HM Government

Strategaeth Seiberddiogelwch Llywodraeth

Adeiladu sector cyhoeddus seibergadarn

2022–2030

Cynnwys

Cynnwys

Rhageiriau Gweinidogol

Rhagair gan y

Prif Weinidog

Yn yr Adolygiad Integredig rwyf yn ei gwneud yn gwbl glir pa mor bwysig yw cydnerthedd cenedlaethol i ddiogelwch a ffyniant y DU. Mae seibergadernid yn hollol ganolog i hyn. Ychydig o wledydd sydd mewn lle gwell i ddelio â'r heriau hyn, ond rhaid i ni fod yn barod ac yn alluog i ymaddasu i'r byd newydd hwn sy'n codi o'n cwmpas. Mae ein Strategaeth Seiber Genedlaethol yn mynd i'r afael â hyn – yn egluro sut bydd y DU yn ymsefydlu'n gadarn yn bŵer seiber democrataidd a chyfrifol gyda'r gallu i amddiffyn a hyrwyddo ei buddiannau fel gwlad sofran mewn byd sy'n cael ei siapio'n sylfaenol gan dechnoleg.

Er mwyn gwireddu'r uchelgais hwn, fodd bynnag, rhaid i lywodraeth arwain drwy osod esiampl ei hun. Yn ogystal â sicrhau bod sefydliadau llywodraeth yn gallu amddiffyn y gwasanaethau a swyddogaethau sy'n cynnal ac yn hybu ein heconomi a'n cymdeithas, rhaid i lywodraeth fod yn batrwm i'r sector preifat, er mwyn sicrhau bod y DU yn parhau i hyrwyddo'r enw da sydd ganddi fel un o'r economïau mwyaf diogel a deniadol i fyw ynddi a gwneud busnes a buddsoddi ynddi.

Rhaid peidio â diystyru maint yr her, ond mae'n hollbwysig mynd i'r afael â hi. Dyna pam rwyf yn falch o gyflwyno yma Strategaeth Seiberddiogelwch Llywodraeth sy'n amlinellu sut byddwn yn sicrhau bod holl sefydliadau llywodraeth – ym mhob rhan o'r sector cyhoeddus – yn gallu gwrthsefyll yr holl fygythiadau seiber a wynebwn.

Neges gan

Ganghellor Dugiaeth Caerhirfryn a'r Gweinidog dros Swyddfa'r Cabinet

Sefydliadau llywodraeth – a'r swyddogaethau a gwasanaethau y maent yn eu cyflawni a'u darparu – yw conglfaen ein cymdeithas. Fodd bynnag, eu pwysigrwydd yw'r hyn sy'n eu gwneud yn darged deniadol i nifer cynyddol o wrthwynebwyr, sydd yn aml yn meddu'r math o alluoedd seiber grymus na fyddent ond ar gael i genedl-wladwriaethau hyd yn eithaf diweddar. Boed yn ymdrech i gael data llywodraeth er mantais strategol neu'n ymgais i darfu ar wasanaethau cyhoeddus er elw ariannol neu wleidyddol, mae'r bygythiad a wynebir gan lywodraeth yn un gwirioneddol ac uniongyrchol.

Caiff sefydliadau llywodraeth eu targedu'n gyson a di-baid: o'r 777 o achosion a reolwyd gan y Ganolfan Seiberddiogelwch Genedlaethol rhwng Medi 2020 ac Awst 2021, roedd tua 40% wedi'u hanelu at y sector cyhoeddus. Nid oes golwg bod y duedd gynyddol hon yn arafu.

Felly mae'n hollbwysig adeiladu a chynnal ein hamddiffynfeydd seiber os ydym i ddiogelu'r swyddogaethau a gwasanaethau rydym i gyd yn dibynnu arnynt. Fel llywodraeth, rydym wedi gwneud cynnydd mawr yn y blynyddoedd diwethaf, ond mae llawer i'w wneud eto. Er mwyn cwrdd â'r heriau a wynebwn yn y degawd nesaf rhaid i ni adeiladu ar ein llwyddiannau a thrawsnewid ein ffordd o ddelio â seiberddiogelwch mewn llywodraeth.

Mae Strategaeth Seiberddiogelwch Llywodraeth yn amlinellu sut byddwn yn gwneud hyn; drwy ddatblygu mwy o seibergadernid ar draws holl sefydliadau llywodraeth, a chydweithio er mwyn cydamddiffyn – gan greu grym amddiffynnol sy'n fwy nag a fyddai gennym wrth weithio ar wahân.

Mae rôl i bob rhan o lywodraeth wrth gyflawni hyn. Mae sefydliadau llywodraeth wedi cael pwerau priodol i reoli eu risgiau seiber – yn ogystal â harneisio gwybodaeth a dealltwriaeth lleol, mae hyn yn caniatáu arloesi ac ystwythder aruthrol. Er hynny, rhaid rhannu gwybodaeth ac arbenigedd o'r fath ar draws llywodraeth er mwyn gwella ein cydymateb, gyda rhagor a gwell galluoedd a gwasanaethau ar y cyd i wneud y dasg yn symlach ac yn fwyfwy effeithiol ac effeithlon. Mae'r strategaeth hon yn darparu'r fframwaith i hyrwyddo hyn.

Mae llywodraeth yn hollol benderfynol o gyflawni hyn. Mae'r ymrwymiad hwn wedi'i adlewyrchu yn Adolygiad Cynhwysfawr o Wariant 2021, gyda £2.6 biliwn wedi'i fuddsoddi mewn TG seiber ac etifeddol, sydd â seiberddiogelwch llywodraeth yn elfen hanfodol. Buddsoddir cyllid ychwanegol o £37.8 miliwn hefyd i ddelio â heriau seiberddiogelwch sy'n wynebu cynghorau lleol er mwyn gwarchod gwasanaethau a data hollbwysig, ochr yn ochr â buddsoddi wedi'i dargedu yn ein hadrannau mwyaf hanfodol.

Strategaeth uchelgeisiol ond angenrheidiol yw hon sy'n galw am weithredu ar draws llywodraeth. Rhaid i ni gwrdd â'n cyfrifoldeb i sicrhau bod swyddogaethau a gwasanaethau llywodraeth yn gallu gwrthsefyll y bygythiadau seiber sy'n eu hwynebu – gan greu llywodraeth gryfach, gadarnach sy'n sail i'n statws fel pŵer seiber.

Crynodeb Gweithredol

Y Cyd-destun

1. Mae'r Adolygiad Integredig[1] a'r Strategaeth Seiber Genedlaethol[2] wedi amlinellu uchelgais y llywodraeth i osod y DU ar sylfaen gadarn fel pŵer seiber democrataidd a chyfrifol, gyda'r gallu i amddiffyn a hyrwyddo ei buddiannau fel gwlad sofran mewn byd sy'n cael ei siapio'n sylfaenol gan dechnoleg. Fodd bynnag, mae cyfreithlondeb ac awdurdod y DU fel pŵer seiber yn dibynnu ar ei seibergadernid domestig, sy'n seiliedig ar sefydliadau llywodraeth a sector cyhoeddus sy'n cyflawni'r swyddogaethau ac yn darparu'r gwasanaethau sy'n cynnal ac yn hybu economi a chymdeithas y DU.

2. Er bod llywodraeth wedi gwneud cynnydd amlwg yn y blynyddoedd diwethaf, mae bwlch sylweddol o hyd rhwng y sefyllfa bresennol o ran seibergadernid llywodraeth a lle mae angen iddo fod. Gwelir y bwlch hwn yn glir yng ngolwg y nifer mawr o ymosodiadau seiber a wynebir gan y sector llywodraeth, a'r datblygu yng ngalluoedd a thechnegau'r gweithredwyr maleisus o lawer math sy'n eu cynnal. Yn ogystal â'r risg o amharu ar swyddogaethau llywodraeth a gwasanaethau cyhoeddus, mae targedu gwasanaethau hanfodol fel gofal iechyd yn gallu peri risg wirioneddol i ddiogelwch y cyhoedd.

Gweledigaeth a Nod

3. Felly gweledigaeth y strategaeth hon yw sicrhau bod swyddogaethau craidd llywodraeth – o ddarparu gwasanaethau cyhoeddus i weithredu cyfarpar Diogelwch Gwladol – yn gallu gwrthsefyll ymosodiadau seiber, gan gryfhau'r DU fel gwlad sofran a chadarnhau ei hawdurdod fel pŵer seiber democrataidd a chyfrifol.

4. Cyflawnir swyddogaethau craidd llywodraeth gan nifer o wahanol sefydliadau sector cyhoeddus, yn cynnwys adrannau llywodraeth, cyrff hyd braich, asiantaethau ac awdurdodau lleol.Felly mae'r strategaeth hon yn ystyried yr holl sefydliadau sector cyhoeddus o'r fath.

5. Er mwyn gwireddu ei gweledigaeth mae'r strategaeth yn ceisio cyflawni un nod sylfaenol – bod yr amddiffyniad rhag ymosodiadau seiber ar swyddogaethau hanfodol llywodraeth yn cael ei gryfhau'n sylweddol erbyn 2025, a bod holl sefydliadau llywodraeth yn y sector cyhoeddus cyfan yn gallu gwrthsefyll gwendidau a dulliau ymosod hysbys erbyn 2030 ar yr hwyraf.

6. Mae'r nod hwn yn un mentrus ac uchelgeisiol. Er mwyn sicrhau'r gallu i ganfod lefel y risg seiberddiogelwch mewn ffordd drefnus a gwrthrychol ar draws llywodraeth bydd angen sefydlu prosesau, mecanweithiau a phartneriaethau cynhwysfawr; tasg sy'n fwy cymhleth oherwydd y gwahanol raddau o aeddfedrwydd, gallu a chapasiti ym maes seiber. Agwedd allweddol ar hyn fydd galluogi adrannau llywodraeth arweiniol i asesu a dehongli cyflwr y cyrff hyd braich a sefydliadau sector cyhoeddus eraill yn eu maes o ran seiberddiogelwch ar lefel macro.

1 Llywodraeth EM; Prydain Fyd-eang mewn oes gystadleuol: yr Adolygiad Integredig o Bolisi Diogelwch, Amddiffyn, Datblygu a Thramor; Mawrth 2021
2 Llywodraeth EM; 'National Cyber Strategy'; Rhagfyr 2021

7. Drwy gyflawni'r nod hwn bydd llywodraeth yn dod yn darged llawer mwy anodd. Yn ogystal â galluogi llywodraeth i ddiogelu ei data a gweithredu heb darfu gormodol, bydd yn sicrhau bod sefydliadau llywodraeth wedi'u trefnu a'u strwythuro i reoli bygythiadau anhysbys a mwy soffistigedig pan fyddant yn codi.

Colofnau strategol a chynigion ar gyfer trawsnewid

8. Mae dull llywodraeth o gyflawni'r nod hwn yn canolbwyntio ar ddwy golofn strategol gydategol, y ddwy wedi'u seilio ar gynnig ar gyfer trawsnewid a fydd yn sbarduno ac yn hyrwyddo gwelliannau ar draws llywodraeth.

9. Y gyntaf yw gosod sylfaen gadarn ar gyfer seibergadernid sefydliadol; sicrhau bod sefydliadau llywodraeth wedi rhoi'r strwythurau, mecanweithiau, offer a chymorth priodol yn eu lle i reoli eu risgiau seiberddiogelwch.

10. Sicrheir hyn drwy fabwysiadu Fframwaith Seiberasesu (CAF) y Ganolfan Seiberddiogelwch Genedlaethol (NCSC) yn fframwaith sicrwydd i lywodraeth, gyda phroffiliau CAF penodol i lywodraeth sy'n datgan y canlyniadau sydd eu hangen gan sefydliadau llywodraeth er mwyn ymateb yn gymesur i'r gwahanol fygythiadau i'w swyddogaethau pwysicaf. Bydd gwirio gwrthrychol gan archwilwyr annibynnol yn ofynnol i adrannau llywodraeth ganolog, er mai mater i adrannau llywodraeth arweiniol fydd addasu a chymhwyso dull gweithredu o'r fath yn y ffordd sy'n fwyaf priodol i'r sefydliadau sector cyhoeddus yn eu maes. Yn ogystal â gwella'r gallu i ganfod risgiau seiberddiogelwch, drwy fabwysiadu'r CAF ceir fframwaith cyffredin i lywodraeth er mwyn eu deall a'u rheoli'n fwy effeithiol.

11. Yr ail yw cydamddiffyn. Gan gydnabod bod graddfa a chyflymder y bygythiad yn galw am ymateb mwy cynhwysfawr a chydgysylltiedig, bydd llywodraeth yn harneisio'r gwerth o rannu data, arbenigedd a galluoedd seiberddiogelwch ar draws ei sefydliadau er mwyn codi grym amddiffynnol a fydd yn fwy pwerus nag y byddai pe baent yn gweithio ar wahân.

12. Ategir hyn drwy sefydlu Canolfan Cydgysylltu Seiber Llywodraeth (GCCC). Fel menter ar y cyd rhwng Grŵp Diogelwch Llywodraeth, y Swyddfa Digidol a Data Ganolog a'r NCSC, bydd y GCCC yn gweithio i wella'r cydgysylltu mewn gweithrediadau seiberddiogelwch, gan drawsnewid y dull o rannu, defnyddio a gweithredu ar ddata seiberddiogelwch a chudd-wybodaeth am fygythiadau ar draws llywodraeth.

Amcanion

13. Mae'r colofnau hyn wedi'u hategu gan bum amcan sy'n pennu'r dimensiynau i seibergadernid, gan ddarparu fframwaith cyson a thermau cyffredin y gellir eu cymhwyso ar draws llywodraeth.

Rheoli risg seiberddiogelwch

14. Er mwyn rheoli risgiau seiberddiogelwch, bydd sefydliadau llywodraeth yn gallu eu canfod, eu hasesu a'u deall. Y man cychwyn ar gyfer hyn yw'r gallu i ganfod a deall asedau, eu gwendidau, a'r bygythiad iddynt – boed o'r tu mewn i'r sefydliad neu'n deillio o'i gadwyn gyflenwi. Drwy atebolrwydd clir a dulliau dibynadwy o roi sicrwydd, bydd perchnogion risgiau yn ymwybodol o'r risgiau y maent yn gyfrifol am eu rheoli, a'u bod yn gwneud hynny mewn ffordd briodol.

15. Rhennir gwybodaeth am wendidau ar draws llywodraeth er mwyn darparu rhagolwg canolog o wendidau critigol a fydd yn rhoi'r gallu i ganfod a rheoli risgiau trawslywodraethol, gan hwyluso camau buan i asesu, cydgysylltu a lliniaru ar raddfa fawr.

Amddiffyn rhag ymosodiadau seiber

16. Bydd y safiad amddiffynnol gan sefydliadau llywodraeth penodol wedi'i gysylltu'n annatod â'u dull o asesu a rheoli risg. Er na fydd byth yn bosibl amddiffyn rhag pob ymosodiad, bydd y rheini sy'n atebol yn gallu dangos eu bod wedi ystyried y risgiau hynny mewn ffordd briodol ac ymateb yn unol â hynny.

17. Bydd mesurau seiberddiogelwch cymesur yn rhan annatod o'r dechnoleg a ddefnyddir gan lywodraeth, a bydd technoleg a gwasanaethau digidol wedi'u dylunio, eu ffurfweddu a'u rheoli'n gywir. Bydd yn hollbwysig bod llywodraeth yn datblygu ei galluoedd, offer a gwasanaethau ar y cyd i ddelio â materion seiberddiogelwch cyffredin ar raddfa fawr, gan wella seiberddiogelwch ar draws llywodraeth yn ogystal â hybu effeithlonrwydd a gwerth am arian.

18. Wrth wraidd hyn mae'r cyfrifoldeb sydd gan lywodraeth i ddiogelu'r data y mae'n eu trin. Yn ogystal â dosbarthu gwybodaeth yn briodol, bydd llywodraeth yn ei thrin a'i rhannu mewn ffordd sy'n gymesur â'r risgiau sydd ynglŷn â hi, gan ddefnyddio'r systemau TG priodol.

Canfod digwyddiadau seiberddiogelwch

19. Ar sail ei dulliau o reoli risgiau a'i mesurau amddiffynnol cymesur, bydd llywodraeth yn datblygu ei gallu i ganfod digwyddiadau seiberddiogelwch ym mhob rhan o'i hystad er mwyn sicrhau bod modd lliniaru risgiau cyn iddynt gael effaith gritigol ar swyddogaethau a gwasanaethau llywodraeth.

20. Mae hyn yn golygu bod â'r gallu i fonitro systemau, rhwydweithiau a gwasanaethau i ganfod digwyddiadau seiberddiogelwch cyn iddynt droi'n achosion. Drwy well cydgysylltu, bydd llywodraeth yn gallu cael ystwythder i ddefnyddio'r mewnbynnau data hyn i ganfod digwyddiadau'n gyflym ac ar raddfa fawr, gan hwyluso ymatebion cydlynol yn ogystal â darparu'r galluoedd i ganfod ymosodiadau mwy soffistigedig.

Lleihau effaith achosion seiberddiogelwch

21. Tra bydd dulliau effeithiol o reoli risg, mesurau amddiffyn priodol a chymesur a gwell gallu o ran canfod yn peri bod llywodraeth yn darged llawer mwy anodd, bydd sefydliadau llywodraeth yn parhau i brofi effaith achosion seiberddiogelwch.

22. Felly bydd llywodraeth yn hollol barod a galluog i ymateb i achosion seiberddiogelwch gyda'r gallu i adfer systemau ac asedau a effeithiwyd ac ailddechrau cyflawni ei swyddogaethau a darparu ei gwasanaethau gyda'r lleiaf o darfu. Un agwedd allweddol ar hyn fydd sefydlu'r mecanweithiau i roi prawf ar gynlluniau ymateb i achosion, a'u hymarfer, ar lefel y sefydliad ac ar draws llywodraeth, yn ogystal â'r gallu i ddysgu gwersi ar ôl achosion ac achosion y bu ond y dim iddynt ddigwydd.

Datblygu'r sgiliau, gwybodaeth a diwylliant priodol ar gyfer seiberddiogelwch

23. Ni ellir gwireddu gweledigaeth a nod y strategaeth hon heb ddatblygu'r sgiliau a gwybodaeth sydd eu hangen ar gyfer seiberddiogelwch, yn ogystal â meithrin newid diwylliannol mewn seiberddiogelwch ar draws llywodraeth.

24. Bydd dealltwriaeth gynhwysfawr gan lywodraeth o'i hangen am sgiliau seiberddiogelwch a bydd yn hybu a hyrwyddo gyrfaoedd seiberddiogelwch mewn llywodraeth. Yn ogystal â llwybrau gyrfa ffurfiol sy'n dilyn canllawiau Cyngor Seiberddiogelwch y DU, bydd camau i fabwysiadu fframwaith tâl sengl ar gyfer gweithwyr seiber proffesiynol yn galluogi llywodraeth i fod yn fwy effeithiol wrth ddenu, datblygu a chadw'r sgiliau hynny, gan ddarparu proffesiwn seiberddiogelwch cynaliadwy mewn llywodraeth.

25. Mae'r angen am sgiliau a gwybodaeth ddigonol ar gyfer seiberddiogelwch yn ymestyn ymhellach na rolau seiberddiogelwch technegol ac yn cynnwys yr holl fathau o swyddogaethau proffesiynol lle mae'n rhaid rhoi ystyriaeth ddigonol i seiberddiogelwch. O'r proffesiwn Digidol, Data a Thechnoleg (DDaT) hyd at swyddogaethau masnachol a chyfreithiol llywodraeth, bydd gwybodaeth ac ymwybyddiaeth ddigonol o ran seiberddiogelwch yn sicrhau bod seiberddiogelwch yn cael ei ystyried lle bynnag y bo angen.

26. Yn ei hanfod, mae'r strategaeth hon yn cydnabod y pwysigrwydd o feithrin diwylliant seiberddiogelwch sy'n grymuso ei bobl i ddysgu, cwestiynu a herio er mwyn hyrwyddo gwelliant parhaus. Y man cychwyn i hyn yw gwella ymwybyddiaeth a gwybodaeth o ran seiberddiogelwch ymysg holl weithwyr y sector cyhoeddus, gan adeiladu ar y seiliau hyn i greu diwylliant seiberddiogelwch cadarnhaol sy'n cymell ac yn grymuso ei bobl i fynd i'r afael â risgiau seiberddiogelwch ar lefel y sefydliad. Cael hyn yn iawn yw'r allwedd i sicrhau newid cynaliadwy.

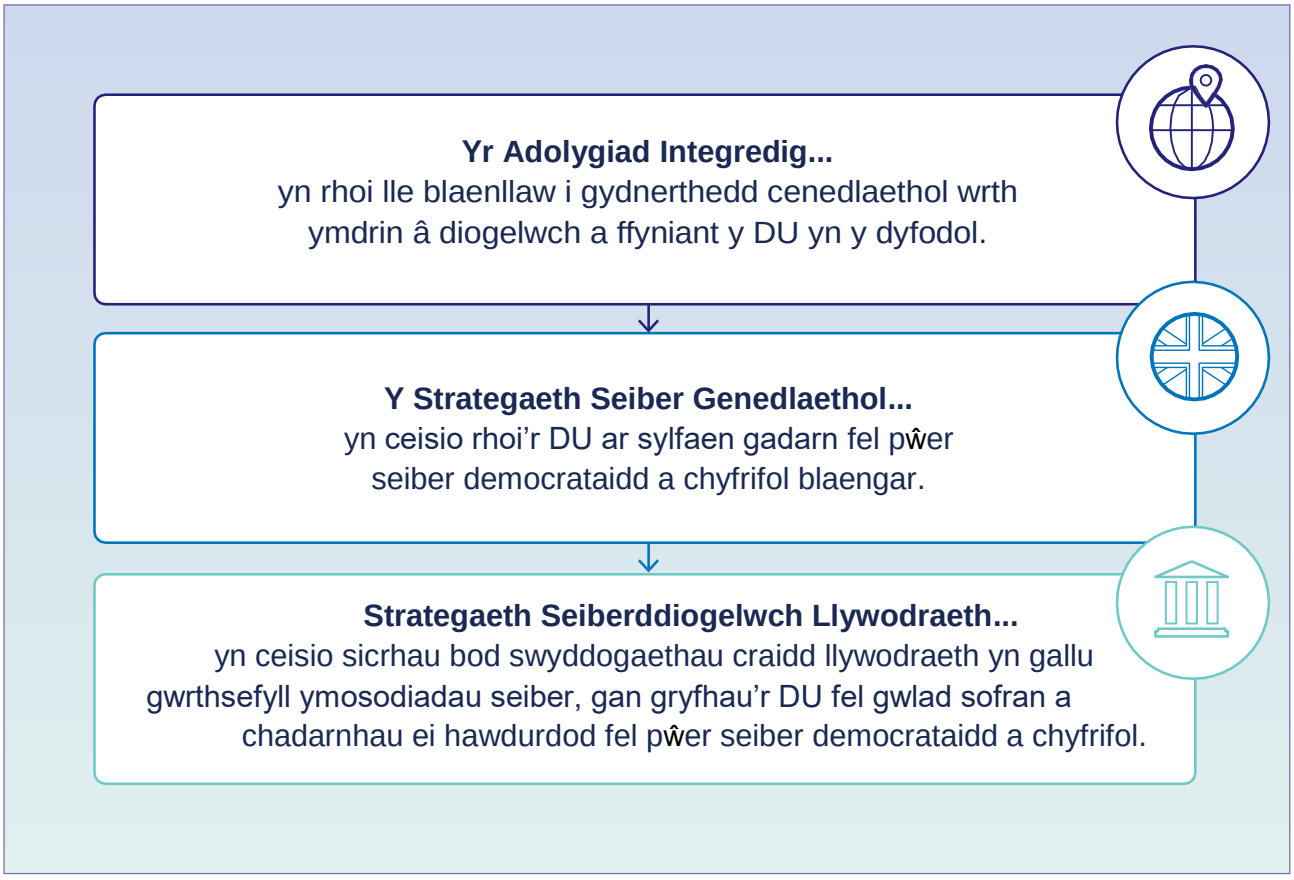
Pennod 1:
Y Cyd-destun

Pwysigrwydd seiberddiogelwch llywodraeth mewn cydnerthedd cenedlaethol

1. Mae'r Adolygiad Integredig o Bolisi Diogelwch, Amddiffyn, Datblygu a Thramor[3] (Adolygiad Integredig) yn rhoi lle blaenllaw i gydnerthedd cenedlaethol wrth ymdrin â diogelwch a ffyniant y DU yn y dyfodol. Wrth i'r byd ddod yn fwy dibynnol ar wasanaethau a chysylltedd digidol, bydd yr angen am seibergadernid yn dod yn fwyfwy hanfodol i'r ymdrech genedlaethol hon.

2. Mae'r Strategaeth Seiber Genedlaethol[4] yn dilyn yr amcan hwn, gan geisio rhoi'r DU ar sylfaen gadarn fel pŵer seiber democrataidd a chyfrifol sydd â'r gallu i ddiogelu a hyrwyddo ei buddiannau fel gwlad sofran mewn byd sy'n cael ei siapio'n sylfaenol gan dechnoleg.

3. Fodd bynnag, mae cyfreithlondeb ac awdurdod y DU fel pŵer seiber yn dibynnu ar ei seibergadernid domestig, a'r sylfaen i hynny yw ei sector cyhoeddus. Mae dyletswydd sylfaenol ar lywodraeth i gyflawni swyddogaethau sy'n cynnal ac yn hyrwyddo economi a chymdeithas y DU, o ddarparu gwasanaethau cyhoeddus hyd at weithredu cyfarpar diogelwch gwladol. Rhaid gallu cyflawni'r swyddogaethau hyn heb darfu gormodol arnynt er mwyn cadw'r ymddiriedaeth a'r hyder cyhoeddus sydd eu hangen i alluogi'r DU i ffynnu ac, yn sgil hynny, cynnal ei dylanwad y tu hwnt i'w ffiniau.



Ffigur 1: Cyd-destun strategol

3 Llywodraeth EM; Prydain Fyd-eang mewn oes gystadleuol: yr Adolygiad Integredig o Bolisi Diogelwch, Amddiffyn, Datblygu a Thramor; Mawrth 2021
4 Llywodraeth EM; 'National Cyber Strategy'; Rhagfyr 2021

Yr heriau a'r cyfleoedd i lywodraeth

Cynnydd

4. Mae llywodraeth wedi gwneud cynnydd sylweddol yn y pum mlynedd diwethaf. Yn ogystal â sefydlu'r Ganolfan Seiberddiogelwch Genedlaethol (NCSC) fel awdurdod technegol cenedlaethol y DU dros seiberddiogelwch, drwy greu Grŵp Diogelwch Llywodraeth a'r Swyddfa Digidol a Data Ganolog yn Swyddfa'r Cabinetdarparwyd arweinyddiaeth ganolog ar seiberddiogelwch a thrawsnewid digidol ar ganol llywodraeth.

5. Drwy gyflwyno'r Safonau Gofynnol ar gyfer Seiberddiogelwch i lywodraeth yn 2018,[5] a'r 'Prawf Iechyd' blynyddol i'w hategu, nodwyd gofynion clir am reolaethau ac ymddygiadau seiberddiogelwch, a rhoi gwell dealltwriaeth i lywodraeth o'i chyflwr o ran seiberddiogelwch. Cafwyd rhagor o ddealltwriaeth drwy gyflwyno'r cynllun GBEST i lywodraeth sy'n darparu fframwaith datblygedig seiliedig ar gudd-wybodaeth ar gyfer efelychu ymosodiadau er mwyn asesu seibergadernid y sefydliad dan sylw.

6. Mae'r angen am seiberddiogelwch yn cael ei gymryd fwyfwy o ddifrif ar y lefelau uchaf, gydag adroddiadau mwy rheolaidd i fyrddau a phwyllgorau archwilio a risg llywodraeth yn nodi'n gyson ei bod yn risg gritigol. Adlewyrchwyd y gydnabyddiaeth hon mewn buddsoddi parhaus a sylweddol yn seiberddiogelwch llywodraeth drwy'r Rhaglen Seiberddiogelwch Genedlaethol a buddsoddi i ddelio â TG etifeddol ym mhob rhan o ystad TG llywodraeth.

7. Mae'r NCSC yn parhau i dyfu a datblygu ei rhaglen Active Cyber Defence i ddelio ag ymosodiadau seiber mewn ffordd gymharol awtomatig ac ystwyth, yn ogystal â chynyddu nifer y gwasanaethau a galluoedd a rennir sy'n cael eu cynnig i wella seibergadernid llywodraeth. Yn ogystal â hyn, drwy gyflwyno ac ehangu llwyfan TG CYFRINACHOL llywodraeth, mae'r dull o reoli gwybodaeth fwy sensitif gan lywodraeth wedi'i drawsnewid a chafwyd gwell cydweithio rhwng y gwahanol ddosbarthiadau.

DAN SYLW: Dull cyfannol o ymdrin â diogelwch llywodraeth

Mae seiberddiogelwch yn un elfen hanfodol mewn set o ddisgyblaethau ac arferion diogelwch sy'n ofynnol i amddiffyn asedau llywodraeth a sicrhau bod modd cyflawni swyddogaethau llywodraeth heb darfu arnynt yn ormodol. Mae'r arferion diogelwch hyn yn croestorri a rhaid rhoi ystyriaeth briodol i bob un yn rhan o ddull cyfannol y sefydliad o reoli risgiau busnes.

Gan gydnabod hyn, ym Medi 2021 cyhoeddodd llywodraeth Safon Swyddogaethol y Llywodraeth GovS 007: Diogelwch[6] (Safon Diogelwch). Mae Safonau Swyddogaethol y Llywodraeth yn set o safonau rheoli sy'n ganllaw i bobl sy'n gweithio yn llywodraeth y DU ac yn cydweithio â hi. Mae'r Safon Diogelwch yn amlinellu'r trefniadau diogelwch a ddylai fod ar waith yn sefydliadau llywodraeth ar hyn o bryd i sicrhau bod llywodraeth yn gallu gweithredu'n effeithiol, yn effeithlon ac yn ddiogel.

Mae'r Safon Diogelwch yn crynhoi ac yn egluro beth sydd angen ei wneud, a pham, gan roi hyblygrwydd i sefydliadau o ran y ffordd y maent yn cyrraedd y safon yn ymarferol. Mae'n pennu disgwyliadau o ran llywodraethu, rolau ac atebolrwydd a'r arferion sydd eu hangen, yn ogystal â gosod sylfaen gadarn ar gyfer rhoi sicrwydd, rheoli risg a meithrin gallu.

5 Swyddfa'r Cabinet; 'Minimum Cyber Security Standard'; Mehefin 2018
6 Swyddfa'r Cabinet; 'Government Functional Standards GovS 007: Security', Medi 2021

8. Cymerwyd camau i ddelio â'r her o ran sgiliau seiberddiogelwch mewn llywodraeth gan greu proffesiwn diogelwch llywodraeth. Drwy ddatblygu fframwaith gyrfaoedd seiber – sy'n nodi gofynion safonol am sgiliau a gwybodaeth ar draws llywodraeth sydd â chysylltiad uniongyrchol â chwricwlwm dysgu seiber a chynnig tâl seiber – mae talentau seiberddiogelwch yn cael eu denu, eu datblygu a'u cadw. Mae cynnig talentau cynnar y llywodraeth hefyd yn meithrin talentau oddi mewn, drwy brentisiaethau a chynlluniau llwybr carlam.

9. Mae natur hanfodol seiberddiogelwch yn cael ei chydnabod y tu allan i lywodraeth y DU hefyd. Mae sefydliadau sector cyhoeddus yn cymryd camau breision, ac mae'r sector iechyd yn un enghraifft nodedig. Mae'r llywodraethau datganoledig hefyd wedi mabwysiadu strategaethau a chynlluniau gweithredu ar seibergadernid ers tro ac mae'r rhain yn hyrwyddo gwelliannau sylweddol mewn seiberddiogelwch yn y sectorau lle mae ganddynt gyfrifoldeb datganoledig.

Yr her

10. Er bod y gydnabyddiaeth gan lywodraeth i risg seiberddiogelwch a'i dealltwriaeth ohoni wedi datblygu, mae hyn wedi amlygu hefyd y bwlch rhwng seibergadernid fel y mae ar hyn o bryd mewn llywodraeth a lle mae angen iddo fod. Gwelir y bwlch hwn yn glir yn yr heriau y mae adrannau wedi'u hwynebu wrth gyrraedd y Safonau Gofynnol ar gyfer Seiberddiogelwch.

11. Mae lefel yr aeddfedrwydd, gallu, buddsoddi, a dealltwriaeth o ddiogelwch rhwng sefydliadau llywodraeth yn anghyson o hyd ac mae maint a chymhlethdod ystad ddigidol llywodraeth, yn cynnwys presenoldeb TG etifeddol, yn gwneud yr her yn llawer mwy cymhleth. Oherwydd maint ac amrywiaeth cadwyni cyflenwi llywodraeth, mae'n anodd rheoli risgiau, ac mae contractau tymor hir yn rhwystro arloesi. Yn ogystal â hyn, oherwydd strwythurau llywodraethu cymhleth, atebolrwydd, ysgogiadau a chymhellion annigonol, a mecanweithiau sydd heb eu datblygu digon i rannu gwybodaeth a galluoedd yn effeithiol, mae cryn effaith ar allu llywodraeth i ganfod risgiau seiber, ac i hyrwyddo newid ar y raddfa a'r cyflymder sydd eu hangen. Mae'r her sy'n codi yn fwy am fod adnoddau'n gyfyngedig.

12. Mae'r gallu i ymateb i faint yr her yn dibynnu hefyd ar bobl. Fodd bynnag, yng nghyd-destun y prinder sgiliau seiberddiogelwch drwy'r wlad[7], mae llywodraeth yn ei chael yn anodd cystadlu â'r sector preifat i ddenu a chadw'r cnewyllyn medrus ac amrywiol o weithwyr seiberddiogelwch proffesiynol sydd ei angen, er pob ymdrech hyd yn hyn. Mae hyn yn cwmpasu mwy na sgiliau seiberddiogelwch technegol ac yn cynnwys pob math o swyddogaethau proffesiynol sy'n galw am wybodaeth ac ymwybyddiaeth o ran seiberddiogelwch. Ar ben hynny, mae cystadlu mewnol am weithwyr seiber proffesiynol mewn llywodraeth yn digwydd yn rhy aml ar draul y gallu i gadw gwybodaeth a pharhau â newid.

7 Ipsos MORI / DCMS; 'Cyber Security Skills in the UK Labour Market 2021'; Mawrth 2021

13. Mae'r angen am wella seibergadernid yn cynyddu wrth i'r byd fynd yn fwyfwy digidol. Er bod y ffaith bod cysylltedd digidol ar gael yn gyffredinol a'r gallu i gynhyrchu data ar raddfa fawr yn cynnig cyfleoedd pwysig i lywodraeth wella ei gwasanaethau a swyddogaethau er budd y DU a'i dinasyddion, mae hyn yn creu risgiau sylweddol hefyd i seiberddiogelwch. Wrth i lywodraeth ddod yn fwy dibynnol ar wasanaethau digidol – o'r defnydd o gynhyrchion a gwasanaethau digidol hyd at symud data a gwasanaethau llywodraeth i'r cwmwl – mae mwy o ddibyniaeth ar y rheini sydd y tu allan i lywodraeth, sydd yn aml ag ôl troed sy'n ymestyn y tu hwnt i'r DU. Mae'r pandemig COVID-19 wedi cynyddu'r risgiau hyn yn ogystal â chreu newid sylfaenol yn y ffordd y mae llywodraeth yn gweithio, lle mae gweithio hybrid yn dod yn norm.

14. Yn sgil rhyng-gysylltedd a dibyniaeth o'r fath cafwyd cynnydd sylweddol yn y risg o ymosod maleisus, a'r potensial i danseilio ymddiriedaeth a hyder cyhoeddus mewn llywodraeth.

Y bygythiad

15. Wrth i risgiau seiberddiogelwch ddatblygu, felly hefyd y bydd y bygythiadau oddi wrth weithredwyr maleisus – o genedl-wladwriaethau i droseddwyr seiber. Tra bydd eu galluoedd a'u technegau'n parhau i ddatblygu a dod yn fwy amrywiol, mae'r masnacholi ar offer a gwasanaethau seiber ymosodol yn gostwng y trothwy gallu fwyfwy ar gyfer y rheini sy'n bwriadu tanseilio neu darfu ar weithrediadau llywodraeth.

16. Ar yr un pryd mae llywodraeth yn darged deniadol o hyd i weithredwyr maleisus o lawer math, ac roedd tua 40%o'r 777 o achosion a reolwyd gan NCSC rhwng Medi 2020 ac Awst 2021 yn rhai a oedd yn effeithio ar y sector cyhoeddus[8]. Y disgwyl yw y bydd hyn yn parhau i gynyddu.

DAN SYLW: Effaith meddalwedd wystlo

Yn 2020, cafodd cyngor Redcar a Cleveland a chyngor Hackney eu taro gan ymosodiadau drwy feddalwedd wystlo. Er bod y sefydliadau hyn yn gymharol fach, cafwyd effaith ddifrifol ac anghymesur ar wasanaethau cyhoeddus hanfodol. Nid yw ymosodiadau o'r fath yn eithriadol ond yn rhan o duedd arwyddocaol sydd ar gynnydd.

Nid yw meddalwedd wystlo yn dibynnu ar y gallu i fanteisio ar wendidau newydd. Yn wir, mae'r rhwystr i gamfanteisio o'r fath wedi mynd yn llai o lawer yn sgil dyfodiad meddalwedd wystlo fel gwasanaeth (RaaS), sy'n caniatáu i 'gwsmeriaid' brynu galluoedd a oedd unwaith ar gael i weithredwyr mwy medrus yn unig.

Wrth i'r defnydd o feddalwedd wystlo gynyddu, ceir costau sylweddol o hyd am adfer yn sgil yr effaith o ymosodiadau drwy feddalwedd wystlo. Yn anad dim, mae hyn yn ategu'r angen am seibergadernid effeithiol ac yn cryfhau'r ddadl dros roi blaenoriaeth briodol i seiberddiogelwch a'r buddsoddi ynddo er mwyn lliniaru'r risgiau cyn iddynt droi'n achosion difrifol.

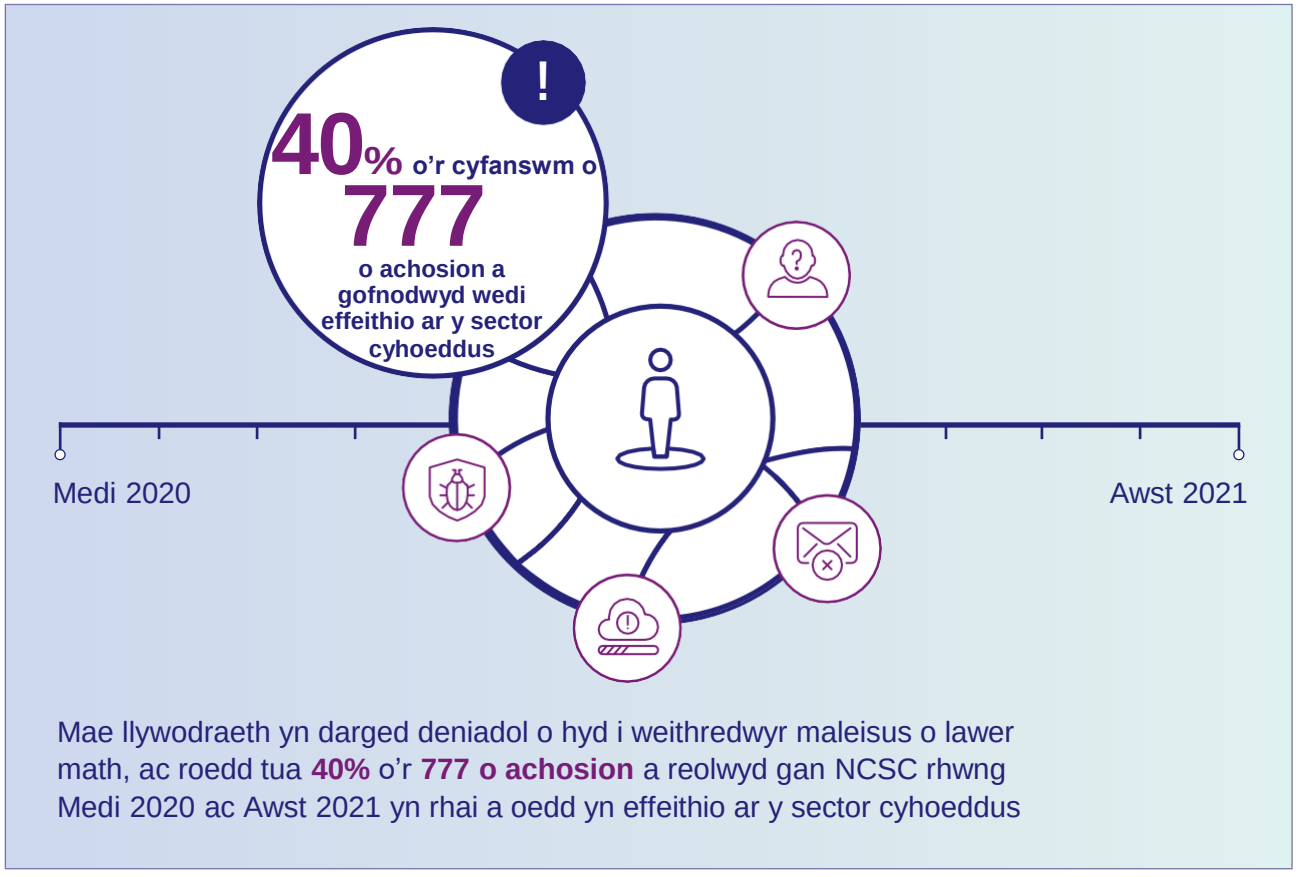
8 NCSC; 'NCSC Annual Review 2021'; Tachwedd 2021

17. Mae'r bygythiad oddi wrth weithredwyr cenedl-wladwriaethau yn achosi cryn bryder, ac mae bron hanner y gweithgarwch gan genedl-wladwriaethau yn cael ei dargedu ar lywodraethau ar draws y byd, a'r DU yn cael ei thargedu drydydd amlaf ar ôl UDA ac Wcrain[9]. Yn yr un modd, mae'r cynnydd sylweddol mewn ymosodiadau drwy feddalwedd wystlo ac achosion a gafodd effaith fawr yn ddiweddar wedi amlygu maint yr effaith a natur amrywiol y sefydliadau a effeithir, yn cynnwys adrannau llywodraeth yn ogystal â sefydliadau yn y sector cyhoeddus ehangach. Mae'r targedu ar wasanaethau gofal iechyd, addysg a gwasanaethau hanfodol eraill yn dangos drwy'r amser pa mor ddifrifol yw ymosodiadau seiber o'r fath, sydd nid yn unig yn amharu'n sylweddol ar y gallu i ddarparu gwasanaethau cyhoeddus hanfodol, ond hefyd yn gallu peri risg wirioneddol i ddiogelwch y cyhoedd.

Y cyfle

18. Er bod llywodraeth yn wynebu heriau sylweddol, mae ganddi nifer o gryfderau a phriodweddau hefyd. Gyda'r fath amrywiaeth sefydliadol, ceir cyfoeth o alluoedd, gwybodaeth a data y mae'n rhaid eu datblygu ac elwa ohonynt. Rhaid i lywodraeth fanteisio'n llawn hefyd ar y buddion a geir o drawsnewid digidol, er mwyn hyrwyddo arloesi, dealltwriaeth dadansoddol ac uwchraddio galluoedd.

19. Mae seibergadernid yn parhau'n amddiffyniad grymus a chosteffeithiol rhag y bygythiad seiber. Felly rhaid i sefydliadau llywodraeth adeiladu ar y seiliau hyn er mwyn gwella eu seibergadernid. Yn bwysicaf oll, mae angen i lywodraeth harneisio ei chydnerthedd, gan grynhoi a datblygu ei galluoedd er mwyn codi amddiffyniad cryfach a fydd yn gallu gwrthsefyll y risgiau seiber sy'n datblygu drwy'r amser.



Ffigur 2: Achosion seiber yn effeithio ar y sector cyhoeddus

9 Microsoft; 'Digital Defence Report'; Hydref 2021

Pennod 2:

Y Dull o Weithredu

Gweledigaeth a Nod

20. Mae dyletswydd ar lywodraeth i gyflawni swyddogaethau sy'n cynnal ac yn hyrwyddo economi a chymdeithas y DU. Rhaid gallu cyflawni'r swyddogaethau hyn heb fod tarfu gormodol arnynt er mwyn cadw'r ymddiriedaeth a'r hyder cyhoeddus sydd eu hangen i alluogi'r DU i ffynnu. Felly mae'n hollbwysig bod y swyddogaethau hyn yn ddigon cryf i wrthsefyll bygythiadau seiber sy'n datblygu drwy'r amser.

21. Er mwyn gwireddu'r weledigaeth hon, bydd mecanweithiau ar waith gan lywodraeth i ganfod a rheoli risgiau hysbys er mwyn cynnal lefel gymesur ac effeithiol o seiberddiogelwch ar draws holl sefydliadau llywodraeth.

22. Bydd hyn yn golygu cryfhau systemau SWYDDOGOL llywodraeth rhag gwendidau hysbys ac na fydd arferion diogelwch amhriodol yn peri bellach fod llywodraeth yn agored i raddau gormodol i ddulliau ymosod hawdd eu hatal, a bod gwybodaeth uwchlaw lefel SWYDDOGOL wedi'i diogelu'n briodol ar systemau dosbarth uwch. O ganlyniad i sefyllfa o'r fath, a'r dealltwriaeth a geir ohoni, bydd llywodraeth yn ymwybodol o ymosodiadau ar ei systemau a bydd yn gallu cynnal ei seibergadernid yn effeithiol.

23. Drwy gyflawni'r nod hwn, bydd llywodraeth yn darged mwy anodd o lawer – yn gorfodi gwrthwynebwyr i weithio'n galetach gan roi'r gallu i gyflawni swyddogaethau llywodraeth heb darfu gormodol ac, yn sgil hynny, cadarnhau awdurdod y DU fel pŵer seiber democrataidd a chyfrifol.

GWELEDIGAETH:

Mae'r strategaeth hon yn ceisio sicrhau bod swyddogaethau craidd llywodraeth – o ddarparu gwasanaethau cyhoeddus hyd at weithredu cyfarpar Diogelwch Gwladol - yn gallu gwrthsefyll ymosodiadau seiber, gan gryfhau'r DU fel gwlad sofran a chadarnhau ei hawdurdod fel pŵer seiber democrataidd a chyfrifol.

NOD:

Bod y gallu sydd gan swyddogaethau craidd llywodraeth i wrthsefyll ymosodiadau seiber yn cael ei gryfhau'n sylweddol erbyn 2025, a bod yr holl sefydliadau llywodraeth ar draws y sector cyhoeddus yn gallu gwrthsefyll gwendidau a dulliau ymosod hysbys erbyn 2030 ar yr hwyraf.

Dadansoddi'r Nod:

Mae nod y strategaeth yn gosod uchelgais clir i lywodraeth. Bydd y camau i'w gyflawni wedi'u seilio ar ddealltwriaeth o risg. Mae hyn yn golygu adnabod meysydd lle mae risg benodol a rhoi blaenoriaeth i'r ymyriadau mwyaf effeithiol i sicrhau bod llywodraeth yn gallu gwella ei seibergadernid yn gyflym.

Mae nod y strategaeth yn canolbwyntio ar reoli 'gwendidau a dulliau ymosod hysbys'. Mae hyn yn cwmpasu mwy na diffygion diogelwch a ddatgelwyd i'r cyhoedd ac yn cynnwys hefyd yr arferion ac ymddygiadau diogelwch amhriodol sy'n peri bod sefydliad yn agored i ymosodiadau seiber i raddau gormodol.

Mae arferion seiberddiogelwch da wedi'u hen sefydlu a bydd effaith y mwyafrif helaeth o ymosodiadau seiber yn cael ei lliniaru drwy eu mabwysiadu. Yn ogystal â gwella seibergadernid y sefydliad yn sylweddol, drwy fabwysiadu arferion seiberddiogelwch sefydledig sicrheir bod y sefydliad wedi'i drefnu a'i strwythuro i reoli bygythiadau anhysbys a mwy soffistigedig pan fyddant yn codi.

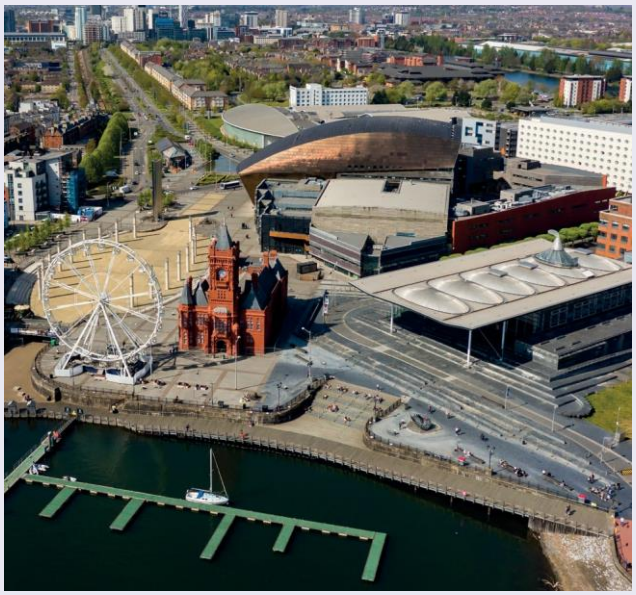
DAN SYLW: Seibergadernid

Seibergadernid yw'r gallu sydd gan sefydliad i barhau i gyflawni a darparu ei swyddogaethau a'i wasanaethau allweddol a sicrhau bod ei ddata wedi'u diogelu, er gwaethaf digwyddiadau seiberddiogelwch niweidiol. Oherwydd y ddyletswydd sylfaenol sydd ar lywodraeth i gyflawni swyddogaethau a darparu gwasanaethau sy'n cynnal ac yn hyrwyddo economi a chymdeithas y DU, mae seibergadernid wrth wraidd y strategaeth hon.

Cwmpas y strategaeth hon

Mae swyddogaethau craidd llywodraeth yn cael eu cyflawni gan nifer o wahanol sefydliadau yn y sector cyhoeddus, yn cynnwys adrannau llywodraeth, cyrff hyd braich, asiantaethau, awdurdodau lleol, a sefydliadau eraill yn y sector cyhoeddus ehangach. Felly mae'r strategaeth hon yn ystyried pob sefydliad o'r fath yn y sector cyhoeddus. Wrth wneud hynny, mae'n cydnabod cwmpas a chymhlethdod y sefydliadau hyn a'u gwahanol raddau o ymreolaeth, yn enwedig y rheini sydd y tu allan i lywodraeth ganolog.

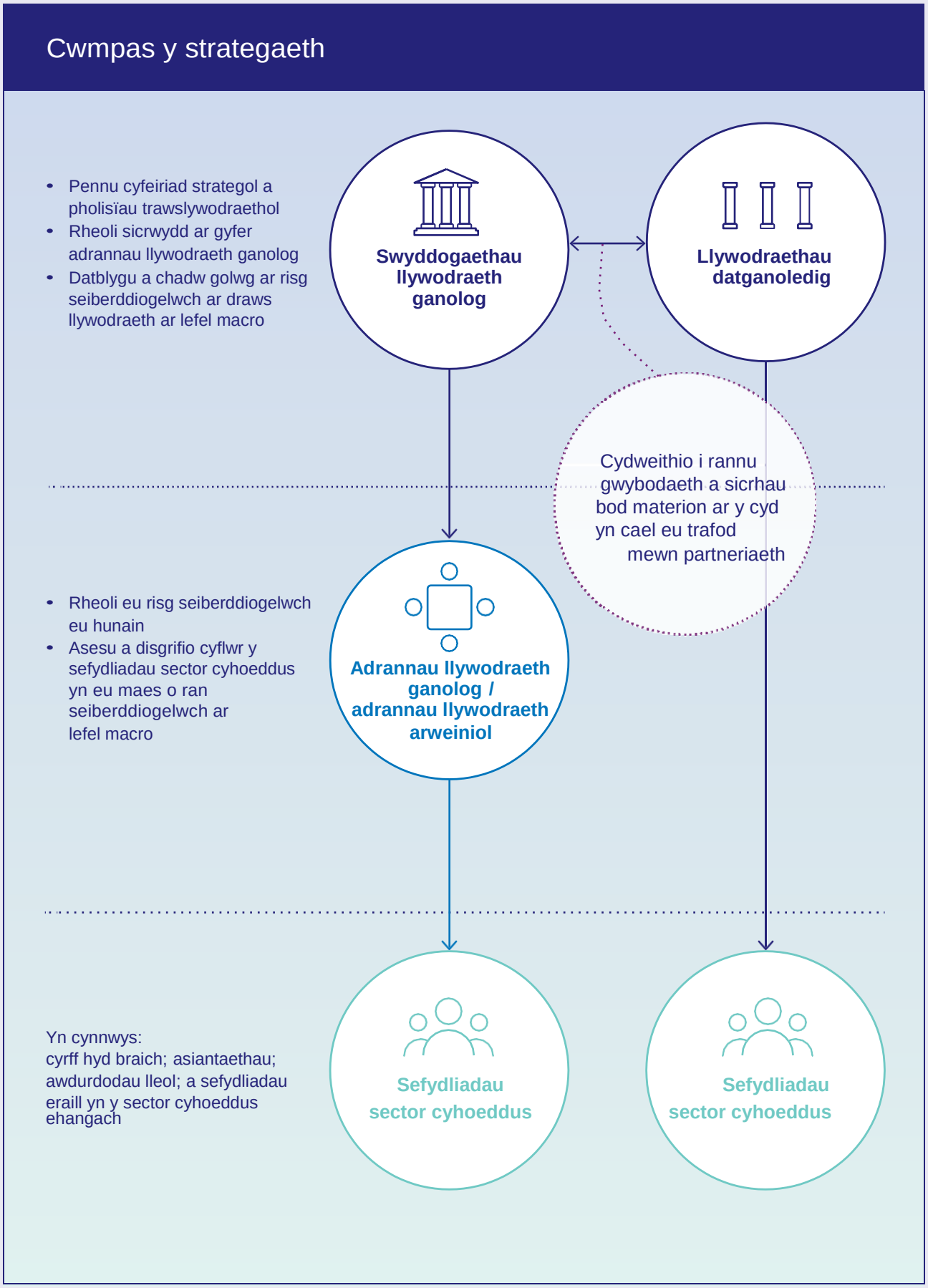
Adrannau llywodraeth arweiniol sydd yn y lle gorau i ddeall nodweddion unigryw y sefydliadau yn eu maes, yn cynnwys eu cyrff hyd braich ac asiantaethau, yn ogystal â chyrff llywodraeth eraill a sefydliadau yn y sector cyhoeddus ehangach. Felly canolbwyntir ar alluogi adrannau llywodraeth arweiniol i asesu a disgrifio cyflwr y sefydliadau hynny o ran seiberddiogelwch ar lefel macro, gan hyrwyddo gwelliannau fel y bo'r angen.



Y llywodraethau datganoledig

Er bod seiberddiogelwch – o fewn cylch gwaith ehangach diogelwch gwladol – yn fater a gedwir yn ôl, mae cyfrifoldeb dros wasanaethau cyhoeddus yng Nghymru, yr Alban a Gogledd Iwerddon wedi'i ddatganoli i'r priod lywodraethau datganoledig. Mae hyn yn cynnwys datganoli iechyd a gofal cymdeithasol, addysg a thrafnidiaeth, ymysg eraill. Felly mae'r llywodraethau datganoledig yn gyfrifol am sicrhau bod y gwasanaethau hynny'n gallu gwrthsefyll risgiau seiber.

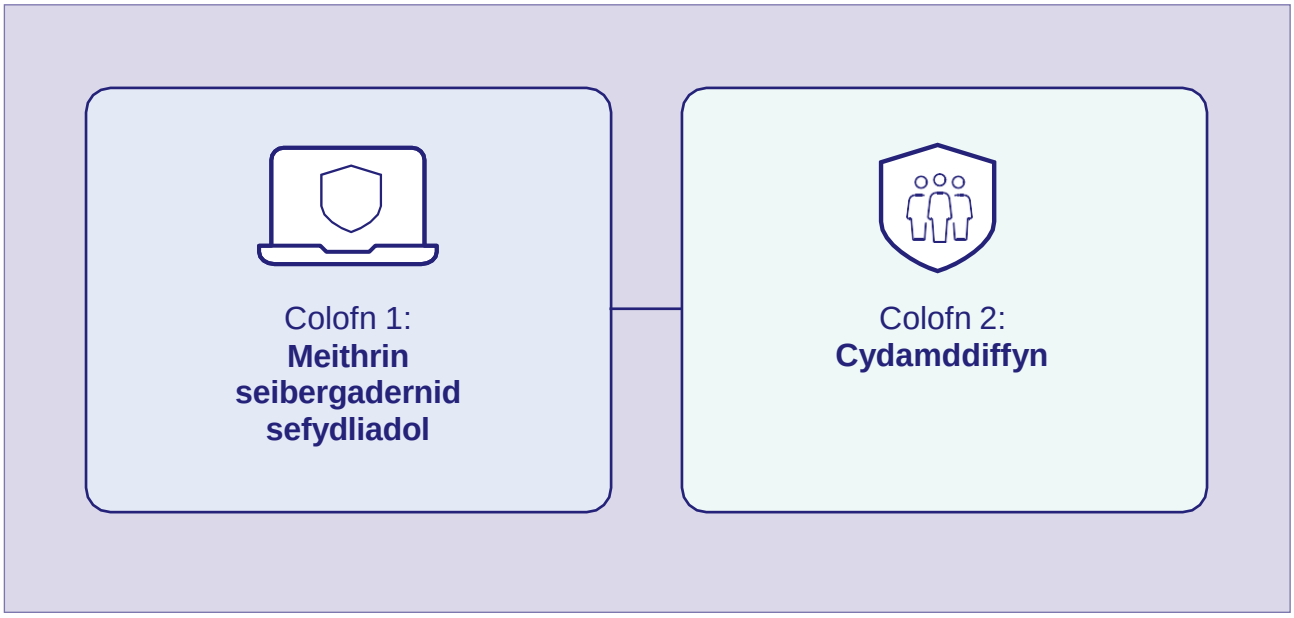
Er bod y materion hyn wedi'u datganoli, mae'r DU gyfan yn rhannu'r weledigaeth sydd yn y strategaeth hon. Felly bydd llywodraeth y DU yn parhau i gydweithio â'r llywodraethau datganoledig i sicrhau bod materion ar cyd yn cael eu trafod mewn partneriaeth, gan rannu cymorth a gwybodaeth briodol i gynnal cadernid y DU.



Ffigur 3: Cwmpas y strategaeth

Colofnau

24. Er mwyn gwireddu gweledigaeth a nod y strategaeth hon, bydd angen newid sylweddol yn y ffordd y mae llywodraeth yn delio â seiberddiogelwch. Yn ogystal â pharhau i gryfhau seibergadernid sefydliadol, bydd llywodraeth yn cydamddiffyn i sicrhau ei bod yn gallu cwrdd â'r heriau mawr y mae'n eu hwynebu. Felly mae'r strategaeth hon yn canolbwyntio ar ddwy golofn strategol hanfodol a chydategol sy'n diffinio ac yn ysgogi dull y llywodraeth o ymdrin â seibergadernid.



Ffigur 4: Colofnau strategol

Colofn 1: Gosod sylfaen gadarn ar gyfer seibergadernid sefydliadol

25. Yn ogystal â bod yn gyfrifol ac atebol am reoli eu risgiau seiberddiogelwch eu hunain, rhaid i sefydliadau llywodraeth gydnabod fwyfwy eu bod yn gydgyfrifol am seibergadernid llywodraeth gyfan. Gan fod y methiannau mewn un sefydliad yn gallu creu goblygiadau sylweddol i nifer o sefydliadau eraill, mae'n hollbwysig bod pob un o'r sefydliadau'n adeiladu ac yn gwella ei safiad ei hun o ran seiberddiogelwch, gan roi sylw i'r risgiau y mae'n eu hwynebu a phwysigrwydd y swyddogaeth y mae'n gyfrifol amdani.

26. Felly bydd sefydliadau llywodraeth yn gofalu bod y strwythurau, mecanweithiau, offer a chymorth priodol ar waith i sicrhau eu bod yn gallu rheoli eu risgiau seiberddiogelwch. Bydd hyn wedi'i seilio ar atebolrwydd gwirioneddol, fel y bydd llywodraeth yn sicr o'i seibergadernid, ar lefel y sefydliad ac ar draws llywodraeth.

CYNNIG AR GYFER TRAWSNEWID - Gwella sicrwydd seiberddiogelwch

Bydd llywodraeth yn mabwysiadu'r Fframwaith Seiberasesu (CAF) fel fframwaith sicrwydd ar gyfer llywodraeth. Datblygwyd y CAF gan yr NCSC – awdurdod technegol y DU ar seiberddiogelwch – ac mae'n adlewyrchu safon ddiwydiant a ddefnyddir gan weithredwyr gwasanaethau hanfodol o dan y Rheoliadau Rhwydwaith a Systemau Gwybodaeth[10] a hefyd yn fwy eang ar draws y sector preifat, yn cynnwys sectorau seilwaith cenedlaethol hanfodol (CNI). Drwy fabwysiadu'r CAF, sicrheir bod llywodraeth yn asesu seibergadernid mewn ffordd sy'n gyson a chymaradwy â sefydliadau eraill sy'n gweithredu gwasanaethau hanfodol y DU.

Bydd proffiliau haenog y CAF ar gyfer llywodraeth, a seilir ar broffiliau o fygythiadau seiber penodol i lywodraeth, yn disgrifio'r canlyniadau a fydd yn ofynnol gan sefydliadau llywodraeth er mwyn ymateb yn gymesur i wahanol fygythiadau i'w swyddogaethau pwysicaf. Bydd yr asesiad o seibergadernid gan sefydliadau llywodraeth ar sail y proffil CAF perthnasol yn cael ei wirio gan archwilwyr annibynnol. Yn ogystal â darparu asesiad gwrthrychol o seibergadernid llywodraeth, bydd yr archwilio mewnol yn tynnu sylw at feysydd hanfodol i'w gwella.

Bydd y broses sicrwydd hon yn ofynnol i adrannau llywodraeth. Fodd bynnag, mater i adrannau llywodraeth arweiniol fydd addasu a chymhwyso'r dull gweithredu hwn yn y ffordd sy'n fwyaf priodol i'r sefydliadau sector cyhoeddus yn eu maes. Bydd llywodraethau datganoledig yn arwain mewn ffordd debyg yn y meysydd y maent yn gyfrifol amdanynt. Bydd yn hanfodol, fodd bynnag, fod adrannau llywodraeth arweiniol a llywodraethau datganoledig yn gallu disgrifio cyflwr y sefydliadau yn eu maes o ran seiberddiogelwch ar lefel macro gan gyfeirio at amcanion y CAF er mwyn sicrhau bod seibergadernid llywodraeth yn cael ei asesu a'i ddeall mewn ffordd gyson a chymaradwy.

Er mai'r CAF yw'r fframwaith a ddefnyddir i ddarparu sicrwydd cyson am seiberddiogelwch adrannau llywodraeth, gall gwahanol adrannau barhau i ddefnyddio pa fframwaith bynnag y maent yn teimlo ei fod yn fwyaf priodol i'w galluogi i reoli eu risgiau seiberddiogelwch. Mae fframweithiau seiberddiogelwch adnabyddus, fel fframwaith seiberddiogelwch Sefydliad Cenedlaethol Safonau a Thechnoleg (NIST) ac ISO 27001, yn gyson â'r CAF, felly ni fydd gofynion am gofnodi sicrwydd yn mynd ar draws strwythurau a phrosesau sydd eisoes wedi'u sefydlu ar gyfer rheoli risgiau seiberddiogelwch o fewn y sefydliad.

10 Rheoliadau Rhwydwaith a Systemau Gwybodaeth 2018

Colofn 2: Cydamddiffyn

27. Er ei bod yn hollbwysig datblygu sylfaen gadarn ar gyfer seiberddiogelwch sefydliadol, mae maint a chyflymder y bygythiad yn galw am ymateb mwy cynhwysfawr a chydgysylltiedig. Felly bydd llywodraeth yn cydamddiffyn; yn harneisio'r gwerth o rannu data, arbenigedd a galluoedd seiberddiogelwch ar draws llywodraeth i godi grym amddiffynnol a fydd yn fwy pwerus drwy weithredu ar y cyd yn hytrach nag ar wahân.

28. Mae hyn yn galw am sicrhau bod holl sefydliadau llywodraeth yn cael mynediad amserol at ddata seiberddiogelwch sy'n berthnasol ac o werth ymarferol sy'n rhoi mwy o allu iddynt reoli risgiau seiber, yn ogystal â chydweithio i sicrhau gwell ffyrdd i gydgysylltu a thargedu galluoedd a gwasanaethau llywodraeth a rennir sy'n ymateb i faterion cyffredin o ran seiberddiogelwch ar raddfa fawr.

29. Drwy wneud hyn, ceir budd mwy byth i seiberddiogelwch llywodraeth. Bydd hefyd yn hwyluso arloesi drwy gydgysylltu camau i ganfod risgiau seiberddiogelwch cyffredin sy'n effeithio ar sefydliadau llywodraeth ac elwa o arbenigedd ac adnoddau llywodraeth er mwyn delio â'r problemau hynny ar raddfa fawr.

CYNNIG AR GYFER TRAWSNEWID - Canolfan Cydgysylltu Seiber Llywodraeth (GCCC)

Bydd llywodraeth yn sefydlu canolfan cydgysylltu seiber i sicrhau gwell cydgysylltu rhwng gweithrediadau seiberddiogelwch ar draws sefydliadau llywodraeth a chael gwelliant gwirioneddol yng ngallu llywodraeth i gydamddiffyn. Drwy weithio ar sail modelau llwyddiannus yn y sector preifat fel Canolfan Cydgysylltu Seiber y Sector Ariannol (FSCCC), bydd y GCCC yn meithrin partneriaethau er mwyn cymryd camau buan i ganfod achosion, ac ymchwilio a chydgysylltu'r ymateb iddynt yn ogystal ag adrodd ar fygythiadau a gwendidau. Agwedd allweddol ar hyn fydd trawsnewid y ffordd o ddefnyddio data seiberddiogelwch a chudd-wybodaeth am fygythiadau ar draws llywodraeth.

Drwy sicrhau dulliau cyflym o'r fath i rannu data, eu defnyddio a gweithredu ar eu sail, bydd mwy o allu o lawer gan lywodraeth i gydamddiffyn wrth reoli achosion, gwendidau a bygythiadau ar raddfa fawr.

Fel menter ar y cyd rhwng Grŵp Diogelwch Llywodraeth, y Swyddfa Digidol a Data Ganolog a'r NCSC, bydd y GCCC yn ffurfio partneriaethau cadarn ag adrannau llywodraeth a'r llywodraethau datganoledig.

DAN SYLW: Seiberddiogelwch seiliedig ar ddata

Mae'r strategaeth hon yn rhoi lle canolog i ddata mewn seiberddiogelwch. Bydd y defnydd diogel o ddata – wedi'u hawtomeiddio ac yn ddarllenadwy gan beiriannau lle bo modd – yn cyfrannu at benderfynu ac yn hybu gwelliannau lle bo angen.

Amcanion

30. Mae colofnau'r strategaeth wedi'u hategu gan bum amcan. Mae'r rhain yn pennu'r agweddau sydd angen eu hystyried mewn perthynas â seibergadernid, gan ddarparu fframwaith cyson a thermau cyffredin y gellir eu cymhwyso at lywodraeth gyfan.

    1) **Rheoli risg seiberddiogelwch:** Mae prosesau, llywodraethu ac atebolrwydd effeithiol ar gyfer rheoli risg seiberddiogelwch yn rhoi'r gallu i ganfod, asesu a rheoli risgiau seiberddiogelwch – ar lefel y sefydliad ac ar draws llywodraeth.

    2) **Amddiffyn rhag ymosodiadau seiber:** Mae dealltwriaeth o risg seiberddiogelwch yn gymorth i fabwysiadu mesurau diogelwch cymesur gyda galluoedd a ddatblygwyd yn ganolog yn rhoi'r gallu i amddiffyn ar raddfa fawr.

    3) **Canfod digwyddiadau seiberddiogelwch:** Drwy ddulliau cynhwysfawr o fonitro systemau, rhwydweithiau a gwasanaethau, gellir rheoli digwyddiadau seiberddiogelwch cyn iddynt droi'n achosion.

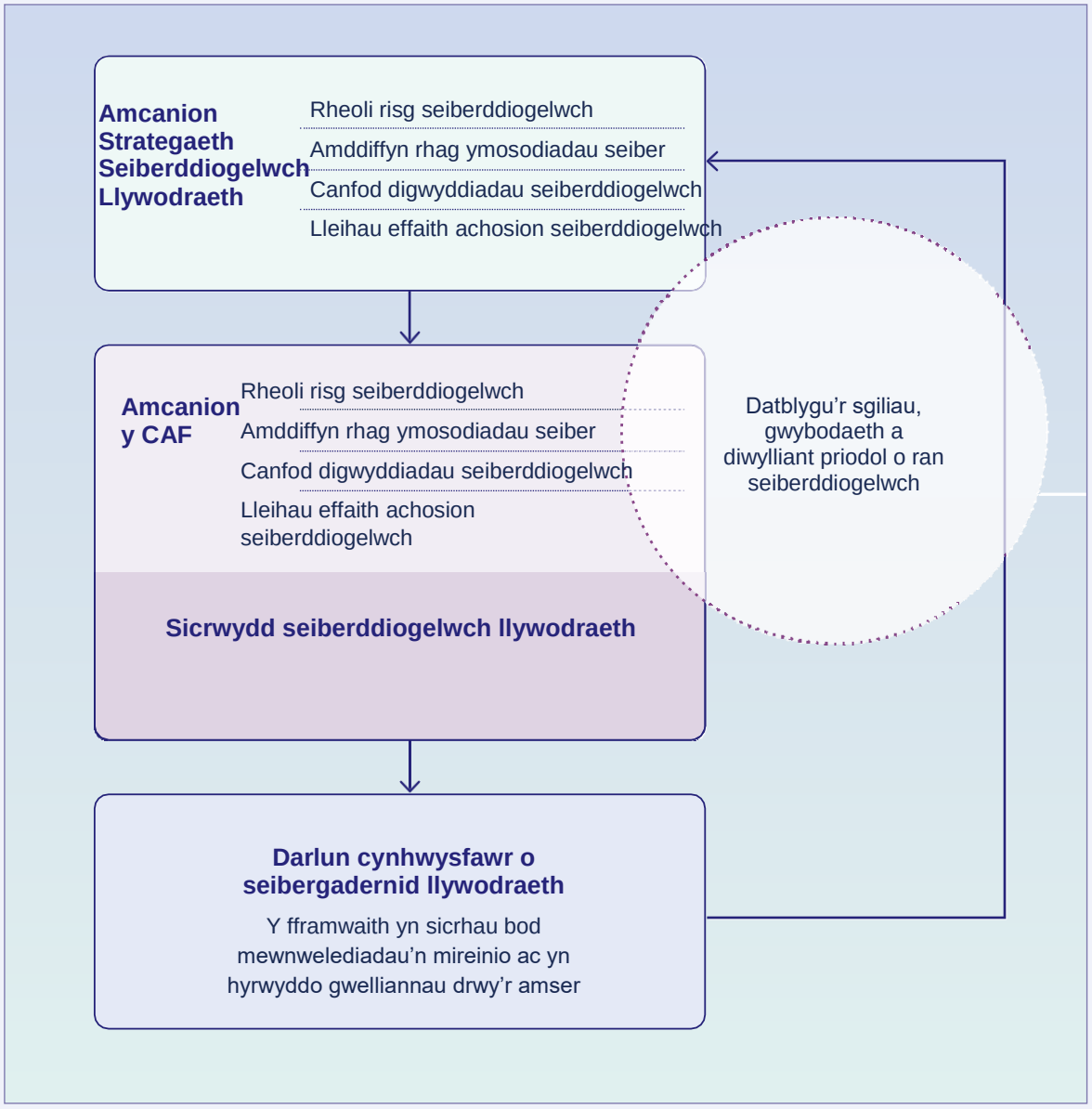
    4) **Lleihau effaith achosion seiberddiogelwch:** Mae achosion seiberddiogelwch yn cael eu hatal a'u hasesu'n gyflym, fel y gellir ymateb yn fuan ar raddfa fawr.

    5) **Datblygu sgiliau, gwybodaeth a diwylliant priodol o ran seiberddiogelwch:** Mae nifer digonol o weithwyr proffesiynol medrus a gwybodus yn diwallu'r holl anghenion a bennir o ran seiberddiogelwch – yn ymestyn yn bellach nag arbenigwyr seiberddiogelwch technegol at yr holl fathau o swyddogaethau proffesiynol lle mae'n rhaid cynnwys seiberddiogelwch yn y gwasanaethau a ddarperir – y cyfan wedi'i seilio ar ddiwylliant seiberddiogelwch sy'n hyrwyddo newid cynaliadwy.

DAN SYLW: Ecosystem sy'n atgyfnerthu'n barhaus

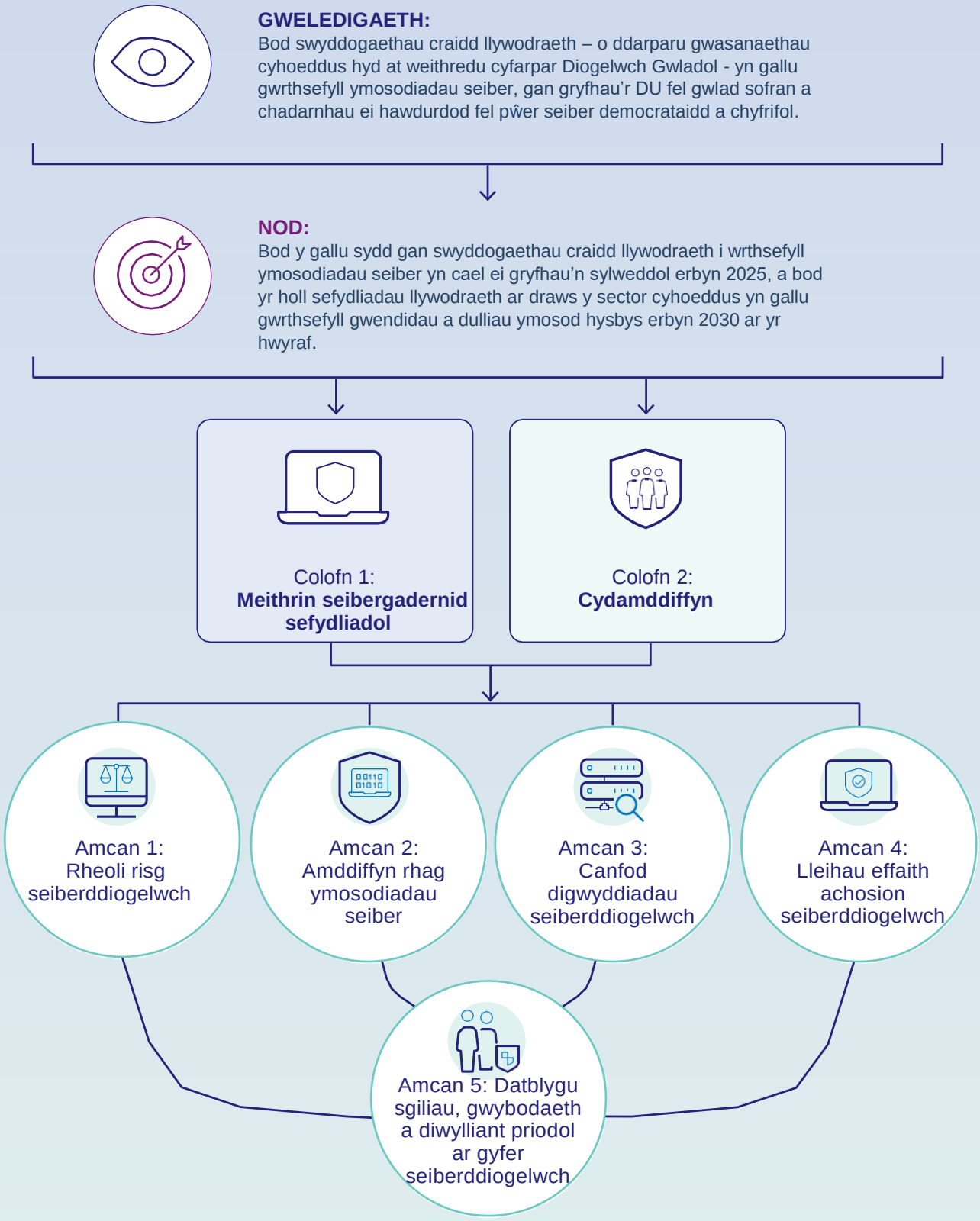
Mae amcanion y strategaeth yn pennu'r elfennau craidd mewn seibergadernid a fydd yn llywio ymdrechion o ran seiberddiogelwch ar draws llywodraeth. Bydd yr amcanion hyn yn cael eu hatgyfnerthu'n barhaus – drwy lywodraethu ac arolygu'r strategaeth, drwy ddatblygu a gweithredu ymyriadau o'r canol ac ar y cyd, a thrwy sicrwydd seiberddiogelwch llywodraeth.

Yn ogystal â darparu fframwaith cyson a thermau cyffredin ar gyfer seiberddiogelwch ar draws llywodraeth, drwy sefydlu ecosystem atgyfnerthol o'r fath ceir darlun cydlynol a chynhwysfawr o seibergadernid llywodraeth a fydd yn mireinio ac yn hyrwyddo gwelliannau drwy'r amser lle mae'r angen mwyaf amdanynt.



Ffigur 5: Ecosystem atgyfnerthol

Strategaeth Seiberddiogelwch Llywodraeth



Ffigur 6: Strategaeth Seiberddiogelwch Llywodraeth

Pennod 3:

Rheoli risg seiberddiogelwch

31. Yr amcan o reoli risg sydd wrth wraidd y strategaeth hon. Dim ond drwy ddeall risg y gellir cymryd camau lliniaru a blaenoriaethu buddsoddi. Felly mae'n hollbwysig cael gwybodaeth gywir am risg i alluogi'r unigolion sy'n atebol i wneud penderfyniadau effeithiol ar sail risg. Mae hefyd yn rhoi'r darlun o'r system gyfan sydd ei angen i ddelio â risgiau systemig a hyrwyddo ymyriadau ar raddfa fawr.

Amcan 1:

Bydd llywodraeth yn rheoli risg seiberddiogelwch

Bydd sefydliadau llywodraeth yn rhoi prosesau rheoli risg a dulliau llywodraethu ac atebolrwydd ar waith fel y bydd modd iddynt ganfod, asesu a rheoli eu risgiau seiberddiogelwch yn effeithiol, gyda digon o weledd cyffredinol i reoli risgiau systemig yn effeithiol.

32. Er mwyn rheoli risgiau seiberddiogelwch, bydd sefydliadau llywodraeth yn gallu eu canfod, eu hasesu a'u deall. Y sail i hyn yw'r gallu i weld a deall yr asedau sy'n cael eu dal a'u gweithredu – boed yn seilwaith, yn wasanaethau neu gymwysiadau digidol, neu'n ddata – a'r bygythiad iddynt. Y gweledd hwn yw'r man cychwyn ar gyfer asesiad cywir o risg. Bydd atebolrwydd clir a sicrwydd cadarn yn sicrhau bod perchnogion risgiau yn ymwybodol o'r risgiau y maent yn gyfrifol am eu rheoli, a'u bod yn gwneud hynny'n briodol.

Llywodraethu ac atebolrwydd

Canlyniad 1:
Bod llywodraeth wedi sefydlu trefniadau llywodraethu gydag atebolrwydd clir fel y gellir rheoli risgiau seiber yn effeithiol ar bob lefel o lywodraeth

33. Er mwyn codi dulliau rheoli risg llywodraeth at y lefel briodol bydd angen newidiadau a gwelliannau mewn llywodraethu ac atebolrwydd ar draws llywodraeth. Gwelir bod risg seiber yn rhan annatod o risg busnes a rheolaeth ar gadernid, a bydd strwythurau sefydliadol effeithiol i reoli seiberddiogelwch a fydd yn galluogi sefydliadau llywodraeth i ddeall a disgrifio pob agwedd ar y risgiau y maent yn berchen arnynt. Mae hyn yn cynnwys sefydlu rolau a chyfrifoldebau ar gyfer eu systemau a gwasanaethau a sianeli clir i roi gwybod am risgiau a'u huwchgyfeirio er mwyn sicrhau bod gan benderfynwyr y gweledded sydd ei angen i wneud penderfyniadau effeithiol. Yn bwysicaf oll, mae'n galw am atebolrwydd clir a thryloyw hyd at lefel Swyddogion Cyfrifyddu a'r bwrdd gweithredol, er mwyn sicrhau bod penderfynwyr yn cael eu hysbysu a'u grymuso i fynegi cyflwr eu sefydliad o ran risg, a'u bod yn cael eu dal yn atebol hefyd am eu penderfyniadau ar risg.

34. Adrannau llywodraeth arweiniol sydd yn y lle gorau i ddeall nodweddion unigryw'r sefydliadau yn eu maes a'r rhain fydd yn llunio'r mecanweithiau i asesu a disgrifio cyflwr y sefydliadau hynny o ran seiberddiogelwch ar lefel macro, gan roi trefniadau llywodraethu priodol ar waith i hyrwyddo'r gwelliannau sydd eu hangen.

35. Tra bydd Swyddogion Cyfrifyddu yn gyfrifol am risg yn eu sefydliad, bydd strwythurau llywodraethu canolog tryloyw yn arfer goruchwyliaeth a chyfrifoldeb dros risg seiberddiogelwch ar draws llywodraeth, gan sicrhau bod risgiau systemig yn cael eu canfod a'u rheoli.

Asedau a gwendidau

Canlyniad 2:
Bod llywodraeth yn cael gwelededdd a dealltwriaeth cynhwysfawr o'i hasedau digidol sy'n ei galluogi i ganfod a rheoli gwendidau a'r risgiau seiberddiogelwch sy'n codi ohonynt

36. Os na cheir gwelededdd cynhwysfawr o asedau TG, digidol a data llywodraeth, yn ogystal â defnyddwyr, ni fydd risgiau seiberddiogelwch yn cael eu canfod a'u rheoli. Nid yn unig y mae gwelededdd cyfyngedig o'r fath yn amharu ar allu'r sefydliad i amddiffyn ei ystad, mae hefyd yn lleihau'r gallu sydd gan lywodraeth i ganfod a chymryd camau ar risgiau cyfanredol a systemig a allai gael effaith ddinistriol ar weithrediadau llywodraeth.

37. Felly bydd dull gweithredol ac awtomataidd ar waith gan holl sefydliadau llywodraeth ar gyfer canfod a rheoli er mwyn cael cadarnhad drwy'r amser o'r systemau, caledwedd a meddalwedd y maent yn berchen arnynt ac yn eu gweithredu – yn cynnwys y rheini a ddarperir gan gyflenwyr – fel y gellir rheoli'r risgiau dichonol y maent yn eu hwynebu. Wrth i sefydliadau llywodraeth symud gwasanaethau i'r cwmwl, dylent fanteisio ar yr offer rheoli asedau sydd ar gael sy'n ei gwneud yn haws o lawer i sefydliad gael gwybod am yr hyn y mae'n berchen arno ac yn ei weithredu, am eu ffurfweddau, ac am eu gwendidau.

38. Mae gwendidau mewn technoleg a gwasanaethau digidol yn cael eu cyflwyno neu eu darganfod drwy'r amser bron. Felly bydd y dull a ddefnyddir gan lywodraeth i reoli'r rhain yn un sy'n adlewyrchu'r sefyllfa gyfnewidiol hon. Bydd mecanweithiau ar waith gan lywodraeth er mwyn gallu cymryd camau buan wrth ganfod, asesu a rheoli gwendidau. Bydd hyn yn golygu darparu llwybr clir i bawb – boed yn gyflogai yn y sector cyhoeddus, yn endid masnachol neu'n unigolyn preifat – i dynnu sylw at wendidau posibl, a chyflwyno rhaglenni effeithiol i reoli gwendidau yn yr holl sefydliadau llywodraeth er mwyn sicrhau bod gwendidau a nodwyd yn cael eu rheoli'n effeithiol ar draws eu hystad TG.

39. Bydd gwybodaeth am wendidau critigol yn cael ei rhannu'n ddiogel ar draws llywodraeth er mwyn sicrhau bod holl sefydliadau llywodraeth yn gallu cymryd camau priodol. Drwy rannu gwybodaeth yn effeithiol, ceir darlun canolog hefyd o wendidau critigol a fydd yn meithrin gallu llywodraeth i ganfod dibyniaethau ar draws ei systemau a gwasanaethau, fel y gellir canfod a rheoli materion o natur fwy systemig, yn ogystal â hwyluso asesu, cydgysylltu a lliniaru cyflym ar raddfa fawr.

DAN SYLW: Gwasanaeth adrodd ar wendidau ar draws llywodraeth

Bydd llywodraeth yn datblygu gwasanaeth cydlynol a chydgysylltiedig ar draws llywodraeth i adrodd ar wendidau. Bydd hyn yn rhoi'r gallu i ymdrin mewn ffordd aeddfed â gwendidau a allai effeithio ar lywodraeth ac ymateb iddynt.

Bydd ymchwilwyr diogelwch ac aelodau o'r cyhoedd yn gallu adrodd yn rhwydd a diogel ar wendidau y maent wedi'u canfod ar ystad ddigidol llywodraeth. Caiff adroddiadau eu brysbennu a hysbysir y sefydliad llywodraeth priodol am wendidau y cafwyd gwybodaeth ddilys amdanynt. Drwy'r gwasanaeth hwn bydd sefydliadau llywodraeth yn gallu dod o hyd i wendidau'n gynt a'u datrys cyn i wrthwynebwyr allu camfanteisio arnynt.

Drwy ddarparu'r gallu hwn yn ganolog, bydd llywodraeth yn gallu mynd i'r afael â gwendidau seiberddiogelwch mewn ffordd gyfannol am y tro cyntaf gan weithredu'n gyflym ac ar raddfa fawr ar draws y sector cyhoeddus.

Asedau data

Canlyniad 3:
Bod llywodraeth yn cael gweledded cynhwysfawr o'r data y mae'n eu trin a'u rhannu fel y bydd yn gallu asesu ac ymateb yn briodol i'r risgiau y maent yn eu dangos

40. Yn ogystal ag asedau TG, bydd sefydliadau llywodraeth yn cael gweledded cynhwysfawr o'u hasedau data. Mae data - yn amrywio o ddata personol i wybodaeth gyfrinachol - yn sail i holl wasanaethau a systemau TG llywodraeth ac fe'u diogelir mewn ffordd gymesur â'r risg ac yn unol â deddfwriaeth diogelu data. Felly bydd dealltwriaeth aeddfed gan sefydliadau llywodraeth o'r asedau data y maent yn eu trin, sut maent yn cael eu storio neu eu lletya, a ble maent yn cael eu rhannu, fel y byddant yn gallu asesu'n ddigonol y risgiau sy'n deillio ohonynt a sicrhau bod mesurau diogelu digonol wedi'u cymryd i'w rheoli.

Risg cadwyni cyflenwi

Canlyniad 4:
Bod llywodraeth yn deall a rheoli risgiau sy'n deillio o gyflenwyr masnachol

41. Mae lle hanfodol i gynhyrchion a gwasanaethau a ddarperir gan gyflenwyr masnachol wrth gyflawni swyddogaethau a darparu gwasanaethau llywodraeth. Wrth i gadwyni cyflenwi llywodraeth fynd yn fwyfwy eang a chydgysylltiedig, mae gwendidau yn systemau cyflenwyr, ac yn y cynhyrchion a gwasanaethau a ddarperir ganddynt, yn creu cyfleoedd sy'n fwyfwy deniadol i wrthwynebwyr sy'n ceisio cael mynediad i rwydweithiau llywodraeth. Gan gydnabod y risg gynyddol hon, bydd llywodraeth yn cymryd camau i gael gwell dealltwriaeth o'i dibyniaethau ar gyflenwyr ac yn sicrhau bod eu cynhyrchion a gwasanaethau wedi'u hintegreiddio â systemau llywodraeth mewn ffordd sy'n rhoi pob sylw i'w heffeithiau ar ddiogelwch a chadernid. Wrth wneud hynny, bydd llywodraeth yn gosod esiampl wrth gaffael a defnyddio cynhyrchion a gwasanaethau masnachol, gan sbarduno gwelliant yn ecosystem ehangach y cyflenwyr hynny ledled y DU.

42. Drwy weithredu'n ganolog i fapio cyflenwyr hanfodol a chyffredin llywodraeth, bydd modd canfod risgiau systemig a chyfanredol i lywodraeth mewn cadwyni cyflenwi a'u rheoli mewn ffordd gydgysylltiedig. Bydd egwyddorion seiberddiogelwch ar gyfer cadwyni cyflenwi yn gosod gofynion clir ar gyfer y cyflenwyr hyn, gan ddisgwyl y byddant yn darparu datganiadau tryloyw o gydymffurfiaeth. Bydd llywodraeth yn gwneud pob defnydd hefyd o'i chysylltiadau masnachol sefydledig a phŵer gwario cyfunol i sicrhau bod ei phrif gyflenwyr yn dilyn yr egwyddorion hyn. Yn ogystal ag atgyfnerthu rheolaethau ac ymddygiadau seiberddiogelwch priodol a chymesur, bydd goruchwyliaeth ganolog o'r fath yn hyrwyddo gofynion safonol ac yn darparu sicrwydd a rennir a fydd yn lleihau dyblygu ac yn sbarduno arbedion effeithlonrwydd ar gyfer sefydliadau llywodraeth a'u cyflenwyr.

43. Tra bydd camau gweithredu o'r fath yn creu disgwyliadau mwy o lawer ar gyfer cyflenwyr hanfodol a thrawslywodraethol, dylid pennu gofynion cadarn a chymesur hefyd ar gyfer cyflenwyr llai a rhai mwy arbenigol, gan ddefnyddio'r offeryn syml Cyber Essentials i gael sicrwydd bod cyflenwyr perthnasol wedi rhoi mesurau diogelu priodol ar waith. Drwy gysoni swyddogaethau masnachol a diogelwch, sicrheir bod seiberddiogelwch yn rhan o bob proses caffael, fel y bydd timau masnachol yn gallu cyfleu'r gofynion yn glir o ran seiberddiogelwch ar sail dealltwriaeth o risg. Cryfheir gofynion seiberddiogelwch yn fframweithiau a chontractau caffael llywodraeth, gan sicrhau bod trefniadau masnachol wedi'u seilio ar risgiau a'u bod yn gyson, gyda chymalau cryf yn ymwneud ag enwi a rheoli is-gontractwyr. Bydd hyn yn ei gwneud yn haws caffael offer a gwasanaethau gyda'r sicrwydd bod mesurau diogelwch ar waith.

44. Drwy gael gwell dealltwriaeth o gyflenwyr a'u dibyniaethau, bydd modd hefyd i lywodraeth ymateb yn well i achosion seiberddiogelwch sy'n deillio o'r gadwyn gyflenwi. Bydd dealltwriaeth o'r fath yn rhoi trosolwg ar effeithiau ar draws llywodraeth a'r gallu i ymwneud mewn ffordd fwy penodol ac effeithlon â'r cyflenwyr, gan sicrhau bod unrhyw achos yn cael ei reoli'n gyflym ac effeithlon. Bydd y GCCC yn chwarae rhan hanfodol wrth hwyluso hyn.

DAN SYLW: Seiberddiogelwch yng nghontractau llywodraeth

Mae llywodraeth yn datblygu atodlenni diogelwch y gellir eu cymhwyso'n rhwydd at lawer math o senarios caffael cyffredin – o waith adeiladu penodol ar seilwaith trydydd parti hyd at gytundebau ymgynghoriaeth cyffredinol. Bydd yr atodlenni hyn o gymorth i sefydliadau llywodraeth wrth ofyn am fesurau seiberddiogelwch cymesur yng nghontractau llywodraeth, a hefyd wrth gynnal profion sicrwydd o danynt.

Trefnir i'r atodlenni diogelwch hyn fod ar gael ar draws llywodraeth fel y bydd sefydliadau llywodraeth yn gallu cael gafael ar gymalau diogelwch sy'n hylaw a pherthnasol. Bydd hyn yn sicrhau bod mesurau diogelwch priodol – cymesur â'r risg – wedi'u cynnwys yn holl gontractau llywodraeth.

Gwybodaeth am fygythiadau

Canlyniad 5:
Bod llywodraeth yn deall y bygythiad y mae'n ei wynebu mewn perthynas â'i swyddogaethau er mwyn cynllunio mesurau lliniaru priodol ar lefel y sefydliad ac ar draws llywodraeth

45. Yn ogystal â'r gallu sydd gan lywodraeth i ddeall beth sydd ganddi a beth yw ei wendidau, bydd hefyd yn deall y bygythiad iddo er mwyn gwneud asesiad cywir o risg. Bydd yn hollbwysig gallu casglu a rhannu gwybodaeth am fygythiadau yn barhaus gan y bydd hyn yn rhoi'r manylion strategol, tactegol, technegol a gweithredol sydd eu hangen ar y rheini sy'n gyfrifol am amddiffyn systemau a rhwydweithiau er mwyn rhag-weld ac amddiffyn rhag ymosodiadau.

46. Felly bydd sefydliadau llywodraeth yn gallu cael a defnyddio gwybodaeth o'r fath am fygythiadau, a hefyd yn gallu ei chynhyrchu drwy fonitro eu system mewn ffordd systematig – wedi'i hawtomeiddio lle bynnag y bo modd. Bydd gwybodaeth am fygythiadau a gynhyrchir yn lleol yn cael ei mireinio drwy wneud defnydd rhesymegol o wybodaeth am fygythiadau sydd gan lywodraeth a'r sector preifat.

47. Bydd mecanweithiau canolog ar waith i hwyluso dulliau mwy cynhwysfawr a phenodol, ac awtomataidd os oes modd, o rannu gwybodaeth am fygythiadau ar draws llywodraeth. Bydd hyn yn galluogi sefydliadau llywodraeth i wneud penderfyniadau effeithiol ar flaenoriaethu ar sail y wybodaeth ddiweddaraf.

DAN SYLW: Gwrthsefyll bygythiadau

Mae'r Strategaeth Seiber Genedlaethol yn amlinellu amcan y DU ar gyfer canfod, archwilio a rhannu gwybodaeth am weithredwyr a gweithgareddau seiber maleisus sy'n gysylltiedig â gwladwriaethau, troseddu neu feysydd eraill er mwyn amddiffyn y DU, ei buddiannau a'i dinasyddion.

Bydd hyn yn cynnwys:

- meithrin dealltwriaeth gynhwysfawr o'r galluoedd seiber sydd gan weithredwyr seiber maleisus sy'n gysylltiedig â gwladwriaethau, troseddu neu feysydd eraill ac o'u bwriad strategol mewn perthynas â'r DU;
- sicrhau bod ymchwiliadau rheolaidd a chynhwysfawr yn cael eu cynnal i'r bygythiadau mwyaf difrifol gan weithredwyr sy'n gysylltiedig â gwladwriaethau, troseddu neu feysydd eraill, gan ddefnyddio'r holl ffynonellau gwybodaeth sydd ar gael a chrynhoi arbenigedd ar draws llywodraeth, asiantaethau gorfodi'r gyfraith a'r sector preifat;
- creu'r gallu i rannu gwybodaeth a data am y bygythiad yn rheolaidd, yn gyflym ac ar raddfa fawr.

Bydd sefydliadau llywodraeth yn cymryd rhan yn yr ymdrechion hyn fel cwsmeriaid a chyfranwyr, gan fanteisio'n llawn ar y wybodaeth sydd ar gael ledled y DU er mwyn darparu dealltwriaeth manylach o'r bygythiad.

Data seiberddiogelwch

Canlyniad 6:
Bod sefydliadau llywodraeth yn cael mynediad amserol at ddata seiberddiogelwch sy'n berthnasol ac o werth ymarferol a fydd yn hybu eu gallu i wneud penderfyniadau effeithiol i reoli risg

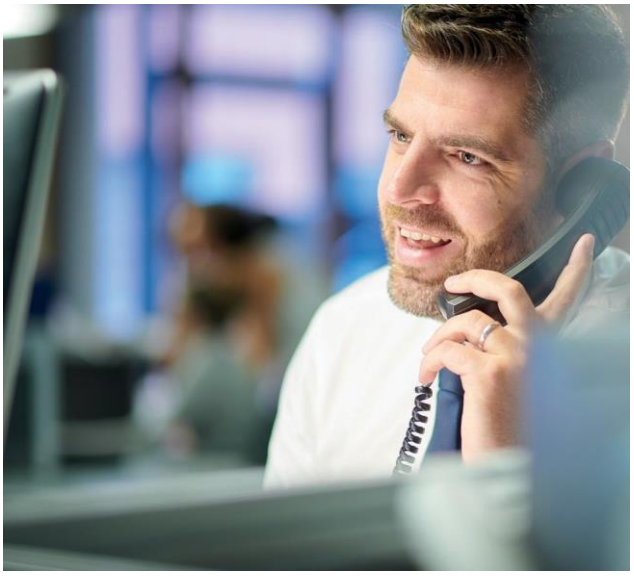
48. Mae data seiberddiogelwch yn ased amhrisiadwy, yn cynnwys gwybodaeth hanfodol am y bygythiadau a gwendidau y mae angen i lywodraeth eu deall er mwyn rheoli'r risgiau sy'n ei hwynebu mewn ffordd effeithiol. Mae'r angen i holl sefydliadau llywodraeth gael mynediad at ddata seiberddiogelwch sy'n berthnasol ac o werth ymarferol yn un hollbwysig, ond er bod rhai rhannau o lywodraeth yn gyfoethog iawn o ran data, mae eraill sydd heb fynediad at y data seiberddiogelwch sydd eu hangen arnynt i wneud penderfyniadau effeithiol sy'n seiliedig ar risg.

49. Yn ogystal â gwneud gwell defnydd o ddata seiberddiogelwch presennol – o ffynonellau fel gwasanaethau trawslywodraethol, systemau sefydliadol a chofnodi a monitro gan ddyfeisiau – ceir mwy o werth drwy ddadansoddi data cyfanredol, a gwell lledaenu ar fewnwelediadau beirniadol ymysg y rheini y bydd angen cael ymateb ganddynt. Bydd y GCCC sydd newydd ei sefydlu yn chwarae rhan hanfodol wrth hwyluso hyn, drwy sicrhau bod data seiberddiogelwch penodol yn cael eu rhannu ar draws llywodraeth – mewn ffordd sy'n briodol i'w dosbarth a'u statws cyfreithiol – a chynorthwyo sefydliadau i wneud defnydd effeithiol ohonynt.

Sicrwydd seiberddiogelwch llywodraeth

Canlyniad 7:
Bod sicrwydd seiberddiogelwch llywodraeth yn rhoi'r gweledegd sydd ei angen ar lywodraeth i wneud penderfyniadau effeithiol a hyder bod mesurau seiberddiogelwch priodol wedi'u rhoi ar waith i reoli'r risgiau i'w swyddogaethau

50. Mae angen sicrwydd o ran seiberddiogelwch i roi gweledegd o risgiau seiberddiogelwch ar draws sefydliadau llywodraeth yn ogystal â hyder bod y risgiau hynny'n cael eu rheoli mewn ffordd briodol a chymesur.Er mwyn cyflawni hyn, bydd proses sicrwydd seiberddiogelwch llywodraeth yn darparu sicrwydd a gaiff ei wirio'n gyson ac annibynnol ar sail proffiliau CAF llywodraeth.[11] Drwy ganolbwyntio ar swyddogaethau pwysicaf y sefydliad, yn cynnwys seilwaith cenedlaethol hanfodol, bydd yn darparu dull gwrthrychol o asesu a yw'r sefydliad yn asesu ac yn rheoli risgiau seiberddiogelwch mewn ffordd gymesur ac o fewn goddefiadau risg derbyniol. Caiff y broses sicrwydd hon ei gwirio a'i chryfhau ymhellach drwy gynnal profion ac ymarferiadau gwirioneddol, fel profion hacio ac ymarferiadau tîm coch. Bydd canlyniadau gweithgareddau sicrwydd ddarllenadwy gan beiriannau lle bo modd, gan hwyluso dadansoddi awtomatig o'r effaith ar seiberddiogelwch.



51. Tra bydd y prosesau sicrwydd hyn yn orfodol i adrannau llywodraeth ganolog, bydd hyn yn darparu model y gall adrannau llywodraeth arweiniol a llywodraethau datganoledig ei addasu a'i gymhwyso yn y sefydliadau sector cyhoeddus yn eu maes.

52. Bydd y gweledegd a geir o gyflwr seiberddiogelwch llywodraeth drwy'r sicrwydd hwn yn rhoi hyder cyffredinol i lywodraeth fod risgiau seiberddiogelwch i'w swyddogaethau yn cael eu rheoli'n ddigonol. Bydd hefyd yn tynnu sylw at broblemau cyffredin a heriau a geir ar raddfa fawr fel y gellir ymyrryd mewn ffordd bwrpasol a chosteffeithiol.

11 Gweler 'Cynnig ar gyfer trawsnewid: Sicrwydd seiberddiogelwch ychwanegol' am ragor o fanylion

Partneriaethau â'r sector preifat ac ar lefel ryngwladol

Canlyniad 8:
Bod partneriaethau strategol â'r sector preifat a phartneriaid rhyngwladol yn cael eu cryfhau ymhellach i wella mesurau amddiffyn rhagweithiol ar raddfa fyd-eang

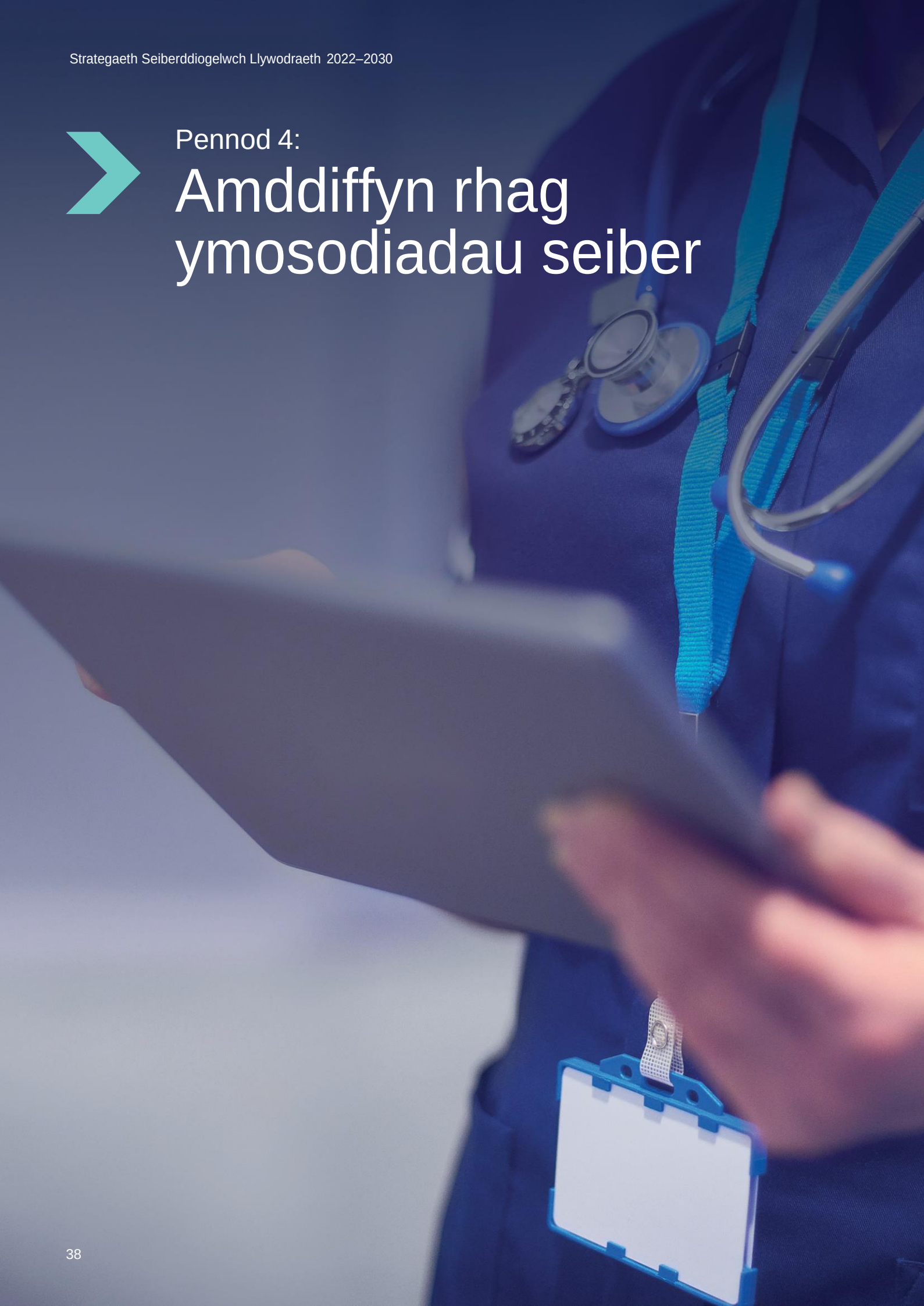
53. Mae llywodraeth yn dibynnu ar bartneriaethau â'r sector preifat a chynghreiriaid rhyngwladol i gryfhau ei seibergadernid. Mae'r dylanwad hwn yn cwmpasu cynhyrchion a gwasanaethau trydydd parti y mae llywodraeth yn eu caffael a'u defnyddio yn ogystal â gwaith i ddatblygu technolegau newydd a dulliau o lywodraethu seiberofod yn y dyfodol.

54. Gan fod partneriaid sector preifat yn chwarae rhan mor hanfodol wrth ddatblygu, gweithredu a chyflawni swyddogaethau llywodraeth, mae'n hollbwysig mynd i'r afael â heriau seiberddiogelwch critigol drwy gydweithio. Felly bydd llywodraeth yn parhau i ddatblygu ei phartneriaethau â sefydliadau sector preifat a chyrff academaidd er mwyn cryfhau pob agwedd ar ddiogelwch, gan feithrin partneriaethau dibynadwy a cheisio canlyniadau ar y cyd.

55. Fel y nodwyd yn y Strategaeth Seiber Genedlaethol, mae maes seiber yn croesi ffiniau rhyngwladol. Drwy rannu gwybodaeth ac arbenigedd â chynghreiriaid rhyngwladol, ceir mwy o allu ar y cyd i ddeall ac amddiffyn rhag gwrthwynebwyr cyffredin, gan gryfhau seibergadernid cyfunol a byd-eang yn sgil hynny. Bydd llywodraeth yn parhau i feithrin partneriaethau â'i chynghreiriaid er mwyn cyflawni amcanion a rennir.

Pennod 4:

Amddiffyn rhag ymosodiadau seiber



56. Mae'r gallu sydd gan lywodraeth i amddiffyn yn effeithiol rhag ymosodiadau seiber yn dibynnu ar ei dealltwriaeth o risg. Drwy ymateb yn uniongyrchol i'r risgiau a wynebir, sicrheir y bydd llywodraeth yn dod yn darged mwyfwy anodd i wrthwynebwyr o bob math.

Amcan 2:

Bydd llywodraeth yn amddiffyn rhag ymosodiadau seiber

Bydd dealltwriaeth llywodraeth o risg seiberddiogelwch yn cyfrannu at fabwysiadu mesurau diogelwch cymesur ar draws sefydliadau llywodraeth, a bydd galluoedd a ddatblygir yn ganolog yn rhoi'r gallu i amddiffyn ar raddfa fawr.

57. Bydd cysylltiad annatod rhwng safiad amddiffynnol gwahanol sefydliadau llywodraeth a'u dull o asesu a rheoli risg. Er na fydd byth yn bosibl diogelu rhag pob ymosodiad, bydd y rheini sy'n atebol yn gallu dangos eu bod wedi ystyried y risgiau hynny mewn ffordd briodol ac wedi ymateb yn unol â hynny.

Technoleg a gwasanaethau digidol diogel

Canlyniad 9:
Bod llywodraeth yn mabwysiadu dull cyffredin o ‘ddiogelu drwy ddylunio’ i sicrhau bod mesurau seiberddiogelwch priodol a chymesur yn rhan o’r dechnoleg y mae llywodraeth yn ei defnyddio, a bod diogelwch gwasanaethau digidol yn cael ei sicrhau’n barhaus drwy gydol eu cylch bywyd

58. Mae llywodraeth yn dibynnu ar wahanol fathau o dechnoleg i gyflawni ei swyddogaethau a darparu gwasanaethau digidol. Mae’r rhain yn cynnwys cynhyrchion ac elfennau pwrpasol sy’n achosi risgiau seiberddiogelwch y bydd angen eu rheoli drwy gydol eu cylch bywyd. Er mwyn gwneud hyn, bydd llywodraeth yn mabwysiadu fframwaith ‘diogelu drwy ddylunio’ i sicrhau bod yr holl dechnoleg a gwasanaethau digidol yn cael eu cynllunio, eu caffael, eu dylunio, eu hadeiladu, eu gweithredu, eu haddasu a’u datgomisiynu mewn ffordd ddiogel, fel y gellir cael sicrwydd parhaus a di-dor yn eu cylch ar sail yr arferion gorau a safonau dibynadwy.

59. Bydd y fframwaith ‘diogelu drwy ddylunio’ hwn yn rhoi gallu ychwanegol i lywodraeth i fanteisio ar arloesi gan ddiwydiant drwy ategu ei gallu i brofi, treialu a defnyddio offer, gwasanaethau a galluoedd masnachol a fydd yn gwella diogelwch ac effeithlonrwydd llywodraeth yn sylweddol.

60. Mae’r gallu i amddiffyn rhag gwendidau a bygythiadau newydd yn cael ei gyfyngu gan bresenoldeb TG etifeddol ac anniogel ar draws ystad TG llywodraeth. Felly bydd llywodraeth yn parhau â’i hymdrechion i reoli, uwchraddio neu gael gwared â TG o’r fath a chymryd y camau diogelu angenrheidiol a buddsoddi’n barhaus i sicrhau bod TG llywodraeth yn ddigon diogel drwy gydol ei chylch bywyd.

DAN SYLW: Fframwaith ‘diogelu drwy ddylunio’ i lywodraeth

Bydd fframwaith ‘diogelu drwy ddylunio’ llywodraeth yn sicrhau’r arfer o gynnwys mesurau seiberddiogelwch mewn systemau a gwasanaethau digidol ar bob cam yn eu cylch bywyd – o gynllunio’r gwasanaeth hyd at gaffael a ffurfweddu technoleg, a’i datgomisiynu ar ddiwedd ei hoes weithredol.

Bydd y fframwaith yn darparu proses barhaus ac ailadroddus ar gyfer diogelwch, gan sicrhau bod proses gyson, gynhwysfawr a chymesur ar gyfer rheoli risgiau seiberddiogelwch drwy gydol y cylch bywyd, a darparu fframwaith cyson i sicrhau diogelwch yn barhaus. Bydd yn sicrhau bod datblygwyr gwasanaethau digidol yn cynnwys arbenigwyr ar ddiogelwch yn eu timau i ddarparu cyngor ar ddiogelwch ar bob cam, yn hytrach na dibynnu ar gyngor byrfyfyr am ddiogelwch ar ddiwedd y prosiect.

Caiff y broses hon ei chynnwys yn y Safon Gwasanaeth[12] ac ym mhroses adwyog yr Awdurdod Seilwaith a Phrosiectau[13] i sicrhau bod seiberddiogelwch yn rhan annatod o’r gwaith o greu gwasanaethau cyhoeddus. Yn ogystal â hyn, cyhoeddir glasbrintiau, patrymau, egwyddorion dylunio ac arferion gorau diogelu drwy ddylunio i sicrhau bod sefydliadau yn y sector cyhoeddus ehangach yn cael dealltwriaeth clir o’r hyn a ddisgwylir i ddiogelu’r gwasanaethau y maent yn eu dylunio, eu darparu a’u gweithredu.

Un elfen hanfodol yn null ‘diogelu drwy ddylunio’ llywodraeth yw sicrhau bod pob technoleg y mae llywodraeth yn ei chaffael yn cynnwys lefel briodol o seiberddiogelwch. Felly bydd yr egwyddorion ‘diogelu drwy ddylunio’ hyn yn rhan annatod o’r Cod Ymarfer Technoleg[14] a fydd yn sicrhau, drwy brosesau rheolaethau gwariant llywodraeth,[15] fod yr holl dechnolegau a ddefnyddir gan lywodraeth yn rhai y gellir eu diogelu’n briodol.

12 Llywodraeth EM; ‘Service Standard’
13 Llywodraeth EM; ‘Infrastructure and Projects Authority: assurance review toolkit’
14 Swyddfa Digidol a Data Ganolog; ‘The Technology Code of Practice’
15 Swyddfa Digidol a Data Ganolog; ‘Digital and technology spend controls’

Rheolaethau seiberddiogelwch

Canlyniad 10:
Bod sefydliadau llywodraeth yn defnyddio rheolaethau seiberddiogelwch sy'n gymesur â'u proffil risg er mwyn sicrhau bod risgiau i'w swyddogaethau wedi'u rheoli'n briodol

61. Er bod technoleg ddiogel yn gosod y sylfaen ar gyfer seiberddiogelwch effeithiol, bydd rheolaethau diogelwch priodol a chymesur yn cael eu rhoi ar waith hefyd. Er y bydd nifer o reolaethau diogelwch yn gyffredin i holl sefydliadau llywodraeth, fel rheolaethau mynediad priodol, bydd y gofynion ehangach yn ymateb i'r bygythiadau a wynebir.

62. Felly, natur y bygythiadau i swyddogaethau pwysig y sefydliad fydd yn pennu pa broffil CAF fydd yn briodol o dan broses sicrwydd llywodraeth. Bydd y proffil CAF hwnnw'n diffinio'r canlyniadau sydd eu hangen er mwyn rheoli'r risg sy'n codi yn sgil y bygythiad mewn ffordd briodol. Bydd y gallu i sicrhau'r canlyniadau cymesur hynny yn dibynnu ar y defnydd o reolaethau penodol: nodir y rhain yn glir i sefydliadau llywodraeth, ochr yn ochr â pholisïau a chanllawiau priodol. Tra bydd adrannau llywodraeth arweiniol yn gallu cymhwyso dull gweithredu o'r fath yn y ffordd fwyaf priodol, byddant yn gallu gwneud defnydd o brosesau, canllawiau a chymorth o'r fath.

63. Mae systemau dosbarth uwch yn darparu'r rheolaethau seiberddiogelwch ychwanegol sydd eu hangen i ddelio â gwybodaeth mewn dosbarthiadau uwchlaw'r lefel SWYDDOGOL. Mae'r systemau hyn yn cael eu rheoli a'u sicrhau'n ganolog i gynnal y lefel briodol o seiberddiogelwch.

Ffigur 7: Rheolaethau mynediad priodol a chymesur

Ffurfweddu diogel

Canlyniad 11:
Bod technoleg llywodraeth wedi'i ffurfweddu'n briodol, a bod proffiliau safonol ar gyfer technoleg a saerniaethau cyffredin yn cael eu datblygu a'u diweddaru'n barhaus

64. Mae technoleg a gwasanaethau digidol yn dibynnu'n llwyr am eu diogelwch ar eu saernïaeth a'u ffurfwedd. Er bod modd delio â rhywfaint o'r risg hon drwy ddull 'diogelu drwy ddylunio', bydd cyfrifoldeb bob amser ar y dylunydd, y gweinyddwr neu'r defnyddiwr i ffurfweddu system neu wasanaeth yn briodol i gwrdd â gofynion o ran diogelwch. Os na wneir hyn yn gywir, gall systemau a data fod heb eu diogelu neu'n hawdd iawn amharu arnynt. Bydd y risg hon yn cynyddu wrth i lywodraeth barhau â thrawsnewid digidol.

65. Er mwyn lleihau'r risg hon, datblygir patrymau a galluoedd ffurfweddu sydd wedi'u 'diogelu drwy ddylunio' mewn partneriaeth â chyflenwyr a'u hyrwyddo ar draws llywodraeth i sicrhau bod cynhyrchion a gwasanaethau cyffredin wedi'u ffurfweddu'n gywir. Bydd y ffurfweddiadau hyn yn hawdd eu harchwilio fel y ceir gweledegdd ar draws llywodraeth er mwyn canfod risgiau cyfanredol ac ymateb i fygythiadau a nodwyd yn gyflym ac ar raddfa fawr.

DAN SYLW: Ffurfweddu diogel ar gyfer setiau meddalwedd swyddfa llywodraeth

Bydd llywodraeth yn cydweithio â phrif ddarparwyr ei setiau meddalwedd swyddfa er mwyn parhau i ddatblygu ffurfweddiadau diogelwch sylfaenol i'w dilyn a'u haddasu gan sefydliadau llywodraeth. Drwy wneud hynny, sicrheir bod holl sefydliadau llywodraeth yn deall sut i ffurfweddu eu setiau meddalwedd swyddfa er mwyn darparu seiberddiogelwch sylfaenol, fel y ceir llai o lawer o risgiau cyffredin wedi'u hachosi gan ffurfweddu diffygiol.

Galluoedd a rennir

Canlyniad 12:
Bod galluoedd, offer a gwasanaethau a rennir yn mynd i'r afael â phroblemau seiberddiogelwch 'cyffredin' ar raddfa fawr

66. Un o'r prif elfennau yng ngholofn 'cydamddiffyn' y strategaeth hon yw'r angen i harneisio galluoedd, offer a gwasanaethau a rennir i wella seiberddiogelwch llywodraeth yn fwy byth yn ogystal â darparu gwerth am arian. Boed hynny'n waith canolog i ddiogelu parthau *gov.uk* i'r sector cyhoeddus cyfan, neu ddatblygu offer a gwasanaethau Active Cyber Defence a threfnu iddynt fod ar gael yn fwy eang, mae ymdrechion o'r fath un ai'n lleihau'r risg a wynebir gan adrannau llywodraeth neu'n eu helpu i'w rheoli'n effeithiol ac effeithlon.

67. Felly bydd llywodraeth yn parhau i ddatblygu a thyfu galluoedd o'r fath.Mae cydgysylltu a chydweithio'n allweddol ar gyfer hyn, er mwyn sicrhau bod atebion wedi'u targedu ble mae'r angen mwyaf amdanynt a hefyd i alluogi llywodraeth i feithrin arloesedd er mwyn gwella seiberddiogelwch ar raddfa fawr.

DAN SYLW: Active Cyber Defence

Active Cyber Defence yw un o raglenni'r NCSC sy'n ceisio 'amddiffyn y rhan fwyaf o bobl yn y DU rhag y rhan fwyaf o'r niwed a achosir gan y rhan fwyaf o'r ymosodiadau seiber y rhan fwyaf o'r amser'. Yn benodol, mae'n bwriadu mynd i'r afael mewn ffordd weddol awtomataidd â rhan helaeth o'r ymosodiadau seiber sy'n effeithio ar systemau llywodraeth.

Mae Active Cyber Defence yn ategu yn hytrach na chymryd lle'r buddsoddi gan berchnogion systemau mewn seiberddiogelwch da. Mae ganddi nifer cynyddol o alluoedd, yn cynnwys:

- Galluoedd i ganfod ac amharu ar fygythiadau – drwy ganfod gweithgarwch maleisus ar raddfa fawr a/neu ysgogi ymateb awtomataidd i amharu arno. Mae'r rhain yn cynnwys:
  - Takedown Service – mae'n dod o hyd i wefannau maleisus ac yn hysbysu perchnogion er mwyn cael gwared â nhw
  - Protective DNS – mae'n atal mynediad anfwriadol at barthau neu IPs lle y gwyddys bod cynnwys maleisus, a maleiswedd sydd eisoes ar rwydwaith sy'n ceisio galw adref
  - Host Based Capability – mae'n dadansoddi metadata technegol sy'n cael eu dal ar ddyfeisiau fel gliniaduron a gweinyddion ar draws adrannau llywodraeth i ganfod gweithgarwch maleisus er mwyn gwneud systemau SWYDDOGOL yn fwy anodd eu targedu [gweler *'DAN SYLW: Host Based**Capability'* am ragor o fanylion)
  - Cyber Threat Intelligence Adaptor – mae'n galluogi sefydliadau awdurdodedig i gael cudd-wybodaeth o werth cyd-destunol mawr ac ansawdd da am fygythiadau seiber gan yr NCSC
- Galluoedd i ddarparu gwiriadau a rhybuddion hunanwasanaeth – i'w gwneud yn haws i sefydliadau wirio a gwella eu cyflwr o ran diogelwch. Mae'r rhain yn cynnwys:
  - Early Warning – mae'n helpu sefydliadau i ymchwilio i ymosodiadau seiber ar eu rhwydwaith drwy eu hysbysu am weithgarwch maleisus a ganfuwyd mewn ffrydiau gwybodaeth
  - Mail Check – mae'n helpu sefydliadau i asesu eu cydymffurfiaeth o ran diogelwch e-bost ac i fabwysiadu safonau e-bost diogel
  - Web Check – mae'n helpu perchnogion gwefannau sector cyhoeddus i ganfod a datrys problemau diogelwch cyffredin, gan wneud gwefannau'n llai deniadol i'w targedu gan ymosodwyr
  - Exercise in a Box – mae'n darparu set o senarios realistig sy'n helpu sefydliadau i ymarfer a mireinio eu hymateb i achosion seiberddiogelwch mewn amgylchedd diogel

Mae'r rhestr hon ymhell o fod yn gyflawn ac mae nifer y galluoedd yn cynyddu drwy'r amser.[16]

Bydd buddsoddi dethol yng ngalluoedd Active Cyber Defence yn elfen allweddol yn llwyddiant y strategaeth hon. Mae hyn yn cynnwys datblygu wedi'i dargedu a darpariaeth ychwanegol ar gyfer sefydliadau yn y sector cyhoeddus ehangach, a galluoedd newydd i ymateb i ddatblygiadau mewn technoleg ac yng ngallu gwrthwynebwyr.

16 NCSC; 'Active Cyber Defence: the fourth year'; Mai 2021

Diogelwch gwybodaeth a data

Canlyniad 13:
Bod data llywodraeth yn cael eu dosbarthu'n briodol a'u trin a'u rhannu mewn ffordd sy'n gymesur â'r risg y maent yn ei chreu

68. Mae gan lywodraeth gyfrifoldeb i ddiogelu data, boed y rheini'n wybodaeth gyfrinachol neu'n ddata personol y mae'n eu trin a'u rhannu i gyflawni swyddogaethau a darparu gwasanaethau. Felly bydd llywodraeth yn trin, yn rhannu ac yn storio neu letya ei hasedau data mewn ffordd sy'n gymesur â'r risgiau y maent yn eu creu.

69. Yn sail i hyn y mae dulliau effeithiol o ddosbarthu gwybodaeth yn unol â modelau bygythiad a gytunwyd ac asesiad cynhwysfawr o'r risgiau sy'n gysylltiedig â'r wybodaeth dan sylw. Mae polisi canolog ar ddosbarthiadau yn pennu'r meini prawf a'r cyfarwyddiadau ar gyfer trin gwybodaeth sydd wedi'i dosbarthu i wahanol haenau.

DAN SYLW: Polisi dosbarthiadau

Bydd llywodraeth yn diweddaru'r Polisi Dosbarthiadau Diogelwch er mwyn gwella'r ffordd o drin gwybodaeth yn yr haen SWYDDOGOL a sicrhau bod y wybodaeth fwyaf sensitif yn yr haen hon yn cael ei diogelu mewn ffordd ddiogel a chyson. Bydd hefyd yn darparu canllawiau cliriach i adrannau a defnyddwyr unigol, yn enwedig mewn perthynas â galluoedd newydd a newidiadau mewn ffyrdd o weithio, fel y byddant yn gallu diogelu gwybodaeth gyfrinachol yn well.

DAN SYLW: Diogelwch wrth rannu data

Mae'r Strategaeth Data Genedlaethol[17] yn amlinellu cenhadaeth y llywodraeth i drawsnewid ei defnydd o ddata er mwyn hybu effeithlonrwydd a gwella gwasanaethau cyhoeddus. Er mwyn cyflawni hyn, mae'r llywodraeth yn trawsnewid ei dull gweithredu ei hun mewn ffordd uchelgeisiol a radicalaidd, gan hyrwyddo gwelliannau mawr mewn effeithlonrwydd wrth reoli, defnyddio a rhannu gwybodaeth ar draws llywodraeth. Yn ogystal â gosod safonau data cadarn sy'n hyrwyddo cysondeb a rhyngweithredu, bydd llywodraeth yn sicrhau bod diogelwch data yn sail i'w dull o weithredu.

17 Llywodraeth EM; 'National Data Strategy'; Rhagfyr 2020

70. Mae'r rhan fwyaf o wybodaeth llywodraeth yn y dosbarth SWYDDOGOL ac mae'n dibynnu ar y dechnoleg a'r rheolaethau a amlinellwyd uchod. Fodd bynnag, fe fydd adegau pan fydd y model bygythiad yn galw am ddiogelu gwybodaeth benodol mewn dosbarth uwch, lle nad yw'r nwyddau technoleg sydd ar gael ar gyfer gwybodaeth SWYDDOGOL yn rhai addas. Er mwyn ateb yr angen hwn, bydd llywodraeth yn parhau i ddatblygu set o gynhyrchion a gwasanaethau integredig er mwyn cael dull addas o weithio ar draws llywodraeth sy'n hwylus, diogel a chydweithredol o dan y dosbarthiad priodol.

71. Lle mae'n rhaid prosesu data sensitif ar systemau SWYDDOGOL er mwyn cyflawni swyddogaeth busnes, rhoddir mesurau diogelu ar waith sy'n gymesur â'r risgiau sy'n codi.

DAN SYLW: Rosa

Mae Rosa yn wasanaeth TG CYFRINACHOL trawslywodraethol. Ers ei lansio, cafodd ei fabwysiadu gan nifer cynyddol o ddefnyddwyr ar gyfer nifer cynyddol o achosion defnydd, gan gyrraedd 12,000 o ddefnyddwyr a 74 o adrannau yn 2021. Bydd llywodraeth yn adeiladu ar sail y llwyddiant hwn drwy barhau i fuddsoddi yn Rosa er mwyn sicrhau ei fod yn parhau i gwrdd ag anghenion cynyddol ei ddefnyddwyr.

Yn ogystal â'i gwneud yn llawer haws trin gwybodaeth llywodraeth yn y dosbarth priodol, drwy gynyddu'r ddarpariaeth o Rosa bydd yn llai tebygol bod gwybodaeth yn cael ei rhoi mewn dosbarth rhy isel, fel y bydd yn llawer mwy anodd i wrthwynebwyr gael gafael arni a'i chamddefnyddio.

DAN SYLW: Harneisio technolegau newydd

Mae cyflymder newid technolegol yn creu heriau yn ogystal â chyfleoedd o ran seiberddiogelwch llywodraeth. Rhaid i lywodraeth allu cymhwyso technolegau o'r fath i wella ei galluoedd seiberddiogelwch ar draws llywodraeth, gan sicrhau bod ei defnydd ohonynt mor ddiogel â'r angen.

Deallusrwydd Artiffisial (AI)

Mae AI yn fath o feddalwedd sy'n gallu dysgu i ddatrys problemau ar gyflymder ac ar raddfa sy'n amhosibl i bobl ac mae'n dod yn rhan annatod o systemau modern. Ym maes seiberddiogelwch, mae tair agwedd benodol ar AI:

- Defnyddio AI i ddiogelu systemau. Mae nifer mawr o algorithmau AI yn gymhleth ac astrus,fel ei bod yn bosibl y byddant yn creu mathau newydd o wendid. Rhoddir blaenoriaeth i ddeall a lliniaru effaith y bygythiadau newydd hyn.
- Defnyddio AI i wella'r gallu i ganfod bygythiadau i seiberddiogelwch ac, mewn rhai achosion, creu'r gallu i ymateb yn awtomataidd i fygythiadau.
- Canfod a lliniaru effeithiau ymosodiadau seiliedig ar AI gan wrthwynebwyr.

Mae'r Swyddfa Deallusrwydd Artiffisial yn uned sy'n cael ei rhedeg ar y cyd gan BEIS a DCMS sy'n gyfrifol am oruchwylio gweithrediad y Strategaeth AI Genedlaethol ehangach.[18] Yn ogystal â hyn, mae Sefydliad Alan Turing a chyrff tebyg yn ymchwilio i ffyrdd posibl i greu a defnyddio AI mewn modd mwy cyfrifol a moesegol. Mae llywodraeth wedi ymrwymo i greu a defnyddio AI mewn ffordd sy'n hyrwyddo diogelwch, tegwch, grymuso, tryloywder ac atebolrwydd.

Cwantwm

Mae cyfrifiaduron cwantwm yn defnyddio priodweddau mecaneg cwantwm i gyfrifiaduro mewn ffordd gwbl wahanol i gyfrifiaduron 'clasurol' ein dyddiau ni. Mewn egwyddor, byddant yn gallu gwneud rhai cyfrifiannau a fyddai'n anymarferol i gyfrifiaduron clasurol.

Mae 'cryptograffeg cwantwm-ddiogel' yn creu problemau mathemategol y credir na fydd modd eu datrys gan gyfrifiaduron clasurol a chwantwm i gymryd lle problemau mathemategol cwantwm-ddatrysadwy. Felly drwy ddefnyddio cynhyrchion sy'n gyson â'r safonau, 'cryptograffeg cwantwm-ddiogel' fydd yn darparu'r dulliau mwyaf effeithiol o liniaru'r risg o fygythiadau difrifol oddi wrth gyfrifiaduron cwantwm yng nghyd-destun diogelwch cryptograffig yn y tymor hir, ac fe'i defnyddir ar draws llywodraeth yn ôl yr angen.

18 Llywodraeth EM; 'National AI Strategy'; Medi 2021

DAN SYLW: Mesurau diogelu uwch

Prif bwrpas y strategaeth hon yw sicrhau bod llywodraeth yn cyrraedd ac yn cynnal lefel gadernid sy'n gymesur â'r risg y mae'n ei hwynebu. Er hynny, derbynnir y posibilrwydd y bydd y gweithredwyr mwyaf soffistigedig yn gallu trechu mesurau seiberddiogelwch cadarn os byddant yn ddigon penderfynol ac yn buddsoddi digon.

Bydd llywodraeth yn defnyddio'r holl alluoedd sydd ar gael iddi er mwyn ymateb i'r bygythiadau mwyaf soffistigedig. Bydd galluoedd o'r fath yn cynnwys technegau canfod a diogelu uwch, yn ogystal â defnydd wedi'i dargedu o allu seiber ymosodol llywodraeth ac ymdrechion rhyngwladol a diplomyddol ehangach i ddrysu ac atal bygythiadau o'r fath.

Pennod 5:

Canfod digwyddiadau seiberddiogelwch

72. Er y bydd mesurau diogelu cadarn wedi'u rhoi ar waith, oherwydd y datblygu ar dechnegau gan wrthwynebwyr a'r gwendidau sy'n dod i'r golwg, bydd ymosodiadau seiber yn parhau. Er mwyn ymateb i newidiadau yn natur y bygythiadau, bydd angen galluoedd canfod cynhwysfawr ar lywodraeth i adnabod risgiau sy'n codi fel y gellir eu rheoli.

Amcan 3:

Bydd llywodraeth yn canfod digwyddiadau seiberddiogelwch

Mae gallu gan lywodraeth i fonitro ei systemau, rhwydweithiau a gwasanaethau i ganfod digwyddiadau seiberddiogelwch cyn iddynt droi'n achosion.Drwy gydgysylltu gwell bydd ystwythder gan lywodraeth i ddefnyddio'r mewnbynnau data hyn i ganfod digwyddiadau seiberddiogelwch yn gyflym ac ar raddfa fawr, gan hwyluso ymatebion cydlynol yn ogystal â darparu'r galluoedd sydd eu hangen i ganfod ymosodiadau mwy soffistigedig.

73. Ar sail dulliau rheoli risg a mesurau amddiffynnol cymesur, bydd llywodraeth yn datblygu ei gallu i ganfod digwyddiadau seiberddiogelwch ym mhob rhan o'i hystad er mwyn sicrhau bod modd lliniaru'r risgiau cyn iddynt gael effaith gritigol ar swyddogaethau llywodraeth.

Canfod o fewn sefydliadau llywodraeth

Canlyniad 14:
Bod rhwydweithiau, systemau, cymwysiadau a dyfeisiau llywodraeth yn cael eu monitro i ddarparu gallu cymesur i ganfod bygythiadau seiber o fewn sefydliadau

74. Er mwyn cyflawni ei gyfrifoldebau i reoli ei risgiau'n ddigonol, bydd galluoedd monitro cymesur gan bob sefydliad llywodraeth yn ogystal â'r gallu i gadw a chwilio logiau er mwyn hwyluso camau i ganfod bygythiadau seiber. Dylai'r monitro fod mor gyfannol â phosibl – o fonitro seilwaith fel parthau hyd at fonitro gan letywyr o ddyfeisiau a gwasanaethau cwmwl, a monitro cyfrifon breintiedig ar rwydwaith y sefydliad ac yn ei gadwyn gyflenwi. Er mwyn cyflawni hyn, gall sefydliadau llai fod yn rhan o gydgasgliad mwy, yn enwedig mewn sectorau a gydgysylltir gan adrannau llywodraeth arweiniol.

75. Bydd llywodraeth yn sefydlu proses a therminoleg gyffredin er mwyn i sefydliadau gofnodi a rhannu gwybodaeth am achosion seiberddiogelwch ac achosion y bu ond y dim iddynt ddigwydd – ar ffurf y gall peiriant ei darllen. Bydd hyn yn sicrhau cysondeb a'r gallu i gymharu rhwng sefydliadau llywodraeth yn ogystal â chaniatáu gweledegd gwell a fydd yn rhoi mwy o allu i lywodraeth ddysgu, addasu a lliniaru ar raddfa fawr.

76. Bydd y galluoedd canfod mewn sefydliadau llywodraeth yn parhau i ddatblygu, yn enwedig yn yr adrannau hynny lle mae lefel is o oddefiant i risg. Mewn amgylchiadau o'r fath, defnyddir dulliau canfod mwy datblygedig, fel monitro ymddygiadol, i ganfod ymosodiadau mwy soffistigedig.

DAN SYLW: Host Based Capability (HBC)

Mae HBC yn wasanaeth sy'n cael ei redeg gan yr NCSC, sydd â'r bwriad o wneud systemau SWYDDOGOL yn darged mwy anodd. Dadansoddir metadata ar ddyfeisiau lletya, fel gliniaduron a gweinyddion, ar draws adrannau llywodraeth gan ddefnyddio gwybodaeth arbenigol a chudd-wybodaeth yn yr NCSC.

Darperir HBC yn dair rhan:

- **Detect:** Mae HBC yn edrych ar y bygythiadau a wynebir gan adrannau fesul sector. Mae'n defnyddio gwybodaeth yr NCSC am ddangosyddion, tactegau gwrthwynebwyr, technegau a gweithdrefnau i ganfod gweithgarwch maleisus.
- **Threat Surface:** Mae adroddiadau'n darparu metrigau i adrannau i'w helpu i ddeall a gwella seiberddiogelwch eu systemau TG.
- **Forewarn:** Mae HBC yn ceisio rhybuddio adrannau am wendidau difrifol y maent yn agored iddynt.

Parheir i gynyddu'r defnydd o HBC ar draws llywodraeth a bydd datblygiadau yn y dyfodol yn cynnwys gallu yn y cwmwl, ac ymatebion i newidiadau mewn technoleg ac yng ngallu ymosodwyr.

Canfod ar raddfa fawr

Canlyniad 15:
Bod galluoedd canfod a rennir yn darparu ar gyfer canfod ar raddfa fawr ar draws llywodraeth

77. Er mwyn gallu canfod bygythiadau'n effeithiol, mae angen rhannu gwybodaeth yn amserol ar draws llywodraeth, fel y bydd modd lliniaru'r effaith o ddigwyddiad a ganfuwyd mewn un sefydliad yn yr holl sefydliadau eraill. Sefydlir mecanweithiau i sicrhau bod modd rhannu'r wybodaeth hon yn rhwydd a diogel, mewn ffordd awtomataidd, gyda'r disgwyl y bydd sefydliadau'n uwchgyfeirio rhybuddion yn gyflym ar hyd llwybrau clir a diffiniedig. Bydd yn hollbwysig cyflawni hyn er mwyn gallu canfod, rheoli a lliniaru bygythiadau sy'n codi ar y raddfa ac ar y cyflymder sydd eu hangen.

78. Er mwyn gwella'r gallu i ganfod ac adnabod gweithredwyr mwy soffistigedig ar rwydweithiau a systemau llywodraeth, sefydlir rhaglen chwilio am fygythiadau strategol a fydd yn cynnwys ystyriaeth i ddefnyddio galluoedd uwch fel tactegau dichell a 'photiau mêl'.

Pennod 6:

Lleihau effaith achosion seiberddiogelwch

79. Hyd yn oed ar ôl rhoi mesurau canfod a diogelu cadarn ar waith, bydd llywodraeth yn parhau i brofi effaith achosion seiberddiogelwch. Felly mae'n hollbwysig bod llywodraeth yn gallu ymateb yn gyflym i achosion seiber pan fyddant yn digwydd a lleihau eu heffaith i'r graddau mwyaf posibl.

Amcan 4:

Bydd llywodraeth yn lleihau effaith achosion seiberddiogelwch

Bydd achosion seiberddiogelwch yn cael eu rhwystro, eu hasesu a'u rheoli'n gyflym, fel y gellir ymateb yn gyflym drwy gamau lliniaru ar draws llywodraeth.

80. Bydd dulliau effeithiol o reoli risg, mesurau amddiffyn priodol a chymesur, a gallu ychwanegol i ganfod bygythiadau yn peri bod llywodraeth yn darged mwy anodd o lawer. Fodd bynnag, bydd llywodraeth hefyd yn gwella ei gallu i ymateb ac ymadfer ar ôl achosion pan fyddant yn digwydd er mwyn sicrhau bod swyddogaethau a gwasanaethau hanfodol yn parhau.

Paratoi i ymateb

Canlyniad 16:
Bod llywodraeth wedi paratoi'n llawn i ymateb i achosion seiber

81. Bydd cynlluniau sefydliadol a thrawslywodraethol ar gyfer ymateb i achosion seiberddiogelwch yn nodi'n glir sut bydd llywodraeth yn ymateb i achos penodol er mwyn lleihau ei effaith. Bydd cynlluniau sefydliadol yn cael eu hymarfer yn rheolaidd drwy gynllunio pen bwrdd ar sail senarios a gweithgareddau timau coch, glas a phorffor, gan eu diweddaru yn ôl yr angen i sicrhau eu bod yn addas i'w diben ac yn parhau i adlewyrchu natur y bygythiadau ar y pryd.

82. Ceir ymarfer rheolaidd hefyd ar draws llywodraeth i sicrhau bod uwch dimau adran ym mhob rhan o lywodraeth – yn cynnwys sefydliadau yn y sector cyhoeddus ehangach sy'n darparu gwasanaethau hanfodol – wedi ymarfer ac wedi paratoi i arwain yr ymateb i achosion seiber a all effeithio ar nifer o sefydliadau ar draws y sector cyhoeddus.

Ymateb i achosion

Canlyniad 17:
Bod llywodraeth yn ymateb yn gyflym i ddigwyddiadau seiber, ar lefel y sefydliad ac ar draws llywodraeth

83. Bydd sefydliadau llywodraeth wedi rhoi strwythurau a galluoedd ar waith – un ai'n uniongyrchol neu drwy gael cymorth gan sefydliad llywodraeth arall – i frysbennu achosion seiberddiogelwch ac asesu eu heffaith yn gyflym. Agwedd allweddol ar hyn fydd pennu llwybrau clir ar gyfer uwchgyfeirio, er mwyn sicrhau bod y bobl briodol yn cael eu hysbysu – o fewn y sefydliad a'r tu allan iddo – a bod yr arbenigedd a'r adnoddau priodol ar gael.

84. Bydd swyddogaethau canolog ar gyfer ymateb i achosion yn rhai sydd â'r gallu a'r capasiti i reoli achosion seiberddiogelwch difrifol a thrawslywodraethol lle mae prosesau a mecanweithiau diffiniedig ar waith i sicrhau bod yr holl bartïon a effeithir yn cydweithio i leihau'r effaith. Bydd y GCCC yn chwarae rhan hanfodol yn hyn.

Ymadfer ar ôl achosion

Canlyniad 18:
Bod llywodraeth yn adfer systemau ac asedau a effeithiwyd gan achosion seiberddiogelwch ac yn ailddechrau cyflawni ei swyddogaethau gyda'r lleiaf o darfu arnynt

85. Yn ogystal â bod yn barod a galluog i ymateb i achosion seiberddiogelwch, bydd llywodraeth yn gallu ymadfer ar eu hôl cyn gynted ag y bo angen er mwyn lleihau unrhyw darfu ar ei swyddogaethau.

86. Bydd y cynlluniau ymateb a weithredir yn sicrhau bod sefydliad yn gallu asesu'r risg o ganlyniad i achos penodol gan ddefnyddio arbenigedd priodol a chymryd yr holl gamau sydd eu hangen i ailddechrau cyflawni ei swyddogaethau at lefel dderbyniol o fewn cyfnod o darfu y gellir ei oddef.

87. Yn dilyn cwblhau prosesau ymateb i achosion, bydd goruchwyliaeth ganolog dros yr ymadfer ar ôl yr achosion mwyaf difrifol yn sicrhau bod risgiau systemig wedi'u canfod a'u lliniaru.

Gwersi a ddysgwyd

Canlyniad 19:
Bod gwersi a ddysgwyd o achosion seiber yn hyrwyddo gwelliannau yn seiberddiogelwch llywodraeth

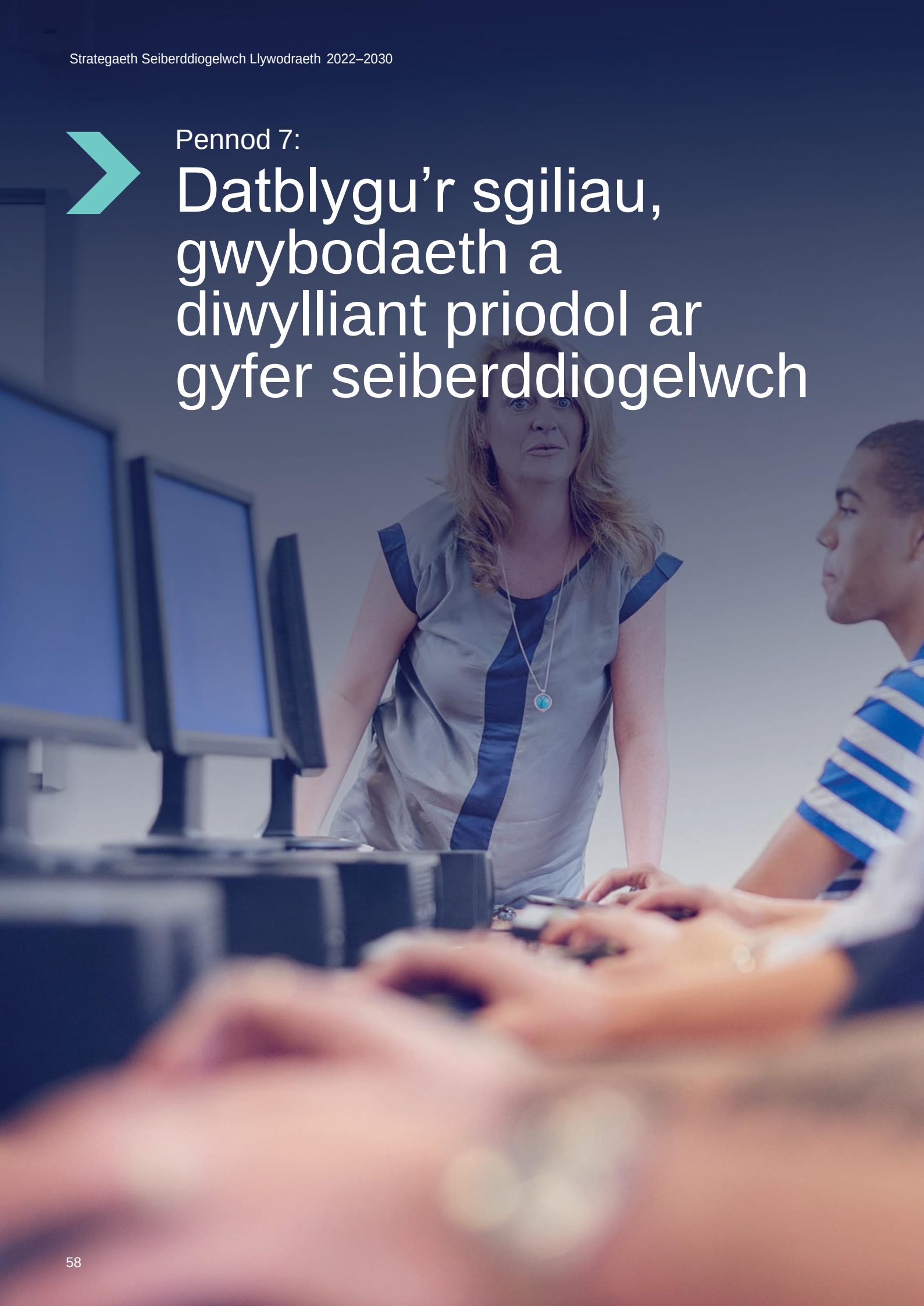
88. Er mwyn parhau i hyrwyddo gwelliannau mewn seiberddiogelwch, bydd llywodraeth yn dysgu gwersi o bob digwyddiad ac achos seiberddiogelwch – o achosion difrifol i rai y bu ond y dim iddynt ddigwydd.

89. Bydd llywodraeth yn gallu dysgu gwersi gwrthrychol o achosion seiberddiogelwch difrifol a thrawslywodraethol, a chynhelir adolygiad annibynnol o'r achosion mwyaf difrifol er mwyn darparu craffu digonol.

90. Yn yr un modd, bydd llywodraeth yn dysgu gwersi o ddigwyddiadau llai difrifol ac achosion y bu ond y dim iddynt ddigwydd. Un agwedd hanfodol ar hyn yw'r angen i greu diwylliant lle mae cydweithwyr ym maes seiberddiogelwch yn teimlo'n hyderus wrth rannu gwybodaeth o'r fath ar draws llywodraeth, heb ofn cael bai neu deimlo annifyrrwch. Drwy wneud hyn, sicrheir bod llywodraeth yn deall achosion sylfaenol y bygythiadau a'i bod yn gallu canfod a rhoi gwybod am atebion i lywodraeth gyfan er mwyn gwella ei seibergadernid ar y cyd.

Pennod 7:

Datblygu'r sgiliau, gwybodaeth a diwylliant priodol ar gyfer seiberddiogelwch



91. Ni fydd yn bosibl cyflawni nod a gweledigaeth y strategaeth hon heb gael pobl sydd â sgiliau priodol, yn cynnwys y rheini sy'n gweithio mewn rolau technegol, polisi a strategaeth, rheoli risg, ac arwain. Yn unol â'r amcanion a nodwyd yn y Strategaeth Seiber Genedlaethol, bydd llywodraeth yn arwain drwy osod esiampl wrth gynyddu nifer, amrywiaeth ac ansawdd gweithwyr seiberddiogelwch proffesiynol ar draws sefydliadau llywodraeth, gan feithrin newid diwylliannol mewn seiberddiogelwch a fydd yn hwyluso newid cynaliadwy.

Amcan 5:
Bydd llywodraeth yn datblygu'r sgiliau, gwybodaeth a diwylliant priodol ar gyfer seiberddiogelwch

Mae gan lywodraeth nifer digonol o weithwyr proffesiynol medrus a gwybodus i gwrdd â'r holl anghenion o ran seiberddiogelwch. Mae hyn yn ymestyn y tu hwnt i arbenigwyr seiberddiogelwch proffesiynol ac yn cynnwys yr holl swyddogaethau proffesiynol lle mae'n rhaid cynnwys seiberddiogelwch yn y gwasanaethau a ddarperir – wedi'i seilio ar ddiwylliant seiberddiogelwch sy'n hybu newid cynaliadwy.

92. Mae angen sgiliau seiberddiogelwch sy'n amrywio o ran eu cwmpas a'u manylder ar draws llywodraeth. Mae'r rhain yn cynnwys sgiliau technegol manwl a'r sgiliau seiberddiogelwch annhechnegol sydd eu hangen mewn arbenigaethau a phroffesiynau eraill, fel digidol, polisi, masnachol a sicrwydd. Gan ddilyn y safonau a'r llwybrau a sefydlwyd gan Gyngor Seiberddiogelwch y DU, bydd llywodraeth yn datblygu ei dealltwriaeth o'r gwahanol fathau o sgiliau a gwybodaeth seiberddiogelwch sydd eu hangen ar draws llywodraeth ac yn ymateb yn unol â hynny, gan sicrhau bod ei gweithlu'n gynhwysol ac yn amrywiol.

93. Fodd bynnag, mae'r dyhead hwn wedi'i bennu yng nghyd-destun bwlch sgiliau seiberddiogelwch ar lefel genedlaethol[19]. Felly canolbwyntir ar fuddsoddi yn y sgiliau hynny a'u datblygu o nifer o wahanol bwyntiau mynediad gyda chynnig cyson o ran gyrfaoedd ar draws llywodraeth i hybu'r gallu i recriwtio a chadw gweithwyr gan leihau'r ddibyniaeth ar gontractwyr. Drwy barhau i greu cyfleoedd dysgu blaengar, fe ddatblygir y proffesiwn ymhellach, gan gryfhau cynnig llywodraeth o ran cyflogaeth a'i gallu i gystadlu.

94. Wrth i broffesiwn diogelwch llywodraeth ganolbwyntio ar wella'r proffesiwn seiberddiogelwch ar draws adrannau llywodraeth, bydd yn cydategu mentrau sgiliau seiberddiogelwch ar draws y sector cyhoeddus, yn ogystal â darparu fframwaith i alluogi sefydliadau yn y sector cyhoeddus ehangach i ddeall a rheoli eu hanghenion o ran sgiliau seiberddiogelwch.

19 Ipsos MORI / DCMS; 'Cyber Security Skills in the UK Labour Market 2021'; Mawrth 2021

DAN SYLW: Sgiliau seiberddiogelwch yn rhan o 'ecosystem seiber' y DU

Cryfhau ecosystem seiber y DU drwy fuddsoddi mewn pobl a sgiliau a dyfnhau'r bartneriaeth rhwng llywodraeth, sefydliadau academaidd a diwydiant yw un o brif golofnau'r Strategaeth Seiber Genedlaethol.

Mae sgiliau seiberddiogelwch yn elfen hanfodol yn yr ecosystem honno ac mae'r Strategaeth Seiber Genedlaethol yn nodi amcan clir i wella ac ehangu sgiliau seiber y DU ar bob lefel. Mae hyn yn cynnwys:

- Cynnydd sylweddol yn nifer y bobl sydd â'r sgiliau y mae arnynt eu hangen i ymuno â'r gweithlu seiber;
- Proffesiwn seiberddiogelwch o ansawdd gwell sy'n gadarnach ac yn fwy cydnabyddedig a strwythuredig;
- Gweithlu seiber mwy amrywiol;
- Cyflenwad cyson ac amrywiol o bobl hyfedr yn dod drwy ein system addysg.

Mae llywodraeth yn rhan allweddol o'r ecosystem hon a bydd ei hymdrechion i ddatblygu'r sgiliau a gwybodaeth briodol o ran seiberddiogelwch yn cyd-fynd ag ymdrechion ehangach ar lefel genedlaethol i wella ecosystem seiber y DU.

95. Er mwyn sicrhau newid cynaliadwy, bydd galw hefyd am newid mewn diwylliant seiberddiogelwch fel y bydd yn cymell ac yn grymuso pobl i herio, cwestiynu, dysgu a hyrwyddo gwelliant parhaus. Elfen ganolog yn hyn yw'r angen i greu amgylcheddau cynhwysol a denu a datblygu gweithlu diogelwch amrywiol sy'n adlewyrchu poblogaeth ehangach y DU.

Sgiliau gofynnol

Canlyniad 20:
Bod dealltwriaeth o holl anghenion llywodraeth am sgiliau seiberddiogelwch

96. Bydd gan lywodraeth ddealltwriaeth cynhwysfawr o faint a chwmpas y sgiliau a gwybodaeth seiberddiogelwch – technegol ac annhechnegol – sydd eu hangen i'w galluogi i weithredu gyda'r cydnerthedd sydd ei angen. Yn ogystal â chyfrannu at ddatblygu strategaethau gweithlu ac adnoddau llywodraeth, bydd y dealltwriaeth hwn yn ategu ac yn cyd-fynd â gwaith Cyngor Seiberddiogelwch y DU i sicrhau bod tacsonomegau, safonau a llwybrau cyson wedi'u datblygu a'u mabwysiadu ar gyfer y proffesiwn seiberddiogelwch ledled y DU.

Denu a chadw talentau

Canlyniad 21:
Bod llywodraeth yn denu ac yn cadw'r gweithlu seiberddiogelwch amrywiol sydd ei angen arni i fod yn gydnerth

97. Yn ogystal â'r bwlch mewn sgiliau seiberddiogelwch yn y DU[20], mae'r gweithlu seiberddiogelwch yn parhau i fod heb yr amrywiaeth sydd ei hangen arno.[21] Mae'n hanfodol denu a chadw gweithlu llywodraeth sy'n gwir adlewyrchu gwahanol ryweddau ac oedrannau, cefndiroedd cymdeithasol, diwylliannol ac ethnig, yn ogystal â niwroamrywiaeth, er mwyn darparu'r gwahanol bersbectifau a'r creadigedd sydd ei angen i fynd i'r afael ag amrywiaeth gynyddol y bygythiadau a wynebir.

98. Wrth ddatblygu ei dealltwriaeth o'i gweithlu, bydd llywodraeth yn elwa o hynny, yng nghyd-destun y gweithlu seiberddiogelwch ehangach yn y DU, i ddatblygu ei dull o ddenu a chadw talentau. Drwy ddatblygu rhaglenni prentisiaeth ac ôl-radd, ynghyd â rhaglen gynhwysfawr i gyrraedd grwpiau sydd heb gynrychiolaeth ddigonol, parheir i ddenu talentau seiberddiogelwch i rolau lefel mynediad. Fodd bynnag, ceir y rhan fwyaf o'r prinder sgiliau yn y DU, yn cynnwys llywodraeth, mewn swyddi uwch.[22] Drwy fabwysiadu fframwaith tâl sengl ar gyfer gallu seiber ar draws llywodraeth, wedi'i gysylltu ag achredu, sicrheir cysylltiad uniongyrchol rhwng tâl a lefel sgiliau. Bydd hyn yn galluogi llywodraeth i gystadlu'n well â'r sector preifat a denu talentau i'r holl swyddi lle mae eu hangen, yn ogystal â darparu cysondeb rhwng adrannau llywodraeth. Rhoddir mwy o gymhelliad i ddilyn gyrfaoedd seiberddiogelwch drwy nifer o wahanol fentrau, gydag ymdrech i gryfhau'r diwylliant cynhwysol a gwella cynrychiolaeth.

99. Mae llywodraeth yn cydnabod hefyd fod talentau seiberddiogelwch ym mhob rhan o'r DU, a bod llawer mwy o gwmnïau seiberddiogelwch ar gyfartaledd yn Ne-ddwyrain, Gogledd-orllewin a De-orllewin Lloegr ac yn yr Alban.[23] Er mwyn hybu twf rhanbarthol yn y sector, mae'r Adran dros Dechnoleg Ddigidol, Diwylliant, y Cyfryngau a Chwaraeon (DCMS) yn cydweithio'n agos â chlystyrau seiberddiogelwch rhanbarthol, gan eu helpu i ddatblygu ac ehangu eu cyrhaeddiad a'u mewnwelediad i ecosystemau rhanbarthol y sector seiberddiogelwch. Bellach mae mwy nag ugain o sefydliadau clwstwr seiberddiogelwch newydd a sefydledig yn y DU sy'n hyrwyddo ac yn buddsoddi mewn seiberddiogelwch. Er mwyn hybu'r ymdrechion hyn, a thynnu ar y cronfeydd talentau rhanbarthol hyn, mae llywodraeth eisoes wedi dechrau sefydlu ei chanolfannau arbenigedd seiberddiogelwch ei hun mewn gwahanol ranbarthau yn y DU a bydd yn parhau i fuddsoddi mewn rhagor o ganolfannau diogelwch rhanbarthol.

DAN SYLW: Gwasanaeth y ganolfan gweithlu ac adnoddau seiber

Bydd llywodraeth yn sefydlu gwasanaeth canolfan gweithlu ac adnoddau seiber mewnol i wella canlyniadau recriwtio a lleihau'r defnydd o gontractwyr. Mae hyn yn cynnwys cydweithio agos â phartneriaid allanol i ddatblygu brand cryf yn ogystal â recriwtio wedi'i dargedu a marchnata cyfleoedd er mwyn cael gwell canlyniadau o ran amrywiaeth. Bydd goruchwyliaeth ganolog ar y gweithlu seiber yn hwyluso model mwy hyblyg a mwy o symud ar draws llywodraeth.

20 Ipsos MORI / DCMS; 'Cyber Security Skills in the UK Labour Market 2021'; Mawrth 2021
21 NCSC / KPMG; 'Decrypting Diversity: Diversity and inclusion in cyber security'; 2020
22 IPSOS MORI/DCMS; 'Cyber Security Skills in the UK Labour Market 2021'; Mawrth 2021
23 IPSOS MORI/DCMS; 'UK Cyber Security Sectoral Analysis 2021'; Chwefror 2021

Datblygu talentau

Canlyniad 22:
Bod llywodraeth yn datblygu ei gweithlu seiberddiogelwch yn barhaus er mwyn sicrhau ei bod yn cael ac yn cadw'r sgiliau sydd eu hangen

100. Drwy gydweithio â Chyngor Seiberddiogelwch y DU, bydd llywodraeth yn parhau i ddatblygu llwybrau gyrfa cynhwysfawr ar gyfer ei gweithwyr seiberddiogelwch proffesiynol. Bydd y llwybrau hyn yn darparu gyrfaoedd amrywiol a buddiol mewn seiberddiogelwch gyda darpariaeth lawn ar gyfer dysgu a datblygu.

101. Agwedd allweddol ar hyn fydd cyflwyno offeryn asesu sgiliau a fydd yn galluogi llywodraeth i fapio'r bwlch sgiliau seiberddiogelwch yn erbyn rolau allweddol gyda'r bwriad o ddatblygu rhaglenni dysgu a ariennir yn ganolog. Drwy greu cwricwla dysgu cynhwysfawr o'r fath, bydd llywodraeth yn rhoi hwb i broffesiynoli rolau seiberddiogelwch. Ategir hyn drwy bartneriaethau ag academïau dysgu cydnabyddedig a sefydliadau diogelwch, gan sicrhau bod y dysgu'n gyson a'i fod yn agored i'r sefydliadau sector cyhoeddus hynny sydd â llai o adnoddau i'w buddsoddi mewn hyfforddiant.

DAN SYLW: Sefydlu academi dysgu diogelwch llywodraeth

Bydd llywodraeth yn sefydlu academi dysgu gyda'r bwriad o uwchsgilio gweithwyr diogelwch proffesiynol llywodraeth a'r gwasanaeth sifil ehangach. Ymysg disgyblaethau diogelwch eraill, bydd yn datblygu sgiliau technegol ac annhechnegol, yn darparu dosbarthiadau meistr a mynediad at gymwysterau, gan gysylltu â chyrff proffesiynol a sefydliadau academaidd er mwyn sicrhau ansawdd sgiliau mewnol drwy asesu ac achredu.

102. Bydd pwyslais mawr ar ddatblygu dull o achredu sydd wedi'i gysylltu â recriwtio a dyrchafu. Bydd hyn yn sicrhau cydnabyddiaeth i statws y proffesiwn y tu mewn a'r tu allan i'r sector cyhoeddus, a bod sgiliau'n cael eu datblygu yn unol â safonau cenedlaethol a ddiffiniwyd gan Gyngor Seiberddiogelwch y DU.

103. Yn ogystal â llwybrau gyrfa mwy ffurfiol, rhoddir pwyslais ar gryfhau cymuned arweinwyr llywodraeth er mwyn sicrhau bod ganddynt y sgiliau sydd eu hangen. Bydd hyn yn rhan o'n dull o weithredu ar gyfer datblygu'r gymuned seiberddiogelwch ar draws llywodraeth, er mwyn hwyluso a hybu'r gallu i rannu syniadau a dulliau o weithredu, yn ogystal â gwersi i'w dysgu wedi i bethau fynd o chwith. Drwy greu'r cymunedau priodol, bydd rhwystrau'n cael eu chwalu a chydweithwyr ar seiberddiogelwch ar draws llywodraeth yn cael eu galluogi i ddatblygu talentau unigol yn ogystal ag arbenigedd cyffredin.

Gwybodaeth seiberddiogelwch mewn swyddogaethau llywodraeth eraill

Canlyniad 23:
Bod gwybodaeth ac ymwybyddiaeth ddigonol o seiberddiogelwch ar draws swyddogaethau proffesiynol llywodraeth yn sicrhau ystyriaeth i seiberddiogelwch

104. Mae'r angen am seiberddiogelwch yn gymwys i bob maes ac mae angen rhoi ystyriaeth briodol iddo yn yr holl swyddogaethau proffesiynol, o'r proffesiwn Digidol, Data a Thechnoleg (DDaT) hyd at swyddogaethau masnachol a chyfreithiol llywodraeth. Er y bydd graddau'r arbenigedd sydd ei angen yn amrywio yn ôl y swyddogaeth dan sylw, mae gwybodaeth briodol am seiberddiogelwch yn hanfodol.

105. Bydd llywodraeth yn datblygu ei dealltwriaeth o'r anghenion hyn ac yn gweithio ar draws proffesiynau eraill i wella gwybodaeth ac ymwybyddiaeth o seiberddiogelwch, gan roi sylw neilltuol i arweinwyr uwch.

Diwylliant seiberddiogelwch

Canlyniad 24:
Bod diwylliant seiberddiogelwch mewn llywodraeth sy'n grymuso pobl i ddysgu, cwestiynu a herio, gan greu'r gallu i wella ymddygiadau'n barhaus ac arwain at newid cynaliadwy

106. Mae lle canolog i bobl a diwylliant sefydliadol wrth leihau risg. Er mwyn gwneud gwahaniaeth go iawn, rhaid canolbwyntio ar bobl yn ogystal â thechnoleg. Bydd yr ymdrech hon yn dechrau drwy wella gwybodaeth ac ymwybyddiaeth o seiberddiogelwch ymysg holl weithwyr y sector cyhoeddus, gan gadarnhau disgwyliadau gweision cyhoeddus a gwneud ymwybyddiaeth o seiberddiogelwch yn rhan annatod o werthoedd gwasanaeth cyhoeddus. Bydd llywodraeth yn darparu cyngor pwrpasol ac yn cyflwyno mentrau hybu ymwybyddiaeth o lawer math i sicrhau bod holl weithwyr y sector cyhoeddus yn cael mwy o allu i'w diogelu eu hunain a'r sefydliadau llywodraeth y maent yn gweithio iddynt.

107. Bydd llywodraeth yn adeiladu ar y seiliau hyn i greu diwylliant seiberddiogelwch cadarnhaol sy'n cymell ac yn grymuso ei phobl i gymryd camau rhagweithiol ar risg seiberddiogelwch y sefydliad. Bydd arweinyddiaeth, cyfathrebu a chysondeb yn allweddol i hyn, ar lefel yr adran ac ar draws llywodraeth. Bydd strwythurau adrodd tryloyw yn ei gwneud yn hawdd adrodd a bydd pob adroddiad yn cael ei drin yn gyfrinachol ac mewn ffordd sensitif. Ni fydd stigma ynglŷn â chamgymeriadau a bydd achosion yn cael eu deall yn wrthrychol a'r canfyddiadau'n cael eu defnyddio fel cyfleoedd i ddysgu a datblygu. Rhoddir gwybod i bobl am bob cynnydd a bydd y buddion i'r sefydliad yn cael eu hamlygu a'u dathlu.

Pennod 8:

Mesur llwyddiant

Cyflawni'r nod

108. Mae'r strategaeth hon yn amlinellu sut bydd llywodraeth yn adeiladu ac yn cynnal ei chadernid yn wyneb risgiau seiber sy'n datblygu drwy'r amser. Ei nod canolog yw y bydd swyddogaethau hanfodol llywodraeth yn cael eu cryfhau'n sylweddol yn erbyn ymosodiadau seiber erbyn 2025, ac y bydd holl sefydliadau llywodraeth ar draws y sector cyhoeddus yn gallu gwrthsefyll gwendidau a dulliau ymosod hysbys erbyn 2030 ar yr hwyraf. Drwy gyflawni'r nod hwn, bydd llywodraeth gyfan yn darged mwy anodd, fel y bydd modd cyflawni swyddogaethau llywodraeth heb darfu gormodol a chadarnhau awdurdod y DU fel pŵer seiber democrataidd, cyfrifol a blaengar.

109. Nod uchelgeisiol yw hwn. Er mwyn cyrraedd y lefel drefnus a gwrthrychol hon o weledd o risg seiberddiogelwch ym mhob rhan o lywodraeth, bydd angen sefydlu prosesau, mecanweithiau a phartneriaethau cynhwysfawr. Mae'r dasg yn fwy cymhleth am fod lefelau gwahanol o aeddfedrwydd, gallu a chapasiti ar draws sefydliadau llywodraeth. Mae hyn yn berthnasol iawn i adrannau llywodraeth arweiniol y gofynnir iddynt ystyried cyflwr y sefydliadau sector cyhoeddus yn eu maes o ran seiberddiogelwch yn ogystal â'u cyflwr eu hunain yn y cyswllt hwnnw.

110. Oherwydd natur ddynamig a chymhleth gwendidau seiberddiogelwch a'r ffaith bod tactegau, technegau a gweithdrefnau ymosod seiber yn datblygu drwy'r amser, mae her yn codi wrth roi cyfrif am wendidau hysbys. Yn ogystal â hyn, ni ellir ystyried bod gwendidau 'hysbys' yn golygu diffygion diogelwch a ddatgelwyd i'r cyhoedd yn unig. Rhaid rhoi cyfrif hefyd am arferion diogelwch amhriodol sy'n peri bod sefydliad yn agored i seiberymosod i raddau gormodol. Er bod mesur seiberddiogelwch yn dasg ymestynnol, drwy sefydlu fframwaith llywodraeth cydlynol i roi sicrwydd o ran seiberddiogelwch, gyda phroffiliau CAF llywodraeth haenog wedi'u seilio ar broffiliau bygythiadau seiber penodol i lywodraeth, ceir dull cyson a dibynadwy o asesu seibergadernid mewn ffordd sy'n gymesur â'r bygythiadau a wynebir.

111. Felly cyflawnir nod y strategaeth pan fydd holl sefydliadau llywodraeth yn cwrdd â'r canlyniadau a nodir yn y proffil CAF priodol o dan fframwaith sicrwydd seiberddiogelwch llywodraeth o fewn y cyfnodau canlynol:

- Bydd sefydliadau llywodraeth y pennir eu bod yn gyfrifol am swyddogaethau hanfodol yn cwrdd â'r canlyniadau a nodwyd mewn proffil CAF 'uwch' erbyn 2025.
- Bydd holl adrannau llywodraeth ganolog yn cwrdd â'r canlyniadau a nodwyd yn eu proffiliau CAF dynodedig erbyn 2026.
- Bydd yr holl sefydliadau llywodraeth eraill yn cwrdd â'r canlyniadau a nodwyd mewn proffil CAF'Sylfaenol' erbyn 2030.

112. Bydd cynnydd tuag at gyflawni'r nod hwn yn cael ei fonitro'n glir, i ddangos effaith lwyddiannus y strategaeth a hefyd i dynnu sylw at feysydd y mae angen canolbwyntio arnynt. Defnyddir y dangosyddion canlynol i fesur cynnydd tuag at y nod:

- Cyfran y sefydliadau llywodraeth o fewn y cwmpas sydd wedi pennu eu swyddogaethau hanfodol.
- Cyfran y sefydliadau llywodraeth o fewn y cwmpas yr aseswyd eu swyddogaethau hanfodol o dan fframwaith sicrwydd llywodraeth.
- Cyfran y sefydliadau llywodraeth o fewn y cwmpas yr aseswyd bod eu canlyniadau sicrwydd wedi'u cyflawni.

Cynnal mesur priodol o gydnerthedd

113. Wrth i natur y risg a'r bygythiad seiber barhau i ddatblygu, mae'n hollbwysig sicrhau bod y canlyniadau sy'n ofynnol i sefydliadau llywodraeth yn parhau'n briodol. Felly bydd yr holl broffiliau CAF, a'r proffiliau o fygythiadau penodol i lywodraeth sy'n sail iddynt, yn cael eu hadolygu'n rheolaidd i sicrhau bod y canlyniadau gofynnol yn ddigon i gynnal seiberddiogelwch yn wyneb y risgiau sy'n datblygu. Drwy wneud hynny, bydd nod y strategaeth hon yn parhau'n ddilys a sicrheir bod y gallu i gyflawni'r canlyniadau gofynnol yn parhau'n ddangosydd cryf o gydnerthedd llywodraeth.

Dangosyddion perfformiad allweddol sylfaenol

114. Fodd bynnag, derbynnir nad yw'r mesurau a dangosyddion hyn yn ddigon ar eu pen eu hunain i roi darlun llawn o gydnerthedd llywodraeth. Felly ategir y mesurau eang hyn gan nifer o ddangosyddion perfformiad allweddol mwy manwl sy'n seiliedig ar amcanion y strategaeth ac a fydd yn arwain y camau i gyflawni'r strategaeth hon.

115. Cymhwysir nifer o egwyddorion allweddol i lywio'r defnydd o ddangosyddion perfformiad allweddol, gan sicrhau eu bod yn gyson, yn briodol, ac yn darparu'r oruchwyliaeth a'r tryloywder sydd eu hangen i ddangos llwyddiant gwirioneddol, yn ogystal â dal llywodraeth yn atebol.

116. Bydd y canlyniadau gofynnol wedi'u hategu hefyd gan bolisïau trawslywodraethol. Bydd effaith polisïau o'r fath yn cael ei monitro a'i mesur, gyda gwerthuso rheolaidd a thrwyadl. Gyda'i gilydd, bydd y mesurau hyn yn rhoi darlun cynhwysfawr o seibergadernid llywodraeth.

DAN SYLW: Egwyddorion mesur perfformiad

- Bydd dangosyddion perfformiad allweddol yn gosod y baich lleiaf posibl ar sefydliadau llywodraeth.
- Bydd data yn cael eu cynhyrchu'n awtomatig neu ar sail llinellau amser sydd wedi'u cynllunio a'u cytuno ymlaen llaw lle bynnag y bo modd.
- Bydd dangosyddion perfformiad allweddol yn gyraeddadwy.
- Ni cheisir cyflawni dangosyddion perfformiad allweddol ar draul canlyniadau seiberddiogelwch gwirioneddol.
- Bydd dangosyddion perfformiad allweddol yn dangos effeithiau a buddion gwirioneddol (gan gydnabod mai cyfyngedig yw'r data mesuradwy sy'n dangos canlyniadau seiberddiogelwch yn uniongyrchol).

Pennod 9:

Gweithredu'r strategaeth

Gweithredu

117. Gellir grwpio'r mentrau a amlinellwyd yn y strategaeth hon fel a ganlyn:

- Mentrau trawsffurfiol a gyflawnir ar unwaith i sicrhau buddion anghymesur ar draws canlyniadau'r strategaeth.
- Mentrau tymor byr neu ganolig a sefydlir yn ystod cyfnod cyntaf yr adolygiad o wariant.
- Mentrau tymor canolig neu hir sydd heb eu cyllido ar hyn o bryd ac a ddarperir yn ystod cyfnod nesaf yr adolygiad o wariant.

118. Mae mentrau tymor hwy sydd heb eu cyllido wedi cyrraedd gwahanol gamau yn eu datblygiad. Adolygir y rhain yn rheolaidd i sicrhau eu bod yn gyson â blaenoriaethau polisi, eu bod yn rhoi gwerth am arian a bod modd eu cyflawni. Cynhelir adolygiad beirniadol mewn cysylltiad â'r adolygiad o wariant nesaf i sicrhau bod cyllid yn cael ei gyfeirio'n briodol er mwyn cyflawni nod y strategaeth hon.

DAN SYLW: Canolfan Diogelwch Llywodraeth ar gyfer Seiber (Cyber GSeC)

Mae Cyber GSeC yn darparu galluoedd a gwasanaethau o lawer math sy'n helpu sefydliadau llywodraeth i wella eu cyflwr o ran seiberddiogelwch a sicrhau lefel briodol o seibergadernid. Felly mae'n chwarae rhan hanfodol yn y broses o gyflawni canlyniadau'r strategaeth hon.

Yn ei blwyddyn dreialu, cydweithiodd GSeC ag adrannau i'w helpu i gyflwyno cynhyrchion Active Cyber Defence a gynhyrchwyd gan y Ganolfan Seiberddiogelwch Genedlaethol (NCSC) a darparodd wasanaethau arbenigol, dibynadwy, fel yr asesiadau ac adroddiadau Cyber Gap Analysis, yn ogystal â mynediad at ymgynghoriaeth seiber arbenigol. Ar sail y llwyddiant hwn, ehangir Cyber GSeC i gyflawni rôl gynyddol bwysig wrth gynorthwyo llywodraeth i ddelio â gwendidau mewn seiberddiogelwch. Yn ogystal â darparu cymorth pwrpasol i sefydliadau penodol, mae'n darparu gallu hanfodol ar gyfer cyflwyno mentrau a weithredir yn ganolog, gan gyrraedd holl sefydliadau llywodraeth a chanolbwyntio'n benodol ar y rheini sy'n wynebu'r risg fwyaf.

Mae Cyber GSeC yn un o set ehangach o Ganolfannau Diogelwch Llywodraeth sy'n delio â gwahanol ddisgyblaethau diogelwch llywodraeth, o seiberddiogelwch hyd at ddiogelwch ffisegol a phersonél. Mae'r holl Ganolfannau Diogelwch Llywodraeth yn cydweithio'n agos ar faterion trawsbynciol, gan sicrhau bod llywodraeth yn parhau i wella ei chyflwr o ran diogelwch yn yr holl ddisgyblaethau diogelwch.

Cynigion ar gyfer trawsnewid

119. Bydd llywodraeth yn rhoi blaenoriaeth i weithredu ei dau gynnig ar gyfer trawsnewid, a fydd yn darparu'r mecanweithiau sydd eu hangen i hwyluso gwelliant sylweddol ac anghymesur mewn seibergadernid ar draws llywodraeth.

1	Mabwysiadu'r CAF yn fframwaith sicrwydd i lywodraeth, gyda phroffiliau CAF haenog – wedi'u hategu gan broffiliau bygythiadau penodol i lywodraeth – i ymateb i'r gwahanol fygythiadau i swyddogaethau llywodraeth, wedi'u dilysu drwy wirio annibynnol a gwrthrychol lle bo'n gymwys.	Cynlluniau peilot i'w cynnal erbyn diwedd 2022,a'i gyflwyno fesul cam yn dilyn hynny
2	Sefydlu'r GCCC er mwyn datgloi a thrawsnewid y ffordd y mae data seiberddiogelwch yn cael eu defnyddio ar draws llywodraeth.	Gallu dechrau gweithredu yn 2022

Cynllun gweithredu

2022-25	2025-30 Er ei bod yn bosibl na fydd mentrau'n llawn weithredol tan y cyfnod hwn, bydd y gwaith cynllunio a datblygu'n dechrau cyn gynted ag y bo modd
Rheoli risg seiberddiogelwch	
Gwella llywodraethu ac atebolrwydd ar draws llywodraeth Gwella mesurau i ganfod asedau a chanfod rheolaeth ar draws llywodraeth Buddsoddi mewn dulliau rheoli gwendidau, yn cynnwys gwasanaeth adrodd ar wendidau i lywodraeth gyfan Mapio risgiau systemig yng nghadwyn cyflenwi llywodraeth a gweithredu strategaeth gaffael llywodraeth Cymryd camau pellach i gryfhau partneriaethau strategol â'r sector preifat, sefydliadau academaidd a phartneriaid rhyngwladol	Rhannu gwybodaeth well a gynhyrchir yn awtomatig am fygythiadau byw ar raddfa fawr ar draws llywodraeth a'r sector cyhoeddus ehangach
Amddiffyn rhag ymosodiadau seiber	
Gweithredu'r fframwaith 'diogelu drwy ddylunio' ar draws llywodraeth Rheoli, uwchraddio neu gael gwared â thechnoleg etifeddol ar draws ystad llywodraeth Datblygu a rhannu ffurfweddiadau cyffredin ar gyfer cynhyrchion a gwasanaethau digidol cyffredin Treialu a datblygu galluoedd newydd ar y cyd i amddiffyn rhag ymosodiadau ochr yn ochr â chyflwyno Active Cyber Defence ar gyfer y sector cyhoeddus yn ôl blaenoriaeth Cyhoeddi a gweithredu polisi llywodraeth newydd ar ddosbarthiadau data	Harneisio technolegau newydd i wella seiberddiogelwch llywodraeth

2022-25	2025-30 Er ei bod yn bosibl na fydd mentrau'n llawn weithredol tan y cyfnod hwn, bydd y gwaith cynllunio a datblygu'n dechrau cyn gynted ag y bo modd
Canfod digwyddiadau seiberddiogelwch	
Datblygu gallu cynhwysfawr a chymesur ar draws llywodraeth i ganfod digwyddiadau seiberddiogelwch Gwella mecanweithiau i rannu gwybodaeth am ddigwyddiadau ac achosion seiberddiogelwch Sefydlu termau cyffredin i sefydliadau ar gyfer cofnodi gwybodaeth am achosion seiberddiogelwch ac achosion y bu ond y dim iddynt ddigwydd	Monitro diogelwch pob un o systemau digidol llywodraeth yn ddi-dor Harneisio technolegau'r dyfodol i dyfu a chyflymu'r gallu i ganfod digwyddiadau seiberddiogelwch Sefydlu rhaglen strategol i chwilio am fygythiadau i lywodraeth, yn cynnwys y defnydd o allu ar y cyd a thactegau dichell
Lleihau effaith achosion seiberddiogelwch	
Cynnal ymarferiadau seiberddiogelwch rheolaidd ar swyddogaethau hanfodol llywodraeth Proses adolygu annibynnol (dysgu gwersi) ar gyfer yr holl achosion a gwendidau seiberddiogelwch difrifol a/neu drawslywodraethol	Darparu gallu ymarfer arbenigol a fydd ar gael ar draws y sector cyhoeddus
Datblygu'r sgiliau, gwybodaeth a diwylliant priodol ar gyfer seiberddiogelwch	
Sefydlu Academi Dysgu Diogelwch Llywodraeth Datblygu llwybrau gyrfa i broffesiynau seiber llywodraeth Sefydlu nifer o bwyntiau mynediad i'r proffesiwn seiber Cyflawni rhaglen i wella diwylliant seiberddiogelwch	Ehangu'r rhaglen prentisiaethau a hyfforddiant seiber Buddsoddi rhagor mewn canolfannau diogelwch rhanbarthol i lywodraeth Mabwysiadu fframwaith tâl sengl ar gyfer y proffesiwn seiber ar draws llywodraeth

Crynodeb o'r Amcanion a'r Canlyniadau

AMCAN	CANLYNIADAU
Rheoli risg seiberddiogelwch CRYNODEB Rhoi prosesau effeithiol ar waith ar gyfer rheoli risg seiberddiogelwch, llywodraethu ac atebolrwydd fel y gellir canfod, asesu a rheoli risgiau seiberddiogelwch – ar lefel y sefydliad ac ar draws llywodraeth.	1. Bod llywodraeth wedi sefydlu trefniadau llywodraethu gydag atebolrwydd clir fel y gellir rheoli risgiau seiber yn effeithiol ar bob lefel o lywodraeth 2. Bod llywodraeth yn cael gweledegdd a dealltwriaeth cynhwysfawr o'i hasedau digidol sy'n ei galluogi i ganfod a rheoli gwendidau a'r risgiau seiberddiogelwch sy'n codi ohonynt 3. Bod llywodraeth yn cael gweledegdd cynhwysfawr o'r data y mae'n eu trin a'u rhannu fel y bydd yn gallu asesu ac ymateb yn briodol i'r risgiau y maent yn eu dangos 4. Bod llywodraeth yn deall a rheoli risgiau sy'n deillio o gyflenwyr masnachol 5. Bod llywodraeth yn deall y bygythiad y mae'n ei wynebu mewn perthynas â'i swyddogaethau er mwyn cynllunio mesurau lliniaru priodol ar lefel y sefydliad ac ar draws llywodraeth 6. Bod sefydliadau llywodraeth yn cael mynediad amserol at ddata seiberddiogelwch sy'n berthnasol ac o werth ymarferol a fydd yn hybu eu gallu i wneud penderfyniadau effeithiol i reoli risg 7. Bod sicrwydd seiberddiogelwch llywodraeth yn rhoi'r gweledegdd sydd ei angen ar lywodraeth i wneud penderfyniadau effeithiol a hyder bod mesurau seiberddiogelwch priodol wedi'u rhoi ar waith i reoli'r risgiau i'w swyddogaethau 8. Bod partneriaethau strategol â'r sector preifat a phartneriaid rhyngwladol yn cael eu cryfhau ymhellach i wella mesurau amddiffyn rhagweithiol ar raddfa fyd-eang

AMCAN	CANLYNIADAU
Amddiffyn rhag ymosodiadau seiber CRYNODEB Dealltwriaeth o risg seiberddiogelwch yn cyfrannu at fabwysiadu mesurau diogelwch cymesur, a galluoedd a ddatblygir yn ganolog yn rhoi'r gallu i amddiffyn ar raddfa fawr.	9. Bod llywodraeth yn mabwysiadu dull cyffredin o 'ddiogelu drwy ddylunio' i sicrhau bod mesurau seiberddiogelwch priodol a chymesur yn rhan o'r dechnoleg y mae llywodraeth yn ei defnyddio, a bod diogelwch gwasanaethau digidol yn cael ei sicrhau'n barhaus drwy gydol eu cylch bywyd 10. Bod sefydliadau llywodraeth yn defnyddio rheolaethau seiberddiogelwch sy'n gymesur â'u proffil risg er mwyn sicrhau bod risgiau i'w swyddogaethau wedi'u rheoli'n briodol 11. Bod technoleg llywodraeth wedi'i ffurfweddu'n briodol, a bod proffiliau safonol ar gyfer technoleg a saerniaethau cyffredin yn cael eu datblygu a'u diweddaru'n barhaus 12. Bod galluoedd, offer a gwasanaethau a rennir yn mynd i'r afael â phroblemau seiberddiogelwch 'cyffredin' ar raddfa fawr 13. Bod data llywodraeth yn cael eu dosbarthu'n briodol a'u trin a'u rhannu mewn ffordd sy'n gymesur â'r risg y maent yn ei chreu

AMCAN	CANLYNIADAU
Canfod digwyddiadau seiberddiogelwch CRYNODEB Dulliau cynhwysfawr o fonitro systemau, rhwydweithiau a gwasanaethau yn rhoi'r gallu i reoli digwyddiadau seiberddiogelwch cyn iddynt droi'n achosion	14. Bod rhwydweithiau, systemau, cymwysiadau a dyfeisiau llywodraeth yn cael eu monitro i ddarparu gallu cymesur i ganfod bygythiadau seiber o fewn sefydliadau 15. Bod galluoedd canfod a rennir yn darparu ar gyfer canfod ar raddfa fawr ar draws llywodraeth
AMCAN	CANLYNIADAU
Lleihau effaith achosion seiberddiogelwch CRYNODEB Rhwystro ac asesu achosion seiberddiogelwch yn gyflym, fel y gellir ymateb yn gyflym ar raddfa fawr	16. Bod llywodraeth wedi paratoi'n llawn i ymateb i achosion seiber 17. Bod llywodraeth yn ymateb yn gyflym i ddigwyddiadau seiber, ar lefel y sefydliad ac ar draws llywodraeth 18. Bod llywodraeth yn adfer systemau ac asedau a effeithiwyd gan achosion seiberddiogelwch ac yn ailddechrau cyflawni ei swyddogaethau gyda'r lleiaf o darfu arnynt 19. Bod gwersi a ddysgwyd o achosion seiber yn hyrwyddo gwelliannau yn seiberddiogelwch llywodraeth
AMCAN	CANLYNIADAU
Datblygu'r sgiliau, gwybodaeth a diwylliant priodol ar gyfer seiberddiogelwch CRYNODEB Nifer digonol o weithwyr proffesiynol medrus a gwybodus yn cwrdd â'r holl anghenion o ran seiberddiogelwch – yn ymestyn y tu hwnt i arbenigwyr seiberddiogelwch proffesiynol ac yn cynnwys yr holl swyddogaethau proffesiynol lle mae'n rhaid cynnwys seiberddiogelwch yn y gwasanaethau a ddarperir – wedi'i seilio ar ddiwylliant seiberddiogelwch sy'n hybu newid cynaliadwy.	20. Bod dealltwriaeth o holl anghenion llywodraeth am sgiliau seiberddiogelwch 21. Bod llywodraeth yn denu ac yn cadw'r gweithlu seiberddiogelwch amrywiol sydd ei angen arni i fod yn gydnerth 22. Bod llywodraeth yn datblygu ei gweithlu seiberddiogelwch yn barhaus er mwyn sicrhau ei bod yn cael ac yn cadw'r sgiliau sydd eu hangen 23. Bod gwybodaeth ac ymwybyddiaeth ddigonol o seiberddiogelwch ar draws swyddogaethau proffesiynol llywodraeth yn sicrhau ystyriaeth i seiberddiogelwch 24. Bod diwylliant seiberddiogelwch mewn llywodraeth sy'n grymuso pobl i ddysgu, cwestiynu a herio, gan greu'r gallu i wella ymddygiadau'n barhaus ac arwain at newid cynaliadwy

Atodiad: Fframwaith Seiberasesu

Datblygwyd y Fframwaith Seiberasesu (CAF) gan yr NCSC – yn rhinwedd ei rôl fel awdurdod technegol cenedlaethol dros seiberddiogelwch – er mwyn darparu dull systematig a chynhwysfawr o asesu'r graddau y mae risgiau seiber i swyddogaethau hanfodol yn cael eu rheoli gan y sefydliad cyfrifol.

Mae'r CAF yn cynnwys pedwar amcan: rheoli risg diogelwch; amddiffyn rhag ymosodiadau seiber; canfod digwyddiadau seiberddiogelwch; a lleihau effaith achosion seiberddiogelwch.

Mae'r amcanion hyn wedi'u seilio ar 14 egwyddor sydd wedi'u hategu gan 39 o ganlyniadau cyfrannol, sy'n pennu beth sydd angen ei gyflawni – yn hytrach na rhestr wirio o'r hyn sydd angen ei wneud. Mae pob canlyniad cyfrannol wedi'i gysylltu â set o ddangosyddion arfer da. Defnyddir y dangosyddion hyn i ddatblygu proffiliau CAF i sectorau penodol, sy'n disgrifio mesurau seiberddiogelwch priodol a chymesur ar gyfer y sefydliadau hynny.

Amcanion, egwyddorion a chanlyniadau cyfrannol y Fframwaith Seiberasesu[24]

Amcan	Egwyddor	Canlyniad cyfrannol
Rheoli risg diogelwch	Llywodraethu	Cyfeiriad cyffredinol
		Rolau a chyfrifoldebau
		Penderfynu
	Rheoli risg	Proses rheoli risg
		Sicrwydd
	Rheoli asedau	Rheoli asedau
	Cadwyn gyflenwi	Cadwyn gyflenwi
Amddiffyn rhag ymosodiadau seiber	Polisïau amddiffyn gwasanaethau	Datblygu polisïau a phrosesau
		Gweithredu polisïau a phrosesau
	Rheoli hunaniaethau a mynediad	Gwirio, dilysu ac awdurdodi hunaniaethau
		Rheoli dyfeisiau
		Rheoli defnyddwyr breintiedig
		Rheoli hunaniaethau a mynediad (IdAM)

24 NCSC, 'Cyber Assessment Framework version 3.0'; Medi 2019

Amddiffyn rhag ymosodiadau seiber	Diogelu data	Deall data
		Trosglwyddo data
		Storio data
		Data symudol
		Diheintio cyfryngau / cyfarpar
	Diogelwch systemau	Diogelu drwy ddylunio
		Ffurfweddu diogel
		Rheoli diogel
		Rheoli gwendidau
	Rhwydweithiau a systemau cadarn	Paratoi cydnerth
		Dylunio ar gyfer cydnerthedd
		Copïau wrth gefn
	Hyfforddi a hybu ymwybyddiaeth staff	Diwylliant seiberddiogelwch
		Hyfforddiant seiberddiogelwch
Canfod digwyddiadau seiberddiogelwch	Monitro diogelwch	Monitro'r cwmpas
		Diogelu logiau
		Creu rhybuddion
		Canfod achosion diogelwch
		Offer a sgiliau monitro
	Canfod digwyddiadau diogelwch er mwyn amddiffyn	Annormaleddau system i ganfod ymosodiadau
		Canfod ymosodiadau'n rhagweithiol
Lleihau effaith achosion seiberddiogelwch	Cynllunio ar gyfer ymateb ac ymadfer	Cynllun ymateb
		Gallu i ymateb ac ymadfer
		Profion ac ymarferiadau
	Dysgu gwersi	Dadansoddi y rhesymau sylfaenol dros achosion
		Defnyddio achosion i hyrwyddo gwelliannau

Rhestr termau

A

Active Cyber Defence (ACD):
Un o raglenni'r NCSC sy'n ceisio lleihau'r niwed o ymosodiadau seiber cyffredin, yn cynnwys nifer o ymyriadau neu wasanaethau sy'n helpu sefydliad i ganfod a datrys gwendidau, rheoli achosion neu awtomeiddio ffyrdd o darfu ar ymosodiadau seiber. Mae rhai gwasanaethau wedi'u bwriadu ar gyfer y sector cyhoeddus yn bennaf, ac mae eraill ar gael yn fwy eang i'r sector preifat neu ddinasyddion, yn ôl y graddau y maent yn gymwys neu'n ddichonol.

Achos seiber:
Digwyddiad sy'n achosi bygythiad gwirioneddol neu ddichonol i gyfrifiadur, dyfais a gysylltwyd â'r rhyngrwyd, neu rwydwaith – neu ddata sy'n cael eu prosesu, eu storio neu eu trosglwyddo ar y systemau hynny – a all alw am weithredu mewn ymateb i liniaru'r canlyniadau.

Adolygiad Integredig:
Mae Prydain Fyd-eang mewn oes gystadleuol: yr Adolygiad Integredig o Bolisi Diogelwch, Amddiffyn, Datblygu a Thramor, yn disgrifio gweledigaeth y llywodraeth ar gyfer rôl y DU yn y byd dros y degawd nesaf a'r camau y bydd llywodraeth yn eu cymryd hyd 2025.

Adran lywodraeth arweiniol:
Adran lywodraeth sydd â sefydliadau sector cyhoeddus eraill o fewn ei maes.

B

Bygythiad seiber:
Unrhyw beth sy'n gallu niweidio neu danseilio diogelwch systemau gwybodaeth a dyfeisiau a gysylltwyd â'r rhyngrwyd (yn cynnwys caledwedd, meddalwedd a seilwaith cysylltiedig), y data sydd arnynt a'r gwasanaethau a ddarparant, yn bennaf drwy ddulliau seiber.

C

Canolfan Cydweithio Seiber y Sector Ariannol (FSCCC):
Menter a gefnogir gan yr NCSC sy'n creu partneriaeth rhwng yr Awdurdodau Ariannol, diwydiant, a'r Asiantaeth Troseddu Cenedlaethol i wella seibergadernid sector ariannol y DU.

Canolfan Diogelwch Llywodraeth ar gyfer Seiber (Cyber GSeC):
Swyddogaeth sy'n darparu galluoedd a gwasanaethau o lawer math i helpu sefydliadau llywodraeth i wella eu cyflwr o ran seiberddiogelwch a chyrraedd lefel briodol o seibergadernid.

Canolfan Gydgysylltu Seiber Llywodraeth (GCCC):
Menter arfaethedig ar y cyd rhwng Grŵp Diogelwch Llywodraeth, y Swyddfa Digidol a Data Ganolog a'r NCSC, yn cyfuno eu priod swyddogaethau a meysydd arbenigedd i gydgysylltu ymdrechion seiberddiogelwch gweithredol yn well ar draws llywodraeth, trawsnewid y ffordd o ddefnyddio data seiberddiogelwch a chudd-wybodaeth am fygythiadau ar draws llywodraeth a gwella gallu llywodraeth i gydamddiffyn.

Canolfan Seiberddiogelwch Genedlaethol (NCSC):
Awdurdod technegol y DU ar gyfer bygythiadau seiber, yn darparu ymateb cenedlaethol unedig i achosion seiber er mwyn lleihau niwed, helpu i ymadfer a dysgu gwersi ar gyfer y dyfodol.

Cryptograffeg:
Gwyddor neu astudiaeth o ddadansoddi a datrys codau a seiffrau.

Cyber Essentials:
Cynllun sy'n cael ei gefnogi gan lywodraeth gyda chymorth diwydiant i helpu sefydliadau i'w hamddiffyn eu hunain rhag bygythiadau ar-lein cyffredin.

Cyflwr seiber macro:
Asesiad o seibergadernid cyffredinol y sefydliadau sydd o fewn maes adran lywodraeth arweiniol.

Cyrff hyd braich:
Term cyffredin sy'n cwmpasu cyrff cyhoeddus o lawer math, yn cynnwys adrannau anweinidogol, cyrff cyhoeddus anadrannol, asiantaethau gweithredol a chyrff eraill, fel corfforaethau cyhoeddus.

Cwantwm:
Mae technoleg cwantwm yn dibynnu ar egwyddorion ffiseg cwantwm. Bydd y dealltwriaeth a rheolaeth gynyddol o'r hyn a elwir yn 'effeithiau cwantwm' fel arosodiad a chyfrodeddiad yn arwain at nifer o ddatblygiadau newydd a fydd yn sail i'n heconomi a'n cymdeithas mewn perthynas â synhwyro, trosglwyddo ac amgryptio data, amseru a chyfrifiadura.

CYFRINACHOL:
Dosbarth diogelwch llywodraeth sy'n cwmpasu gwybodaeth sensitif iawn sy'n cyfiawnhau mesurau amddiffynnol cryfach i ddiogelu rhag bygythiadau oddi wrth weithredwyr penderfynol a galluog iawn.

Ch

Chwilio am fygythiadau:
Chwilio am fygythiadau seiber yw'r broses ragweithiol o chwilio rhwydweithiau a dyfeisiau i ganfod bygythiadau sy'n osgoi rheolaethau diogelwch.

D

Data seiberddiogelwch:
Unrhyw ddata sy'n berthnasol i seiberddiogelwch, yn cynnwys data am fygythiadau a gwendidau seiber.

Deallusrwydd Artiffisial (AI):
Technoleg lle mae system gyfrifiaduro wedi'i chodio i 'feddwl drosti'i hun', gan ymaddasu a gweithredu'n ymreolus. Gwneir defnydd cynyddol o AI ar gyfer tasgau mwy cymhleth, fel diagnosis meddygol, darganfod cyffuriau, a gwaith cynnal rhagfynegol.

Defnyddiwr:
Person, sefydliad, endid neu broses awtomatig sy'n cael mynediad i system, boed wedi'i awdurdodi neu beidio.

Digidol, Data a Thechnoleg (DdaT):
Y swyddogaeth lywodraeth arbenigol sy'n delio â thechnoleg gwybodaeth a thrawsnewid yn y maes hwn.

Diogelu drwy Ddylunio:
Y ddisgyblaeth o gynnwys mesurau seiberddiogelwch mewn systemau a gwasanaethau digidol ar bob cam yn eu cylch bywyd – o gam cynllunio'r gwasanaeth, hyd at gaffael a ffurfweddu technoleg a'i datgomisiynu ar ddiwedd ei hoes weithredol.

E

Etifeddol:
Systemau, gwasanaethau neu unrhyw gydrannau sy'n cael eu cynnal neu eu cadw'n aneffeithiol gan dimau mewnol, contractwyr, cyflenwyr neu werthwyr.

Ff

Fframwaith Seiberasesu (CAF):
Fframwaith asesu a ddatblygwyd gan yr NCSC sy'n darparu dull systematig a chynhwysfawr o asesu'r graddau y mae risgiau seiber i swyddogaethau hanfodol yn cael eu rheoli gan y sefydliad cyfrifol.

Fframwaith Seiberddiogelwch Sefydliad Cenedlaethol Safonau a Thechnoleg (NIST):
Set o ganllawiau a gyhoeddwyd gan Sefydliad Cenedlaethol Safonau a Thechnoleg UDA i alluogi sefydliadau i reoli risg seiberddiogelwch yn well a'i lleihau, yn ogystal â datblygu dulliau cyfathrebu am risg a rheoli seiberddiogelwch.

Ffurfweddu diogel:
Mesurau diogelwch a weithredir wrth adeiladu a gosod cyfrifiaduron a dyfeisiau rhwydwaith er mwyn lleihau gwendidau seiber diangen.

G

GBEST:
Mae GBEST yn fframwaith efelychu ymosodiadau seiliedig ar gudd-wybodaeth sy'n cael ei ddatblygu a'i reoli gan Swyddfa'r Cabinet. Mae'n deillio o fframwaith CBEST Banc Lloegr ond mae'n canolbwyntio ar feithrin seibergadernid cyffredinol llywodraeth.

Grŵp Diogelwch Llywodraeth:
Yr uned yn Swyddfa'r Cabinet sy'n gyfrifol am oruchwylio, cydgysylltu a darparu diogelwch amddiffynnol yn holl adrannau llywodraeth ganolog, eu hasiantaethau a chyrff hyd braich.

Gwasanaeth adrodd ar wendidau:
Mecanwaith y gellir ei ddefnyddio i rybuddio sefydliad am ddiffygion diogelwch cyn i ymosodwyr fanteisio arnynt.

Gweithredwyr gwasanaethau hanfodol:
Sefydliadau mewn sectorau hollbwysig sy'n dibynnu'n helaeth ar rwydweithiau gwybodaeth, er enghraifft, cyfleustodau, gofal iechyd, trafnidiaeth, a sectorau seilwaith digidol sy'n bodloni'r meini prawf yn Rheoliadau Rhwydwaith a Systemau Gwybodaeth 2018.

Gwendidau:
Diffygion diogelwch mewn rhaglenni meddalwedd y gall ymosodwyr gamfanteisio arnynt.

H

Host Based Capability (HBC):
Mae HBC yn gyfrwng meddalwedd sydd ar gael i adrannau llywodraeth ar gyfer y dyfeisiau SWYDDOGOL a ddefnyddir ganddynt. Mae hyn yn cynnwys gliniaduron, cyfrifiaduron pen bwrdd a gweinyddion. Gosodir y cyfrwng ar ddyfeisiau ac mae'n gweithio yn y cefndir i gasglu metadata technegol.

I

ISO 27001:
Safon y Sefydliad Safonau Rhyngwladol sy'n ymdrin â'r gofynion ar gyfer system rheoli diogelu gwybodaeth.

LI

Llywodraeth:
Y sefydliadau sy'n gweithredu ac yn cyflawni'r swyddogaethau sy'n rhedeg y DU, yn cynnwys adrannau llywodraeth ganolog, cyrff hyd braich, asiantaethau, awdurdodau lleol a sefydliadau eraill yn y sector cyhoeddus ehangach.

Llywodraeth ddatganoledig:
Deddfwrfeydd a gweithrediaethau ar wahân yng Nghymru, yr Alban a Gogledd Iwerddon yn dilyn datganoli, yn gyfrifol am nifer o faterion polisi domestig ac sydd â phŵer i wneud deddfau yn y meysydd hyn.

Llywodraeth ganolog:
Llywodraeth ganolog yw'r holl sefydliadau sy'n cael eu rheoli'n uniongyrchol neu'n anuniongyrchol gan weinidogion llywodraeth.

M

Meddalwedd wystlo:
Meddalwedd faleisus sy'n gwrthod mynediad i'r defnyddiwr at ei ffeiliau, cyfrifiadur neu ddyfais nes telir pridwerth.

Model bygythiadau:
Techneg beiriannu i ganfod bygythiadau, ymosodiadau, gwendidau, a gwrthfesurau a allai effeithio ar system TG.

P

Parthau:
Mae enw parth yn dangos lleoliad sefydliad neu endid arall ar y rhyngrwyd ac mae'n cyfateb i gyfeiriad Protocol Rhyngrwyd (IP).

Profion hacio:
Gweithgareddau sydd â'r bwriad o roi prawf ar allu rhwydwaith neu gyfleuster i wrthsefyll hacio, sydd wedi'u hawdurdodi neu eu noddi gan y sefydliad lle y cynhelir y profion.

Proffil bygythiadau:
Disgrifiad o'r bygythiad i sefydliad a'i asedau, sy'n sail i'r proffil CAF dynodedig o dan broses sicrwydd arfaethedig llywodraeth.

Proffil CAF:
Datganiad o ganlyniadau gofynnol sy'n cyfateb i'r Fframwaith Seiberasesu sy'n adlewyrchu 'proffil bygythiadau' y sefydliad.

Pŵer seiber:
Pŵer seiber yw'r gallu i ddiogelu a hyrwyddo buddiannau cenedlaethol mewn seiberofod neu drwyddo.

R

Risg seiber:
Y dichonoldeb mewn bygythiad seiber penodol i gamfanteisio ar wendidau system wybodaeth ac achosi niwed.

Rosa:
Gallu a gwasanaeth TG mewn llywodraeth sy'n rhoi'r gallu i gydweithio hyd at y lefel GYFRINACHOL gyda'r technolegau diweddaraf.

Rh

Rhaglen Seiberddiogelwch Genedlaethol:
Rhaglen waith a sefydlwyd i weithredu'r Strategaeth Seiberddiogelwch Genedlaethol, a chyflawni ei chanlyniadau strategol.

Rheolaethau seiberddiogelwch:
Y prosesau ac offer y mae sefydliad wedi'u rhoi ar waith i ganfod, atal, lleihau neu wrthweithio risgiau diogelwch.

Rheoli achosion:
Rheoli a chydgysylltu gweithgareddau i ymchwilio i ddigwyddiadau seiber niweidiol gwirioneddol neu ddichonol a all beryglu neu niweidio system neu rwydwaith, a chymryd camau cywiro.

Rheoliadau Rhwydwaith a Systemau Gwybodaeth (NIS):
Rheoliadau yn y DU sy'n darparu mesurau cyfreithiol i hybu lefel ddiogelwch (seibergadernid a chadernid ffisegol) rhwydweithiau a systemau gwybodaeth ar gyfer darparu gwasanaethau hanfodol a gwasanaethau digidol.

Rhwydwaith:
Casgliad o gyfrifiaduron lletyol, ynghyd â'r is-rwydwaith neu ryngrwydwaith y gallant gyfnewid data drwyddynt.

S

Safonau Seiberddiogelwch Gofynnol:
Set o safonau seiberddiogelwch gofynnol a gyflwynwyd yn 2018 y mae llywodraeth yn disgwyl i adrannau lynu wrthynt a rhagori arnynt lle bynnag y bo modd.

Sector cyhoeddus:
Y rhan o'r economi sy'n cynnwys holl lefelau llywodraeth a mentrau a reolir gan lywodraeth.

Seiberddiogelwch:
Amddiffyn systemau a gysylltwyd â'r rhyngrwyd (yn cynnwys caledwedd, meddalwedd a seilwaith cysylltiedig), y data sydd arnynt, a'r gwasanaethau a ddarparant, rhag mynediad nas awdurdodwyd, niwed neu gamddefnydd. Mae hyn yn cynnwys niwed a achoswyd yn anfwriadol, neu'n ddamweiniol, gan weithredwr y system o ganlyniad i fethu â dilyn gweithdrefnau diogelwch neu gael ei ysgogi i wneud hynny.

Seibergadernid:
Y gallu sydd gan sefydliad i barhau i gyflawni a darparu ei brif swyddogaethau a gwasanaethau a sicrhau diogelwch ei ddata er gwaethaf digwyddiadau seiberddiogelwch.

Seiber ymosodol:
Ychwanegu, dileu neu drin data ar systemau neu rwydweithiau er mwyn cael effaith ffisegol, weledol neu wybyddol. Yn aml bydd gweithrediadau seiber ymosodol yn camfanteisio ar wendidau technegol, yn defnyddio systemau neu rwydweithiau mewn ffyrdd na fyddai eu perchnogion neu weithredwyr yn eu bwriadu neu eu cymeradwyo, a gallant ddibynnu ar ddichell neu gambortreadu.

Seilwaith Cenedlaethol Hanfodol (CNI):
Yr elfennau seilwaith hanfodol hynny (sef asedau, cyfleusterau, systemau, rhwydweithiau neu brosesau a'r gweithwyr hanfodol sy'n eu gweithredu a'u hwyluso), y byddai eu colli neu eu peryglu'n gallu arwain at:

a. effaith niweidiol fawr ar argaeledd, cyfanrwydd neu'r gallu i ddarparu gwasanaethau hanfodol – yn cynnwys y gwasanaethau hynny y byddai peryglu eu cyfanrwydd, os digwyddai hynny, yn gallu arwain at golli bywyd neu anafu nifer mawr o bobl – gan ystyried effeithiau economaidd neu gymdeithasol mawr; a/neu
b. effaith sylweddol ar ddiogelwch gwladol, amddiffyn gwladol, neu weithrediadau'r wladwriaeth.

Sicrwydd seiberddiogelwch:
Gwirio bod systemau a phrosesau yn cwrdd â'r gofynion diogelwch penodedig a bod prosesau ar waith i wirio cydymffurfiaeth barhaus.

Swyddfa Digidol a Data Ganolog:
Rhan o Swyddfa'r Cabinet – mae'n arwain y swyddogaeth ddigidol, data a thechnoleg i lywodraeth, gan geisio sicrhau trawsnewid ar raddfa fawr drwy gydweithio ag adrannau a swyddogaethau llywodraeth eraill fel gweithwyr proffesiynol yn y meysydd masnachol, cyflawni prosiectau a diogelwch.

Swyddogaethau llywodraeth ganolog:
Unedau llywodraeth ganolog sydd â chyfrifoldebau trawslywodraethol ac yn darparu gwasanaethau a galluoedd trawslywodraethol.

SWYDDOGOL:
Y lefel isaf yn system Dosbarthiadau Diogelwch Llywodraeth, yn diffinio lefel y cyfrinachedd sydd ei hangen i ddiogelu ased, sy'n cwmpasu'r rhan fwyaf o waith llywodraeth.

T

Tîm coch:
Tîm profion hacio sy'n cyflawni rôl ymosodol, gan ymosod ar systemau cyfrifiadurol er mwyn ymchwilio i'r ffyrdd y byddai gwrthwynebwr gwirioneddol yn ymosod.

Tîm glas:
Tîm sy'n gyfrifol am amddiffyn systemau gwybodaeth y sefydliad drwy gynnal ei safiad diogelwch yn erbyn ymosodwyr ffug (y tîm coch).

Tîm porffor:
Tîm mewn ymarfer profi seiberddiogelwch sy'n cyflawni rôl y tîm coch a'r tîm glas.

Y

Ymarferiad Efelychu Gwrthwynebwyr Seiber Llywodraeth (GCASE):
Mae GCASE yn debyg i GBEST ond ei fod yn darparu sicrwydd llai manwl, er bod modd ei weithredu'n gyflymach.

Ymateb i achosion:
Y gweithgareddau sy'n ymdrin ag effeithiau uniongyrchol byrdymor o achos seiber, a gallant helpu hefyd i ymadfer yn y tymor byr.

Ymosodiad seiber:
Camddefnydd bwriadol o systemau cyfrifiadurol, mentrau a rhwydweithiau sy'n dibynnu ar dechnoleg ddigidol er mwyn gwneud niwed.


WHITEHALL
SW1
CITY OF WESTMINSTER
POLICE

Swyddfa'r Cabinet
70 Whitehall
Llundain
SW1A 2AS