Secure System Development Lifecycle

Scope and Policy: scoping a system (purpose/entities/data/transmitted/main assets) * defining a policy (high-level/system specific)

Threat analysis: Assets * Threat * Attack * Safeguards * Vulnerabilities * Impacts * Risk * Risk Analysis and Management

Requirement Analysis: what safeguards * usually process of refinements

Specification: define how security relevant components and subsystems will operate.

Implementation: Procurement of components or tender

Documentation: Testing * Security Evaluation

Installation: Preliminaries * Roles in Procedures * Contents of Procedures * Dual Control * Auditing Mechanisms

Management And Audit: Security Management * Categories of Security Management (fault/configuration and change/ accounting and auditing/ performance/ security programme)* Purpose of Security Auditing * Roles and Independence * Procedural Aspects

Governance, Risk & Compliance

Governance = processes + structures (implemented by the board, inform, direct, and manage activities of the org towards the achievement of its objective)

Layers of architecture: benefits (common language, define landscape, reduce complexity) * SASBA model (contextual, conceptual, logical, physical, component), each layer gives (assets/what, motivation/why, process/how, people/who, location/where, time/when)

Types of governance: Corporate governance (corp obj set and pursued)* Regulatory governance

Implementing: Structure * Codification * Capability * Data (risk reports, aggregate risk position)

Authorities and Delegations (RACI Charts, roles/teams): Responsible (performs task) * Accountable (final decision) * Consulted (has important context 2 influence decision)* Informed (might be impacted)

Delegation: decisions up 2 a certain size for risk (size could = monetary risk, size of business impact)

Risk (common approach, consistent scopes): Risk Matrices (simplistic) * Risk Management (balance between achieving strategic goals and reducing unacceptable loss vs its cost and operational opportunity)

Policies and Standards: Constraints and freedoms makes governance easier (and ensures consistency) * enable measurement

Policy and the social learning cycle : (Context - prioritisation → policy – broadcast dissemination → localisation [NEEDS THIS 2 BE RELEVANT]- delivery/implementation → new context [UNDERSTANDING/SKILL NEEDED])

Regulatory Governance: Focus on lower risks * Inhibit mitigation actions (incident reporting) * Sets a Maximum standard * Abdication 2 the standard vs risk management
Should regulation be principle based (e.g ensure data is protected) or rules based (e.g encryption)?

Reporting and Metrics
'If you're not measuring it, you're not managing it'

- Compliance status: red/amber/green * misleading and poor prioritisation (attach a narrative instead) * simple (apparently) * misleading risk reporting * behind the risk (instead of ahead of)

- Capability Maturity Models: simple model (ad hoc → managed → defined → measured → optimised) * one dimensional * add progression maturity

- Risk Reporting: red/amber/green likelihood vs impact * risk performance reporting (inherent, residual, target) * vulnerabilities (# of vulns vs lengths of time unpatched)

NOTE: accepted risks should still be reported

Framework and Standards: ISO 27000 * COBIT * NIST * UK NIS-R CAF

Risk Appetite: link org objectives to risks (make concious decisions) * amount of risk org is prepared to accept (loss or disruption to business) * e.g score as categories (averse, guarded, cautious, open, eager)

Identity Management

Processes/tools/social contracts for managing digital identity for secure access.

Attributed Identity = info given at birth * given name, date of birth, place of birth etc

Biographical Identity = reflects individuals history * education/qualifications, where live, employment

Biometric Identity = accuracy depends on type * intrusive * special tech required * better for verification post-enrolment

Digital Identity = you can have multiple * systems can act on behalf of people * might need multiple ids for multiple tasks * must hold a credential used by service provider to authenticate user

To Prove Identity

Validity = enough supporting evidence 2 confirm person with that name exists * access data, examine history, evaluate quality

Verification = applicant data subject of valid Id referenced? * use info only data subject hsould know

Documentary Evidence = paper based * how do you reconstruct visual check (photocopies?) * data is static (can't hold history of data) * logistics of centralised checking process? * easily forged/bought * obtained falsely * docs breed other docs (cross checking redundant – they created each other)

Electronic evidence = opposite. Harder to falsify mutliple, collaborative, long-term data sets.

Registration and Enrolment: sensitive access should have more thorough enrolment process * high assurance w face-to-face w qualified interviewer (doesn't scale well) * over-reliance an resulting system an issue (implies 100% secure which is impossible, y companies use third-parties 4 liability) * insider threats (robust processes can mitigate, or only highly trusted enrollers) * biometric enrolment (secure procedure, binding of biometric template 2 enrollee, check template quality and match-ability)

Privacy: Anonymity (easier for free services but can use anonymous payment systems, communication channels leak data)* Pseudo-anonymity (pseudonyms used, usually short lives, generated regularly)* Unlinkability (unable to associate 2 psyudonyms, difficult in practice since auth process may reveal info)

De-identifiaction = remove/alter enough data in set s.t individual cant be idntified but still useful * remove personal identifiers * de-localisation (GL15 5NB → GL15) * record order sampling * numeric item banded, extremes truncated * dates reduced (27/02/1997 → 1997)

Uses for an identity: Identification * User authentication * identity verification

Remote working: Reduced office space * reduced travel* start-up cost of tech * cost of equipment, home office furnititure etc

VPN: hacker target * consists of 'protected' network and 'outside' network * cyprotgraphic protocols (confidentiality, sender auth, message integrity) * Provide: extended geographic connectivity, increased sec thru encrypted traffic, decreased costs compared 2 leased lines * Security implications: client-side sec, 'inside' network that can be accessed might need 2 be reduced, security logging on corporate LAN might need adjust 2 include VPN * sec policy needs 2 be adjusted * legal obligations on data stored remotely (e.g GDPR)

Single sign on = sign in once per session and forwarded 2 other processes requiring auth * as strong as initial auth * complementary controls (geolocation, ID device) etc * e.g RACE and Kerberos

Business Benefits of IDM: Simple admin reducing costs * increased security w strong auth * greater access for partners, emplyees, customers * single sign on to hosted SP * higher regulatory complaince thru implementation of sec, audit, and access policies

Regulation: Health Insurance and Accountability Act * Sarbanes-Oxley Act * Gramm-Leach Bliley Act (Financial Privacy Rule, Safeguards Rule)

Legistlative
EC Data Protection Directive: harmonise national laws * free flow of PI
UK Data Protection Act 1998: Data Controller ensure data processing (fair and lawful * limited purpose * adequate, relevant, not exessive * accurate * not kept longer than necessary * accccordance with data subjects rights * secure * not transferred 2 counties w/o adequate protection)
GDPR: Data processor as well as data controller * right to erasure * data breach notification * data impact assessment * increased enforcement w max(euro 20m, 4% global turnover), legal ability 2 stop company from processing data
USA: fractured legislation across industry, state law, and federal
Asia-Pacific Economic Cooperation: 9 principles (prevent harm, notice, collection limitation, use of PI, choice, integrity of PI, sec safeguards, access and correction, accountability)

Common Principles: notice prior to collection * collect min necessary * ID purpose and limit 2 that purpose * info secure/accurate/complete up-to-date * data subject allowed 2 view, correct, sometimes delete * deidentify/destroy data no longer needed

Business Focus: Brand risk (dont erode customer trust) * Employee data management (localised and tailored) * Increased regulation (internation incongruence, solutions for data transfer e.g model contracts, relationships w data protection authorities) * customer sensitivity (awareness of rights increasing) * extended enterprise (relationships w partners/distributors etc more complex, orgs w inconsistent policies b clear on liability) * Advances in tech.

Identity Theft (fraud): techniques incl. Bin diving/ eavesdropping/ database breach/ impersonation etc * statistics exaggerated

Deployment Models:
Silo: operated by single user for fixed resource community * big orgs but not usually multinational
Walled Gardens: common user community of collection of businesses * op rules agreed by all participating * visa services visa/issueing banks/ acquiring banks
Federated IdM : distributed * no single entity operates * multiple id providers * distributed and partitioned store 4 ID info* IdPs sign up to code of practice * issues: is federated id same as local, Different cultures = different conventions for info/names , movers and leavers need to be updated in federation * Provide bridge between segregated id silos * advantages: SP might not wanna be IdP, extend employee ids to SP, roles/ credentials/auth policies crossed over 2 SP, single auth mechanisms for Sps, cross-domain single sign on w/o having to homogenize sys of auth approaches * consider policy adherence

ID management components
Data Repository Components: deal w storage and management * provide API * policy storage * e.g LDAP

Security Components: authentication, authorisation, auditing (not CIA) * Authentication provider (generate tokens) * Authorisaiton Provider (access control) * Auditing Provider (tracking, provide analysis)

Lifecycle components: monitor individual data overtime * provisioning (Creation, linkage, changing, decommissioning) * Longevity (historic record of ID for auditing/examintaion/snapshots e.g privilige at certain type, attestation = what resources accessable in what time frame)

Consumable Value Components: user interaction aspects of IdMs * single sign-on * personalisation * self-service (register for apps and manage profile w/o admin)

Management Components: User Management * Access control management * Privacy Management * Federation management

How To Manage:

Global schemes: not feasible * identity = context specific * IDM schemes for specific domains e.g kerberos within companies

User Perspective: password policies * security awareness training

Legacy Problems: if u have 2 double run, double effort

Cultural Differences: e.g Japan doesn't like fingerprinting, facial recognition generally okay

Impacts of bad IDM: Escalated costs (time spent logging in/password resets/ data redundancy) * Inability 2 do job * reduced security * placement of liability * inability 2 change

Open issues: authenticity of identity * longevity of info (track changed over time? Provide evidence 4 historical investigations) * privacy * identity theft * legal structures (what protections for holder of ID or relying party)

Process and Procedural Management

Enrolment and registration: face-to-face or remote * different strength * human error * risk of inconsistency * industries w specific requirements * HR (central auth for registration usually)

Authentication: IdM Database issues (accuracy, scalability, extendability, interoperability, speed of implementation for environment, complexity, who owns the data)

Life Cycle Management: update and removal (respecting user entitlement and regulation reqs like holding onto data for 7 months etc) * manual or automatic (more timely deletion, ensure privilige alterations happen simultaneously) * permeation of privilige/data changes * source of info feed (who has the authority 2 update priv?)

Provisioning = manage info related to authentication and authorisation * Account provisioning * Resource provisioning (business assets) * Account deprovisioning (termiante/reallocate access rights, risk introduced if done wrrong) * Authoriative sources (one source should be primary 2 prevent incorrect info being entered, how does info permeate thru system)

Workflow: controlling data provisioning process * routed thru predetermined path for review/consistency/auidability

Passwork management: single-sign-on or password synchronisation (lower admin costs) * policies * manage change and reset * issues: change req came from claimed identity? Different policies across domains/silos

Delegated Admin: what happens if those with auth are unavailable? * Delegation needs to be auditable

Self-service admin: individuals manage certain aspects of own identity * reduce admin overhead * but what can they manage and what validity checks (starts new workflow for update?)

Matching business and technical: technical deployment (legacy, can we support auth technology e.g do employees have smart phones?) * Architecture/Infrastructure considerations (online/offline, heterogeneous? partner/remote infrastructure?) * Cost (other effected infrastructure need to be changes? Manual vs automatic incl. License fees for third part solutions/cost of creating or purchasing own vs man hours)

Risk Assessment

Nist SP 800-30 REV1 guidelines

3 Tiers: 1 – Organisational (related 2 orgs goals, reason de etre, primary outpit) * 2 – Mission/Business Process Level (assessment for business units = particular service/product) * 3 – Information System Level

Risk assess thru sys dev life cycle (pre-system, acquisition, system acquisition, sustainment) for products/services if offered and org

Assessments limitations: chosen methodologies * subjectivity, quality, trustworthiness of data * interpretation of results (shud be in bus context, result producer should make clear and understandable) * Skills and expertise of assessment conductors

Triangle: Framing risk (desc. env in which risk-based decisions are made) * Assessing risk * Responding to risk * Monitoring risk

Risk assessments identify: Relevant threats to org * Vulnerabilities, internal/external * Impact shud threat b exploited * Likelihood harm will occur

Risk = measure of extent to which entity is threatened by a potential circumstance or event
Risk assessment = Process of identifying, estimating, and prioritising info sec risks
Threat = any circumstances or event with potential to adversely impact org operations or assets
Threat Source = intent and method targeted at exploitation of a vuln OR a situation that may accidentally exploit a vulnerability
Threat Events = characterised by tactics, techniques, and procedures employed by adversaries
Threat Scenarios = model, develop, analyse threat events
Threat Shifting = response of adversaries to perceived safeguards/countermeasures/etc. Adversaries aren't static.
Vulnerability = weakness in info system, system sec procedures, internal controls, or implementation exploitable by a threat source.
Predisposing Condition = condition within org which affects likelihood that threat events, once initiated, result in adverse impact
Likelihood of occurrence = weighted risk factor based on probability that a given threat is capable of exploiting a given vuln (Adversarial: based on intent/capability/targeting, Other: historial evidence/empirical data/etc)
Impact = magnitude of harm that would result
Risk Aggregation = roll discrete or low level risks into general/higher level risks
Uncertainty = inherent in evaluation of risk (emergent properties – affecting integrated but not separate systems -, changing user expectations, regulation changes, leadership changes, etc)

Assessment Approaches: Quantitative * Qualitative * Semi-Quantitative (bins/scales/or representative numbers, more judgement than would be in purely quantitative)

Analysis approaches: Threat-orientated (begin with threat sources/events) * Asset/Impact-Orientated (begin w impact of concern/critical assets) * Vulnerability orientated (begin w predisposing conditions or exploitable weakness)

Choice Of Methodology: Time Frame * Complexity/Maturity of process/org missions (how focused an assessment can be)* Phase of life cycle * Critically/Sensitive (of the info on the info systems)

Step 1: Prepare For Assessment
1.1: Identify purpose of risk assessment (at all 3 tiers)
1.2 Identify Scope (Org applicability, effectiveness time frame, architectural/tech considerations)
1.3 Identify The Specific Assumptions And Constraints (threat sources considered, threat events, vulns and pre-disposing conditions, process to det likelihood, adverse impacts considered, tolerable risks, guidance on uncertainty, level of analysis detail and how categorise threats)
1.4 Identify Information Sources (Where info coming from so relevant and pitched right, internal or external)

1.5 ID the risk model and analytical approaches used (risk orientated? Qualitative etc)

Step 2 Conduct the Assessment
2.1 Identify and Characterise Threat Sources of Concern
2.2 ID potential threat events, relevance, threat sources (many-to-many)
2.3 ID Vulnerabilities and Predisposing Conditions
2.4 Determine Likelihood
2.5 Determine Adverse Impacts from Threat Events
2.6 Determine Risk to the Organisation (make uncertainty explicit)

Step 3 Communicate and Share Risk Assessment Results
3.1 Communicate risk assessment results (Executive briefings/risk assessment reports/ dashboards, formal/informal)
3.2 Share Risk Information (where data came from, intermediate data b4 results, org should provide guidance on how to share)

Step 4 Maintain The Assessment
4.1 Conduct Ongoing Monitoring of Risk Factors (they change and use to refresh risk assessments, can be provided by external)
4.2 Updating Existing risk assessments with results from ongoing monitoring

New World:
Agility: IT env dynamic but info sec not dynamic * used 2 be slow enough for thorough risk management
Social Infrastructure: Jobs for life not the norm so staff management harder
Social Media Trends: new attack surface * harder to manage info flow * BYOD/remote working hard to manage
Software Development Life Cycle: historically slow and predictable * Now: Pluralistic (teams, departments, lots of software/applications), adaptive (adjusts to needs) , efficacious (Efficient in productivity), self-sustaining (doesn't require oversight), complementary (matches flow of org)
Valuation: historically static assets/ vulnerability/threat valuation * New world strength of countermeasures (resilience, speed of risk knowledge, solidarity of social network)
Dependencies: old links between components within app, app to context, internal and external * New links between physical, logical, and social realms
Lenses of Risk: Perceived directly (our own perception of risk and judgement)* Perceived through science (reduce uncertainty by connecting behaviours and consequences) * Virtual risks (uncertain risks, impacted by cultural filters)

Cloud Computing

Essential Characteristics: On-demand Self Service (dont need human interaction)* Broad Network Access (available over network and thru standard interfaces) * Resource Pooling (dynamic allocation, pooled to service multiple consumers) * Rapid Elasticity (provisioning and release, scale quickly on demand) * Measured Service (metering automatically, only pay for needed, SP can reallocate)

Service Models: Software-as-a-Service (application runs directly on cloud providers infrastructure)* Platform-as-a-Service (consumer deploy own apps on cloud infrastructure, prog lang/tools/support provided by CP) * Infrastructure-as-a-Service (greater control of underlying infrastructure. Eg OS, CP provides underling physical components)

Deployment Models: Private cloud (provisioned 4 exclusive use by single org comprising multiple business unity)* Community cloud (provisioned for exclusive use by specific community of consumers from orgs w shared concerns)* Public cloud (provisioned 4 open use by general public over public network)* Hybrid cloud (two or more clouds that remain distinct entities but are bound together by underlying technology)

Benefits: Computing as a utility (operational costs vs capital costs) * Reduced infrastructure * Focus on core capabilities * Agility from on-demand provisioning * Align IT reqs w business strategies quickly

Threats 2 Cloud Computing: Data Breaches * Misconfiguration and inadequate change controls * Lack of cloud security architecture and strategy * Insufficient identity, credential, access and key management * Account hijacking * Insider threat * Insecure interfaces and APIs * Weak control plane (control plane = configures data plane, poor control of data infrastructure logic/security/verification) * Metastructure and Applistructure Failures (Metastructure = the CSP/ Customer line of demarcation w usually API interactions) * Limited Cloud Usage Visibility (shadow IT, or sanctioned app misuse) * Abuse and Nefarious use of Cloud Services (e.g DDOS)

Security Guidance
*CSA provides * risk-based approach bc so many options * not all will be necessary*

Identify the asset (data? Application/function/process? Allow for scope creep) * Evaluate the Asset (requirements of protection e.g CIA? Sensitive?) * Map Assets to Deployment Models (narrow analysis scope) * Evaluate Potential Cloud Service Model (IAAS, SAAS, etc, may have specific requirements)

Domain Breakdown
Section 1: Cloud Architecture
Domain 1: Cloud Computing Architectural Framework (sets out clear terminology, detail frameworks, important who controls what in ISAAS etc)

Section 2: Governing in the Cloud
Domain 2: Governance & Enterprise Risk Management (extension of orgs general)
Domain 3: Legal Issues Contracts and Electronic Discovery (should also be passed 2 subcontractors)
Domain 4: Compliance and Audit Management (assignment of responsibilities, demonstration of compliance)
Domain 5: Information Management and Data Security (not same as traditional)
Domain 6: Interoperability and Portability (risk of being locked into a provider, to mitigate: virtualise where possible and store infrastructure data in portable format)

Section 3: Operating In The Cloud:
Domain 7: Traditional Security, Business Continuity, Disaster Recovery
Domain 8: Data Centre Operation
Domain 9: Incident Response (what/how is reported by provider 2 consumer, maybe possible 2 freeze a snapshot for incident analysis)
Domain 10: Application Security
Domain 11: Encryption and key Management (how do orgs demonstrate 2 auditors who is in control of enc key? Maintain in house of by trusted cryptographic service)
Domain 12: Identity, Entitlement, and Access Management (internet facing so use federation based on open-standards
Domain 13: Virtualisation (security of OS running as guest and hyper-visor layer)
Domain 14: Security as a Service (maybe centralise security resources 4 what couldn't be done alone, secure comm between tenant and consumer)

Security Benefits of Cloud
European Network and Information Security Agency outlined
Benefits of Scale: cheaper implemented on a larger scale
Security as Market Differentiation: incentive 2 provide better security
Standardised Interfaces for Managed Security Services: more open and readily availble market for security services (so can switch providers more easily w lower set up costs)
Rapid, Smart scaling of resources: good 4 peaking services and so can increase support 4 needed defensive measures (e.g filtering, traffic shaping)
Audit and Evidence Gathering: IaaS can support on-demand VM cloning * reduce downtime for analysis * cost-effective storage for logs by clouds
Timely, effective, and efficient updates and defaults: VMs prehardened with latest patches * updates more rapid across homogeneous platform * updates centralised and automated (sometimes) so shorter window of vulnerability
Audit and SLAs Force better risk management: Increased exposure of risks * ID penalties for risk scenarios in SLAs => incentivise more rigorous internal audits and risk assess procedures * hypothetical apparantly

Resource Concentration: Customers share benefit of cheaper security * reduced cost of physical access contol and perimiterisation

Payment Card Industry Data Security Standard

Written by council of card vendors * Consistent * baseline for tech and op reqs * ways 2 develop and enhance cardholder sec * minimum set of control objectives (still need law and regulation) * is contractual not law

Applicability: Cardholder Data can be stored (Primary Account Number - must be unreadable -, Cardholder Name, Expiration date, service code) * Sensitive Auth Data can't be stored (full track data = mag stripe/chip 2 prove possession, CAV2 etc 4 possession - merchant can only hold onto 4 as long as it takes 2 process payment, they don't need it but makes it harder for payments 2 be revoked - , PIN 2 prove identity) * Account Data (cardholder data + sensitive auth data)

PCI-DSS is applicable if PAN is stored, processed or transmitted (some say if account data is): Merchants * Processors * Acquiring banks * Issuing banks * Service provides

Scope of assessment: all system components (systems that provide security services, facilitate segmentation, impact the security of the cardholder data environment, virtualisation components) * ID scope annually at min and prior to annual assessment (can use Data Loss Prevention tools to scan for cardholder data and ensure none outside scope)

Cardholder Data Environment = people, processes, and technology that store/process/transmit cardholder data or sensitive auth data

Reducing CDE

- Network segmenting: reduce scope * reduce cost of assessment * reduce cost and difficulty of implementing/maintaining tools * reduce risk to org
- Eliminate unnecessary data
- Consolidate data in one place (feed where needed)

Wireless: Allowed but not recommended (specific testing procedures in place)

Third parties/outsourcing: Possible to offload but must document role of each SP and what reqs apply to assessed entity/SP * Two choices for 3PP: they undergo PCI-DSS and provide evidence to customer; their services reviewed during each customer assessment

Report on Compliance (sets out whether org is compliant) key parts: Executive summary (high level network diagram, desc business)* Description of scope of work and approach taken (how scope validated) * Details of the reviewed environment (desc CDE etc) * Contact info and report date * Quarterly scan results (four most recent, must cover all externally accessible IP address)* Findings and observations

Anything not compliant is considered an 'open item'

Overview of PCI-DSS Requirements

- Build and Maintain a Secure Network and System (1 – Install/maintain firewall config to protect cardholder date, 2- don't use vendor defaults)
- Protect Cardholder Data (3 – Protect stored cardholder data, 4 – Encrypt transmission of cardholder data across open public network)
- Maintain a vulnerability Management Program (5 – Protect sys against malware and regularly update anti-virus software or programs, 6 - dev and maintain secure systems and applications)

- Implement Strong Access Control Measures (7 – restrict access to cardholder data by business need to know, 8 – identify and authenticate access to sys components, 9 – restrict physical access to cardholder data)
- Requiring Monitor Test Networks (10 – track and monitor all access to network resources and cardholder data, 11 – regularly test security systems and processes)
- Maintain And Information Security Policy (12 – maintain policy that addresses info sec for all decisions)

Criticisms: Still have card data breaches * checklist activity and distracts from thorough security and risk management

Bring Your Own Device (BYOD)

Mobiles rich target

Important Questions: Who owns device? Who manages the device? Who secures the device?

Security Risks

- Security facts: PII unknowingly synced onto corp networks * likelihood of damage * cost of preventative measures when working with such a spectrum of device types
- Specific security controls required by law or contract
- Comply w policies (acceptable risk/ subjective reasonableness/etc)

Benefits For Employees: Choose tech you want to use * bring you own app? * work from home

Drawbacks for Employees: Company control over employee owned devices 4 security * expense met by employee not org * might be responsible 4 repair of damages that occurred at work

Benefits For Business: Cost Efficiency (less on sourcing devices, employees provide or have allocated budget, employees might take better care of own, employees keep up w cutting edge tech better than purchasing cycle allow) * Choice (devices sit users so more productive) * Mobility

Drawbacks for Business: Cost Increase (management, security repercussions, paying employees service which could include personal) * Security (easily lost, personal use = riskier, multiple OS/device types, jailbroken or modded more exposed, off-site data storage like cloud, malicious applications, social engineering, loss of control over device/data/security)

Securing BYOD

- Tools: Employee education * Logging * Mobile Device Management tools * Network Access Control * Guest Networking * Endpoint integrity checking/malware protection/ security tools
- Strategy: LAN or WAN to link-up devices (segregate the network) * Secure ID services * MDM services * A virtual desktop infrastructure/hosted virtual desktop so apps run and data is stored on a central server that is streamed to device * Training and procedures for proper usage
- BYOD secure with same reqs for other devices already on network

7 Steps to a BYOD security plan: Identify introduces risk element * Form committee for BYOD and understanding risks * Decide how to enforce policies for devices connections to your network * build a project plan to include capabilities * Evaluate solutions * Implement solutions * Periodically reassess solution

4 Steps to securing BYOD: Minimise device risk w mobile device management solutions * Reduce app download risks through policy and training * If developing apps, scan code for vulns * Conduct a company-wide mobile security audit

10 Steps to a secured BYOD policy: Review current security policy for web applications, VPN, remote access * Determine which devices you are willing to support * Set expectations clearly * Write clear, consider policies (signed by all employees who want to bring own devices) * Make PINs madatory * Enforce encyrption f data at rest * determine off-limit apps * Provide training * Look for apps that incl. Support for auditing, reporting, and central management * Consider MDM software

NIST Guidance

For enterprise: dedicated network for BYOD that is external

For user: software kept updated * for accounts, principle of least privilige, password protected, * for sessions: ensure protected from physical access * Network config (disable unneeded, limit use of remote access technology, configure wireless networking by disabling auto conntect etc) * Attack prevention (anti-virus, firewalls, content filtering software) * Different browser for personal vs work * Authorised app stores only * Don't jailbreak/root * Don't use unknown charging stations * be careful when syncing device to a pc (malware propogation, sensitive data syncing, etc)

Security and The Supply Chain

Supply chain = orgs, people, activities, info, resources involved in moving a product or service from supplier 2 customer

The further upstream, the closer to the raw material

Components of chain: Physical (requires storage/trasnportation) * Information (Which drives the supply chain)

Risks: Internal Focus (operational /technical /financial/legal/regulatory/environmental/HR/political) * Supplier focus (good relationships /perform as needed/ HR/ supply chain disruption/ will they stay solvent/ supplier env/ market dynamics/ disaster recovery/ political/ regulatory) * Customer focus (distribution/will they pay/ the relationship/ market/ brand/ product & liability/ env/ political)

Balance (and communicate control risks) between: Supply risk (how much do we supply) * Demand risk (Demand too high/little) * process risk (how are we managing the balance)

Note: these processes/activities are wrapped inside environmental risk and info/cyber risk

Risk Management Process: Understand the Supply Chain (where invoices, single point of failure) → Improve/Simplify the supply chain → Identify the critical paths → Manage the critical paths (recovery/ what-if/ scenario planning) → Improve network visibility (open communication channels and greater data exchange) → Establish a supply chain continuity team (proactive and reactive) → Improve process (go back 2 stage 1)

Visibility and Control: you only have contract with tier 1 supplier (put req clauses in your contract, you can audit them) * maybe limited visibility of tier 2 and higher upstream (but may have your data shared from tier 1 so your data could be lost)

Acquirer Issues: Stating meaningful cyber security reqs * Integrating cyber security into procurement * Devoting the necessary resources * Understanding how supplier meets reqs
Supplier Issues: ID what info they are being shared * specify cyber sec reqs for indirect suppliers * Measure the effectiveness of cyber security arrangements * ID cyber related risks * ID tech & tech suppliers * Control the CIA of information

Current Approach (Supplier Focused)

Procurement Cycle: ID requirement → Plan procurement process → Apply tendering and contracting process → Negotiate and award contract → Contract and delivery management → Monitor performance (usually when info sec is brought in, which is costly since changing contracts is costly)→ Review requirements →

The Approach:

Acquirers: Specify standards 2 be complied with (e.g ISO/IEC 27001/27002) * Audits (no need 2 warn suppliers, use audit standards ISAE 3402/SSAE16 SOC 1/2/3) * Assessments to asses suppliers * Purchase from reputable suppliers

Suppliers: Get certified * Submit to audits * Follow best practices * Do nothing – knock prices low

Toolbox: Policy * Standards * Risk Assessment * Controls

New Approach (Follow the information)

Types of info in a supply chain: Commercial info (order quanities, orders and invoices, prices) * Intellectual Property * Legal regulatory and priviliged info (contracts, legal advice) * Logistical info (delivery schedules, shipping) * Management info (finanical reports, process performace) * PII (Consumer details, employee data) * Etc

NOTE: Bucketing data makes it easier to define reqs and id info sharing patterns

Approach: ID Suppliers → ID shared info → Determine risk → Focus on high risk suppliers → treat the risk → Monitor the risk →

Benefits: Similar to classic risk management (easier to orgs to adopt) * Easier to manage contracts (classify them on info shared) * Focus resources * Requirements proportional to risk (may be less expensive) * Templates for risk profiles (presented upfront, more consistent) * Risk driven

Other things to do: Adopt standards throughout chain * Integrate security into procurement process * Apply info sec toolbox (policy, standards, risk assessment, controls) * Adopt new tech appropriately (cloud etc) * Harness resilience approaches particularly to the upstream (incident management/ crisis management/ planning/ rehearsing/ exercising/ supplier/ supply chain mapping, consider the timing aspects for recovery and maximum downtime, alternative suppliers, access to info, working on a reduced estate, digital supply chain management)

Big Data

Big data = tech and architecture designed to economically extract value from large volumes of wide variety of data by enabling high-velocity capture, discovery, and/or analysis

The V Characteristics: volume * velocity * variety (sources, format, [un]structured)

Other V Characteristics: Veracity (trustworthiness – too much to clean and verify?) * Value (add value by processing intractable and producing insights) * Variability (process amalgamation of non-conformant data)

Storage And Querying:

Types of data: structured (standard format, relational DB) * semi-structured (self-describing, separate semantic elements, XML/JSON)* unstructured (free form, usually text heavy or media files)

SQL solutions: structured data * vertical scaling (increase data supported by increasing power of hosting sever) * sophisticated querying that's efficient/quick

NOSQL: all types* horizontal scaling (more data by distributing over multiple servers/shards)

Note: can use mix of both for big data

Security Problem:

In general: Rich target * Might not be built w security in mind (nosql had few sec controls that RBDMS)

Five Categories: Cyber Security (rich target) * Data in the cloud (cloud security isn't lift and shift)* Consumerism * Interconnected Supply Chains (the info needed 2 keep it working)* Privacy (detecting PII and legal/reg requirements with this volume is difficult)

Challenges:

- Random distribution: hard 2 tell which distributed server data is being processed on (security problems, regulation breaches) * Can get services that guarantee geographical location
- Privacy: DB solutions often treat data same w no consideration 2 sensitivity

- Computation: False insights can skew or affect results
- Integrity: prevention and detection of maliciously poisoned, or incorrect data, 2 preserve integrity of results
- Communication: protect comm between nodes holding data
- Access control: prevent malcious actor accessing nodes 2 extract/compromise * prevent malicious nodes joining environment

Techniques 2 protect privacy

- Rules and legality: abide geographical rules, applicable laws
- Encryption: storage (sensitive data stored differently) * Computation (blind processing or homomorphic encryption 2 preserve privacy of data when processed) * Communication
- Authentication
- Meta data & tagged data: so not all records treated same and approp controls for private info
- Unstructured distribution: don't store interrelated in same cluster
- Anonymisation: data perturbation/swapping techniques 2 protect from association
- Tracing activity: log data

Big Data As A Security Solution: Can be used for detection in the prevent-detect-respond paradigm (compare network behaviours against baseline)

Policies have to be re-written with big data in mind

Big data has a shelf life of usefulness