| CYNGOR SIR YNYS MÔN | |
|---|---|
| Adroddiad i: | Pwyllgor Archwilio a Llywodraethu |
| Dyddiad: | 3 Rhagfyr 2019 |
| Pwnc: | Adroddiad Blynyddol Diogelwch Seiber 2019 |
| Pennaeth Gwasanaeth | Carys Edwards, Pennaeth Proffesiwn AD a Thrawsnewid<br>(01248) 752502<br>CarysEdwards@ynysmon.gov.uk |
| Awdur yr Adroddiad: | Lee Evans, Rheolwr y Gwasanaeth TG a Rheoli Perfformiad<br>(01248) 752526<br>LeeEvans@ynysmon.gov.uk |
| **Natur a Rheswm dros Adrodd:**<br><br>Mae'r adroddiad yn caniatáu i'r Pwyllgor fonitro trefniadau'r Cyngor wrth liniaru Bygythiadau Seiber ac yn rhoi manylion am weithgareddau monitro a gweithgareddau sicrwydd eraill sy'n ymwneud â'r maes hwn. | |

## 1. Rhagarweiniad

Mae'r adroddiad hwn yn darparu gwybodaeth sy'n ymwneud â'r Bygythiadau Seiber sy'n wynebu'r Cyngor a sut mae'r Adain Technoleg Gwybodaeth yn gweithredu i'w lliniaru.

## 2. Argymhelliad

Nodi'r sicrwydd a ddarperir yn yr adroddiad.

CYNGOR SIR
YNYS MÔN
ISLE OF ANGLESEY
COUNTY COUNCIL

Adain TG
IT Division

## Adroddiad Blynyddol

# DIOGELWCH SEIBER 2019

**SWYDDOGOL**


Desg Gymorth TG / IT Service Desk
Cyngor Sir Ynys Môn / Isle of Anglesey County Council
(01248) 752525
DesgGymorthTG@ynysmon.gov.uk ITServiceDesk@anglesey.gov.uk
http://monitor.ynysmon.gov.uk/tgch http://monitor.anglesey.gov.uk/ict


SHORTLISTED SCDI IT SERVICE & SUPPORT AWARDS Best Small Service Desk 2017

OUTSTANDING ACHIEVEMENT SCDI IT SERVICE & SUPPORT AWARDS Most Improved Service Desk 2017

CYBER ESSENTIALS PLUS

# Adroddiad Blynyddol Diogelwch Seiber 2019

## 1. CEFNDIR

Mae adroddiadau am ymosodiadau seiber wedi dod yn gyffredin yn y newyddion ac mae ymosodiadau proffil uchel yn digwydd bob wythnos a hyd yn oed yn bob dydd. Yr enghraifft fwyaf adnabyddus oedd yr ymosodiad gan y feddalwedd wystlo o'r enw 'WannaCry' ar y Gwasanaeth Iechyd Gwladol. Ar y gorau, mae ymosodiadau o'r fath yn erydu ymddiriedaeth gwasanaethau a chwsmeriaid ac yn achosi difrod i enw da, ac ar y gwaethaf gallant barlysu sefydliad a'i rwystro rhag darparu gwasanaethau hanfodol.

Mae ymosodiadau seiber yn amrywio o ran eu dull a'u cymhlethdod ond maent yn gyson yn eu hamcan, sef creu anhrefn, difrodi neu ddwyn.

Diogelwch Seiber yw'r arfer o amddiffyn systemau cyfrifiadurol rhag bygythiadau seiber a diogelu cyfanrwydd, cyfrinachedd ac argaeledd y wybodaeth a gedwir gan y sefydliad.

Fel yn achos unrhyw sefydliad sydd wedi ei gysylltu â'r Rhyngrwyd, mae rhwydwaith y Cyngor o dan ymosodiad cyson 24 awr ac mae swmp a sylwedd y data personol sensitif a gedwir gan y Cyngor yn golygu bod raid lleihau'r risg o ymosodiadau llwyddiannus gymaint ag sy'n rhesymol bosib. Mae'r perygl o ymosodiadau seiber yn cael ei gydnabod gan y Cyngor a'i gofnodi yn y Gofrestr Risg Gorfforaethol sy'n cael ei monitro gan yr Uwch Dîm Arweinyddiaeth (UDA).

Mae'r adroddiad hwn yn crynhoi'r Bygythiadau Seiber y mae'r Cyngor yn eu hwynebu a rhai o'r mesurau lliniaru y mae'r Cyngor wedi ei sefydlu. Un o egwyddorion allweddol diogelwch seiber effeithiol yw "diogelwch trwy guddio", felly dim ond trosolwg lefel uchel y bydd yr adroddiad yn ei roi ac ni fydd yn manylu ar y technolegau neu'r cynhyrchion a ddefnyddir.

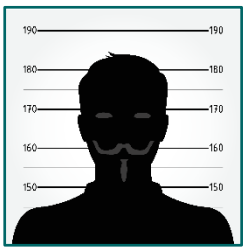
## 2. PWY YW'R YMOSODWYR POSIB?

Fel sy'n wir yn achos pob sefydliad, mae ymgeision i ymosod yn dod o wahanol ffynonellau ac yn amrywio o ran dull a chymhelliant. Maent yn disgyn i'r categorïau eang isod;

### Troseddwyr

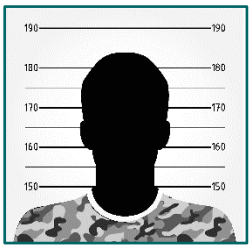

Wedi'u hysgogi gan elw ariannol yn unig. Mae seiberdroseddu yn caniatáu i droseddwyr weithredu'n rhyngwladol ac yn ddienw, ac mae'n ffordd risg isel o fedru dwyn o gymharu â throseddau traddodiadol, a gallai'r enillion fod yn llawer uwch. Mae'r gost isel o'u sefydlu yn golygu y gall troseddwyr lansio ymosodiadau ar filoedd o ddioddefwyr posib a dim ond nifer fach o lwyddiannau sydd eu hangen arnyn nhw i sicrhau enillion ariannol mawr.

### Hacwyr ymgyrchu a Cheiswyr Bri




Unigolion neu grwpiau o ymosodwyr sy'n cyflawni eu gweithgareddau maleisus i hyrwyddo agenda o'u dewis. Gall ymosodiad o'r fath gynnwys amharu ar argaeledd system neu "hagru" gwefannau corfforaethol a chyfryngau cymdeithasol gyda neges a ddewiswyd gan yr ymosodwyr – gallai'r neges fod yn bwnc gwleidyddol, cred grefyddol neu ideoleg gymdeithasol neu hyd yn oed dim ond i ddangos eu gallu technegol i'w cymheiriaid.

### Gwladwriaethau Tramor




Grwpiau a noddir gan wladwriaethau. Cynghorau Lleol yw'r Porth i'r llywodraeth ganolog a gwasanaethau cyhoeddus hanfodol. Mae gan ymosodwyr a noddir gan wladwriaethau amcanion penodol sy'n cyd-fynd â buddiannau gwleidyddol, masnachol neu filwrol y gwledydd y maent yn hanu ohonynt. Mae'r mathau hyn o ymosodiadau yn hynod soffistigedig ac yn anodd eu darganfod. Mae'r Ganolfan Diogelwch Seiber Genedlaethol wedi cyhoeddi cyngor sy'n nodi bod y risg o ymosodiad gan y grwpiau hyn yn real, yn enwedig ar adegau pan gynhelir digwyddiadau cenedlaethol mawr fel etholiadau.

### Bygythiadau mewnol


Mae bygythiad o'r fath i ddiogelwch neu ddata sefydliad yn dod o'r tu mewn iddo. Daw'r math hwn o fygythiad gan weithwyr neu gyn-weithwyr, ond gall hefyd ddeillio o drydydd partïon, gan gynnwys contractwyr, gweithwyr dros dro, gweithwyr parhaol neu gwsmeriaid. Dywedir yn eang bod 50% o'r achosion gwaethaf o danseilio diogelwch gwybodaeth yn digwydd trwy gamgymeriad anfwriadol gan unigolion, megis agor e-bost maleisus.

## 3. BETH YW'R BYGYTHIADAU SEIBER?

# Maleiswedd

Ymadrodd ymbarél yw maleiswedd neu "feddalwedd faleisus" sy'n disgrifio unrhyw raglen neu gôd maleisus sy'n niweidiol i systemau.

Mae Maleiswedd yn ceisio difrodi neu anablu cyfrifiaduron, gweinyddwyr, rhwydweithiau a dyfeisiau cyfrifiadurol eraill.

Mae enghreifftiau yn cynnwys Firysau, Ceffylau Pren Troea, Meddalwedd Wystlo a Chofnodwyr Bysellau;

**1879**

**o ymosodiadau maleiswedd wedi eu rhwystro**

### Firysau

Y math mwyaf adnabyddus o Faleiswedd. Mae firysau yn bennaf yn ceisio amharu ar system neu ddinistrio data. Maent yn ymledu o gyfrifiadur i gyfrifiadur trwy rwydweithiau, e-bost a chyfryngau symudol. Gall haint firws ddigwydd trwy i'r dioddefwr redeg ffeil faleisus neu dim ond trwy roi cofbin i mewn i ddyfais.

### Meddalwedd Wystlo

Math o feddalwedd yw hon sy'n amgryptio ffeiliau'r dioddefwr. Ar ôl atal mynediad i ddata'r dioddefwr, mae'r ymosodwr wedyn yn mynnu bod y dioddefwr yn talu pridwerth cyn y bydd yr ymosodwr yn adfer mynediad i'r data.

Mae'r feddalwedd yn dangos cyfarwyddiadau ar sut y gall y dioddefwr dalu'r pridwerth ac yn aml maent yn cynnwys rhif cymorth lle rhoddir "help" i gyflawni'r trafodiad. Gall yr anhrefn a achosir ddod â sefydliad i stop stond a gall cost y pridwerth fod cymaint â degau o filoedd o bunnau heb fawr o siawns mewn gwirionedd i'r troseddwyr gael eu dwyn o flaen eu gwell.

### Cofnodwyr Bysellau

Math o feddalwedd yw hon sy'n cael ei gosod ar gyfrifiadur dioddefwr heb yn wybod iddynt ac sy'n cofnodi trawiadau bysellau dros gyfnod o fisoedd neu hyd yn oed flynyddoedd. Mae'r wybodaeth a gesglir yn cael ei throsglwyddo yn ôl i'r ymosodwr dros y Rhyngrwyd a byddant yn hidlo'r wybodaeth i chwilio am fanylion mewngofnodi, cyfrineiriau a gwybodaeth am gardiau credyd a ddefnyddir wedyn i hwyluso troseddau ariannol.

**781**

**o fathau o faleiswedd wedi eu rhwystro bob mis**

### Ceffylau Pren Troea

Mae'n edrych fel meddalwedd ddefnyddiol sydd ddim yn faleisus er mwyn iddi gael ei gosod yn ddiniwed gan ddioddefwyr ar eu cyfrifiaduron. Bydd yn lawrlwytho mathau eraill o faleiswedd heb yn wybod megis meddalwedd cofnodi bysellau neu feddalwedd wystlo a heb unrhyw arwyddion amlwg a fyddai'n codi amheuaeth.

## Lliniaru

**Meddalwedd Gwrth-Faleiswedd**

Mae holl gyfrifiaduron a gweinyddwyr y Cyngor yn gweithredu meddalwedd gwrth-faleiswedd sy'n sganio am nodweddion codau maleisus hysbys ac sy'n rhwystro mynediad os darganfyddir rhai.

Mae yna sawl ffynhonnell bosib o ymosodiad trwy feddalwedd faleisus ac mae'r rhain yn cynnwys; atodiadau e-bost, gwefannau maleisus a chyfryngau symudol.

**Hidlo E-byst**

Mae'r holl atodiadau e-bost a dderbynnir gan y Cyngor yn cael eu dadansoddi i ddarganfod a ydynt yn faleisus.  Mae unrhyw fathau o ffeiliau y gwyddys y gallant fod yn beryglus naill ai'n cael eu blocio neu eu glanhau'n awtomatig fel bod unrhyw "gynnwys gweithredol" yn cael ei ddileu.

Mae'r Cyngor hefyd wedi tanysgrifio i wasanaeth sy'n sicrhau bod e-byst o ffynonellau maleisus hysbys yn cael eu blocio'n awtomatig.


**980 o wefannau amheus yn cael eu rhwystro bob mis**

.

**Hidlo Cynnwys y We**

Mae'r Cyngor wedi tanysgrifio i Wasanaeth Datrys Enw Parth Amddiffynnol y Ganolfan Seiberddiogelwch Genedlaethol (NCSC).

Yn syml, mae hyn yn golygu bod unrhyw gyfeiriad gwe y mae cyfrifiaduron y Cyngor yn ymweld ag ef yn cael ei wirio yn erbyn rhestr o wefannau maleisus hysbys a rhwystrir mynediad os bydd angen.

Yn ogystal, mae'r Cyngor yn defnyddio gwasanaeth hidlo cynnwys y we i rwystro mynediad i wefannau annymunol fel Gemau, Hapchwarae, Pornograffi a gweithgaredd Anghyfreithlon.

**Cyfryngau Symudol**

Yn hanesyddol bu cyfryngau symudol fel Cryno Ddisgiau a Chofbinnau yn ffordd gyfleus a rhad o drosglwyddo data. Fodd bynnag, gellir eu defnyddio hefyd i ymledu maleiswedd o un rhwydwaith i'r llall ac mae'n hawdd eu colli hefyd, gan arwain at dorri rheolau diogelwch data. Mewn ymateb i'r risg hon mae'r Cyngor wedi rhoi'r gorau i ddefnyddio Cofbinnau ar gyfrifiaduron y Cyngor ac eithrio ar gyfer nifer fach o bobl lle mae achos busnes digon cryf dros wneud hynny.

# Gwendidau mewn Meddalwedd

Diffygion neu fylchau mewn côd meddalwedd yw'r rhain ac os yw ymosodwr yn gwneud yn fawr ohonynt gallant beri i'r feddalwedd ymddwyn mewn modd annymunol ac annisgwyl, er enghraifft caniatáu i ymosodwr gael mynediad i'r system o bell a heb ganiatâd.

Os yw'r feddalwedd yn gyfredol ac yn dal i gael ei chefnogi gan y cyflenwr, mae pecynnau côd sydd wedi'u cywiro, sef "diweddariadau" neu "drwsiadau" ar gael i fynd i'r afael â'r gwendidau hyn ac i gau'r bwlch diogelwch posib. Yn dibynnu ar y feddalwedd, gallai fod yn broses faniwal i ddiweddaru pob dyfais neu efallai y bydd modd rheoli'r broses yn ganolog.

## Lliniaru

**Mabwysiadu Windows 10 yn fuan**

Er mwyn manteisio ar ei nodweddion diogelwch gwell, fe wnaeth y Cyngor benderfyniad strategol sawl blwyddyn yn ôl i uwchraddio pob cyfrifiadur personol neu liniadur i Windows 10. Amlygodd y prosiect hwn fod yna lawer iawn o feddalwedd gwaddol nad oedd bellach yn cael ei diweddaru gan y cyflenwr ac roedd hynny'n risg bosib i'r dyfodol. Penderfynwyd cael gwared ar y feddalwedd honno a lleihau faint o feddalwedd yr oedd angen ei diweddaru yn gyffredinol.

**Rhithioli Cymwysiadau**

Yn draddodiadol, gosodwyd meddalwedd cymwysiadau ar bob cyfrifiadur neu liniadur ac 'roedd yn faich sylweddol i reoli diweddariadau diogelwch meddalwedd. Wrth i Windows 10 gael ei gyflwyno, penderfynwyd symud i ffwrdd o'r model hwn i "rithioli cymwysiadau". Yn syml, mae hyn yn golygu bod prif gopi ar gyfer yr holl gymwysiadau sy'n rhedeg ar weinydd canolog. Mae pob un o'r cyfrifiaduron neu'r gliniaduron yn cyrchu'r copi canolog hwn o'r feddalwedd sy'n golygu mai dim ond un copi y mae'n rhaid ei gadw'n gyfredol a'i reoli.

**Cynnal Prawf ar Wendidau**

Yn unol â gofynion Swyddfa'r Cabinet a'r diwydiant, mae'r Cyngor yn trefnu i "hacwyr moesegol" trydydd parti gynnal prawf i asesu pa mor fregus yw rhwydwaith y Cyngor. Mae'r broses hon yn nodi unrhyw feddalwedd sydd wedi dyddio, sydd heb ei thrwsio ac sy'n peri risg. Yna mae'r feddalwedd a amlygwyd naill ai'n cael ei diweddaru neu fe roddir y gorau i'w defnyddio.

# Bygythiadau Mewnol

Yn ôl McAfee, mae 43% o ddigwyddiadau seiber yn cael eu hachosi gan Fygythiadau Mewnol - gellir categoreiddio'r rhain fel gweithredoedd damweiniol gan staff, gweithredoedd maleisus gan staff neu weithredoedd gan gontractwyr.

Mae llawer o'r bygythiadau a drafodwyd yn yr adroddiad hwn wedi bod yn dechnegol eu naws, ond mae llwyddiant yr ymosodiadau hynny fel arfer yn dibynnu ar fod unigolyn yn clicio dolen faleisus, yn agor atodiad maleisus, yn datgelu cyfrinair neu ryw weithred arall.

## Lliniaru

**Hyfforddiant Diogelwch Seiber**

Er mwyn sicrhau bod staff yn ymwybodol o'r risgiau sy'n gysylltiedig â Bygythiadau Seiber, chwaraeodd y Cyngor ran flaenllaw gyda chaffael pecyn E-Ddysgu dwyieithog, Cymru Gyfan ar Ymwybyddiaeth Seiber.

Defnyddiwyd y modiwl Ymwybyddiaeth Seiber ar blatfform e-Ddysgu'r Cyngor ac mae'r Uwch Dîm Arweinyddiaeth wedi gorchymyn bod yn rhaid i'r holl staff sy'n defnyddio offer TG gwblhau'r modiwl hwn.

**Safon Diogelwch Safonol ar Gyfer Staff (BPSS)**

Rhaid i'r holl staff sydd â mynediad at ddata SWYDDOGOL-SENSITIF sy'n deillio o swyddfa'r cabinet fynd trwy'r broses BPSS sy'n ei gwneud yn ofynnol iddynt gynhyrchu prawf adnabod, prawf cenedligrwydd a chael eu gwirio gan y Gwasanaeth Datgelu a Gwahardd.

**Cytundebau Prosesu Data**

Mae'n ofynnol i bob contractwr sydd naill ai'n cynnal systemau TG y Cyngor neu sydd â mynediad o bell i systemau TG y Cyngor lofnodi Cytundeb Prosesu Data (CPD).

Mae'r CPD yn amlinellu cyfrifoldebau'r contractwr o ran Diogelwch Seiber ac mae hefyd yn golygu bod raid iddynt, yn unol â'r gyfraith, dderbyn atebolrwydd ariannol llawn am unrhyw achosion o dorri rheoliadau a hawliadau am iawndal sy'n codi o ganlyniad i'w methiant i gydymffurfio.

**Cytundeb Polisi**

Mae gan y Cyngor bolisïau amrywiol ar waith ar gyfer defnyddio TG yn ddiogel, gan gynnwys Polisi Defnydd Derbyniol a Pholisi Diogelwch TG. Mae'r Polisi Defnydd Derbyniol a'r Polisi Diogelwch TG yn amlinellu cyfrifoldebau staff o ran amddiffyn diogelwch systemau TG y Cyngor ac mae'n orfodol bod yr holl staff sy'n defnyddio offer TG yn adolygu ac yn derbyn y polisïau hyn.

## Gwe-rwydo

Defnyddir y math hwn o ymosodiad i gael gwybodaeth ariannol neu wybodaeth gyfrinachol arall gan ddioddefwr. Gwneir hyn yn nodweddiadol trwy anfon e-bost sy'n edrych fel pe bai'n dod o sefydliad cyfreithlon fel banc ond sy'n cynnwys dolen i wefan ffug sydd yr un fath â'r un go iawn. Mae manylion mewngofnodi'r dioddefwr yn cael eu dal gan y wefan ffug wrth fewngofnodi a'u trosglwyddo i'r ymosodwr.

Tra bo ymosodiad Gwe-rwydo generig yn cael ei e-bostio i filoedd o ddioddefwyr posib ar y tro, mae math arall o We-rwydo o'r enw "Gwe-drywanu". Mewn ymosodiad Gwe-drywanu targedir sefydliad penodol neu hyd yn oed unigolyn ac felly bydd y wefan ffug a'r e-bost yn cael eu teilwra i edrych yn fwy cyfarwydd a chredadwy i'r dioddefwr. Er enghraifft, gall yr ymosodwr geisio dynwared Desg Gymorth TG y sefydliad.

### Lliniaru

**Hidlo E-byst a chynnwys y we**

Fel y nodwyd yn flaenorol, mae gan y Cyngor dechnoleg hidlo soffistigedig gyda'r nod o rwystro e-byst Gwe-rwydo a hefyd i rwystro'r gwefannau maleisus y maent yn ceisio dargyfeirio dioddefwyr atynt.

**Hyfforddiant Diogelwch Seiber**

Mae ffurfweddu systemau e-bost a systemau hidlo cynnwys y we yn gydbwysedd rhwng blocio cynnwys yr amheuir ei fod yn faleisus a sicrhau nad yw gweithgareddau busnes cyfreithlon yn cael eu rhwystro. Gyda hyn mewn golwg, mae'n anochel y bydd rhai negeseuon e-bost Gwe-rwydo yn dod drwodd ac mae'n hanfodol bod yr holl staff yn ymwybodol o Fygythiadau Seiber.

Fel y nodwyd yn flaenorol, rhaid i holl staff y Cyngor sy'n defnyddio offer TG gwblhau modiwl E-Ddysgu gorfodol ar Ymwybyddiaeth o Diogelwch Seiber. Mae gan y modiwl hwn adrannau penodol ar beryglon e-byst maleisus a Gwe-rwydo yn benodol. Mae staff hefyd yn adolygu'r Polisi Diogelwch TG sy'n nodi'r peryglon a ddaw yn sgil e-byst maleisus ac yn cofnodi eu bod yn derbyn y polisi.

## 4. PA SICRWYDD SYDD YN EI LE?

Mae'r rhan hon o'r adroddiad yn manylu ar rai o'r gwiriadau a wneir i sicrhau bod y camau amddiffyn sydd gan y Cyngor yn ddigonol i leihau'r risg o ymosodiad seiber llwyddiannus i lefel resymol.

## Achrediad PSN gan Swyddfa'r Cabinet

Rhwydwaith cyflym y Llywodraeth yw Rhwydwaith y Sector Cyhoeddus (PSN) a ddefnyddir gan y sector cyhoeddus i gyfnewid data mewn modd diogel. Gan fod y PSN i bob pwrpas yn caniatáu cysylltu â systemau Swyddfa'r Cabinet a'r Adran Gwaith a Phensiynau, rhaid i'r Cyngor gael asesiad annibynnol trwyadl bob blwyddyn. Mae methu â chyflawni'r safon Diogelwch Seiber ofynnol yn arwain at ddatgysylltu o'r rhwydwaith ac anallu i brosesu cymorthdaliadau budd-dal.

Mae'r Cyngor wedi llwyddo yn yr asesiad PSN blynyddol bob blwyddyn ers iddo ddod yn ofyniad.

## Cyber Essentials+ ac Achrediad IASME

Trwy raglen a ariennir gan Lywodraeth Cymru ac a reolir gan Gymdeithas Llywodraeth Leol Cymru, mae awdurdodau lleol wedi bod yn cynnal prawf ar eu trefniadau Diogelwch Seiber a llywodraethu gwybodaeth yn erbyn yr arfer gorau.

Ar ôl proses archwilio drwyadl, mae'r Cyngor yn un o ddim ond saith awdurdod yng Nghymru sydd wedi cyflawni safon Cyber Essentials Plus a'r Achrediad IASME llawn.

'Roedd yr achrediad yn cynnwys profion ar ddiogelwch yr holl systemau a dyfeisiau TG. 'Roedd y profion hyn yn debyg i ymosodiad seiber, ac yn ogystal fe gynhaliwyd archwiliad trylwyr ar y safle a oedd yn rhoi sylw i bolisïau diogelwch TG a pholisïau llywodraethu gwybodaeth a lle bu'n rhaid cael mewnbwn sylweddol gan gydweithwyr yn y meysydd Adnoddau Dynol a Llywodraethu Gwybodaeth.

## Archwilio Mewnol

Oherwydd bod bygythiadau seiber yn cael eu cofnodi ar y Gofrestr Risg Gorfforaethol, adolygir trefniadau'r Cyngor yn y maes hwn gan y Gwasanaeth Archwilio Mewnol. Yn ystod 2018/19 cynhaliodd y tîm Archwilio Mewnol adolygiad i sefydlu a oes gan y Cyngor "drefniadau amddiffyn, canfod ac ymateb digonol ar waith i liniaru'r risg i rwydwaith, systemau, gwybodaeth a gwasanaethau'r Cyngor yn sgil ymosodiad seiber".

O ganlyniad i'r adolygiad daethpwyd i'r casgliad bod gan y Cyngor nifer o reolaethau gweithredol effeithiol i reoli'r risg i Ddiogelwch Seiber ac i atal a lleihau'r effaith ar wasanaethau, systemau a gwybodaeth y Cyngor yn sgil ymosodiadau maleisus, allanol.

## 5. BETH YW'R HERIAU I'R DYFODOL

Hyd yn hyn, mae'r Cyngor wedi gallu dangos a rhoi sicrwydd bod mesurau rhesymol ar waith i reoli Bygythiadau Seiber i lefel dderbyniol. Fodd bynnag wrth i nifer a soffistigedigrwydd y bygythiadau hyn dyfu mae'r baich yn tyfu hefyd o ran;

- Ymchwilio i fygythiadau sy'n dod i'r amlwg a datblygu mesurau amddiffynnol
- Ariannu, gweithredu a monitro'r nifer gynyddol o dechnolegau amddiffyn rhag bygythiadau sydd raid wrthynt.
- Cydgysylltu â chydweithwyr diogelwch yn WARP a NCSC i rannu gwybodaeth.
- Adnoddau i ddatblygu polisïau, codi ymwybyddiaeth a monitro cydymffurfiaeth.

Nid yw'r heriau hyn yn unigryw i'r Cyngor a chedwir llygad ar yr adnoddau y bydd eu hangen a gwneir ceisiadau am arian ychwanegol fel y bydd angen.

## 6. ARGYMHELLIAD

Argymhellir nodi'r sicrwydd a roddir yn yr adroddiad.