EY Tailored Training Matrix: Veilig omgaan met informatie in een digitaal tijdperk

The better the question. The better the answer.
The better the world works.

Shape the future
with confidence

EY Tailored Training Matrix: Veilig omgaan met informatie in een digitaal tijdperk

Onze wereld digitaliseert en dit raakt ook de samenleving. Enkele recente voorbeelden zijn remote werken van medewerkers (versneld door de COVID pandemie) en de toenemende inzet van kunstmatige intelligentie (AI). Deze digitale transformatie biedt organisaties veel voordelen, maar brengt ook risico's met zich mee op het gebied van informatiebeveiliging. Cybercriminaliteit, en de complexiteit ervan, neemt drastisch toe, waarbij zowel de frequentie als impact groeien. De frequentie van bijvoorbeeld ransomware aanvallen wereldwijd wordt geschat te vervijfvoudigen tussen 2021 en 2031; van een aanval elke 11 seconden naar elke 2 seconden. De geraamde financiële impact van deze aanvallen wordt geschat op 265 miljard in 2031.[1]

> “Naar schatting zal in 2031 elke 2 seconden een cyberaanval plaatsvinden.

Proactieve beveiligingshouding en -cultuur

Cyber incidenten vragen niet alleen om een gedegen IT-technische beveiliging van organisaties, maar benadrukken ook de noodzaak voor een proactieve beveiligingshouding en -cultuur waarin voortdurende informatiebeveiliging bewustwording en training centraal staan. Immers, cyberaanvallen zullen nooit volledig voorkomen kunnen worden door IT-technische maatregelen. Daarnaast blijkt uit onderzoek van IBM dat een overgroot deel van de cyberaanvallen het gevolg is van menselijk handelen en stelt dit onderzoek dat van alle beveiligingsmaatregelen informatiebeveiliging training voor medewerkers de impact van cyber incidenten het meest verlaagt.[2]

Diverse onderzoeken tonen aan dat de menselijke factor een cruciaal punt is binnen informatiebeveiliging, waarbij 50%-95% van de cyberincidenten wordt veroorzaakt door menselijk handelen.[3] Ondanks dit richten veel organisaties hun inspanningen voornamelijk op IT-technische oplossingen en minder op training en bewustwording. Bovendien blijkt uit onderzoek dat training vaak niet direct leidt tot daadwerkelijk veiliger gedrag.[4]

Gebaseerd op onderzoek[5] en hiernaast visueel weergegeven, dient informatiebeveiliging training (1) zich te vertalen in een hoger informatiebeveiliging bewustzijn (2), wat zich op beurt dient te vertalen in voorgenomen veilig gedrag (3) en daadwerkelijk veiliger gedrag in omgang met informatie (4). Echter, doordat training en communicatie (1) zich niet goed vertaalt naar daadwerkelijk gedrag (4) is er sprake van een zogenaamd “conversieverlies” bij elke stap.[5]

Enkele voorbeelden van oorzaken hiervan zijn:

- Training (1) leidt onvoldoende tot beveiliging bewustzijn (2) doordat relevantie van informatiebeveiliging (het waarom) onvoldoende wordt overgebracht aan de training deelnemer.
- Beveiliging bewustzijn (2) leidt niet tot een veiliger voorgenomen gedrag (3) doordat een training deelnemer niet begrijpt wat hij/zij anders moet doen, en
- Voorgenomen gedrag (3) leidt niet tot daadwerkelijk veiliger gedrag (4) doordat een training deelnemer niet begrijpt hoe hij/zij zich daadwerkelijk veiliger moet gedragen.

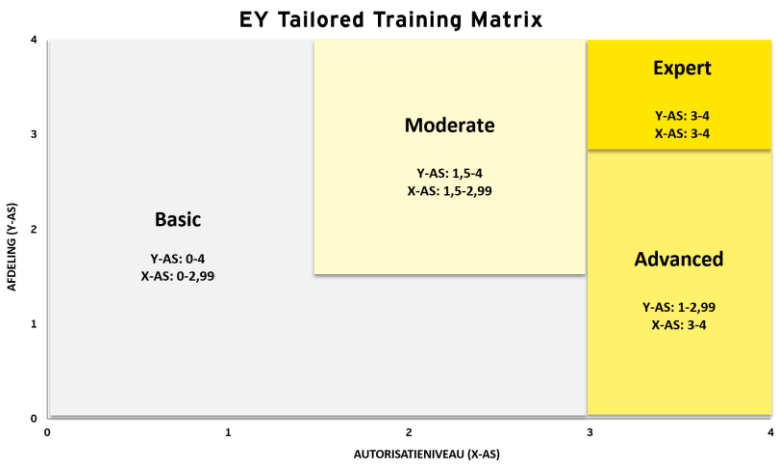
> “Meer dan 50% van alle cyberincidenten valt te wijten aan menselijk gedrag.

Tailored training

Een mogelijke verklaring hiervoor is dat organisaties investeren in generieke informatiebeveiliging trainingen. Hierdoor begrijpt de ontvanger de informatie niet altijd, is de informatie niet altijd relevant voor de ontvanger waardoor de informatie niet goed wordt geregistreerd, is de methode van training niet altijd effectief en/of is de frequentie van training niet altijd voldoende. Het is daarom belangrijk om trainingen te personaliseren naar de behoeften en belangen van medewerkers binnen een organisatie. Deze aanpak, beter bekend als "tailored training", kan de impact van training (1) op daadwerkelijk veiliger gedrag (4) sterk verbeteren. Ondersteund door onderzoek[6] stellen wij daarom dat training effectiever ingezet kan worden en zich beter vertaalt naar daadwerkelijk veiliger gedrag wanneer deze rekening houdt met de verschillende doelgroepen waarop zij gericht is. Praktische handvatten hoe dergelijke training programma's vorm te geven ontbreken echter.

EY introduceert daarom de "EY Tailored Training Matrix"; een dynamisch model dat organisaties helpt trainingen effectiever in te zetten door medewerkers van organisaties in te delen in vier profielen op basis van twee eenvoudig te classificeren dimensie. Op de Y-as staat de afdeling waarin een medewerker werkzaam is en op de X-as het autorisatieniveau van een medewerker afgeleid van het functietype.
Deze dimensies leiden tot een positie in de matrix en daarmee een indeling in één van de vier volgende profielen: "Basic", "Moderate", "Advanced' en "Expert". De matrix is hieronder weergegeven. Wij lichten eerst de twee dimensies toe waarmee organisatie medewerkers kunnen indelen in de matrix waarna wij beschrijven hoe organisaties de vier resulterende profielen kunnen inzetten om informatiebeveiliging training effectiever in te zetten.

> "Onderzoek wijst uit dat op maat gemaakte training voor veiliger gedrag zorgt.



Voor de Y-as van de EY Tailored Training Matrix zijn diverse type afdelingen geclassificeerd op gevoeligheid van informatie en afhankelijkheid van informatie (systemen) die binnen dergelijke afdelingen worden gebruikt. Wij maken hierbij onderscheid tussen a) medewerkers werkzaam op generieke (backoffice) afdelingen die binnen veel organisaties aanwezig zijn (bijv. human resources, inkoop en financiële administratie) en b) medewerkers werkzaam binnen het primair proces van een organisatie (sector specifieke afdelingen).
Voor elk van de generieke afdelingen hebben wij de gevoeligheid van informatie en afhankelijkheid van informatie(systemen) geclassificeerd op basis van het veelgebruikte CIA-model[7] voor informatiebeveiliging, waarbij een score is toegekend aan de Confidentiality (vertrouwelijkheid), Integrity (integriteit) en Availability (beschikbaarheid). Het gemiddelde van de CIA-score geeft de score op de Y-as weer voor de generieke afdelingen. Voor medewerkers werkzaam in het primair proces (sectorspecifieke afdelingen zoals een zorgmedewerker in een ziekenhuis of hypotheekadviseur in een bank) hebben wij de gevoeligheid van informatie en afhankelijkheid van informatie(systemen) geclassificeerd op basis van een gemiddelde score per sector.

Voor de X-as van de EY Tailored Training Matrix maken wij onderscheid tussen zes type functies met elk een bijbehorende score binnen de matrix. Deze score 1 t/m 4 geeft de gemiddelde relevante weer van informatiebeveiliging voor het type functie. De scores voor de Y- en X-as zijn hieronder weergegeven.

Scores Y-as

Medewerkers werkzaam op generieke afdelingen	Score
Administratie	1,3
Klantenservice	1,7
Faciliteiten & Kantoor Management	0,3
Finance & Accounting	2,7
Human Resources	3,0
IT	3,7
Legal & Compliance	2,0
Logistiek en voorraadbeheer	1,7
Marketing & Public Relations	1,7
Inkoop	2,7
Productie	3,0
Research & Development	3,0
Risk Management & Internal Audit	1,3
Sales	2,3

Medewerkers werkzaam in het primair proces (sector specifieke afdeling)	Score
Accommodatie, recreatie en toerisme	2
Milieu, agrarisch sector en food	1
Bouw en Techniek	1
Entertainment	2
Finance	4
Gezondheidszorg en welzijn	4
IT Dienstverlening	4
Nieuws en Media	3
Onderwijs, cultuur en wetenschap	2
Openbaar transport	3
Overheid	3
Retail en handel	3
Vastgoed	1
Water en Nutsvoorzieningen	4
Zakelijke Dienstverlening	3

Scores X-as

Autorisatieniveau van de medewerker	Toelichting	Score
Senior management (C-level executives)	Betreft C-level executives (CEO, CTO, CFO etc.). Dergelijke functies hebben vergaande organisatorische rechten en mandaat, en bijbehorende rechten in IT-systemen. Om deze reden zijn dergelijke functies vaak het doelwit van phishing aanvallen.	4
IT systeem- en netwerkbeheerders	Betreft IT systeembeheerders, netwerkbeheerders met vergaande (superuser) toegang tot informatiesystemen en netwerkcomponenten. Voorbeelden zijn rechten om gebruikers aan te maken en rechten toe te kennen, back-ups benaderen en instellingen in firewalls en andere netwerkcomponenten aanpassen.	4
IT-ondersteunend personeel	Betreft ondersteunend personeel met hogere IT systeem toegang dan een gemiddelde eindgebruiker, maar niet superuser/ administratieve rechten. Voorbeelden zijn IT servicedesk medewerkers.	3
Uitvoerend management	Betreft uitvoerend management zoals afdelingshoofden en teamleiders. Deze medewerkers beschikken veelal over hogere rechten dan de medewerkers die zij aansturen.	3
Administratief personeel	Betreft medewerkers in diverse administratieve uitvoerende functies. Hoewel deze functies veelal niet over hoge rechten beschikken, behandelen zij veelal gevoeligere informatie dan de gemiddelde medewerker en zijn zij in staat om deze informatie in te zien en aan te passen. Voorbeelden zijn HR medewerkers (gevoelige persoonsgegevens) en medewerkers van de financiële administratie (financiële gegevens).	2
Overige medewerkers	Betreft alle overige medewerkers niet behorend tot een van de bovenstaande categorieën. Voorbeelden zijn facilitair medewerkers en tot klantenservicemedewerkers. Gemiddeld genomen hebben dergelijke functies lagere autorisatierechten binnen de IT omgeving van een organisatie.	1

Door medewerkersgroepen te classificeren met bovenstaande scores kunnen zij worden ingedeeld in de matrix. Deze indeling leidt tot de onderstaande vier profielen en bijbehorende training eigenschappen.

Basic	Moderate	Advanced	Expert
Profiel beschrijving			
Veelal operationele functies met beperkte toegang tot gevoelige informatie en beperkte autorisaties.	Functies werkzaam op afdelingen of in sectoren met hoger dan gemiddelde (maar niet de hoogste) toegang tot gevoelige informatie en autorisaties.	Functies met veelal een hogere hiërarchische positionering met als gevolg toegang tot gevoelige informatie en verhoogde autorisaties.	Functies met hoge mate van verantwoordelijkheid (organisatorisch dan wel IT-technisch) en bijkomende informatie- en systeemtoegang.
Training inhoud			
▪ Basis begrip van de noodzaak voor informatiebeveiligin g en de rol van de medewerker hierin. Bijvoorbeeld: leren hoe verdachte e-mails te herken-nen, inzicht geven in het belang van sterke, unieke wachtwoorden en het beheer hiervan. ▪ Basisrichtlijnen meegeven voor veilig gebruik van computers/smart-phones (bijvoorbeeld gebruik van openbare Wi-Fi netwerken, scherm vergrendelen bij verlaten werkplek et cetera).	▪ Begrip vormen bij de medewerker welke informatie hij/zij toegang toe heeft en extra bescherming vereist. Bijvoorbeeld een HR medewerker uitleggen welke informatie in het licht van de AVG/GDPR als gevoelig zijn aangemerkt. ▪ Medewerkers trainen op de te volgen regels en protocollen in de omgang met gevoelige informatie met daarbij aandacht voor generieke beveiligingsmaatregel en. Bijvoorbeeld dat dergelijke informatie niet onversleuteld verzonden mag worden of dat uitgeprinte informatie beveiligd vernietigd dient te worden. Tevens is het van belang niet alleen het "wat" en "waarom", maar ook het "hoe" uit te leggen (bijv. hoe data sharing platforms en/of met wachtwoord beveiligde zip bestanden te gebruiken).	▪ Begrip vormen bij de medewerker over welke verhoogde rechten of bevoegdheden hij/zij beschikt en op welke wijze dit een risico voor de organisatie vormt. ▪ De medewerker trainen in het identificeren van informatiebeveiliging risico's en good practices die relevant voor zijn of haar functie. Bijvoorbeeld voor een netwerkbeheerder uitleggen welke informatie-beveiligingsrisico's op netwerken van toepassing zijn en welke good practices toe te passen (bijv. hanteren leverancier baselines voor configuratie van netwerk componenten). Bijvoorbeeld voor een bestuurder toelichten wat de rol van een bestuurder is in het informatiebeveiliging management systeem (ISMS) en welke good practices beschikbaar zijn (bijv. standaarden waartegen de bestuurder kan laten rapporteren). ▪ Medewerkers uitleggen welke wet- en regelgeving zij compliant mee dienen te zijn (bijvoorbeeld de rol van bestuurders in het licht van de NIS2).	▪ Begrip vormen bij de medewerker over welke verhoogde rechten of bevoegdheden hij/zij beschikt en op welke wijze dit een risico voor de organisatie vormt. ▪ De medewerker informeren over actuele ontwikkelingen in het cyber dreigingenlandschap. ▪ De medewerker trainen in het identificeren van informatiebeveiliging risico's en good practices die relevant voor zijn of haar functie. Bijvoorbeeld voor een netwerkbeheerder uitleggen welke informatie-beveiligingsrisico's op netwerken van toepassing zijn en welke good practices toe te passen (bijv. hanteren leverancier baselines voor configuratie van netwerk componenten). Bijvoorbeeld voor een bestuurder toelichten wat de rol van een bestuurder is in het informatie-beveiliging management systeem (ISMS) en welke good practices beschikbaar zijn (bijv. standaarden waartegen de bestuurder kan laten rapporteren). ▪ Medewerkers uitleggen welke wet- en regelgeving zij compliant mee dienen te zijn (bijvoorbeeld de rol van bestuurders in het licht van de NIS2).

Basic	Moderate	Advanced	Expert
Training methode			
1. Korte virtuele (online based learnings) dan wel fysieke trainingen (bijv. over het herkennen van phishing mails en melden van incidenten). 2. Ad-hoc communicatie zoals visuele geheugensteun op de werkplek (bijv. posters over veilige wachtwoorden), intranet posts en/of informatieve video's die de basisconcepten van informatie-beveiliging verduidelijken.	1. Uitgebreidere basistraining waarbij relevante voorbeelden van te beschermen informatie worden gegeven en middels demo's (live of video) concrete maatregelen worden uitgelegd. 2. Trainingssessies geleid door een cybersecurity expert waarin praktijkvoorbeelden van incidenten worden ontleed en de oorzaak wordt toegelicht en betrokken op de rol van de medewerker.	1. Fysieke training en/of werksessies voor groepen van medewerkers (bijv. netwerkbeheerders, bestuurders etc.). 2. Simulaties van een cyber crisis/ incident zodat de medewerker zijn rol hierbinnen en de te nemen stappen begrijpt. 3. Medewerkers waar relevant (bijv. voor CISO's of bestuurders) deel laten nemen aan kennisplatforms waar kennisuitwisseling met branchegenoten plaatsvindt.	1. Fysieke training en/of werksessies voor groepen van medewerkers (bijv. netwerkbeheerders, bestuurders et cetera.). 2. Simulaties van een cyber crisis/ incident zodat de medewerker zijn rol hierbinnen en de te nemen stappen begrijpt. 3. Medewerkers deel laten nemen aan inspiratie evenementen over informatiebeveiliging (bijv. cybersecurity voor bestuurders evenement). 4. Medewerkers waar relevant voorzien van markt erkende certificaten en/of praktijkopleidingen (bijv. CCNP voor netwerk-beheerders, CISSP voor CISO's en CISM voor bestuurders). 5. Medewerkers waar relevant (bijv. voor CISO's of bestuurders) deel laten nemen aan kennisplatforms waar kennisuitwisseling met branchegenoten plaatsvindt.
Training frequentie			
1. Basis training jaarlijks. 2. Informerende communicatie op meerdere momenten gedurende het jaar.	1. Uitgebreidere basis training elk jaar. 2. Trainingssessie met cybersecurity expert minimaal elke 2 jaar.	1. Training 1 keer per jaar. 2. Cyber crisis/ incident simulaties minimaal elke twee jaar. 3. Deelname aan kennisplatform, indien relevant voor de functie, minimaal jaarlijks.	1. Training 1-2 keer per jaar. 2. Cyber crisis/ incident simu-laties minimaal elke twee jaar. 3. Deelname aan evenementen incidenteel. 4. Certificering of (praktijk)-opleiding incidenteel. 5. Deelname aan kennis-platform, indien relevant voor de functie, minimaal twee keer per jaar.

De EY Tailored Training Matrix stelt organisaties in staat medewerkers effectiever van informatiebeveiliging training te voorzien en beter voor te bereiden voor de informatiebeveiligingsrisico's die voor hen het meest relevant zijn. Wij bevelen organisaties aan een gelaagdheid te hanteren waarbij alle medewerkers worden voorzien van de training gerelateerd aan het "Basic" profiel en indien van toepassing aangevuld met de specifieke training vanuit het profiel waarin de medewerker is ingedeeld ("Moderate", "Advanced" en "Expert"). Menselijk gedrag is een kritieke factor in cybersecurity. Met gerichte training en bewustwording kunnen we effectief bijdragen aan het verminderen van cyberincidenten.

Bronvermeldingen:

1. https://atos.net/en/lp/turning-tables-on-ransomware/the-impact-of-ransomware-attacks-on-business
2. Ponemon Institute (2024). Cost of a Data Breach Report 2024. IBM Security Report.
3. Bronnen:
    a. Ingham, L. (2018). 88% of UK data breaches caused by human error, not cyberattacks - https://www.verdict.co.uk/uk-data-breaches-human-error/.
    b. Haeussinger, F. and Kranz, J. (2013). Understanding the Antecedents of Information Security Awareness - An Empirical Study . Proceedings of the Nineteenth Americas Conference on Information Systems: 1-9.
    c. McCormac, A., Calic, D., Parsons, K., Butavicius, M., Pattinson, M. and Lillie, M. (2018). The effect of resilience and job stress on information security awareness. Information & Computer Security 26(3): 277–289.
    d. Humaidi and Balakrishnan, 2015: Humaidi, N. and Balakrishnan, V (2015). Leadership Styles and Information Security Compliance Behavior: The Mediator Effect of Information Security Awareness. International Journal of Information and Education Technology 5 (4): 311-318.
4. Bronnen:
    a. Khando, K., Gao, S., Islam, S.M., Salman, A. (2021). Enhancing employees' information security awareness in private and public organisations: A systematic literature review. Computers & Security 106: 1-22.
    b. Hanus, B., Windsor, J.C., Wu, Y. (2018). Definition and Multidimensionality of Security Awareness: Close Encounters of the Second Order. The DATA BASE for Advances in Information Systems 49: 103-132.
    c. Karjalainen, M., Siponen, M., Puhakainen, P. and Sarker, S. (2013). One Size Does Not Fit All: Different Cultures Require Different Information Systems Security Interventions. PACIS 2013 Proceedings: 1-15.
    d. Talib, S., Clarke, N.L. and Furnell, S.M. (2010). An Analysis of Information Security Awareness within Home and Work Environments. IEEE 2010 International Conference on Availability, Reliability and Security: 196-203.
    e. Abawajy, J . (2014). User preference of cyber security awareness delivery methods. Behavior & Information Technology 33(3): 237-248.
    f. Annetta, L.A. (2010). The "I's have it: a framework for serious educational game design. Review of General Psychology 14(2): 105-113.
    g. Cone, B.D., Irvine, C.E., Thompson, M.F. and Nguyen, T.D. (2007). A video game for cyber security training and awareness. Computers & Security 26(1): 63-72.
5. De Bruin, J.M. and Mersinas, K. (2022). Individual and Contextual Variables of Cyber Security Behaviour: An empirical analysis of national culture, industry, organisation, and individual variables of (in)secure human behaviour. Cornell University Arxiv
6. Bronnen:
    a. Chua, H.N., Wong, S.F., Low, Y.C. and Chang, Y. (2018). Impact of employees' demographic characteristics on the awareness and compliance of information security policy in organizations. Telematics and Informatics 35: 1770-1780.
    b. Hu, Q., Dinev, T., Hart, P. and Cooke, D. (2012). Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture. Decision Sciences 43(4): 615-659.
7. Lundgren, B. and Möller, N. (2019). Defining Information Security. Science & Engineering Ethics 25: 419-441.

EY | Building a better working world

EY is building a better working world by creating new value for clients, people, society and the planet, while building trust in capital markets.

Enabled by data, AI and advanced technology, EY teams help clients shape the future with confidence and develop answers for the most pressing issues of today and tomorrow.

EY teams work across a full spectrum of services in assurance, consulting, tax, strategy and transactions. Fueled by sector insights, a globally connected, multi-disciplinary network and diverse ecosystem partners, EY teams can provide services in more than 150 countries and territories.

All in to shape the future with confidence.

ey.com