ICT Services

January 2016

Version 1.0

Security & Identity Management Strategy

People Centric Security

This strategy is about trust; letting the right people, get to the right information, when they need it with the least hassle. Systems need to know who to let in and who to block in order to protect business assets. Getting it right is very much a shared responsibility; managers in the services know what information individuals are entitled to see. IT can create those conditions using technical controls and importantly, remove them when no longer required.

Cloud services, employee agility and partnership working are increasingly part of the digital workplace. Security and identity management are key enablers in this space.

Maintaining the security and integrity of the corporate infrastructure is fundamental to allow the organisation to access its business information more flexibly and share it securely with its partners. Identity management is the extra layer of intelligence that recognises users and their entitlements and allows them in.

Digitally literate users increasingly expect a consumer like experience. This strategy sets about protecting our valuable corporate assets whilst making life in the digital workplace as simple as possible. To get this right, we will focus on the people at the centre, those using the technology to help them work more efficiently; but whilst IT can set the controls, only services can determine the risk appetite.

This strategy is an essential foundation capability but one that has to be worked on in partnership to achieve a pragmatic balance.

The Weakest Link

Security is an enabler of sharing. We aim to help services find straightforward ways to make informed decisions. Helping the organisation to identify its most sensitive data and to take reasonable steps to protect it. This isn't easy in a climate where the Anti-Virus Institute registers some 390,000 new malicious programs every day. This is a number that has more than doubled in two years.

A recent survey (*Computing September 2015*) explored the main threats to security. Causing most concern were Spammers, Organised Crime, Crackers & Hacktivists. Main threats to information security placed *email* and *mobile devices* at the top of the list. Specific technologies are used in these areas to mitigate risk but achieving absolute security through technical controls alone is an impossibility; human beings are almost always the weakest link. With the freedom to work flexibly comes increasing responsibility for data confidentiality. This strategy recognises that users are a vital part of the integrated security infrastructure in a digital workplace and increasing awareness to influence behaviour will be a key activity in this area.

Related Strategies

Network Strategy

Digital Strategy

Application Strategy

Device Strategy

Information Strategy

Business Intelligence Strategy

Key Drivers:

- User experience
- Security
- Accessibility
- Flexibility
- Partnership working
- Interoperability
- Responsiveness

Principles of Resilience for Digital Business Risk and Security

Being resilient is closely allied to being secure. Resilience is about being able to absorb the impact of incidents and bounce back rapidly. This strategy aims to build resilience and will do so in dialogue with the departments in order that decisions around the appetite for accepting certain risk for the achievement of success can be made in partnership.

To help inform decisions that impact security, we will apply these principles:

1. Check box compliance is not enough, we will actively support a shift to risk based decision making. Risk based thinking allows cybersecurity investment to be targeted where the business decides the greatest risk resides.
2. We will focus on supporting business outcomes alongside protecting the infrastructure. Using our relationships to fully engage the business in security decisions, understand IT dependencies and impacts on service delivery and citizen welfare to add value to decision making and help facilitate risk based outcomes.
3. Information cannot all be controlled but understanding its flow is vital. In a digital workplace, we will not own all of the infrastructure anymore and increasingly information will be stored in places belonging to third parties. This will involve an organisational shift in the way we approach protecting our assets.
4. Accept the limits of technology and become People-Centric to support a digital workforce. This approach is all about emphasising individual trust and accountability and de-emphasising restrictive, preventive security controls.
5. We will invest in detection and response technology. Automation enabling us to react faster to a compromised IT environment.

The Digital Workplace in 2020

Digitally literate users will take mobility and partnership working for granted by 2020. This strategy will continue to protect corporate assets by ensuring that the Council remains compliant with national security standards, such as the Public Services Network, affording the opportunity for organisations to benefit from accessing shared services right across Central Government and the wider public sector. Similarly, it will ensure that we continue to comply with the Information Governance (IG) Toolkit to support increasing interoperability with NHS organisations and partners. Decisions involving security and risk will increasingly be made in partnership and will become a natural part of the conversation to ease working practices beyond traditional boundaries.

This strategy is mindful of the impact of the Internet of Things (IoT) on the horizon. Identity management of people alone is not without significant challenge; increase that by multiples of inanimate objects producing an explosion of data and the impact is massive. Health is regularly cited as an area in which IoT could have tremendous benefit, similarly sensors in other areas such as flood defence and smart metering could change services radically. IoT must get privacy and security right or risk an erosion of trust and reputational damage. The road to 2020 will need increased dialogue between services and IT to come up with solutions that satisfy customers needs.

Security and Identity Management are key enablers as we work to converge services and infrastructures. Robust Identity Management is a vital capability in order to be able to on-board new customers / stakeholders in a secure and resilient way. The next 3 years will see investment in automation, intelligence and detection tools to make this happen.