

2016/2017 Risk Register

Cyber Attack Prevention Action Plan No: 1

Champion – Director of Resources

| | |
|--------------------------|-------------------------|
| Issue Description | Cyber Attack Prevention |
| Council Objective | Value for money |

| EXISTING CONTROLS IN PLACE |
|---|
| <ul style="list-style-type: none"> ✓ Two corporate firewalls in place, with redundancy should one be compromised or fail ✓ Separate firewall for PSN (Public Services Network secure) originated traffic ✓ Proxy server and separate web filters based on user profiles ✓ Desktop Anti-virus (McAfee) ✓ Wave safe end control (end point security for restricting/ blocking USB devices) ✓ Intrusion Protection (IPS) ✓ Application control (Deep pack inspection including SSL traffic) ✓ Appsure Backup solution ✓ Virus awareness communications ✓ Web logs (monitoring) ✓ CERT UK, networking, attending conferences ✓ Patch policy, every Tuesday from Microsoft/ application vendors for security updates ☐ Test environment for enable new patches or updates ✓ Data Leak Prevention (DLP) ✓ Anti-virus/ anti-malware at the firewall level ✓ Fusemail spam and email filtering ✓ Fortimail internally hosted spam and email filtering for PSN (Public Services Network secure) originated email exchange ✓ Network address translation (NAT) across all firewalls to 'hide' our network IP ranges behind outward facing Public ones ✓ Network connection redundancy through a separate link to the outside from the Cem and Crem ✓ SSID filtering and secure authentication through Cisco wireless controller ✓ Demilitarized zone for outward facing web servers ✓ Reverse proxy for outward facing web services, that are required to be hosted internally |

| Required action / control | Responsible for action | Risk Action | Progress | Status | Due Dates |
|---|---------------------------|---|---|----------|------------|
| Staff engagement & awareness programme of potential cyber threats | A. Scrivens | Review existing ICT Computer Security Policy with assistance from Blackpool Policy services. | Current Policy has been reviewed with ICT & Blackpool's Policy Team. The conclusion was the policy was and still is fit for purpose. However, when the new ICT manager starts in August, once this person is settled they would be in the best position to determine how this should be developed. The long term action for this post will be to ultimately review and maintain this policy going forward. | COMPLETE | April 2016 |
| | A. Scrivens / R. Mckelvie | Review current ICT Security iPool module content, contact Blackpool to see if there has been any updates to their content since original version done (2011). Liaise with ICT to add wording for Fylde and make any relevant or necessary changes etc. Re-vamp and modernise content. | The decision was made to use the dedicated LearningPool.com version which is a standardised format design especially for all Local Government Authorities containing all the latest best practices. Allan Oldfield has communicated this new course to all staff, also adding about the requirement for completing this new course with a deadline date of October 2016. | COMPLETE | April 2016 |
| | A. Scrivens | Use recent PowerPoint slides and quiz published by ICT to show what virus look like, add onto new iPool module as a quiz. | Available online. This is now live and published for staff to complete. Allan Oldfield has sent round comms for all staff to complete by October 2016. | COMPLETE | April 2016 |

| | | | | | |
|-----------------|-------------|--|--|----------------------------------|----------------|
| | A. Scrivens | Relaunch ICT Security iPool Module, setup as next compulsory course for all staff to complete. | This is now live and published for staff to complete. Allan Oldfield has sent round comms for all staff to complete by October 2016. | COMPLETE | May 2016 |
| | R. Mckelvie | IT network policy enforcement logon software | Log on prompt has been reviewed. Options will be explored to further improve additional policy information at log on. | COMPLETE | May 2016 |
| | S. Stott | ICT to attend team briefs, undertake as an action once for all team briefs (AUG), | This has been done via a different approach, we cascaded the information via the intranet and the Chief Executives 5 points. | COMPLETE | August 2016 |
| | S. Stott | Assess the impacts from team briefs via surveymonkey to analysis findings | <p>An interactive quiz has been developed and distributed to staff based on the content previously distributed via the 5 point and on the intranet. Looking at the results of the quiz so far all staff have achieved a 100% score.</p> <p>We will continue to develop and distribute this but the results are encouraging and show that we have achieved a better understanding of the issue and what to do if you experience an issue.</p> | COMPLETE | September 2016 |
| | S. Stott | Mystery Shopping exercise with website checks by staff. | <i>Not yet due for reporting</i> | <i>Not yet due for reporting</i> | March 2017 |
| Next Generation | R. Mckelvie | Establish quotes for product (<i>approx. £15,000</i>) | The Fortigate unit which provides our main Unified Threat Management also includes this feature so after looking at options and | COMPLETE | March 2016 |

| | | | | | |
|----------------|-------------|--|--|----------|------------|
| Threat Control | | | <p>comparing functionality and cost; this solution is the most logical and fits in with our wider application/ appliance consolidation and rationalisation strategy.</p> <p>In implementing the virtual appliance to existing assets for both email and network infrastructure security we have been able to procure a robust solution for £1,552.80- a significantly lower cost than purchasing a standalone new appliance.</p> <p>This also reduces support considerations as the technology is already familiar to employees.</p> | | |
| | R. Mckelvie | Purchase and deploy | <p>The Fortisandbox solution has been purchased and implemented by ICT services.</p> <p>By using an existing platform and not procuring an additional appliance for this security element the solution is fit for purpose and will also modularly cover our secure email space for GCSX adding an additional layer where our most sensitive and protected communication takes place.</p> | COMPLETE | April 2016 |
| | R. Mckelvie | Publicise this via Vine & Directorate communications | <p>A Vine article has been produced and communications to the directorate via 5 points have been circulated to staff.</p> <p>These provide a high level overview to the staff using our infrastructure assets of the technology and security considerations we</p> | COMPLETE | April 2016 |

| | | | | | |
|---|-------------|---|---|-----------------|------------|
| | | | undertake and help move the awareness and education agenda for this space forward. | | |
| Baseline network/ check for changes to files/ configuration. | M. Don | Re-deploy existing software to detect file / network changes | <p>Network monitoring via PRTG software is in place and installed on our infrastructure server- which includes our full server space, switches and routers.</p> <p>This allows us to monitor changes and take action before malicious infections or exploits spread if introduced to our network.</p> | COMPLETE | April 2016 |
| | R. Mckelvie | Prioritise backups, the way which areas are selected first based on the Business Continuity Plan. | <p>The initial action has been completed with backups being prioritised according to the BIA spreadsheet, an action which also came out of the external ICT audit.</p> <p>This will require periodic review to ensure that the backup arrangements in place meet the organisation/ service managers' expectations around how often they are taken.</p> | COMPLETE | May 2016 |
| Block certain high risk sites. | R. Mckelvie | Web filtering software in place, review and implement | <p>Web filtering software is now in place and all high risk sites have been blocked.</p> <p>Further testing will continue going forward, the first date for testing will be on July 23rd (provisional date) where ICT will be migrating our Checkpoint firewalls which currently provide firewall protection and network address translation to our Fortigate 100D.</p> | COMPLETE | April 2016 |

| | | | | | |
|--|-------------|---|---|----------------------------------|------------|
| | | | <p>In doing this we will also be implementing a new Fortigate 100D and pairing the two devices for high availability, performance and resilience.</p> <p>Robust web filtering via Fortigate 100d appliance is in place with rule sets set up for groups according to access needs with the policy of least privilege applied.</p> | | |
| Review ICT Strategy / Plan | R. Mckelvie | Make sure virus controls are highlighted as high risks, ensure capacity within department is set at the appropriate level to reach maintain set standards | <p>McAfee anti-virus software is in place across our virtual desktop infrastructure, server space, and on laptop devices when issued.</p> <p>AV policies have been reviewed and hardened according to best practice following the cryptomalware exploits introduced to the network.</p> | COMPLETE | May 2016 |
| CERT liaison, to implement best practice advice | S. Stott | Implement any actions through network groups, lean on Wyre & BLP ICT for council advice where possible. | <i>Not yet due for reporting</i> | <i>Not yet due for reporting</i> | March 2017 |
| Server consolidation excise | S. Stott | Continue to reduce the amount of servers to eliminate virus, storage, backup constraints | <i>Not yet due for reporting</i> | <i>Not yet due for reporting</i> | March 2017 |