**Module 5 Risk Management**

**5.3 Risk Assessments**

**Risk & Threat Definitions (See NIST)**

* Risk
* Threat
* Impact
* Vulnerability
* Exploit
* Risk assessment
* Risk management

**Threat Assessment**

* Threat Agent/Source – intent & method targeted at intentional exploitation of vulnerability/situation & method that may accidentally exploit vulnerability
* Threat Vector – method/path threat uses to access target
* Threat Assessment – structured process used to identify & evaluate various risk/threats that organisation might be exposed to (See threat analysis)

**Threat Assessment Types**

* Environmental – natural events

1. Eg. Weather, storms, flooding, earthquakes, fire etc.

* Manmade – human cause

1. Eg. Flooding, fire, accidents etc.

* Internal vs. External

1. Origin of threat source
2. Is threat agent inside organisation (employee, contractor, consultant) ?

**Risk Assessments**

* AKA risk analysis/calculation
* Analysing threats, vulnerabilities & impacts of loss of information-processing capabilities (system)/loss of information itself
* Process

1. Identify assets
2. Identify associated threats & vulnerabilities
3. Determine likelihood of exploit/compromise
4. Determine impact of exploit/compromise
5. Prioritise risk activities/security controls

**NIST Risk Management Framework**



**Quantitative vs. Qualitative Risk Analysis**

* Qualitative

1. Estimating risk values (likelihood & impact)
2. Normally using scale (1-5)
3. Subjective & less accurate

* Quantitative

1. Using real values to calculate risk equation
2. Numeric
3. Return on Investment (ROI)/return on Security Investment (ROSI)
4. SLE (Single Loss Expectancy) X ARO (Annual Rate of Occurrence) = ALE (Annualised Loss Expectancy)

**Risk Calculation**

* Use formula SLE X ARO = ALE
* ALE (Annual Loss Expectancy) value – monetary measure of how much loss can expect in a year
* SLE (Single Loss Expectancy) value – how much can expect to lose at any 1 time. Divided into 2 components

1. AV (Asset Value) – value of item
2. EF (Exposure Factor) – percentage of loss

* ARO (Annualised Rate of Occurrence) – likelihood, often drawn from historical data of event occurring within a year

**Risk Calculation Example**

* You can reasonably expect every SLE (equal to AV X EF) will be equivalent to $1000 & there will be 7 occurrences a year (ARO), so ALE is $7000
* Conversely, if only 10% chance of event occurring within year time period (ARO=0.1), then ALE drops to $100

**Risk Response/Strategies**

* Avoidance – making decision not to engage in actions associated with risk
* Transfer – sharing burden of risk with another party (insurance)
* Mitigation – taking steps to reduce likelihood/impact of risk
* Acceptance

1. Choosing to live with risk
2. Must be conscious choice by management

**Risk Register**

* Recording information about identified risk
* Can be specialised software program, cloud service or master document (spreadsheet)
* Contains details about risks, risk decisions, mitigating controls, risk owner, time frames, residual risk etc.
* Ensures organisation risk tolerance/appetite aligned

**Supply Chain Assessments**

* AKA 3rd-party assessments
* Review vendor’s security posture
* Any organisation connected to yours virtual/physical
* Often accomplished with checklists

**Change Management**

* Change (IT) – addition/removal/altering of information technology environment
* Change management process goal – allow for change w/o disruption/minimal disruption to systems & services
* Need to reassess security risks with any change

1. Change itself
2. The after-effects

**Testing**

* Part of Risk Analysis Process
* Provides visibility into risk components
* Vulnerability assessments
* Penetration tests
* Table-top exercises