

10 Belangrijke Punten

Voor de aanschaf van een Security & Privacy Trainings Oplossing



Digitale Transformatie, cloud computing en het gebruik van mobiele apparaten zorgen ervoor dat de manier waarop we werken drastisch aan het veranderen is. De verbeterde prestaties en het grotere gebruikersgemak zorgen echter ook dat de kwetsbaarheid voor cybercriminaliteit toeneemt. Met name de aanvallen gericht op gebruikers via laptops, mobiele telefoons, email en andere kanalen komen steeds vaker voor en zijn ook steeds vaker succesvol.

Overheden spelen de laatste jaren op deze kwetsbaarheid in door nieuwe regelgeving rondom data privacy in te voeren. Bekende voorbeelden zijn de European Union's General Data Protection Regulation (GDPR) / Algemene Verordening Gegevensbescherming (AVG) die in mei van 2018 van kracht is gegaan en de California Consumer Privacy Act (CCPA) die in januari 2020 zijn intreden zal doen. Deze nieuwe regelgeving pleit samen met andere industrie standaarden, zoals de ISO 27001 en de Payment Card Industry Data Security Standard (PCI-DSS), voor training van de werknemers op het gebied van online beveiliging.

Bedrijven moeten snel schakelen om in te spelen op de veranderende technologietrends en trainingsprogramma's zijn nodig om te zorgen dat de organisatie aan alle compliancy voldoet zonder daarin de productiviteit en inzetbaarheid van haar werknemers vermindert. Traditionele manieren van training geven zoals het gebruik van PowerPointpresentaties zijn vaak verouderd, niet schaalbaar en niet interactief genoeg voor de gebruikers. Wij zijn van mening dat auditors in te toekomst strenger zullen zijn wanneer het aankomt op het toetsen van de compliance. 'Prep-Kits' en aantonen dat er cursussen bestaan is niet meer voldoende. Bedrijven moeten kunnen aantonen dat er voldoende kennis is van de getoetste onderwerpen en laten zien dat een aanzienlijk percentage van het personeel een jaarlijkse opleiding heeft afgerond met een toereikende score.

Hoewel compliance eisen vergelijkbaar zullen blijven, veranderen de trainingsbehoeften constant. Met factoren als de grootte van de organisatie, cultuur, industrie, regio, taal, beschikbare trainingsplatforms en budget moet rekening worden gehouden bij de aanschaf van een ...



**10 belangrijke punten om
rekening mee te houden
tijdens de aanschaf van een
a Security & Privacy
Trainings Oplossing**

1

Brede Content Library

Met voortdurend veranderende technologie en trends op de werkplek zoals cloud computing, gedistribueerde teams, thuis werken en gebruik van zowel zakelijke als persoonlijke (BYOD) apparaten, is het lastig voor uw personeel en IT-afdeling om het overzicht te bewaren en up to date te blijven.

Geeft u trainingen die ervoor zorgen dat uw organisatie voldoet aan compliance en het risico op een cyberaanval door menselijke fout minimaal houden? Is uw trainingsmateriaal afgestemd op uw bedrijfscultuur, strategie en HR/IT beleid?

Verder zijn wij van mening dat het succes van security en privacy training vergroot wordt wanneer deze twee onderwerpen samen in het lesmateriaal worden verwerkt. Het is belangrijk om niet alleen de focus te leggen op wetgeving binnen de industrie (GDPR, HIPAA, ISO), maar ook om toe te lichten hoe ze zouden moeten worden verwerkt in het de dagelijkse gang van zaken. Zo is het bijvoorbeeld belangrijk dat werknemers binnen de HR-afdeling weten hoe ze persoonsgegevens moeten bewaren en wanneer deze wel of niet mogen verstrekken. Zaken als toereikend wachtwoord management, multi-factor authentication, social engineering awareness en veilig gebruik van mail en cloud toepassingen zijn allemaal aan elkaar gerelateerd. Gebruikers moeten weten wat ze moeten doen en wie ze moeten aanspreken wanneer ze vermoeden dat er een fout is gemaakt met betrekking tot privacy van gegevens

Daarnaast moet de stof interactief en relevant zijn. Trainingsprogramma's moeten zowel algemene als functie specifieke lessen bevatten die makkelijk zijn aan te passen op individuele behoeften. Lessen die gebruik maken van audio, tekst en gamificatie zijn interactief en hebben meer kans om de cultuur en het gedrag van mensen binnen een organisatie te beïnvloeden. Door deze drie factoren in het lesmateriaal te verwerken is het mogelijk voor werknemers om op hun eigen tempo de stof zich eigen te maken op een manier die voor hen het beste blijft hangen.

Kies een leverancier die inhoudelijke kan bieden en vermijd meerdere

2 Modulair & Maatwerk

De bekende fastfoodketen Burger King heeft al 40 jaar 'Have it Your Way' als slogan. De mogelijkheid om een hamburger precies naar je wensen te krijgen is fijn, zo geldt dat ook voor wanneer je een online security en privacy traingsprogramma aanschaft. Sommige (voornamelijk kleinere) organisaties kiezen voor een off the shelf 'Happy Meal' lespakket, terwijl grotere bedrijven graag hun eigen programma willen ontwerpen door hun extra behoeftes.

Wat je behoeften ook zijn, het is fijn om je eigen programma te kunnen ontwerpen en deze vervolgens te kunnen personaliseren met een eigen huisstijl en logo. Ben je op zoek naar 2 lessen van 35 minuten of ga je voor 7 lessen die elk 10 minuten duren en over de loop van het jaar worden aangeboden aan de medewerkers. Jij beslist wat het beste werkt voor jouw werknemers en hoe training over security, privacy en compliance het best geïntegreerd kunnen worden in het trainingsprogramma van het gehele bedrijf. De mogelijkheid om ontwikkelingstrajecten te maken is een handige manier om een aangepast curriculum toe te wijzen aan teams, specifieke rollen en kantoren waar gebruikers volgens een vast schema in hun eigen tempo een cursus kunnen volgen.

De beste verstrekkers van onderwijs bieden klanten de mogelijkheid om hun bedrijfsbeleid te integreren en contactgegevens toe te voegen aan het lesmateriaal. Ze zullen aanpassing van de cursusfunctionaliteit mogelijk maken die voldoen aan het SCARM (Shareable Content Object Reference Model) en wordt herkend door de meeste Learning Management Systems (LMS). U moet bijvoorbeeld de mogelijkheid hebben om tekst en spraak te beheren, kennisbeoordelingen toe te voegen, vragen over de eindevaluatie van de cursus te kunnen plaatsen, het beoordelingscijfer te bepalen en ervoor te kiezen om lineaire progressie te activeren - een instelling die bepaalt of gebruikers door kunnen naar de volgende les op basis van hun eerder behaalde resultaten



3

Cloud-Based & Interoperabel

Sommige bedrijven noemen zichzelf 'Born in the Cloud', we wachten nog steeds op de band die hier een Bruce Springsteen draai aan geeft. Vrijwel alle organisaties maken in de loop van de tijd een digitale transformatie door, migreren naar cloudservices en hebben een hybride van cloud- en legacy-applicaties. Grotere organisaties kunnen opleidingsafdelingen hebben met meerdere leveranciers, afdelingen, wereldwijde kantoren en dochterondernemingen die hun eigen oplossingen beheren.

Ongeacht uw industrie is het belangrijk om een leverancier te kiezen die flexibiliteit biedt en uw platform-, integratie- en consolidatiebehoefte het best kan ondersteunen in de loop van de tijd. Dit betekent dat de verkoper 3 mogelijkheden kan ondersteunen: (1) Voer uw programma uit vanaf het LMS van uw leverancier in de cloud; (2) Gebruik een eigen LMS die zich in de cloud of op locatie bevindt; en (3) het gebruik van een hybride oplossing bestaande uit een combinatie van leveranciersinhoud, LMS en software-API's om informatie over cursisten, cursussen en rapporten uit te wisselen. Bij punt vijf gaan we dieper in op rapportage.

4

Planning & Beoordeling

Wilt u een boost geven aan het succes van uw awareness programma, cultuurverandering stimuleren en indruk maken op uw management? Begin met een goede strategie en plan.

Er staat meer aan het einde van dit rapport, maar hier zijn enkele snelle tips:

- Zoek uit wie wat moet leren
- Coördineer uw programma en eventuele simulaties met HR & Training
- Stel doelen en bepaal hoe u de voortgang wilt meten
- Neem een nulmeting van het programma en gebruikerskennis
- Verzamel al uw rapportagevereisten (CISO, DPO, HR)
- Denk na over communicatie en campagnes

5 Rapportage

Bedrijven hebben hun eigen tools en voorkeuren voor het uitvoeren van rapportage. In het geval van een LMS en trainingsprogramma's gaan de meeste rapportages over gebruikersregistratie en gegevens aangaande het voltooien van de cursus. Je moet weten wie er is geregistreerd, een tijdstempel van wanneer ze de vereiste vakken hebben gevolgd, hun beoordelingsscore als die bestaat en of ze zijn geslaagd.

Wanneer u de rapportagemogelijkheden van leveranciers beoordeelt, wilt u flexibiliteit en diepgang. Er moeten standaard off the shelf rapporten beschikbaar zijn, maar ook de mogelijkheid om zelf rapporten samen te stellen op de manier die het beste past bij de behoeftes binnen uw organisatie. U wilt de mogelijkheid hebben om gegevens in een spreadsheet overzichtelijk te maken, te analyseren of naar een ander rapportagesysteem over te hemelen indien nodig.

Neem contact op met uw data privacy en compliance officer voor rapportage en operationele vereisten met betrekking tot GDPR en andere voorschriften voor gegevensbescherming. LMS-beheerders moeten het opslaan of overdragen van gegevensbestanden met persoonlijke informatie minimaliseren. Het verwijderen van gebruikers uit de gebruikersdatabase moet worden bijgehouden als bewijs van verwijdering.



6 Flexible Administration

Fancy dashboards zijn leuk, maar de oplossing moet de regionale vereisten en personeelsstructuur van uw organisatie ondersteunen.

Zorg ervoor dat u groepen of teams in uw LMS kunt maken en dat de informatie die u voor elke gebruiker nodig hebt, kan worden opgeslagen in de gebruikersdatabase. De mogelijkheid om aangepaste velden naar behoefte te maken is ook belangrijk. Een voorbeeld hiervan is het instellen van de taalvoorkeur van een leerling.

Met een goed LMS kunt u ook de toegang tot velden in het gebruikersprofiel beperken, zodat ze niet kunnen worden gewijzigd tijdens of na registratie in het systeem. We hebben ervaren hoe het uitvoeren van rapporten per afdeling een totale nachtmerrie kan zijn wanneer gebruikers ontelbare verschillende beschrijvingen hebben voor hun afdeling, functie, etc. Sta gebruikers alleen toe hun wachtwoord en contactgegevens bij te werken.

Het laden van batches is een onmisbare functie om een LMS te beheren. U moet de mogelijkheid hebben om uw gebruikerspopulatie, team en toegewezen cursussen en ontwikkelingstracks tijdens de implementatie te laden en vervolgens de database na verloop van tijd te onderhouden.

Privacyregelgeving zoals GDPR bepaalt dat gebruikers het "recht om te worden vergeten" hebben. Als u werkzaamheden binnen de AVG vallen, wilt u controleren of uw leverancier het automatisch opschonen van uw LMS-gebruikersdatabase ondersteunt die gedurende een bepaalde periode zijn gemarkeerd als non-actief.



7 Meertalige Ondersteuning

Meertalige ondersteuning is van cruciaal belang voor klanten die een oplossing in hun lokale taal nodig hebben of om kantoren, personeel en partners wereldwijd te ondersteunen. Bedrijven willen het beheer van hun inhoud en platform centraliseren en de mogelijkheid hebben om hetzelfde programma voor iedereen in hun gewenste taal te lanceren. Ze willen bijvoorbeeld tekst en stem in dezelfde taal of een mix (bijvoorbeeld Engels) kiezen met een tweede taal in ondertitels.

Wanneer u nadenkt over ondersteuning in meerdere talen, kunt u onderstaand een aantal belangrijke punten vinden die wij uit ervaring in het leveranciersonderzoek zouden:

- Wat is de diepgang van talen voor cursussen die vooraf zijn vertaald? Worden de talen die u nodig heeft ondersteund?
- Kan de leverancier aangepaste vertalingen leveren voor talen die niet worden ondersteund? Kunnen aangepaste e-mails van het LMS worden verzonden naar gebruikers die een aangepaste, niet-standaard taal gebruiken voor zaken als registratie, cursusuitnodigingen of wachtwoordresets?
- Zijn de cursussen en LMS meertalig te gebruiken, kunt u een taalvoorkeur voor elke leerling selecteren?
- Heeft de verkoper aantrekkelijke prijzen voor het bundelen van meerdere talen?



8

Simulaties & Phishing

Phishing criminaliteit is een groeiende bedreiging voor cyberbeveiliging die wordt gebruikt om malware, ransomware te plaatsen of gegevens te stelen door in te spelen op de gebruikers achter de apparaten via e-mail, sociale media en websites. Veel bedrijven gebruiken e-mail phishing-simulaties ter versterking van de trainingen.

Deze tools stellen gebruikers bloot aan verschillende phishing-presentatiestijlen en niveaus van verfijning en moeilijkheidsgraad. Simulatie is een geweldige manier om werknemers te identificeren die meer ondersteuning en opleiding nodig hebben. Het stelt uw personeel, IT-beveiliging en klantenserviceteam ook in staat om standaardprocedures te oefenen om schadelijke e-mails te identificeren, analyseren en blokkeren en vervolgens geïnfilterde apparaten uit gebruik te nemen.

De meeste leveranciers hebben een phishing-simulatietool of een aanbevolen partner. In deze whitepaper gaan we niet diep in op de evaluatie van phishing-simulatoren. Belangrijke kenmerken zijn de mogelijkheid voor gebruikers om zelf verdachte e-mails te rapporteren vanuit hun e-mailbox en om gebruikers automatisch in te schrijven voor een korte phishing-cursus wanneer ze klikken op een koppeling in een phishing-e-mail, beter bekend als "Taking the Bait".



9

Flexible Sales Packages

Niemand vindt het leuk om te kopen wat ze niet nodig hebben en om licenties op de plank te hebben liggen. Zorg ervoor dat het aanbod van uw leverancier aansluit op uw huidige behoeften en flexibel genoeg is om op potentiële toekomstige behoeften in te spelen. Als u een klein bedrijf heeft en alleen behoefte of budget heeft voor de eerdergenoemde 'Happy Meal', houd u daar dan aan.

Sommige leveranciers bieden waardevolle abonnementen op trainingspakketten met cursussen, toegang tot een cloud LMS en het gebruik van een phishing-simulator. De mogelijkheid om je verpakte cursusmateriaal aan te passen is een sterk onderscheidend vermogen.

Voor grote ondernemingen en internationale organisaties is de flexibiliteit om abonnementstoegang tot cursuscatalogi te kopen op het gebied van beveiliging, privacy en compliance en vervolgens uw cursussen op maat aan te passen, cursusduur en trainingstraject een groot voordeel. Pakketten op bedrijfsniveau kunnen gebundelde ondersteuning voor een LMS, versterkingsmaterialen, simulatoren en meerdere talen bevatten.

Laat je niet opjagen door gadgets en marketinggimmicks, deze doen het alleen goed op beurzen. Als ze niet bedoeld zijn voor productie, haal ze dan besluitvormingstafel.



10 Experience & Support

Bij het selecteren van een leverancier moet u meer rekening houden met functionaliteit en de kosten van licenties. Hier zijn enkele zaken om mee te nemen:

Heeft de verkoper praktische ervaring met het implementeren van security-, privacy- en complianceprogramma's in uw branche?

Heeft de verkoper kennis van programma-ontwerp, operationele best practices, volwassenheid van programma's en benchmarking?

Vraag naar het servicebeleid van de leverancier. Heeft het gekwalificeerde partners? Hoe lang duurt het voordat ik antwoord krijg op een serviceverzoek?

Vraag om klantreferenties, lees hun blogs en whitepapers - zijn ze een solide materiedeskundige en thought leader?

Onderzoek financiële gezondheid, bedrijfsstatus en nieuwsberichten. Is er activiteit die van invloed kan zijn op uw toekomstige vermogen om de gewenste serviceniveaus te krijgen?



Conclusie

Hoe je dit document het beste kan gebruiken

Wij wensen u veel succes bij het vinden van een leverancier van security-, privacy- en compliance-educatie die aan uw behoeften voldoet. Ter beoordeling zijn hier enkele vragen die u kunt overwegen voordat u met het evaluatieproces begint:

- Wie moeten we trainen (bijv. werknemers, aannemers, partners)?
- Maak een lijst van onze compliance vereisten aangegeven door de industrie en de overheid
- Verzamel historische feedback van IT, CISO, CIO, klantenservice, HR en uw privacyfunctionaris – zoalseerdere inbreuken, gegevenslekken, beleidsmisbruik
- Organisatiestructuur, M&A, nieuwe kantoorlocaties, teams, partners
- Nieuw product, diensten en technologische hulpmiddelen
- Meertalige vereisten, nieuwe kantoren en regio's
- Programma volwassenheid, centralisatie, management, andere training
- Kennis, personeel en cultuur van medewerkers
- Learning management systeem (LMS) – nodig of niet
- Rapportage, gegevensconsolidatie en exportvereisten
- Aangepaste programmastructuur: lange cursussen of korte maandelijkse
- Heeft uw bedrijf een opleidingsafdeling en coördinator?
- Bedrijfs grootte en implementatie - Grote onderneming, middelgrote, MKB
- Ondersteuning van leveranciers - "We hebben hulp nodig!" of "Laat ons met rust, we got this!"
- Wat is je budget? Contract voor één of meerdere jaren mogelijk?

De evaluatie

Eén maat past inderdaad niet bij iedereen. Nadat u doelen heeft gesteld en enkele leidende vragen hebt beantwoord, raden we u aan prioriteit te geven aan de 10 gebieden met een numeriek gewicht naar keuze. Scoor uw leveranciers voor elk gebied (bijv. 1-5), vermenigvuldig elke score met het gewicht en bereken een totale kwantitatieve score.

Aan de kwalitatieve kant, praat met leveranciers om een idee te krijgen van hun cultuur, vraag om referenties, lees beoordelingen en overweeg de stabiliteit van de verkoper. Combineer kwalitatief met kwantitatief en volg altijd je gevoel!



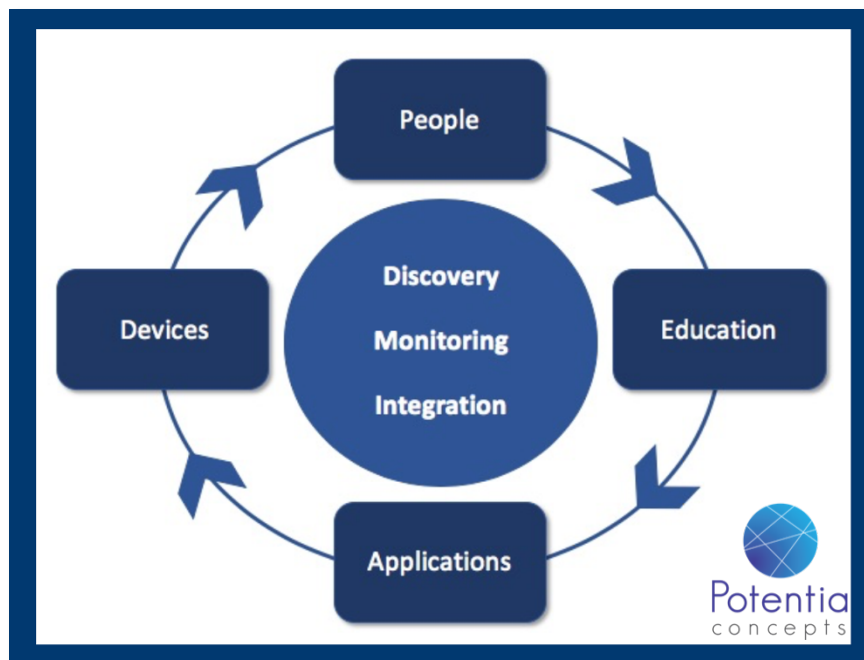
Wat is Human Factor Control and Enablement (HFCE)?

Werknemers zijn uw sterkste pluspunt, maar kunnen ook uw zwakste schakel zijn. Bij het bouwen van uw "zero-trust" en "defense in depth" omgeving is het belangrijk om OSI "Layer-8 - People" te integreren.

HFCE is een programma ontwikkeld door Potentia Concepts om organisaties te helpen hun security- en privacyhouding te versterken en risico's door menselijke factoren te verminderen.

HFCE fase -1 begint met het bekijken en beoordelen van het IT-ecosysteem van een organisatie, kennis van user security, de volwassenheid van het leerprogramma en de ontwikkeling van een nieuw awareness program.

In HFCE fase-2 herontdekken we bedrijfs- en gebruikersapparaten, IT-applicaties en implementeren we een nieuwe IT Access Management-strategie.





Adam Hoey, CEO en oprichter van Potentia Concepts, gehuisvest in Washington DC and Amsterdam.

Wanneer hij niet op de fietst zit, schrijft Adam graag over digitale innovatie, productstrategie, mobiliteit, privacy en human-factor beveiliging.

Lees meer over Adam op:

[Potentia Concepts](#)

[Linked In](#)

Contact Us

Amsterdam | Washington DC

www.potentiaconcepts.com

info@potentiaconcepts.com

