Business Analysis and Cybersecurity, May 10th 2019 Syndicate exercise 1

BA MANAGER FORUM

How does cybersecurity affect your organisation?	Are there any specific vulnerabilities within your organisation?	What is your organisation's threshold for cybersecurity?
• Concerns around attacks • Data breeches • Physical harm implications (i.e loss of service and interfering with product) • Protect Vulnerable customers • Impacts on end user • Access Management – Different levels • Safety and user devices (human error) • User management /governance: – Recertification – Encryption – Whitelisted – Recognised devices • FUNCTIONAL V NFR's – Standards – Testing • Document Classification • New customer assessments to become accredited • Company strategy / vision - emphasis on customer and data/trust. • Brand reputation • Stifling innovation - Software and Cloud • Projects – Key consideration – full NFR's and involvement upfront • External threats (e.g. Brexit) • Implications for Customer Service – End user experience – Enabling them to do what they want • Limits knowledge, share/grow skills	• Comms – email = gateway to other systems • Social media • Cloud – 365 access changes • Human error • Protecting commercial information • Exposed to information leaks, requires secure protection so that competitors cannot get hold of this • Holding personal data • Internal / external email • Printed materials due to processes limited to people completing the job. • Correct disposal of docs • Human error • Access (network) • Authorisations and tracking of this • Multiple systems to control • Physical access • As a university we trust everybody • Authorised backdoor • Spreadsheet anarchy tend to be reactive • Payment systems – storage of bank/card details • Legacy systems – under supported systems • 3rd party /partners – number of 3rd parties involved • Sheer size of systems and surface area of attack • Issues – Cloud, AI • Cloud specific vs on premise	• Locked down access • Training to address awareness • Idiot proofing – reduce human error (e.g. memory sticks) • Not the weakest in market (e.g bank access privileges) • Embedded into organisation culture • Awareness high • Risk management is carried out • Accreditation assessment • Testing carried out • Security built into process and policies • We are aspirational not the back up tools • Have risk register • Intellectual property email policy • Blackening Bitcoins • Increasing tools • Creating funding • Ensuring latest possible versions on systems • Increased focus on training staff and supplying tools (e.g. ability to flag suspicious emails) • Recruitment of more senior roles dedicated to cyber security • More accountability for senior leaders • Phish our own staff to improve protection • Privacy by design • Cyber security is everyone's job • Varying between tech solutions and human freedom or much more locked down

I-PERCEPTIONS

• Limits flexibility • Disciplinary rules and standards • Systems that are not up to standard • Denial of service • Sales force could download data • Spreadsheets and Access db • Touches everyone in the company – training, cultural change – affects our customers too • Brand/reputation of the company itself • Cost of protecting legacy systems • Social Engineering • Internal technical vulnerabilities • Arm – secure chip design • I.P – Key security issue • Reputational impact very large • Lack of consideration of malicious actors – the abuser role as well as user roles – Sometimes just lack of concern or not considered malicious • Importance of standards • Holding client data • Commercially valuable data • P1 Date and IP Data Loss • Physical and software controls on higher security data • The thought that security issues = business rules (e.g. password expiry makes people think security is taken care of) • Safety culture and governance (& therefore security); but is this from an asset centric (safety) point of view?	• Type of data (i.e. health or financial) • Data transfer • Processes / staff are the biggest vulnerability – unsafe workarounds • Social Engineering – personation, lack of challenge – visitors – unrestricted communication challenges • Varying skill levels • Secure methods being harder than insecure • Not CTOI – don't know areas specifically • Support standard between 3rd parties could compromise business choices • NO – not that I am going to tell you!	• Transfer the risk at a loss due to magnitude of data logs • "staying out of the newspapers" Others getting burnt, driven behaviour in others. • Money spent if tied to Cyber Security • Quiet is Good, so that is the way to be good at cybersecurity and build reputation • Risk analysis driven. £ Budget has an impact here i.e. not willing to take the risk, or spend the money • Stripping things back to the core – transfer data if you must. • Security has a stigma, this may be changing, maybe because it is brought in early. • It is all about Risk, Benefit VS Cost

• Separate Security Department – infrastructure. • The need to resource • A Separate function • Risk level vs cost assessment – is it worth doing more? • Have we done a security audit? WE might have done but telling me would increase the risk?! • What about cloud? - More people are moving stuff to the cloud		

Continue overleaf if required

What do BAs currently do with regard to cybersecurity?	What should/could they do?
• Identify risks through stakeholders • Community of Practice (COP) to discuss variations / vulnerabilities • Ensuring processes are up to date – BA is aware • Risk with use of contractors, third party, new starters, BA • SMART Meter – no data transfer • Understanding the information and processes • Fill in info sec templates / questions • Classify doc security (overstating confidentiality) – trying to manage this, BA's helping challenge / understanding. • Engage with SMEs – What are constraints? Build Flexibility • Taking customer feedback • Building understanding of risk • Data journeys alongside business processes (helps security understand) • Engage the security team • Discuss with Info Sec • Specific feed from Security Teams • Flexible benefits in place for security • NFR's around security, pushes around where data is stored • Copy and paste approach to non-functional penetration testing • Attribute costs to data compromise • Checklist driven process • Leave application level security to the devs • Procurement processes include consideration of security • By data presents a risk • View is often secure at the time • We think of data at an operational level, our cyber security behaviours are often only at that level • We ask the questions of the business and relate answers to security • BA : Know Business Operation and Sec : Know security model • Security left off investigation	• Realistic approach for individual roles – review, standard material and SME checks • Having security officer involved throughout entire process (at start of process to provide steer and design stage) • Include personas such as hacker (malicious user), untrained staff • Worst scenario considerations • Understand controls on the data and who to engage • Quantify the data and the risk to the organisation • Understand the process and the value • Understand user experience and trade off with info security rules • Translate the jargon from info security to bring to life • Security model / vision/ working practices need to be shared to ensure security requirements are understood and considered when eliciting reqs • Security is a functional req, why – more things are accessible with more access points, the internet, more access points for the 'bad people' • NFR's • NFR Owners • EZE Process Owners, Data Owners and ISO's = Driving Accountability, not owning as in BA but ensuring the right people do and are aware of the job scope and requirements • Considerations bought into functional requirements the abuser role as well as user roles – do we need ENIS Data • Pull NFRs and functional requirements together so non-func. do not drift away • Consulting the experts (Security SME's) – not checklists • Translating info sec need in meaningful way to business • Openness • Build data awareness • Shift from IT to Biz Focus • Ensure holistic view not just 'technical' view

- Consider development methodology and ensure info/cyber sec representation.
- Consider as part of procurement process more
- Consideration for vendor selection
- Build audit into change (i.e. Salesforce Shield).
- Highlight risk for business case
- Ensure we are aware of risks
- Consider security at biz case stage
- Raise to biz stakeholders at the start
- Refer to required standards in A/C
- Incremental improvements better
- Wider consideration of peoples’ vulnerabilities
- Forward looking and retrospective considerations thinking about “closing the door” behind you
- Build relationships of security
- Early lifecycle engagement
- WE should think about the tactical and strategic level
- Shadowing – thinking outside the box, the tick boxes of security (slide)

Do bContinue overleaf if required

How will you increase the awareness and knowledge on cybersecurity in your BA teams?	What one thing will you aim to implement when you go back to your work?
• Bring CISO in to Community of Practice and keep doing it to raise awareness • Ensure holistic approach to cyber security – beyond technical concerns • Build security considerations into your analysis processes – workshops, docs etc. • Form part of scenario planning – what would be the impact of an attack to your reputation? Customer? • IT Cyber security / present 5-10 mins at meetings • Build relationships / get security in earlier • Discussion within teams – why and how can we improve / involve? • BA presence at project review / gates • Have a template and keep updating over projects, systematic approach. • Identify the right SMEs and stakeholders • 3 Amigos – introduce ideas, have just enough knowledge • Need to continually keep up to date with CS Knowledge • Speak to CS Experts • Use Psychology in the application of CS • Cyber security essentials certificate – many organisations are taking part in this, BA's could understand more about what is involved • Work out bad and good situations • Better working with IT Security – arrangements • Better working arrangements with solutions architects • Use of Personas • Update and improve frameworks to bake security in • Encouragement – make sure it is done • Knowing the questions to ask – Checklist • Build the relationships with the experts (better knowledge with the BA Team) • Bring SME into the BA Team – Share the Knowledge • Make sure the refit is very much "holistic view" • Talk to Cyber security team to obtain checklist	• Introduce the concept of malicious actors – fraudsters/ hackers – "Hacker" persona and "anti-user" (abuser role) • Role play game of trying to hack into a computer • Think more about unhappy paths/scenarios • Increase awareness of malicious actors/hacker persona/abuser role and unhappy paths/scenarios • Consider access and segregation of data – have we got it right?? • Work with change team – ensure governance in place • Consider full stack of changes when doing analysis; security, performance MI, NFRs **SO** important • Check security policy exists and if not facilitate the creation of one • Train people on things like ethical hacking • Introduce into 3 amigos, test with them and do more initial analysis around CS issues • BA becoming aware of new relationships and technology services • Thoroughly explore risks • Create traceability between solution architect and IT Security • Invite the BA Team to next BA Away day • Blog about it • Share learning at next team meeting • Clarify the expectations of our BA's in terms of security • Raise awareness of data security as a state objective of your project • Manifesting security in all services

• People and process as well as tech • Functional and non-functional, this doesn’t go away • Use all incidents – real world occurrences within my organisation • Get info on ISMS – become more aware • OWASP – best practice web security	