, or other imposition or offense
- Information extracted from a return, including names of dependents or the location of business
- The taxpayer’s name, address, and identification number
- Information collected by the IRS about any person’s tax affairs, even if identifiers, such as name, address, and identification number are deleted
- Status of whether a return was filed, under examination, or subject to other investigation or processing, including collection activities
- Information contained on transcripts of accounts

Own IT. Secure IT. Protect IT

Data Glossary

Family Educational Rights and Privacy Act (FERPA)

- Directory information such as a:
    - Student's name
    - Student address
    - Student telephone number
    - Date and place of birth
    - Honors and awards
    - Dates of attendance

Own IT. Secure IT. Protect IT

Data Glossary

Other Categories of sensitive data types:

- These are data types that have been defined by State law as not publicly releasable without first being redacted:
  - Security assessment reports
  - Network/System vulnerabilities

Own IT. Secure IT. Protect IT

Security Specifications in Solicitation Documents

SECURITY SPECIFICATIONS

SOLUTIONS HOSTED ON STATE INFRASTRUCTURE:
Vendors shall provide a completed VRAR - Vendor Readiness Assessment Report State Hosted Solutions at offer submission. This report is located at the following website: https://it.nc.gov/documents/vendor-readiness-assessment-report-vrar..
The *[Insert name of procurement project here]* will be required to receive and securely manage data that is classified as *[list data classification category here from the Statewide data classification and handling policy]*. Refer to the North Carolina Statewide Data Classification and Handling policy for more information regarding this data classification. The policy is located at the following website: https://it.nc.gov/document/statewide-data-classification-and-handling-policy.
To comply with policy, State agencies are required to perform annual security/risk assessments on their information systems using NIST 800-53 controls.

Own IT. Secure IT. Protect IT

Security Specifications in Solicitation Documents

SECURITY SPECIFICATIONS

SOLUTIONS NOT HOSTED ON STATE INFRASTRUCTURE:
Vendors shall provide a completed VRAR - Vendor Readiness Assessment Report Not State Hosted Solutions at offer submission, which includes cloud. This report is located at the following website: https://it.nc.gov/documents/vendor-readiness-assessment-report-vrar.
The *[Insert name of procurement project here]* will be required to receive and securely manage data that is classified as *[list data classification category here from the Statewide data classification and handling policy]*. Refer to the North Carolina Statewide Data Classification and Handling policy for more information regarding this data classification. The policy is located at the following website: https://it.nc.gov/document/statewide-data-classification-and-handling-policy.
To comply with policy, State agencies are required to perform annual security/risk assessments on their information systems using NIST 800-53 controls. This requirement additionally applies to all vendor provided, agency managed Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) solutions. Assessment reports such as the Federal Risk and Authorization Management Program (FedRAMP) certification, SOC 2 Type 2, or ISO 27001 are required for any cloud service providing support for data classified as Restricted or Highly Restricted. A current assessment report will be required prior to contract award for the selected vendor

Own IT. Secure IT. Protect IT

Security Specifications in Solicitation Documents

SECURITY SPECIFICATIONS

ADDITIONAL SECURITY SPECIFICATIONS
Add other security specifications for the RFP here. This can include additional federal specifications that are not covered by the information in section 1. Some examples of additional federal specifications are, but not limited to, PCI assessments, IRS1075 audits, HIPAA BAA, and 42 CFR Part 2 specs.

Use the form's hierarchical outline numbering scheme to order the specifications. Avoid using "must", "shall" or "should" statements in this section. Instead, prompt the Vendor to describe their proposed solution to each specification, as appropriate.).

Own IT. Secure IT. Protect IT

Definitions

Infrastructure-as-a-Service (IaaS) – A model of service delivery whereby the basic computing infrastructure of servers, software, and network equipment is provided as an on-demand service upon which a platform to develop and execute applications can be established. Security provisions beyond the basic infrastructure are carried out mainly by the State agency.

Platform-as-a-Service (PaaS) – A model of service delivery where the computing platform is provided as an on-demand service upon which applications can be developed and deployed. Its main purpose is to reduce the cost and complexity of buying, housing, and managing the underlying hardware and software components of the platform, including any needed program and database development tools. Security provisions are split between the provider and the State Agency.

Own IT. Secure IT. Protect IT

Definitions

Software-as-a-Service (SaaS) – A model of service delivery where one or more applications and the computational resources to run them are provided for use on demand as a turnkey service. Its main purpose is to reduce the total cost of hardware and software development, maintenance, and operations. Security provisions are carried out mainly by the provider. In some occasion, there may be different providers, i.e. one provides SaaS, while another provides Infrastructure as a Service. Contracts must include clearly defined roles and responsibilities for security and incident responses.

Own IT. Secure IT. Protect IT

Definitions

Federal Risk and Authorization Management Program (FedRAMP) – A government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

NIST 800-53 - Defines the standards and guidelines for federal agencies to architect and manage their information security systems. It was established to provide guidance for the protection of agency's and citizen's private data.

SOC 2 Type II – The Service Organization Control (SOC) 2 Type II examination demonstrates that an independent accounting and auditing firm has reviewed and examined an organization's control objectives and activities and tested those controls to ensure that they are operating effectively.

Own IT. Secure IT. Protect IT

Definitions

ISO 27001 - ISO/IEC 27001:2013 specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in ISO/IEC 27001:2013 are generic and are intended to be applicable to all organizations, regardless of type, size or nature.

PCI Assessment – An audit for validating compliance with the Payment Card Industry Data Security Standard (PCI DSS), a set of security standards for merchants who accept, process, store or transmit credit card information.

IRS 1075 - This publication provides guidance to ensure the policies, practices, controls, and safeguards employed by recipient agencies, agents, or contractors adequately protect the confidentiality of FTI.

Own IT. Secure IT. Protect IT

Definitions

Business Associate Agreement (BAA) – A business associate is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity. According to the HIPAA Privacy Rule, the types of functions or activities that may make a person or entity a business associate include payment or health care operations activities, as well as other functions or activities regulated by the HIPAA Administrative Simplification Rules.

42 CFR Part 2 – applies to all records relating to the identity, diagnosis, prognosis, or treatment of any patient in a substance abuse program that is conducted, regulated, or directly or indirectly assisted by any department or agency of the United States.

Own IT. Secure IT. Protect IT

NASPO – Data Privacy and Security: Where are we in 2019

Social security numbers, driver’s licenses, tax information, birth certificates, death and criminal records, financial information, family status information and voting records, are among the personal citizen data state governments are entrusted with every day.

State government agencies need to pay close attention when reviewing contracting terms of services for cloud solutions specifically the data-use and data-sharing terms, and anything related to privacy issues to better protect citizens’ personal information. At a minimum, government contracts with cloud service providers should include provisions to guarantee that the technology provider: protects personal information from unauthorized access or disclosure; protects data confidentiality; and prevents data breaches. Private companies alike ought to take responsibility for protecting our data and increase transparency about how they are using this information and whom they are sharing it with. Moreover, we cannot talk about data privacy efforts without recognizing the need for a stronger data security culture.

Own IT. Secure IT. Protect IT

Follow the Data!

Let’s Connect!

@NCDIT
@BroadbandIO
@ncicenter

NCDIT

@NCDIT

NC Department
of Information
Technology

NC DIT

it.nc.gov