**Wk 1**

**Cybersecurity Compliance Framework & System Administration**

**What Challenges do Organizations Face?**

* **Security Event: an event on a system or network detected by a security device or application**
* **Security Attack: a security even that has been identified by correlation and analytics tools as malicious activity that is attempting to collect, disrupt, den, degrade or destroy information system resources or the information itself**
* **Security Incident: an attack or security event that has been reviewed by IBM security analysts and deem worthy of deeper investigation**
* **In 2014, there were about 82 million events. Roughly 12k were attacks**
* **45 % of bad guys are outsiders. 55% of bad guys are insiders.**

**Compliance Basics**

* **Security: designed for protection from theft or damage, disruption, or misdirection**
* **Physical controls: for servers in the data centers**
* **Technical Controls: features and functions of the service (e.g. encryption)**
* **Operational Controls: How a server is configured, updated, monitored, and patched. How staff are trained and what activities they perform**
* **Privacy: how information is used, who that information is shared with, or if that information is used to track**
* **Compliance: Tests that security measures are in place. Which and how many depend on the specific compliance. Often will cover additional non-security requirements such as business practices, vendor agreements, organizational controls, etc.**

**Two Categories of Compliance: Foundational and Industry**

**Foundational: General specifications, (not specific to an industry) important, but generally not legally required. Ex: SOC, ISO**

**Industry: specific to an industry or dealing with a specific type of date. Often legal requirements Ex: HIPAA, ICI DSS**

**Overview of US Cybersecurity Law**

* **The Computer Fraud and Abuse Act is a United States cybersecurity bill that was enacted in 1984**
* **Federal Information Security Management Act of 2002 (FISMA), Federal Information Security Modernization Act of 2014 (FISMA 2014)**
* **FISMA assigns specific responsibilities to federal agencies, the National Institute of Standards and Technology (NIST) and the Office of Management and Budget (OMB) in order to strengthen information security systems**

**National Institute of Standards and Technology (NIST)**

**NIST’s cybersecurity and privacy activities strengthen the security of the digital environment. NIST;s sustained outreach efforts support the effective application of standards and best practices enabling the adoption of practical cybersecurity and privacy**

**5 Key General Data Protection Regulation Obligations: Rights of EU Data Subjects, Security of Personal Data, Consent, Accountability of Compliance, Data Protection by Design and by Default**

* **Data Subject: an identified or identifiable living natural person**
* **Controller: determines the purpose and means of processing of personal data**
* **Processor: processes personal data on behalf of the controller**
* **Personal Data: any information relating to a Data Subject**
* **Processing: any operation performed on personal Data (includes storage, access, anywhere in the world)**

**GDPR (General Data Protection Regulation)**

**SOC Reports**

* **Some industry/jurisdictions require SOC2 or local compliance audit**
* **Many organizations who know compliance, know SOC2 Type 2 consider it a stronger statement of operational effectiveness than ISO 27001 (continuous testing)**
* **Many organization’s clients will accept SOC2 in lieu of the right-to-audit**

**SOC1 vs SOC2 vs SOC3**

* **SOC1: Used for situations where the systems are being used for financial reporting. Also referenced as Statement on Standards for Attestation Engagements (SSAE) 18 AT-C 320 (formerly SSAE 16 or AT 801)**
* **SOC2: Addresses a service organization’s controls that are relevant to their operations and compliance, more generally that SOC1. Restricted use report contains substantial detail on the system, security practices, testing methodology and results. Also, SSAE 18 standard, sections AT-C 105 and AT-C 205**
* **SOC3: General use report to provide interested parties with a CPA’s opinion about same controls in SOC2**

**5 Elements Auditors are Looking For**

* **Accuracy: controls results being assessed for pass/fail**
* **Completeness: do controls implementation cover the entire offering: e.g. no gaps in inventory, personnel, etc.**
* **Timeliness: are controls performed on time (or early) with no gaps in coverage. If a control cannot be performed on time, are there appropriate assessment (risk) approvals BEFORE the control is considered “late”**
* **Resilience Notice: are the checks/balances in place such tat if a control does fail, would you and correct? At all? Within a reasonable timeframe?**
* **Consistency: sifting control implementation raises concerns about above, plus increases testing**

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

* **Administrative Safeguards include: Security Management Process, Security Personnel, Information Access Management, Workforce Training and Management, and Evaluation**
* **Technical Safeguards Include: Access Control, Audit Controls, Integrity Controls, Transmission Seurity**
* **Physical Safeguards Include: Facility Access and Control and Workstation and Device Security**

**CIS Center for Internet Security**

**CIS Controls 7.1 has 3 Implementation Groups**

* **Implementation Group 1: an organization with limited resources and cybersecurity expertise available to implement sub-controls**
* **Implementation Group 2: an organization with moderate resources and cybersecurity expertise to implement sub-controls**
* **Implementation Group 3: A mature organization with significant resources and cybersecurity experience to allocate to sub-controls**