EIGHTH ANNUAL LEADERSHIP EVENT

CS SUMMIT

Security solutions through collaboration.

Industry Standard Frameworks

Amos Aesoph, CSO, Xigent Solutions

Goals

- Understand what a cybersecurity framework is
- Understand what goes into choosing the right framework for your environment
- Gain a familiarity with a few of the most common frameworks in use

10 Biggest Breaches of 2018 (so far)

- Saks, Lord & Taylor – 5 million records, hacking
- PumpUp – 6 million records, unsecured data
- Sacramento Bee – 19.5 million records, hacking
- Ticketfly – 27 million records, hacking
- Panera – 37 million records, unsecured data, negligence
- Facebook – 87 million records (maybe more?), unsecured data
- MyHeritage – 92 million records, unsecured data
- UnderArmour – 150 million records, unauthorized access
- Exactis – 340 million records, unsecured data
- Aadhaar – 1.1 billion records, hacking

https://blog.barkly.com/biggest-data-breaches-2018-so-far

Three Things to Know

1. What is a cybersecurity framework?
2. How do I choose the right framework for me?
3. What are some of the most common choices?

What is a Cybersecurity Framework?

- Documented processes that are used to define the policy set
- A “blueprint” for building a cybersecurity program
- Manage risk and reduce vulnerabilities
- A good framework will cover:
  - Identify
  - Protect
  - Detect
  - Respond
  - Recover

How Do I Choose the Right Framework?

- Keep your goal in mind: protection of information and valuable assets from threats
- Complete a thorough risk assessment
  - Administrative
  - Technical
  - Physical
- Does your industry require or otherwise encourage a particular framework?
- Would a hybrid approach work best for your organization?

What are some of the most common?

- NIST SP 800-53
- COBIT
- ISO 27001
- PCI-DSS
- HIPAA

National Institute of Standards and Technology Special Publication 800-53 (5th Revision in Dec 2018)

- Catalog of security controls for all US federal information systems
- Includes areas: Access control, BC/DR, Incident Response, many others
- May be applied to all organizations

National Institute of Standards and Technology Special Publication 800-53 (5th Revision in Dec 2018)

NIST Special Publication 800-53 (Rev. 4)

Security Controls and Assessment Procedures for Federal Information Systems and Organizations

RISK ASSESSMENT Control Family

Showing **6** controls:

No.	Control	Priority	Low	Moderate	High
RA-1	RISK ASSESSMENT POLICY AND PROCEDURES	P1	RA-1	RA-1	RA-1
RA-2	SECURITY CATEGORIZATION	P1	RA-2	RA-2	RA-2
RA-3	RISK ASSESSMENT	P1	RA-3	RA-3	RA-3
RA-4	RISK ASSESSMENT UPDATE				
RA-5	VULNERABILITY SCANNING	P1	RA-5	RA-5 (1) (2) (5)	RA-5 (1) (2) (4) (5)
RA-6	TECHNICAL SURVEILLANCE COUNTERMEASURES SURVEY	P0			

National Institute of Standards and Technology Special Publication 800-53 (5th Revision in Dec 2018)

RA-3 RISK ASSESSMENT

Family: RA - RISK ASSESSMENT

Class:

Priority: P1 - Implement P1 security controls first.

Baseline Allocation:

Low	Moderate	High
RA-3	RA-3	RA-3

National Institute of Standards and Technology Special Publication 800-53 (5th Revision in Dec 2018)

Control Description

The organization:

a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;

b. Documents risk assessment results in [Selection: security plan; risk assessment report; [Assignment: organization-defined document]];

c. Reviews risk assessment results [Assignment: organization-defined frequency];

d. Disseminates risk assessment results to [Assignment: organization-defined personnel or roles]; and

e. Updates the risk assessment [Assignment: organization-defined frequency] or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

National Institute of Standards and Technology Special Publication 800-53 (5th Revision in Dec 2018)

Supplemental Guidance

Clearly defined authorization boundaries are a prerequisite for effective risk assessments. Risk assessments take into account threats, vulnerabilities, likelihood, and impact to organizational operations and assets, individuals, other organizations, and the Nation based on the operation and use of information systems. Risk assessments also take into account risk from external parties (e.g., service providers, contractors operating information systems on behalf of the organization, individuals accessing organizational information systems, outsourcing entities). In accordance with OMB policy and related E-authentication initiatives, authentication of public users accessing federal information systems may also be required to protect nonpublic or privacy-related information. As such, organizational assessments of risk also address public access to federal information systems. Risk assessments (either formal or informal) can be conducted at all three tiers in the risk management hierarchy (i.e., organization level, mission/business process level, or information system level) and at any phase in the system development life cycle. Risk assessments can also be conducted at various steps in the Risk Management Framework, including categorization, security control selection, security control implementation, security control assessment, information system authorization, and security control monitoring. RA-3 is noteworthy in that the control must be partially implemented prior to the implementation of other controls in order to complete the first two steps in the Risk Management Framework. Risk assessments can play an important role in security control selection processes, particularly during the application of tailoring guidance, which includes security control supplementation.

Control Objectives for Information and Related Technology

- Focused on identifying and mitigating risk
- Frequently found in Finance
- Compliance with Sarbanes-Oxley

International Organization for Standardization 27001

- Designed to be very systematic
- provides best practice recommendations on information security management within the context of an overall Information security management system (ISMS)
- similar in design to management systems for quality assurance (the ISO 9000 series), environmental protection (the ISO 14000 series) and other management systems

Payment Card Industry Data Security Standard

- Mandated by VISA, MasterCard, AmEx, etc
- Intended to reduce fraud
- Generally applied to a segment of network or business
- Updates are frequent
- Compliance varies (QSA to SAQ)

Health Insurance Portability and Accountability Act, Title II

- Privacy and Security Rules on Protected Health Information (PHI)
- Administrative, Physical and Technical
- Required specifications – must be implemented
- Addressable specifications – open to evaluation and determination

In Conclusion

- All frameworks overlap
- There is no wrong answer
- “…failed to comply with security standards and allowed its customers’ financial information and other private information to be compromised by cutting corners on security measures that could have prevented or mitigated the security breach that occurred.” – Don’t get to this point!