Cyber Security - Using our industry standards and BPs

Robert Brown, Cyber Security Officer, INdigital

Steps towards ensuring .....

C. I. A.

Confidentiality

“Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…”

A loss of confidentiality is the unauthorized disclosure of information.

Steps towards ensuring .....

C. I. A.

Confidentiality

Integrity

“Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…”

A loss of integrity is the unauthorized modification or destruction of information.

Steps towards ensuring .....

C. I. A.

Confidentiality

Integrity

Availability

“Ensuring timely and reliable access to and use of information…”

A loss of availability is the disruption of access to or use of information or an information system.

Steps towards ensuring .....

C. I. A.

Confidentiality

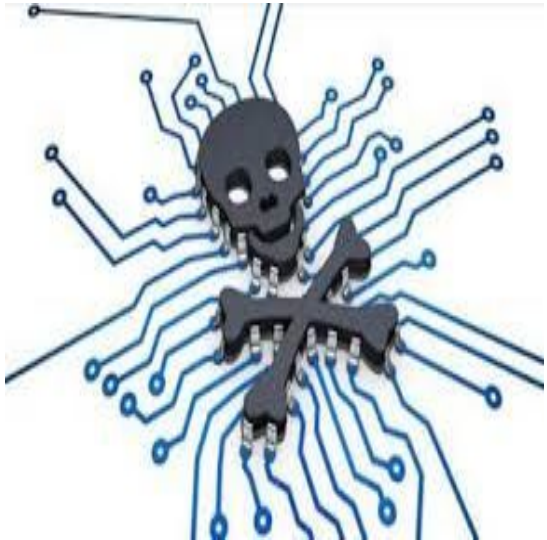
Integrity

Availability

As an organization you do your due diligence for all 3. As a 911 service provider, we will prioritize according to our governance requirements and the systems or data we are working with.

Cyber Security to the Forefront

- Cyber Security is and has always been good and essential business practice - E911 and now NG911
- Industry standards, best practices and organizations
    - NENA, NIST, APCO, ISO, COBIT
    - FCC, National 911 Program Office, CISA, DHS
    - Always evolving and improving with ongoing committee



Industry Standards & Best Practices

- NENA 75-001 Security for Next Generation 9-1-1 Standard (will eventually become NENA-STA-040.2)
- NENA 75-502 Next Generation 9-1-1 Security Audit Checklist Information Document
- NIST 800-39 Managing Information Security Risk
- NIST 800-60 Guide for Mapping Types of Information and Information Systems to Security Categories
- NIST 800-53 Rev.4 Security and Privacy Controls for Federal Information Systems and Organizations (Rev.5 available now for public comment)
- NIST Frameworks CSF (Cybersecurity Framework) and RMF (Risk Management Framework)

NIST RMF vs. CSF

NIST RMF vs. CSF

- Other frameworks include International Organization of Standardization (ISO) and Control Objectives for Information and Related Technologies (COBIT)
- NIST RMF and CSF they do not have to be in opposition as they can complement each other
- RMF is the more complicated, requires authorization
- Which you choose depends on your environment and best fit, for example the RMF is required by Federal Agencies
- CSF is more commonly used

Building from our industry's standards, guidelines, and practices….

Frameworks provide a common taxonomy and mechanism for organizations to:

1) Describe their current cybersecurity posture;
2) Describe their target state for cybersecurity;
3) Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process;
4) Assess progress toward the target state;
5) Communicate among internal and external stakeholders about cybersecurity risk.

….. ALL Steps towards developing your Cybersecurity Program

NIST CORE FRAMEWORK

IDENTIFY

Develop an organizational understanding to manage cybersecurity risk to: systems, assets, data, and capabilities.

NIST CORE FRAMEWORK

PROTECT

Develop and implement the appropriate safeguards to ensure delivery of services.

NIST CORE FRAMEWORK

DETECT

Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.

NIST CORE FRAMEWORK

RESPOND

Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.

NIST CORE FRAMEWORK

RECOVER

Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cyber-security event.

NIST Framework Core

Functions	Categories	Subcategories	Informative References
IDENTIFY			
PROTECT			
DETECT			
RESPOND			
RECOVER			

Identify

Identify Governance - Laws, regulations, industry standards, organizational SOP, mission and vision statements, etc.
Identify Systems - hardware and software inventories, services, networks, points of interconnect, system owners, dependencies, function served, end users, inputs, outputs, version number, patch level, physical location, etc.
Identify Data - data owners, dependencies, origination, transit, at rest, where does it reside, function served, end users, etc.
Identify Current State - stakeholders, awareness, risk levels, security controls, plans (Disaster Recovery, COOP, IRP, Communications, etc.)

Questions to ask your team?

- Do we have an inventory?
- Do we have security controls such as endpoint protection, firewalls, etc.?
- What controls do we have in place for physical security/ protection?
- Do we have plans such as - DR, COOP, IRP, etc.? Have those plans been updated and communicated? Have the plans been exercised/tested?
- Have we identified and classified risks?
- Have we classified our data and systems according to CIA or by another risk assessment?
- Have we done a vulnerability assessment?
- Do we have a monitoring solution?
- Do we conduct cyber awareness training and phish testing?
- What do we have in place for policy and procedure supporting our cyber security posture?

Resources

https://csrc.nist.gov/

https://www.nist.gov/itl/applied-cybersecurity/nice (NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION)

https://www.cisa.gov/

https://www.nena.org/page/NG911_Security

https://www.nena.org/page/NGSecurityChecklist

https://www.apcointl.org/ext/pages/APCOng911Guide/APCO_NG911_Report_Final.pdf - (Chapter 7)

https://www.911.gov/docs-and-tools/?category=cybersecurity&sort=date

INdigital SM

Robert Brown
rbrown@indigital.net

Thank you...
Questions?

Classify or Categorize Systems and Data

You will take the previously identified systems/data and categorize them based on the potential risk.

Results -

public information = {(confidentiality, n/a), (integrity, moderate), (availability, low)}

Potential Impact	Security Objective		
	C	I	A
Low			
Medium			
High			
N/A			

INdigital TDOS IVR Mitigation Strategy