MUNICIPAL YEAR 2019/2020 - REPORT NO. 241

Agenda – Part:	**Item: 7**

MEETING TITLE AND DATE:
Audit and Risk Management Committee
March 5th 2020

Subject:
Cyber Security Report 2019

Key Decision:

Wards: All

Cabinet Member consulted:

REPORT OF:
Executive Director of Resources

Contact officer and telephone no:
Martin Sanders Service Management and Governance Manager
Martin.Sanders@enfield.gov.uk
Farooq Shah Head of Information Management and Technology
Farooq.Shah@enfield.gov.uk

1. EXECUTIVE SUMMARY

1.1. This report is the first annual Cyber Security report setting out a review of activities to date in 2019/20, risks and proposed remediation.

1.2. The report has been compiled using Industry Standard Reporting tools and evidence from companies in that sector.

1.3. There has been a worldwide increase of 140% in the past year in cyber attacks and this has been reflected within Enfield Council.

1.4. We have been successful in thwarting these attacks, but as these attacks become more sophisticated and are created and distributed using software rather than individuals, then the capacity and methods to thwart these attacks must change.

1.5. To maintain statutory compliance and to remain secure, the products and tools used need upgrading, replacing and new tools introduced.

1.6. The whole council needs to remain vigilant and awareness needs to be raised and supported by training.

1.7. The existing ICT security resources need reviewing to support the additional tools and increased threat.

2. RECOMMENDATIONS

2.1 Recognise and accept the risks and findings in this report

2.2 To support the delivery of existing projects in place due to conclude in March 2020 and those in the pipeline for June 2020

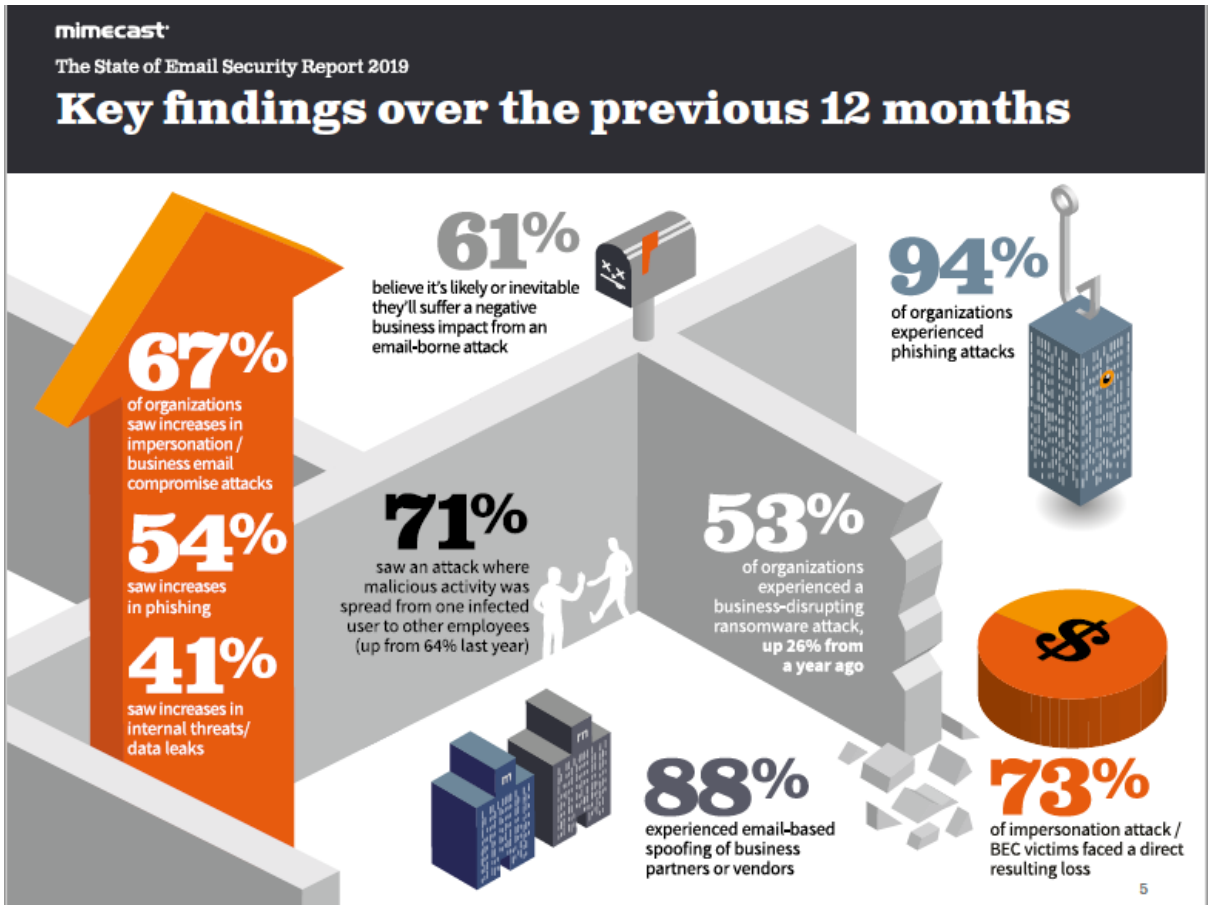
2.3 To note the proposal to address the key risks from June 2020 and for annual updates to this Committee

3. BACKGROUND

3.1 Scale of the challenge:

A 2019 Study from computer and network security company eSentire has found that cyber-attacks in the UK spiked by a colossal margin over the course of last year. According to the study, Britain was stung by 140% more cyber-attacks than the previous year, something driven chiefly by a global increase in botnet activity. This increase in attack traffic also caused nearly 40% of small and medium enterprises in the UK to experience at least one cybersecurity incident.

Research firm Vanson Bourne conducted a Mimecast-commissioned global survey of IT departments across different organisations to gain useful insights into the current state of email security. Data was collected from December 2018 through February 2019 across the US, UK, Germany, Netherlands, Australia, South Africa and United Arab Emirates.



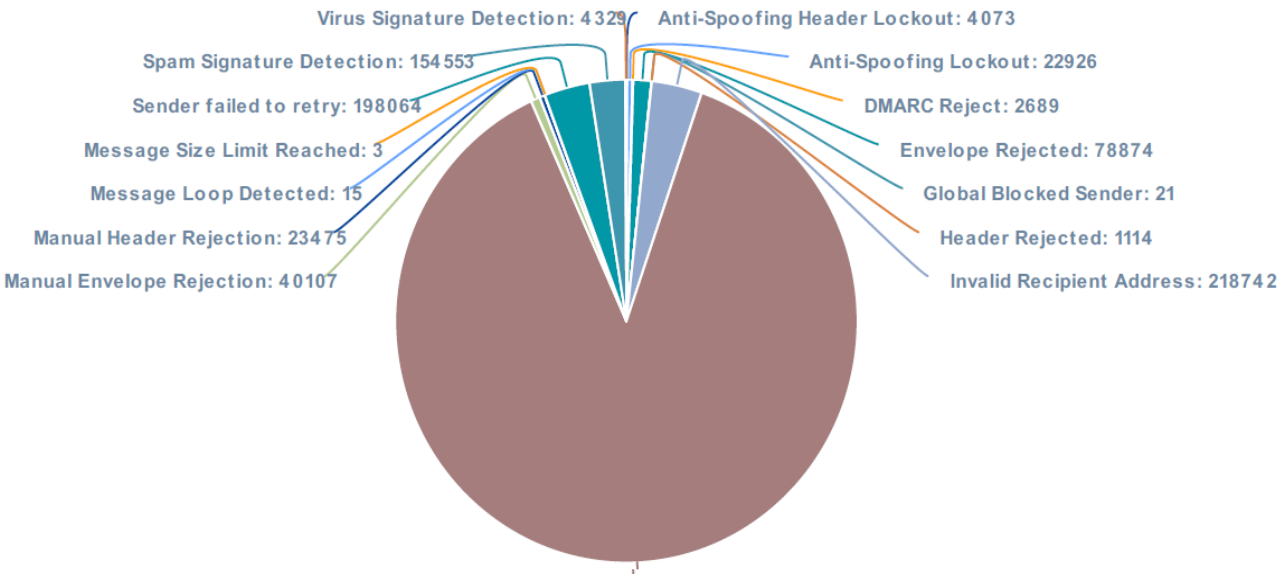
We have noticed this trend and have been successful in thwarting those attacks, however, with the increased volume and the complexity of these attacks, the potential for successful breach has also increased.

3.2 Enfield Annual Security Incidents Trends

Email Stats From 25 March 2019 To 31 Dec 2019

Month-Year	Total Inbound Email	Rejections (includes viruses & spam)	Legit Inbound Email	% Rejections	Total Outbound Email	Total Internal Email
Mar - 2019	186,601	104,441	82,160	55.97 %	100,342	3,859
Apr - 2019	1,296,902	724,399	572,503	55.86 %	340,573	33,582
May - 2019	1,246,949	631,480	615,469	50.64 %	370,368	35,416
June - 2019	1,183,560	585,366	598,194	49.46 %	360,520	28,411
July - 2019	1,309,342	657,545	651,797	50.22 %	387,587	29,527
Aug - 2019	1,346,116	801,210	544,906	59.52 %	312,076	26,712
Sep - 2019	1,407,580	763,699	643,881	54.26 %	400,539	27,443
Oct - 2019	1,506,724	781,580	725,144	51.87 %	439,985	28,302
Nov - 2019	1,092,009	417,743	674,266	38.25 %	405,190	26,197
Dec - 2019	1,301,180	758,665	542,515	58.31 %	378,450	22,764
Total	**11,876,963**	**6,226,128**	**5,650,835**		**3,495,630**	**262,213**
Mean	**1,187,696.25**	**622,612.81**	**565,083.5**	**52.44 %**	**349,563**	**26,221.3**

Types of Rejection



Incident Reports:

Incident Type	*2018*	*2019*
Total Reported Incidents	**128**	**141**
Disclosure in error	**49**	**60**
Lost data / hardware	**23**	**27**
Emails (Spear phishing / Spoofing)	**38**	**37**
Physical Security Failure	**1**	**1**
Stolen data / hardware	**3**	**5**
Technical failure	**13**	**5**
Unauthorised Access	**1**	**4**
Others (process/procedure/Training)	**0**	**2**

3.3 Cyber Security project in 2019

3.3.1 Social Engineering and phishing attacks (Completed)

Social Engineering and phishing attacks are on the rise, varied and more sophisticated. A large portion of the ICT Security team's time is now occupied managing phishing attacks, which requires activities across all the ICT Service Functional Towers (FTs) to contain risks in timely manner.

The team has been proactive for a long-time providing user awareness guidance, engaging users via internet and display TV screens located throughout the council but more needs to be done. We have created Phishing Awareness Training and agreed at the Information Governance Board that we would use our Data Protection Officer to run a Face-to-Face (F2F) training for likely targeted teams (e.g. Finance) and Senior Managers (whaling attack).

3.3.2 Multi Factor Authentication (being introduced in spring 2020)

The existing method of security control we use to access systems is by a username and password. This is susceptible to password cracking and brute force attacks leaving the Council's cloud based infrastructure at risk.

Multifactor Authentication (also known as Two-Step verification) is a multi-layered security approach. By requiring multiple authentication factors such as username and password plus One Time Pass (OTP) will present a significant challenge for attackers. Even if an attacker manages to learn the user's password, it is useless without also having possession of the additional authentication method. This follows the approach of:

- Something you know (typically a password)
- Something you have (a trusted device that is not easily duplicated, like a phone)
- Something you are (biometrics)

To combat the risks posed to the cloud solution the Authority uses, rolling out Multi-Factor Authentication solution for all users is highly recommended.

3.3.3 Email Spoofing (completed)

The council has implemented measures to reduce email spoofing for the enfield.gov.uk domain. This helped reduce the overall number of spoofed emails that came through; however, users are still being fooled by simple measures such as using the display name as was the case when the Council's payroll department were contacted by an external email showing the same name as an executive Director of the council requesting change of bank salary bank account. This simple attack has been successful and highlights the need for an awareness drive to ensure they are recognised as such.

3.3.4 PSN (Public Services Network) Certification (March 2020)

The Public Services Network is a closed private network used by public sector bodies to exchange information securely. The council's IT systems are complex and require continuous updating, patching and vulnerability management throughout the year to maintain compliance to the PSN certification.

One of the main issues in achieving PSN re-certification is the use of unsupported services and software packages. The Council is currently running several services and packages using software that is outdated and not maintained or supported. As these applications are no longer updated or patched, they expose the Council to risks and threaten our compliance with PSN, which does not allow unsupported software.

ICT are collaborating with services using these applications to get replace them, but by their nature, there are multiple factors which affect the ability to replace these quickly and progress is slow.

ICT had put in place some mitigations in terms of firewalling and access control as part of the Remediation Action Plan (RAP). However, these are temporary measures and can only provide limited assurance and still pose a significant risk.

For the current PSN re-certification, ICT in collaboration with the cabinet office's PSN department is working on delivering compliance. To achieve recertification, the Council must carry out five main tasks which includes getting an external company to carryout IT Health Check (ITHC). Any risk found as part of that health check that falls under Critical or High category would result in an automatic PSN recertification failure.

Both an Onsite ITHC and an Offsite Penetration Test (Pen Test) found 0 critical vulnerabilities and 53 High vulnerabilities, which affected 1600 different applications and devices.

- 50% of those vulnerabilities are on old, end of life desktops, which are in the process of being replaced;

- 10% of these are on end of life, unsupported applications such as our Customer Relationship System (LAGAN).

- Five categories of non-compliance covering 254 different devices and applications are currently in progress to completed in March 2020

- To date, we have brought into compliance 20 out of the 53 distinct high vulnerabilities covering over 40 applications and systems.

We are in a continuous communication with the cabinet office and are working with them on our Remediation Action Plan (RAP) with a view of achieving re-certification once we have either eliminated all risks deemed high or provided a containment plan to any risks we cannot wholly eliminate due to legitimate business needs.

3.3.5 PCI (Payment Card Industry) Compliance (Completed)

We have achieved PCI re-certification ahead of schedule this year in August 2019. Going forward, the changes in the cashier’s office and the mode of payment that is currently in consideration for card processing will reduce the risks of failure in the future.

3.3.6 Active directory clean-up (June 2020)

Active Directory (AD) is a Microsoft technology used to manage users account information, credentials, groups, printers and other peripherals on a network. Over the years, the Active Directory has become bloated with a lot of inherited objects which could potentially cause security problems for the infrastructure.

There is currently an active remediation project in flight to clean up and review, disable and delete stale AD objects such as:

- Users
- Computers
- Groups
- Organisation Unit
- Unused/Unlinked Group Policy Objects

Completion of this project will provide some assurance on the security of the systems that control user/object access to the systems.

NEXT STEPS

4.1 Projects in the Pipeline

4.1.1 Firewalls (June 2020)

The authority is currently running over 80 Firewalls with over 10,000 rules, governing what is allowed in and out of the network. This not only impacts the performance of devices, but where new rules have been added to meet service requests, obsolete ones were not removed which may expose the network to additional risks.

To avoid conflicting rules, identify vulnerabilities and meet auditing and compliance mandates, there is a need for a project to review all firewall rules and justify existence of each rule in place.

4.1.2 Geolocation locking (April 2020)

We are seeing a high number of brute force attacks against user accounts from foreign countries.

By setting Conditional access control using Geolocation, we can be assured that user logins can only happen within a specified set number of countries. The EU General Data Protection Regulation (GDPR) restricts transfers of personal data to countries outside the EEA therefore, this solution will also help with the GDPR requirements for data protection.

4.2 Proposal to address the key risks (June 2020)

The current security set-up is based on a reactive model, where threats that penetrate our environment are identified by manual process and this opens us up for risk as by the time we identify risks it may be too late.
We are now moving to a more proactive monitoring model where we will implement

intelligent tools to constantly monitor and protect our networks. This will include:

- Incident Management software: e.g. if your password is compromised, we must resolve this manually, this software would report and resolve it more quickly and accurately.
- Active Threat hunting: e.g. this software searches for and mitigates threats that we haven't seen before and provides reports on incidents and remediation undertaken
- Protection from ransomware attacks such as unauthorised data changes or deletion
- Governance Risk and Compliance: Software that measures our estate against the compliance standards (e.g. PSN, PCI and GDPR) and reports where non-compliant.

We are also reviewing the resources required in the ICT Security Team to deal with the increased volume of threats which also impact on statutory and audit security compliance and project delivery where security issues need addressing.

5 ALTERNATIVE OPTIONS CONSIDERED

5.1 Do Nothing

Not considered, Enfield would lose its' statutory compliance certifications and put it's entire network and services at risk

5.2 Increase staff resources without changing it's approach to tools and software

The increasing number and nature of security threats cannot be resolved by increased staffing alone, new products that identify, isolate and resolve risks are also required.

6 REASONS FOR RECOMMENDATIONS

6.1 The proposed approach is adopted by leading ICT organisations building on the existing security and compliance approach, but recognising that the increasing volumes and types of cyber security threats require an approach that increases and makes use of industry standard tools to protect an organisation of our size and type.

6.2 Failure to implement these changes will result in the organisation being non-compliant with the Public Services Network(PSN) and Payment Card Industry (PCI) meaning that we will not be able to share data with other public sector organisations or take on line payments.

6.3 In addition, the existing software and infrastructure will be unable to keep pace with cyber security threats making the entire council network vulnerable to attack.

7 COMMENTS OF AND OTHER DEPARTMENTS

Not applicable.

8 KEY RISKS

8.1 There are multiple sources of payment processing solutions the authority uses some of which are not properly managed within PCI framework potentially

leading to noncompliance.

8.2 Over stretched ICI Security team and increased demand from the business will weaken the security position of the council.

8.3 Security risk awareness among staff is low

8.4 Increased ransomware attacks pose direct risk to the authority's systems

8.5 End of life software that is still in use

9 IMPACT ON COUNCIL PRIORITIES

- Good homes in well-connected neighbourhoods
- Build our Economy to create a thriving place
- Sustain Strong and healthy Communities

9.1 Managing Cyber Security well contributes to the Council's ability to address the values set out within the Council's priorities

10 PERFORMANCE MANAGEMENT IMPLICATIONS

Not applicable.

11 EQUALITIES IMPACT IMPLICATION

11.1 The Council is committed to Fairness for All to apply throughout all work and decisions made. The Council serves the whole borough fairly, tackling inequality through the provision of excellent services for all, targeted to meet the needs of each area. The Council will listen to and understand the needs of all its communities.

Please see Appendix Attached

Appendix

Key Threats:

- **Phishing:**

  Scammers will convince users to click on misleading links to provide sensitive information or company data, or even download content to their computer or server.

- **Malware:**

  If a victim of phishing does end up initiating a download, there's a good chance that the program received is harmful or malicious and comes in various forms, tasked with anything from spying on the system to manipulating its code.

- **Distributed Denial of Service (DDoS):**

  Floods the server with requests from multiple sources, leading it to become overwhelmed to the point of slowing down substantially or even crashing.

- **Brute Force or Password Attacks:**

  These threats involve an attacker attempting to gain access to a network by using a program to ascertain a working password.

- **Ransomware:**

  This is a type of malware that, when opened, encrypts the system so that no one can use it anymore. The computer or server affected will remain locked until a hefty ransom is paid to get the encryption key to unlock the system.

Security Controls in place:

- **Email protection:**
  Mimecast includes - email protection and back up of email in the cloud to protect from phishing and malware

- **Mobile Device Management: (Mobile phones)**
  Lookout - mobile security to protect from phishing, malware and ransomware. The increasing volume of mobile devices require additional licences.

- **Microsoft Azure Cloud:**
  Microsoft Security Centre: Azure disk Encryption: Azure Cloud APP Security: Advance Treat Protection: Backup and Site Recovery: AZURE Key Vault: AZURE PIM: Threat Intelligence (Dark Trace): Making use of treat feeds to detect malicious intrusion and data exfiltration to command and control servers. These all protect from Distributed Denial of Service, Ransomware, Brute Force or Password Attacks as well as provide Disaster Recovery protection. However, as threats increased and the amount security applications increase, we require more resource to operate them

- **Managed Clients – Device Endpoint Protection (e.g. laptops, desktops, servers)**
  System Centre Configuration manager: Microsoft Defender: Threat Analytics: Windows 10 Enterprise Security. These protect against all the above risks. These

products regularly become outdated as threats change and need replacement and updating more frequently than we have existing budget and resources to do.

- **Hybrid Security Solutions (e.g. Working from Home, 3rd Party sites, on site connectivity)**
  Firewalls: Directs Access VPN: Fortinet VPN: Express Route (Direct Connection to Azure): Log Management: Pen Testing: Vulnerability Scanning. These protect from Distributed Denial of Service (DDoS) and Brute Force or Password Attacks. Products such as Direct Access and Remote Desktop Access that we use to work from home become out of date and therefore stop working with our protection and have to be replaced.

List of Security controls in place to address known threats and compliance requirements

Area	Tools	Outstanding Risks	Phishing	Mal-ware	DDoS	Brute Force	Ransom-ware	Compliance
Email protection	Mimecast	The license type has limitations that would not allow archiving and investigations beyond 30 days	Y	Y			Y	Y
Mobile Device Management	Lookout - mobile security	The number of licences is insufficient for the estate.	Y	Y			Y	Y
Microsoft Azure Cloud	Microsoft Security Centre	No. of applications increased and need more Computing, Storage and FTE resources to monitor alerts			Y	Y	Y	
Managed Clients – Device EndPoint Protection	System Centre Configuration manager: Microsoft Defender & MDM	These products become outdated quickly and need replacement and updating frequently	Y	Y	Y	Y	Y	Y
Hybrid Security Solutions	Firewalls, Direct Access, VPN, Fortinet, Proxy	Direct Access/ Remote Desktop Access that we use to work from home become out of date and stop working with our protection and have to be replaced			Y	Y	Y	Y
Vulnerability management	Tenable.io	Initial phase of review						Y
Protective Monitoring / Compliance (e.g. PSN)	Caretower Managed Service via McAfee SIEM	All LBE kit should be onboarded for monitoring but are not now. A resource is (Appliances and FTE) required to on-board all LBE Kit						Y
Multifactor Authentication	Microsoft MFA	This has not been rolled out to all users				Y		Y
Geolocation locking	Microsoft Azure Security	Access from countries we do not do business with increase the risk						