Report to:	**Audit, Best Value and Community Services (ABVCS) Scrutiny Committee**
Date of meeting:	**27 September 2017**
By:	**Orbis Chief Information Officer**
Title:	**Cyber Security and Information Governance - Keeping East Sussex County Council (ESCC) Safe**
Purpose:	**An Information Governance overview explaining how IT & Digital Division protect business services and keep our users safe**

RECOMMENDATIONS

1) Note the strategies and controls in place to maintain the security and integrity of the corporate infrastructure and plans to adapt it to continuously meet future needs.

1 Background

1.1 Between March 2014 and April 2017[1] **111** UK councils experienced **256** ransomware incidents, such is the risk posed by cybercrime to government today. Despite stating that no data was stolen and no ransoms were paid, the climate is such that local government must adopt robust solutions to mitigate the risk of information getting into the wrong hands and disruption to business services before *and* after impact. To give an idea of local scale, in a typical month, the council receives and rejects **4.8 million** potentially malicious email messages, **77%** of all malware is installed via email. The threat of cyber crime is on the up, driven by career criminals that are highly skilled, innovative and will stop at nothing to target organisations that hold people's private information. The risk is very real and the IT & Digital Team are alert to the threat, using a combination of information governance and policy, robust risk assessment and technical controls to protect business services from disruption and keep our users safe.

2 What are the Risks?

2.1 **Data Breach:**

With changes in the General Data Protection Regulations (GDPR) coming into force on 25 May 2018, fines from the Information Commissioner (ICO) for a data breach will increase. Under the new legislation, fines currently at a maximum £500,000 will become €20million euro or 4% of turnover. For ESCC, this equates to circa £30million. To maintain perspective though, the ICO states that 'issuing fines has always been and will continue to be, a last resort.' In 2016/17 out of 17,300 cases, only 16 resulted in fines for the organisations concerned.

2.2 **Cyber Attack:**

The National Cyber Security Centre (NCSC) has highlighted the substantial risk to British web infrastructure with elevated levels of Cyber Crime being reported against all areas of government. Cyber-attacks often include multi vector attacks featuring internet based, social engineering and targeted exploits against hardware, software and personnel. The remote nature of the internet makes this an international issue and an inevitable organisational risk.

3. Our Strategic Response

3.1 In a recent survey, the top three concerns cited by organisations around a potential cyber-attack are: loss of sensitive data; financial repercussions and; the expected impact on service delivery. Our component based IT Strategy recognises these challenges and specifically seeks to respond to this volatile landscape by supplying services that are continuously relevant, accessible, operate at optimal performance and most importantly

[1] https://inews.co.uk/essentials/news/uk/cyber-crime-britains-public-bodies-hacked-400-times-last-three-years/

address these risks and add value. Ongoing work in two specific strategy areas is particularly pertinent.

3.2 Our **Information Management Strategy** recognises that information is critical to every part of our business; it underpins our ability to drive sustainable growth, keep vulnerable people safe from harm, build resilience for individuals and families to live independently and make the best use of our resources. Increasingly our services are provided with greater openness and in collaboration with a range of partners from all sectors. The effective and efficient provision of these services depends on information passing between organisations in a timely and secure manner. Sharing our knowledge and information to maximise its value is about understanding and managing information risks and striking a balance in transparency whilst ensuring adequate protection is in place. Holding respect for the origins and ownership of our information is at the core of our decisions, so that the public can maintain trust and confidence in the way our business operates.

3.3 The strategy adopted adds value by ensuring compliance with the rigorous standards of the Public Service Network (PSN) and the Information Governance Toolkit which provides the Council with the means of sharing information and digital services across the public sector and our health partners.

3.4 Our people centric **Security & Identity Management Strategy** recognises that a successful cyber-attack can shut down operations - not just for a few hours, but rather for multiple days and weeks. The collateral damage, such as information leaks, reputational damage and so on, can continue for much longer. Added to that, backup systems, applications and data may also be infected and therefore, of little usable value during response and recovery operations in the short term - they may need to be cleansed before they can be used for recovery. This takes time and skilled resources.

3.5 We recognise that security is an enabler of sharing, so 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 our valuable business assets. Getting it right is very much a shared responsibility; whilst IT can create those conditions using technical controls and importantly, remove them when no longer required, only managers in the services know what information individuals are entitled to see. Good security is achieved in partnership and is at its most effective when user awareness contributes equally to the balance of controls.

4. Security Controls

4.1 Since being resilient is closely allied to being secure, a number of principles of resilience for business risk and security are inbuilt into IT & Digital processes. Resilience is about being able to absorb the impact of incidents and bounce back rapidly. To help inform decisions that impact security, these principles are routinely applied to service design:

- **Check box compliance is not enough**, we 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.
- **We 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.
- **Information cannot all be controlled** but understanding its flow is vital. In a digital workplace, we do not own all of the infrastructure anymore and increasingly information is stored in places belonging to third parties. This involves an organisational shift in the way we approach protecting our assets.
- **Accept the limits of technology**, adopting a people-centric approach to support a digital workforce. This is all about increasing awareness to change behaviours. Emphasising individual trust and accountability and de-emphasising restrictive, preventive security controls.
- **Investing in detection and response technology**. Automation enabling us to react faster to a compromised IT environment.

5. Delivering the Strategy

5.1 IT & Digital Strategy translates into a number of initiatives currently underway that contribute to the security of the organisation (*explained in more detail the accompanying presentation in appendix 1*):

- Enhancing user awareness – with 77% of all malware installed via email, users to be given learning experiences of *phishing* at point of use in a safe and secure environment;
- Implementing SIEM – A new Security Information and Event Management system is due to come online in Quarter 4 (Enhanced logging and analysis of potential issues or threats within the network);
- Policy Notification Software – Mandatory training and notifications of critical statutory changes pushed to users desktops to ensure awareness;
- GDPR training and workshops to cascade vital skills and information to those affected by new Data Protection laws.
- Move of ESCC servers to the Orbis Primary Data Centre for resilience (ISO27001 certified Tier 3 environment)
- Development of "Security Advocates". Trained staff that can cascade and share cyber security insights and highlight potential issues into the workforce.

6. Assurance

6.1 IT & Digital have had a number of recent audits that give assurance to processes and practices in place that support information governance and security. The below Audit Reports have all returned an opinion of **Substantial Assurance** evidencing that there are robust and tested principles in place.

- Cyber Security
- Network Starters, Transfers & Leavers
- Storage Area Network Audit
- Microsite Management Report
- Social Media
- Information Governance (in 2015)

7. Continuing to Protect the Digital Workplace

7.1 Through our IT Strategy, the IT & Digital Team continue to protect users and corporate assets by ensuring that the Council remains alert to threats and compliant with national security standards. Retaining corporate compliance with government / partner accreditations will remain a priority to protect business information and allow the Council to share securely with its partners. This though is in the context of a national shortage of cyber trained staff and shrinking budgets, reducing the capacity of operational staff to respond and recover from cyber incidents in the future.

7.2 Mindful of developing technology, the risks will increase without investment in automation, intelligence and detection tools. The Internet of Things (IoT) is *increasing* the landscape to defend, making the security job harder everyday. The IoT will have a massive impact with identity management expanding to be about *things* as well as people. Multiples of inanimate objects producing an explosion of data is not without significant challenge. 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. Information governance, Security and Identity Management are key enablers in this sphere.

MATT SCOTT
Orbis Chief Information Officer

Contact Officer: Nicky Wilkins
Tel. No. 07827 980154 Email: nicky.wilkins@eastsussex.gov.uk

BACKGROUND DOCUMENTS

None.