IMPACT VAN CYBERINCIDENTEN OP PATIËNTVERTROUWEN: EEN VERKENNING

Auteur:

Sjoerd Jetze Dalmeijer

Datum:

december 2021

let's change
YOU. US. THE WORLD.

DE HAAGSE HOGESCHOOL

INLEIDING

Cyberincidenten, zoals een ransomware-aanval, een datalek of datadiefstal, vinden in alle sectoren van de samenleving plaats. Ze gebeuren in het bedrijfsleven, bij de overheid, in het onderwijs en ook binnen de gezondheidszorg. De impact van cyberincidenten kan verschillend zijn afhankelijk van het type incident; de impact wordt meestal direct ervaren bij de primaire bedrijfsvoering. De secundaire effecten, vaak voor de langere termijn, op het personeel, de klanten of patiënten zijn vaak lastiger te meten. Cyberincidenten in de gezondheidssector hebben in de afgelopen jaren in veel verschillende landen plaatsgevonden. Zo deed de NOS in 2017 een anoniem onderzoek bij Nederlandse ziekenhuizen:

> Nederlandse ziekenhuizen zijn kwetsbaar voor aanvallen met een gijzelvirus. Zeker vijftien Nederlandse ziekenhuizen hebben de afgelopen drie jaar te maken gehad met zulke ransomware-aanvallen. In één ziekenhuis werden zelfs 75 computers geïnfecteerd, blijkt uit een rondgang van de NOS onder vijfentwintig ziekenhuizen (Nos.nl, 2017).

De impact van de cyberincidenten en de gevoeligheid van de vertrouwelijke data die mogelijk gelekt of gegijzeld zijn, zien we terug in het feit dat de ziekenhuizen alleen aan het onderzoek wilden meedoen op basis van anonimiteit. De ziekenhuizen gaven hiervoor zelf de volgende verklaring:

> “Als we uitleggen waar we kwetsbaar zijn, trekken we de aandacht van hackers”, aldus een woordvoerder van een academisch ziekenhuis. Twintig andere ziekenhuizen lieten weten vanwege de gevoeligheid ook anoniem niet mee te willen doen (Nos.nl, 2017).

De cyberincidenten die plaatsvinden variëren van datalekken en datadiefstallen tot ransomware-aanvallen (Martin et al., 2017). In 2016 was een ziekenhuis in het Verenigd Koninkrijk twee dagen lang genoodzaakt om alle operaties uit te stellen en patiënten naar andere ziekenhuizen door te verwijzen vanwege een ransomware-aanval (Evenstad, 2016).

De impact van cyberincidenten in de zorgsector zijn meestal direct voelbaar en merkbaar, operaties en zorg moeten worden uitgesteld en er kan serieuze reputatieschade ontstaan voor de zorgverlener en het zorginstituut. Er wordt veel onderzoek gedaan naar deze directe impact en de schade die cyberincidenten kunnen veroorzaken. Patiëntveiligheid is ook een onderwerp dat bij cyberincidenten wordt onderzocht, maar in de huidige literatuur ontbreekt het aan empirisch onderzoek naar de impact van cyberincidenten op het patiëntvertrouwen. Wel worden er aannames en implicaties beschreven die aangeven dat cyberincidenten, zoals datalekken, datadiefstallen en ransomware-aanvallen, in potentie het patiëntvertrouwen kunnen raken en verminderen (Martin et al., 2017; Coventry & Branley 2018).

Om de (mogelijke) impact van cyberincidenten op het patiëntvertrouwen te kunnen meten en onderzoeken, hebben we de volgende onderzoeksvraag opgesteld:

Wat is de impact van cyberincidenten op de (positieve) effecten van patiëntvertrouwen?

Op basis van deze onderzoeksvraag, de bestaande en huidige literatuur over cyberincidenten in de zorg, onderzoek naar het meten van patiëntvertrouwen en onderzoek naar de (positieve) effecten van patiëntvertrouwen, hebben we een vragenlijst ontwikkeld die de (mogelijke) impact van cyberincidenten op het patiëntvertrouwen in kaart brengt.

THEORETISCH KADER

Huidig onderzoek naar cyberincidenten in de zorg en het patiëntvertrouwen

In de huidige wetenschappelijke literatuur wordt beschreven dat cyberincidenten – zoals een datalek (onbevoegden krijgen abusievelijk toegang tot vertrouwelijke gegevens), datadiefstal (onbevoegden breken de ICT-beveiliging om toegang te krijgen tot vertrouwelijke gegevens) en ransomware-aanvallen (aanvallers versleutelen systemen en data waardoor deze niet meer te gebruiken zijn) – in potentie het patiëntvertrouwen kunnen raken en verminderen (Martin et al., 2017; Coventry & Branley, 2018). Maar tot op heden ontbreekt hard empirisch bewijs dat cyberincidenten daadwerkelijk invloed hebben op het patiëntvertrouwen.

Het bestaande onderzoek kan onderverdeeld worden in drie hoofdcategorieën:

1. Onderzoek naar cyberincidenten in de zorg
2. Onderzoek naar het meten van patiëntvertrouwen
3. Onderzoek naar de (positieve) effecten van patiëntvertrouwen

1. Onderzoek naar cyberincidenten in de zorg

In de literatuur zijn verschillende voorbeelden beschreven van cyberincidenten die zich in de zorg hebben afgespeeld. Het gaat bijvoorbeeld om incidenten waarbij gevoelige medische informatie in de zorgsector is gelekt of moedwillig is gestolen door een hacker (Ross, 2017). Een ander voorbeeld uit de literatuur zijn ransomware-aanvallen gericht op ziekenhuizen (Coventry & Branley, 2018; Martin et al., 2017). Uit deze onderzoeken valt op te maken dat de impact van ransomware-aanvallen bijzonder groot kan zijn. Bijvoorbeeld omdat operaties moeten worden uitgesteld en patiënten moeten worden doorverwezen naar andere ziekenhuizen. In deze onderzoeken wordt vooral gekeken naar de directe impact van de cyberincidenten op de bedrijfsvoering en de patiëntveiligheid (Jalali & Kaiser, 2018).

2. Onderzoek naar het meten van patiëntvertrouwen

Er zijn verschillende onderzoeken gedaan naar (de positieve effecten van)patiëntvertrouwen. Daarnaast heeft onderzoek zich gericht op de ontwikkeling van methoden om patiëntvertrouwen te meten. Bekend is het gepubliceerde onderzoek van Anderson en Dedrick (1990), waarin zij de ‘Trust in Physician Scale’ (het vertrouwen in dit meetinstrument) presenteren. Sindsdien begon er systematisch onderzoek plaats te vinden naar patiëntvertrouwen. Er zijn daarna nog verschillende andere meetinstrumenten ontwikkeld, zoals de Kao-questionnaire (Kao et al., 1998) en de Safran-questionnaire (Safran et al., 1998), maar de meest gehanteerde en gangbare is de Wake Forest physician trust scale (WF-questionnaire) van Hall et al. (2002). In de WF-questionnaire staan tien vragen die het patiëntvertrouwen meten op een viertal dimensies: ‘competence’, ‘honesty’, ‘fidelity’ en ‘global trust’ (Bachinger et al., 2009).

Naast het onderzoek dat zich richt op het meten van patiëntvertrouwen is er ook onderzoek uitgevoerd naar de (positieve) effecten van patiëntvertrouwen. Dat vertrouwen essentieel is in de relatie tussen patiënt en arts lijkt vanzelfsprekend, aangezien vertrouwen in alle menselijke interacties een van de basisfundamenten is. Maar hoe wordt vertrouwen, en dan specifiek patiëntvertrouwen, omschreven, welke factoren spelen hierin een rol en welke (positieve) effecten worden hiermee in verband gebracht?

Patiëntvertrouwen valt binnen en heeft overlap met de algemene definitie van vertrouwen, maar wordt gekenmerkt door de specifieke relatie tussen patiënt en zorgverlener en de context van het zorgproces. Thom et al. (2004, p. 125) definiëren patiëntvertrouwen als een interpersoonlijk vertrouwen waarbinnen ‘a core concept is that trust is the acceptance of a vulnerable situation

in which the truster believes that the trustee will act in the truster's best interests'. Voor het meten en operationaliseren van patiëntvertrouwen kunnen we de kenmerken groeperen in de volgende dimensies: technische competenties, interpersoonlijke competenties, agency en het aanvullende domein vertrouwelijkheid.

3. Onderzoek naar de (positieve) effecten van patiëntvertrouwen

Uit onderzoek is naar voren gekomen dat er een sterk verband bestaat tussen patiëntvertrouwen en behandelingstrouw, continuïteit en vertrouwelijkheid. In de praktijk wordt dit gekenmerkt door het opvolgen van het doktersadvies, het volgen van medicatievoorschriften, het tijdig zoeken van medische en preventieve hulp, de terugkomst voor controle, een langdurige relatie met de zorgverlener en het zorginstituut en het delen van persoonlijke en gevoelige informatie. Dit levert allemaal een positieve bijdrage aan het zorgproces (Thom et al., 2004). De positieve effecten kunnen volgens de literatuur worden onderverdeeld in de volgende variabelen: behandelingstrouw, continuïteit en vertrouwelijkheid.

Behandelingstrouw
Een groeiende hoeveelheid bewijs toont aan dat een hoge mate van patiëntvertrouwen leidt tot het volgen van medische adviezen. Thom et al. (1999) hebben in een studie naar patiëntvertrouwen gevonden dat 62% van de personen in de groep met een hoge mate van patiëntvertrouwen altijd de voorgeschreven medicatie gebruikt en de medische adviezen opvolgt. Dit ten opzichte van slechts 14% van de personen in de groep met een laag niveau van patiëntvertrouwen.

Continuïteit
In dezelfde studie van Thom et al. (1999) kwam naar voren dat slechts 3% van de personen in de groep met een hoge mate van patiëntvertrouwen na zes maanden een andere arts hadden gezocht ten opzichte van 24% procent van de personen in de groep met een lage mate van patiëntvertrouwen. Uit aanvullend onderzoek van Safran et al. (2001) bleek dat er een sterk verband bestaat tussen patiëntvertrouwen en een wisseling van zorgverleners of zorginstelling door patiënten (Thom et al., 2004).

Vertrouwelijkheid
Vertrouwen tussen patiënt en zorgverlener is een noodzakelijke randvoorwaarde voor de welwillendheid van een patiënt om persoonlijke en soms gevoelige informatie te delen met de zorgverlener. Persoonlijke informatie en communicatie zijn nodig om goede diagnoses te kunnen stellen binnen de reguliere gezondheidszorg, en ze vormen de basis van de meeste behandelingen in de geestelijke gezondheidszorg (Fuertes et al., 2007; Bordin, 1979). Thom et al. (2004) geven een indicatie dat een hoge mate van patiëntvertrouwen kan leiden tot meer openheid om gevoelige informatie te delen.

Hypotheses over de impact van cyberincidenten op patiëntvertrouwen

Om de impact van cyberincidenten op patiëntvertrouwen te kunnen onderzoeken, bouwen we voort op het bestaande onderzoek dat focust op de positieve effecten van patiëntvertrouwen. Op basis van de indicaties en aannames in de huidige literatuur dat cyberincidenten een negatieve invloed kunnen hebben op patiëntvertrouwen (Martin et al., 2017; Coventry & Branley, 2018) gaan we in dit onderzoek uit van de aanname dat een cyberincident een negatief effect kan hebben op de bekende bestaande positieve effecten van patiëntvertrouwen.
Op basis van de bekende positieve effecten van patiëntvertrouwen uit het hiervoor beschreven onderzoek kunnen we een aantal hypotheses formuleren over de verwachte negatieve effecten van cyberincidenten op patiëntvertrouwen. Deze hypotheses zullen in het vervolg van het onderzoek getoetst worden.

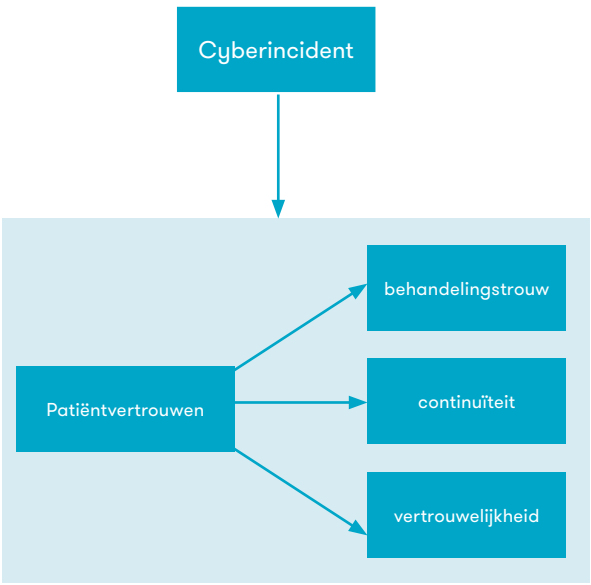
Cyberincidenten kunnen de volgende effecten veroorzaken:

Patiëntvertrouwen
Een vermindering van het niveau in patiëntvertrouwen
Minder vertrouwen van de patiënt in de zorgverlener
Minder vertrouwen van de patiënt in de zorginstelling
Behandelingstrouw
Een verminderd niveau in behandelingstrouwheid
Minder vertrouwen in de aangeboden/geleverde zorg
De patiënt stelt een behandeling of zorg uit of ziet er geheel van af
De patiënt wacht met het zoeken van (preventieve) medische hulp
Continuïteit
De patiënt wisselt van zorgverlener
De patiënt wisselt van zorginstelling
Vertrouwelijkheid
De patiënt is minder open over persoonlijke (gevoelige) informatie

Bij de hypothese over vertrouwelijkheid moet worden vermeld dat deze initieel in de WF-questionnaire ook werd gemeten, maar is komen te vervallen vanwege matige resultaten. Maar gezien de duidelijke relatie tussen vertrouwelijkheid en cyberincidenten en de implicaties als gevolg daarvan, alsmede de hierboven gemelde indicaties in de huidige literatuur van een potentieel effect van cyberincidenten op patiëntvertrouwen, is in het voorliggende onderzoek besloten om deze variabele wel mee te nemen en te meten.

Om de onderzoeksvraag te kunnen beantwoorden, bouwen we voort op het bestaande onderzoek naar patiëntvertrouwen en de bestaande effecten van patiëntvertrouwen. Thom et al. (2004) geven aan dat een hoger niveau van patiëntvertrouwen een positief effect heeft op en een relatie met behandelingstrouw, continuïteit en vertrouwelijkheid. Op basis van deze constatering is de fundamentele hypothese van dit onderzoek als volgt: een cyberincident kan het niveau van patiëntvertrouwen negatief beïnvloeden en verminderen, waardoor de behandelingstrouw, continuïteit en vertrouwelijkheid ook negatief kunnen worden beïnvloed. Deze aanname, die we zullen onderzoeken, is weergegeven in figuur 1, het causale model.

Figuur 1. Het causale model van de impact van cyberincidenten op patiëntvertrouwen



METHODE

Om de impact van cyberincidenten op patiëntvertrouwen te kunnen onderzoeken, zijn er twee (nieuwe) vragenlijsten ontwikkeld op basis van de huidige literatuur en onderzoek. Eén vragenlijst richt zich op het type data-incident datalek/datadiefstal, de andere vragenlijst op het type data-incident ransomware-aanval. Deze vragenlijsten zijn uitgezet onder een panel van respondenten van I&O Research in Amsterdam. I&O heeft een steekproef getrokken die representatief is voor de Nederlandse bevolking. De vragenlijsten hebben uitgestaan in de periode februari-maart 2021. De vragenlijst over het datalek/de datadiefstal is door 1027 mensen beantwoord, de vragenlijst over een ransomware-aanval door 933 mensen.

Zoals eerder vermeld in het theoretisch kader, wijken we in dit onderzoek af van de reeds bestaande WF-questionnaire (Hall et al., 2002) op basis van een aantal afwegingsgronden. De primaire overweging hiervoor is dat de WF-questionnaire specifiek gericht is op het patiëntvertrouwen tussen de arts en de patiënt, terwijl de focus van dit onderzoek breder is en gericht op het patiëntvertrouwen in zowel de zorgverlener als het zorginstituut. De secundaire overweging kent een praktische kant: gezien de onderzoeksvraag en de fundamentele hypothese richt het merendeel van de vragen zich op de te verwachten en te meten effecten van de afhankelijke variabelen: behandelingstrouw, continuïteit en vertrouwelijkheid. De vragen die Hall et al. (2002) in de WF-questionnaire gebruiken, zijn als bron gebruikt bij het formuleren van de geoperationaliseerde definitie van patiëntvertrouwen. Mede op basis van deze vragen zijn de onderstaande twee definities van patiëntvertrouwen in de zorgverlener en het zorginstituut geformuleerd. Deze definities waren voor de respondenten inzichtelijk wanneer hen werd gevraagd naar het niveau van patiëntvertrouwen.

Stelling uit de questionnaire datalek / datadiefstal *
1)Een datalek of datadiefstal vermindert mijn vertrouwen in de deskundigheid* van de zorgverleners (arts, verpleegkundige of ander medisch personeel) van een ziekenhuis.
Definitie van patiëntvertrouwen in de zorgverlener:
* Bij de deskundigheid van een zorgverlener kunt u aan de volgende dingen denken: de zorgverlener heeft goede (medische) kennis, is bekwaam in het uitvoeren van (medische) behandelingen, de zorgverlener luistert en communiceert goed met de patiënt, de zorgverlener geeft duidelijke voorlichting over de diagnose en behandelmogelijkheden, de zorgverlener doet altijd wat het beste is voor de patiënt en de zorgverlener gaat professioneel om met de persoonlijke informatie van de patiënt.
Stelling uit de questionnaire
2) Een datalek of datadiefstal vermindert mijn vertrouwen in de deskundigheid* van een ziekenhuis.
Definitie van patiëntvertrouwen in het zorginstituut:
* Bij de deskundigheid van een zorginstelling kunt u aan de volgende dingen denken: de zorginstelling heeft voldoende en deskundige zorgverleners in dienst, de zorginstelling heeft goede kwalitatieve faciliteiten voor medische zorg (bijvoorbeeld de nieuwste medische apparatuur en operatiekamers), de zorginstelling luistert en communiceert goed met de patiënt, de zorginstelling doet altijd wat het beste is voor de patiënt en de zorginstelling gaat professioneel om met de persoonlijke informatie van de patiënt.

** er is hier alleen een overzicht gegeven van de stellingen uit de questionnaire datalek / datadiefstal, omdat de gehanteerde definitie bij een ransomware aanval geheel identiek is.*

Opzet van de questionnaire en operationalisatie

Voor de operationalisatie van de gemeten variabelen hebben we gekozen voor een enkele factorstructuur in de questionnaire, in lijn met Hall et al. (2004), waarbij voor elke indicator een enkele vraag of stelling is geformuleerd om de waarde te meten. Hieronder staat een overzicht van de gehanteerde variabelen en de geoperationaliseerde indicatoren voor de bijbehorende items; voor de stelling en vragen zie appendix.

Variabele	Indicator
Patiëntvertrouwen	Niveau van vertrouwen in zorgverleners
	Niveau van vertrouwen in zorginstellingen
Behandelingstrouw	Niveau van vertrouwen in de aangeboden zorg
	Het zoeken van medische (preventieve) hulp
	Het opvolgen van medische adviezen en voorschriften
	Het uitstellen van zorg
	Het afzien van zorg
Continuïteit	Het wisselen van zorgverlener
	Het wisselen van zorginstelling
Vertrouwelijkheid	Openheid over persoonlijke informatie met zorgverlener
	Openheid over persoonlijke informatie met zorginstelling

De gehanteerde methode en opzet van de questionnaire voor het meten van patiëntvertrouwen, behandelingstrouw, continuïteit, vertrouwelijkheid en de impact van cyberincidenten hierop is als volgt:

- Een casus waarin een type cyberincident wordt beschreven.
- Elf vragen en stellingen waarmee het effect van het cyberincident op patiëntvertrouwen, behandelingstrouw, continuïteit, vertrouwelijkheid wordt gemeten met een Likertschaal.

Vanuit de epistemologische dimensie hebben we ervoor gekozen om als analyse-eenheid niet het individu te hanteren, maar de ondervraagde groep als geheel. We kijken naar het algemene niveau van patiëntvertrouwen en de bijbehorende variabelen. Zodat we in potentie uitspraken kunnen doen op het bevolkingsniveau van volwassen personen, omdat elke volwassen persoon hoogstwaarschijnlijk op een bepaald moment in zijn leven een patiënt kan zijn. In lijn met de analyse-eenheid van de gehele ondervraagde groep is er in beide casussen voor gekozen om het patiëntvertrouwen te meten op het niveau van de zorgverlener in het algemeen. Wat in de operationalisatie betekent dat er gevraagd is naar het vertrouwen in de deskundigheid van ‘zorgverleners (arts, verpleegkundige of ander medisch personeel) van een ziekenhuis’.
Binnen dit onderzoek is de keuze van de zorginstelling waar het cyberincident plaatsvindt, bewust gesitueerd in een ziekenhuis. De overweging en onderbouwing van deze keuze is als volgt. Met de zorginstelling ‘het ziekenhuis’ krijgt elk individu op enig moment in zijn leven hoogstwaarschijnlijk te maken, in het niet zelf als individueel patiënt dan wel wanneer een ander persoon in de nabije omgeving van de respondent als patiënt in het ziekenhuis terechtkomt. Anders geformuleerd: een ziekenhuis sluit in potentie goed aan bij de gemiddelde belevingswereld van de ondervraagde respondenten. Een aanvullende overweging is dat beide beschreven type cyberincidenten – een datalek/datadiefstal en een ransomware-aanval – een vergelijkbare zichtbare en merkbare impact op de zorginstelling hebben. Een ransomware-aanval bij een huisartsenpraktijk, waar in potentie ook alle respondenten weleens mee te maken zou kunnen krijgen, als zorginstelling zou een minder merkbare impact hebben dan bij een ziekenhuis, en zou daarom de vergelijking van de meetwaarden en resultaten van de twee types cyberincidenten lastiger maken.

RESULTATEN

De resultaten van het onderzoek naar de impact van cyberincidenten op patiëntvertrouwen zijn onder te verdelen in vier categorieën:

1. Vertrouwen in de deskundigheid van zorgverleners in een ziekenhuis (patiëntvertrouwen)
2. Behandelingstrouw
3. Continuïteit
4. Vertrouwelijkheid

1. Vertrouwen in de deskundigheid van zorgverleners in een ziekenhuis (patiëntvertrouwen)

Een ruime meerderheid van 67,4% van de ondervraagde respondenten geeft aan dat een datalek het vertrouwen in de zorgverleners niet vermindert. Bij de tweede casus is ditzelfde patroon terug te zien; daar geeft een nog hoger percentage van 77,4% van de ondervraagden aan dat een ransomware-aanval het vertrouwen niet vermindert. Hiertegenover staat dat bij een datalek of datadiefstal 16,5% aangeeft dat het hun vertrouwen wél vermindert en bij een ransomware-aanval is dit 8,8%.

Wanneer we kijken naar de effecten van een cyberincident op het vertrouwen in de deskundigheid van een zorginstelling, zien we bij de eerste casus een vermindering van vertrouwen van 33,4% en bij de tweede casus van 24,4%. Daar staat tegenover dat bij casus 1 een kleine meerderheid van 44,3% en bij casus 2 een wat ruimere meerderheid van 53,3% aangeeft dat het incident hun vertrouwen niet vermindert.

Wanneer we de vragen en de casussen met elkaar vergelijken, kunnen we een aantal eerste constateringen doen. De impact van een cyberincident is groter op de zorginstelling dan op de zorgverlener, en een datalek of datadiefstal lijkt meer impact te hebben dan een ransomware-aanval. In algemene zin kunnen we constateren dat ongeveer één op de tien personen minder vertrouwen heeft in de deskundigheid van de zorgverleners, en dat een kwart tot een derde van de mensen minder vertrouwen heeft in de zorginstelling nadat een cyberincident heeft plaatsgevonden.

Casus 1 Datalek/datadiefstal

#	Vragen	helemaal eens		eens		neutraal		oneens		helemaal oneens	
		n	%	n	%	n	%	n	%	n	%
V1	Een datalek of datadiefstal vermindert mijn vertrouwen in de deskundigheid* van de zorgverleners (arts, verpleegkundige of ander medisch personeel) van een ziekenhuis.	29	**2,8**	140	**13,6**	166	**16,2**	451	**43,9**	241	**23,5**
V2	Een datalek of datadiefstal vermindert mijn vertrouwen in de deskundigheid* van een ziekenhuis.	63	**6,1**	280	**27,3**	229	**22,3**	326	**31,7**	129	**12,6**

Casus 2 Ransomware-aanval

#	Vragen	helemaal eens		eens		neutraal		oneens		helemaal oneens	
		n	%	n	%	n	%	n	%	n	%
V1	Een ransomware aanval vermindert mijn vertrouwen in de deskundigheid* van de zorgverleners (arts, verpleegkundige of ander medisch personeel) van een ziekenhuis	18	**1,8**	70	**7,0**	138	**13,7**	506	**50,4**	271	**27,0**
V2	Een ransomware aanval vermindert mijn vertrouwen in de deskundigheid* van een ziekenhuis	34	**3,4**	211	**21,0**	223	**22,2**	382	**38,0**	153	**15,2**

2. Behandelingstrouw

Wanneer we de vragen en resultaten bekijken die de potentiële effecten van een cyberincident op de variabele behandelingstrouw meten, kunnen we de volgende bevindingen rapporteren. Bij casus 1 geeft een meerderheid van 71,6% aan dat het vertrouwen in de kwaliteit van de aangeboden zorg niet wordt verminderd, bij casus 2 is dit exact dezelfde meerderheid van 71,6%. Aan de andere kant kunnen we constateren dat bij casus 1 13,1% en bij casus 2 11,4% van de respondenten wel minder vertrouwen in de kwaliteit van de aangeboden zorg heeft. De impact van een cyberincident op het vertrouwen is dat ongeveer **één** op de tien personen minder vertrouwen heeft, het type cyberincident lijkt hierbij niet veel verschil te maken.

De impact die een datalek of datadiefstal heeft op het tijdig zoeken van hulp voor een (medisch) probleem, is dat 14,3% aangeeft dat ze mogelijk zouden wachten en 70,5% dat het cyberincident geen invloed heeft. Bij een potentiële ransomware-aanval geeft 19,5% aan dat een cyberincident een negatieve invloed kan hebben op het tijdig zoeken van hulp en 59,5% dat het geen impact heeft. Bij beide typen cyberincidenten geeft een ruime meerderheid van de ondervraagden aan dat deze geen negatieve invloed hebben, maar hier staat wel tegenover dat **één** op de tien tot ongeveer **één** op de vijf personen wacht met het tijdig zoeken van hulp. Een ransomware-aanval lijkt hierop een grotere negatieve invloed te hebben.

Vraag 5 van de questionnaire richt zich op het fenomeen 'het opvolgen van medische adviezen en medicatievoorschriften zoals aangegeven door de zorgverlener'. De uitkomsten van de effecten van een cyberincident zijn dat bij casus 1 een zeer ruime meerderheid van 85,6% en bij casus 2 van 81,1% aangeeft dat dit geen invloed heeft. Slechts een heel klein percentage van 3,5% bij de eerste casus en 6,8% bij de tweede casus geeft aan dat het potentieel wel een negatieve invloed heeft. Deze laatste percentages zijn dusdanig laag dat we in algemene zin kunnen concluderen dat een cyberincident geen tot weinig negatieve impact heeft op de opvolging van medische adviezen en medicatievoorschriften.

De laatste twee vragen van behandelingstrouw meten het mogelijk negatieve effect op het uitstellen of afzien van een medische behandeling of afspraak bij een ziekenhuis. Bij een datalek of datadiefstal geeft respectievelijk 72% en 78,9% van de ondervraagden aan dat dit geen negatief effect heeft. En 11,9% geeft aan dat ze mogelijk een medische behandeling of afspraak uitstellen en 7,1% dat ze er mogelijk geheel van afzien. Wanneer we dezelfde effecten bij een ransomware-aanval bekijken, kunnen we constateren dat 58,7% aangeeft dat ze een medische behandeling of afspraak niet zouden uitstellen en 71,6% dat ze er niet van afzien. 20,6% van de ondervraagden geeft aan dat ze mogelijkerwijs wel een medische behandeling of afspraak uitstellen en 11,1% dat ze er mogelijk van afzien. De resultaten lijken te indiceren dat een ransomware-aanval een grotere impact heeft op het uitstellen of afzien van een medische behandeling of afspraak bij een ziekenhuis, waarbij **één** op de vijf personen mogelijkerwijs uitstelt en **één** op de tien personen er geheel van afziet.

Casus 1 Datalek/datadiefstal

#	Vragen	helemaal eens		eens		neutraal		oneens		helemaal oneens	
		n	%	n	%	n	%	n	%	n	%
V3	Een datalek of datadiefstal vermindert mijn vertrouwen in de kwaliteit van de aangeboden zorg van een ziekenhuis.	37	**3,6**	98	**9,5**	157	**15,3**	481	**46,8**	254	**24,7**
V4	Een datalek of datadiefstal kan ervoor zorgen dat ik wacht met zoeken van hulp voor een (medisch) probleem.	14	**1,4**	133	**13,0**	156	**15,2**	484	**47,1**	240	**23,4**
V5	Een datalek of datadiefstal kan ervoor zorgen dat ik niet de medische adviezen en (medicatie-) voorschriften volg zoals aangegeven door de zorgverlener (arts, verpleegkundige of ander medisch personeel) van een ziekenhuis.	6	**0,6**	30	**2,9**	112	**10,9**	533	**51,9**	346	**33,7**
V6	Een datalek of datadiefstal kan ervoor zorgen dat ik een (medische) behandeling of afspraak bij een ziekenhuis uitstel.	12	**1,2**	110	**10,7**	166	**16,2**	476	**46,3**	263	**25,6**
V7	Een datalek of datadiefstal kan ervoor zorgen dat ik van een (medische) behandeling of afspraak in een ziekenhuis afzie.	9	**0,9**	64	**6,2**	144	**14,0**	505	**49,2**	305	**29,7**

Casus 2 Ransomware-aanval

#	Vragen	helemaal eens		eens		neutraal		oneens		helemaal oneens	
		n	%	n	%	n	%	n	%	n	%
V3	Een ransomware-aanval vermindert mijn vertrouwen in de kwaliteit van de aangeboden zorg van een ziekenhuis.	17	**1,7**	97	**9,7**	171	**17,0**	505	**50,3**	214	**21,3**
V4	Een ransomware-aanval kan ervoor zorgen dat ik wacht met zoeken van hulp voor een (medisch) probleem.	28	**2,8**	168	**16,7**	210	**20,9**	431	**42,9**	166	**16,5**
V5	Een ransomware-aanval kan ervoor zorgen dat ik niet de medische adviezen en (medicatie-) voorschriften volg zoals aangegeven door de zorgverlener (arts, verpleegkundige of ander medisch personeel) van een ziekenhuis.	7	**0,7**	61	**6,1**	121	**12,1**	539	**53,7**	275	**27,4**
V6	Een ransomware-aanval kan ervoor zorgen dat ik een (medische) behandeling of afspraak bij een ziekenhuis uitstel.	27	**2,7**	180	**17,9**	208	**20,7**	411	**40,9**	178	**17,7**
V7	Een ransomware-aanval kan ervoor zorgen dat ik van een (medische) behandeling of afspraak in een ziekenhuis afzie.	17	**1,7**	94	**9,4**	173	**17,2**	493	**49,1**	226	**22,5**

3. Continuïteit

Een hoge mate van continuïteit van een patiënt bij een zorgverlener en zorginstelling wordt als een positief effect van patiëntvertrouwen genoemd. Een hoge mate van continuïteit betekent in werkelijkheid dat een patiënt weinig van zorgverlener en zorginstelling wisselt. Dit zorgt ervoor dat de zorgverlener en de zorginstelling een langdurige relatie met de patiënt kan opbouwen, die positief bijdraagt aan het stellen van diagnoses en het volgen en uitvoeren van een (langdurige) behandeling. Wanneer een patiënt vanwege een cyberincident (vaker) zou wisselen van zorgverlener of zorginstelling, spreken we in dit onderzoek van een lage mate van continuïteit.

Het type cyberincident datalek of datadiefstal kent de volgende potentiële effecten op continuïteit: 66,4% van de ondervraagden geeft aan niet te wisselen van zorgverlener en 48,1% geeft aan niet te zullen wisselen van zorginstelling. Bij het type cyberincident ransomware-aanvallen zien we dat 65,7% niet wisselt van zorgverlener en 48,3% niet zal wisselen van zorginstelling. Bij beide type incidenten geeft een ruime meerderheid aan dat deze geen negatief effect hebben. Aangezien de percentages getalsmatig bijna identiek zijn, lijkt het type incident geen verschil te maken. Wanneer we kijken naar de gerapporteerde negatieve effecten vallen er bij beide type cyberincidenten wederom bijna identieke percentages te zien. Bij een datalek of datadiefstal geeft 13,3% aan dat ze mogelijk zouden wisselen van zorgverlener en 27,7% dat ze mogelijk zouden wisselen van zorginstelling, bij een ransomware-aanval is dit respectievelijk 14% en 27,7%. We kunnen vrij zeker vaststellen dat het type cyberincident weinig verschil maakt, en dat de potentiële negatieve effecten kunnen betekenen dat na een cyberincident één op de tien personen zou kunnen wisselen van zorgverlener en bijna één op de vier personen zou kunnen wisselen van zorginstelling.

Casus 1 Datalek/datadiefstal

#	Vragen	helemaal eens		eens		neutraal		oneens		helemaal oneens	
		n	%	n	%	n	%	n	%	n	%
V8	Een datalek of datadiefstal kan ertoe leiden dat ik voor een andere zorgverlener (arts, verpleegkundige of ander medisch personeel) in het ziekenhuis kies.	30	**2,9**	103	**10,0**	212	**20,6**	481	**46,8**	201	**19,6**
V9	Een datalek of datadiefstal zou ertoe kunnen leiden dat ik voor een ander ziekenhuis kies.	54	**5,3**	230	**22,4**	249	**24,2**	347	**33,8**	147	**14,3**

Casus 2 Ransomware-aanval

#	Vragen	helemaal eens		eens		neutraal		oneens		helemaal oneens	
		n	%	n	%	n	%	n	%	n	%
V8	Een ransomware aanval kan er toe leiden dat ik voor een andere zorgverlener (arts, verpleegkundige of ander medisch personeel) in het ziekenhuis kies	22	**2,2**	119	**11,9**	202	**20,1**	453	**45,1**	207	**20,6**
V9	Een ransomware aanval zou er toe kunnen leiden dat ik voor een ander ziekenhuis kies	45	**4,5**	233	**23,2**	241	**24,0**	353	**35,2**	132	**13,1**

4. Vertrouwelijkheid

De impact van een cyberincident op de vertrouwelijkheid vertaalt zich naar de mate waarin een patiënt zich veilig voelt om (gevoelige) informatie te delen met een zorgverlener of zorginstelling. Bij casus 1 rapporteert 49,3% van de ondervraagden niet minder informatie te delen met een zorgverlener en 41,8% niet minder informatie te delen met een zorginstelling. Maar 30,3% geeft aan potentieel wel minder informatie te delen met een zorgverlener en 36,3% minder informatie te delen met een zorginstelling. Bij casus 2 geeft 48,5% aan niet minder informatie te delen met een zorgverlener en 43,1% niet minder informatie te zullen delen met de zorginstelling. Maar 29,1% geeft aan potentieel wel minder informatie te delen met de zorgverlener en 34,5% minder informatie te delen met een zorginstelling. Uit de verschillende percentages lijkt naar voren te komen dat er qua impact weinig verschil is wat betreft het type cyberincident, maar in algemene zin kunnen we wel concluderen dat bijna één op de drie personen na een cyberincident mogelijk minder persoonlijke (gevoelige) informatie met de zorgverlener of zorginstelling zal delen.

Casus 1 Datalek/datadiefstal

#	Vragen	helemaal eens		eens		neutraal		oneens		helemaal oneens	
		n	%	n	%	n	%	n	%	n	%
V10	Een datalek of datadiefstal kan ervoor zorgen dat ik minder persoonlijke (gevoelige) informatie deel met een zorgverlener (arts, verpleegkundige of medisch personeel) van het ziekenhuis.	49	**4,8**	262	**25,5**	209	**20,4**	360	**35,1**	146	**14,2**
V11	Een datalek of datadiefstal kan ervoor zorgen dat ik minder persoonlijke (gevoelige) informatie deel met een ziekenhuis.	69	**6,7**	301	**29,3**	228	**22,2**	308	**30,0**	121	**11,8**

Casus 2 Ransomware-aanval

#	Vragen	helemaal eens		eens		neutraal		oneens		helemaal oneens	
		n	%	n	%	n	%	n	%	n	%
V10	Een ransomware aanval kan er voor zorgen dat ik minder persoonlijke (gevoelige) informatie deel met een zorgverlener (arts, verpleegkundige of medisch personeel) van het ziekenhuis	47	**4,7**	245	**24,4**	224	**22,3**	363	**36,2**	124	**12,4**
V11	Een ransomware aanval kan er voor zorgen dat ik minder persoonlijke (gevoelige) informatie deel met een ziekenhuis	64	**6,4**	282	**28,1**	225	**22,4**	321	**32,0**	112	**11,2**

CONCLUSIES

De resultaten van het onderzoek naar de impact van cyberincidenten op patiëntvertrouwen laten de volgende gemengde effecten zien:

- Als het gaat om de effecten op de verschillende afhankelijke variabelen – patiëntvertrouwen, behandelingstrouw, continuïteit en vertrouwelijkheid – blijft bij alle variabelen bij een meerderheid van de respondenten het vertrouwen intact en blijven de positieve effecten van patiëntvertrouwen onaangetast.

- Hiertegenover staat dat bij alle afhankelijke variabelen een cyberincident bij een kleiner percentage van de respondenten, variërend tussen ongeveer 10 en 30%, wel een meetbaar en terugkerend negatief effect heeft.

- Wanneer we kijken naar de verschillende uitkomsten tussen de twee gehanteerde casussen – de typen cyberincidenten datadiefstal of datalek en ransomware-aanval – is er geen duidelijk patroon te herkennen en te duiden. De uitslagen variëren wel in sommige gevallen, maar soms is het percentage hoger bij casus 1 en soms bij casus 2. Deze verschillen zijn mogelijk te verklaren door de variatie van de respectievelijke opvattingen en samenstelling van de groepen respondenten.

- Een aanvullend patroon dat zichtbaar lijkt te worden, is dat de negatieve impact groter is op het vertrouwen in de zorginstelling dan op het vertrouwen in de zorgverlener. Dit komt naar voren bij de afhankelijke variabelen patiëntvertrouwen, continuïteit en vertrouwelijkheid. Bij deze variabelen lijkt er een significant grotere impact te zijn op het vertrouwen in de zorginstelling, bij patiëntvertrouwen en continuïteit is de impact relatief gezien bijna 50% groter.

De meeste en grootste impact van de vermindering van vertrouwen en de negatieve effecten hiervan zijn gemeten bij het patiëntvertrouwen, het uitstel of afzien van een medische behandeling of afspraak en het delen van persoonlijke gevoelige informatie met de zorgverlener. Het patiëntvertrouwen in de zorginstelling heeft in casus 1 een negatieve impact bij 33,4% van de respondenten. Ook bij het delen van persoonlijke gevoelige informatie met de zorgverlener of zorginstelling ligt het percentage rond of boven de 30%. Dit betekent dat bij ongeveer één op de drie respondenten het cyberincident een negatief effect kan veroorzaken. Wat zijn de mogelijke consequenties van de gemeten effecten gerelateerd aan een cyberincident? Wat zijn de consequenties van een verminderd patiëntvertrouwen op de afhankelijke variabelen? Deze vragen staan centraal in dit onderzoek.

In algemene zin kunnen we constateren dat een cyberincident een negatief effect heeft op het niveau van patiëntvertrouwen en dat hierdoor de bekende positieve effecten op behandelingstrouw, continuïteit en vertrouwelijkheid verminderd. Dit is een bevestiging van de essentiële functie van een hoge mate van vertrouwen tussen de patiënt en de zorgverlener en zorginstelling. Wanneer het vertrouwen afneemt, kan dit ervoor zorgen dat de patiënt minder persoonlijke informatie wil delen met de zorgverlener of zorginstelling, waardoor het mogelijk moeilijker wordt om een goede diagnose te stellen of de effectiviteit van een medische behandeling kan verminderen. Wanneer de continuïteit van de patiënt ten opzichte van de zorgverlener of zorginstelling vermindert, kan er minder goed een langdurige relatie met de patiënt worden opgebouwd; de kennis van de medische historie van de patiënt zou hieronder kunnen komen te lijden. De meeste directe impact kan wellicht ontstaan bij het potentieel uitstellen of afzien van een medische behandeling of afspraak van een patiënt. Hierdoor zou een behandeling of diagnose wellicht in een te laat stadium van het ziektebeeld en proces kunnen worden uitgevoerd. Het antwoord op de hoofdvraag van dit onderzoek luidt als volgt:

Een cyberincident kan het patiëntvertrouwen verminderen, waardoor de positieve effecten op behandelingstrouw, continuïteit en vertrouwelijkheid negatief kunnen worden beïnvloed. Een belangrijke kanttekening bij deze conclusies en resultaten van het onderzoek is dat de vragenlijst de intenties van de respondenten heeft gemeten en niet het gedrag naar aanleiding van een bestaand cyberincident. De intenties van mogelijk toekomstig gedrag van de respondenten zegt iets over het eigen inschattingsvermogen hoe een respondent in een dergelijk scenario in de toekomst zou kunnen reageren. Hiertegenover staat wel dat er duidelijke en zichtbare patronen naar voren zijn gekomen in de potentiële negatieve impact van cyberincidenten op patiëntvertrouwen. Daarom denken wij dat dit aanleiding kan geven voor kwalitatief vervolgonderzoek wanneer zich in de toekomst een mogelijk cyberincident voordoet, en dat dit onderzoek heeft bijgedragen aan kennisvergaring omtrent cyberincidenten en patiëntvertrouwen.

LITERATUURLIJST

Anderson, L. A., & Dedrick, R. F. (1990). Development of the Trust in Physician Scale: a measure to assess interpersonal trust in patient-physician relationships. *Psychological reports, 67(3 Pt 2), 1091-1100.* https://doi.org/10.2466/pr0.1990.67.3f.1091

Bachinger, S. M., Kolk, A. M., & Smets, E. M. (2009). Patients' trust in their physician--psychometric properties of the Dutch version of the "Wake Forest Physician Trust Scale". *Patient education and counseling, 76(1), 126-131.* https://doi.org/10.1016/j.pec.2008.11.020

Bordin, E. S. (1979). The generalizability of the psychoanalytic concept of the working alliance. *Psychotherapy: Theory, Research & Practice, 16*(3), 252-260. https://doi.org/10.1037/h0085885

Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. *Maturitas, 113, 48-52.* https://doi.org/10.1016/j.maturitas.2018.04.008

Evenstad, L. (2016). *NHS trust recovers after cyber attack*. Computerweekly.com. Geraadpleegd 29 oktober 2021 op http://www.computerweekly.com/news/450402278/NHS-trust-recovers-after-cyber-attack

Fuertes, J. N., Mislowack, A., Bennett, J., Paul, L., Gilbert, T. C., Fontan, G., & Boylan, L. S. (2007). The physician-patient working alliance. *Patient education and counseling, 66(1), 29-36.* https://doi.org/10.1016/j.pec.2006.09.013

Hall, M. A., Zheng, B., Dugan, E., Camacho, F., Kidd, K. E., Mishra, A., & Balkrishnan, R. (2002). Measuring patients' trust in their primary care providers. *Medical care research and review: MCRR*, *59*(3), 293-318. https://doi.org/10.1177/1077558702059003004

Jalali, M. S., & Kaiser, J. P. (2018). Cybersecurity in Hospitals: A Systematic, Organizational Perspective. *Journal of medical Internet research, 20(5), e10059.* https://doi.org/10.2196/10059

Kao, A. C., Green, D. C., Zaslavsky, A. M., Koplan, J. P., & Cleary, P. D. (1998). The relationship between method of physician payment and patient trust. *JAMA: Journal of the American Medical Association, 280*(19), 1708-1714. https://doi.org/10.1001/jama.280.19.1708

Martin, G., Martin, P., Hankin, C., Darzi, A., & Kinross, J. (2017). Cybersecurity and healthcare: how safe are we? *BMJ (Clinical research ed.), 358, j3179.* https://doi.org/10.1136/bmj.j3179

Nos.nl. (2017, 26 juni). Geraadpleegd 29 oktober 2021 op https://nos.nl/artikel/2179941-zeker-vijftien-ziekenhuizen-geinfecteerd-met-ransomware

Ross J. (2017). Cybersecurity: A Real Threat to Patient Safety. *Journal of perianesthesia nursing: official journal of the American Society of PeriAnesthesia Nurses, 32(4), 370-372.* https://doi.org/10.1016/j.jopan.2017.05.005

Safran, D. G., Taira, D. A., Rogers, W. H., Kosinski, M., Ware, J. E., & Tarlov, A. R. (1998). Linking primary care performance to outcomes of care. *The Journal of family practice, 47(3), 213-220.*

Safran, D. G., Montgomery, J. E., Chang, H., Murphy, J., & Rogers, W. H. (2001). Switching doctors: predictors of voluntary disenrollment from a primary physician's practice. The Journal of family practice, 50(2), 130-136.

Thom, D.H. et al., (1999). 'Validation of a Measure of Patients' Trust in Their Physician: The Trust in Physician Scale. Medical Care 137, no. 5.

Thom, D. H., Hall, M. A., & Pawlson, L. G. (2004). Measuring patients' trust in physicians when assessing quality of care. Health affairs (Project Hope), 23(4), 124-132. https://doi.org/10.1377/hlthaff.23.4.124

APPENDIX:

vragenlijsten onderzoek naar impact van cyberincidenten op patiëntvertrouwen.

1. Casus 1 datalek / datadiefstal

Inleiding
Soms vinden er cyberincidenten plaats in de ziekenhuizen. Een groot gedeelte van deze cyberincidenten zijn datalekken en datadiefstallen. Door een fout of onoplettendheid van een ziekenhuismedewerker komen dan de medische en persoonlijke gegevens van de patiënten op straat te liggen, bijvoorbeeld gegevens zoals naam, leeftijd en adres. Maar het kunnen ook gegevens over medische problemen zijn. Dit noemen we een datalek. Daarnaast komt het voor dat cybercriminelen data stelen. We noemen dit een datadiefstal. Criminelen stelen soms medische gegevens om burgers af te persen of om de data door te verkopen aan andere criminelen.

Stel, u heeft een medisch probleem waarvoor u naar het ziekenhuis moet om hulp te krijgen van een zorgverlener. En zeer recent heeft er een datalek of datadiefstal plaatsgevonden bij een ziekenhuis, hoe zou dit u beïnvloeden?

Om deze impact en invloed te kunnen meten vragen wij u de onderstaande stellingen te beantwoorden, met het bovenstaande voorbeeld in gedachte.

1. **Een datalek of datadiefstal vermindert mijn vertrouwen in de deskundigheid* van de zorgverleners (arts, verpleegkundige of ander medisch personeel) van een ziekenhuis**

   Helemaal eens / eens / neutraal / oneens / helemaal oneens

   * Bij de deskundigheid van een zorgverlener kunt u aan de volgende dingen denken; de zorgverlener heeft goede (medische) kennis, is bekwaam in het uitvoeren van (medische) behandelingen, de zorgverlener luistert en communiceert goed met de patiënt, de zorgverlener geeft duidelijke voorlichting over de diagnose en behandelmogelijkheden, de zorgverlener doet altijd wat het beste is voor de patiënt en de zorgverlener gaat professioneel om met de persoonlijke informatie van de patiënt.

2. **Een datalek of datadiefstal vermindert mijn vertrouwen in de deskundigheid* van een ziekenhuis**

   Helemaal eens / eens / neutraal / oneens / helemaal oneens

   * Bij de deskundigheid van een zorginstelling kunt u aan de volgende dingen denken; de zorginstelling heeft voldoende en deskundige zorgverleners in dienst, de zorginstelling heeft goede kwalitatieve faciliteiten voor medische zorg (bijvoorbeeld de nieuwste medische apparatuur en operatiekamers), de zorginstelling luistert en communiceert goed met de patiënt, de zorginstelling doet altijd wat het beste is voor de patiënt en de zorginstelling gaat professioneel om met de persoonlijke informatie van de patiënt.

3. **Een datalek of datadiefstal vermindert mijn vertrouwen in de kwaliteit van de aangeboden zorg van een ziekenhuis.**

   Helemaal eens / eens / neutraal / oneens / helemaal oneens

4. **Een datalek of datadiefstal kan ervoor zorgen dat dat ik wacht met zoeken van hulp voor een (medisch) probleem**

   Helemaal eens / eens / neutraal / oneens / helemaal oneens

5. **Een datalek of datadiefstal kan ervoor zorgen dat ik niet de medische adviezen en (medicatie) voorschriften volg zoals aangegeven door de zorgverlener (arts, verpleegkundige of ander medisch personeel) van een ziekenhuis**

   Helemaal eens / eens / neutraal / oneens / helemaal oneens

6. **Een datalek of datadiefstal kan ervoor zorgen dat ik een (medische) behandeling of afspraak bij een ziekenhuis uitstel**

   Helemaal eens / eens / neutraal / oneens / helemaal oneens

7. **Een datalek of datadiefstal kan ervoor zorgen dat ik van een (medische) behandeling of afspraak in een ziekenhuis af zie**

   Helemaal eens / eens / neutraal / oneens / helemaal oneens

8. **Een datalek of datadiefstal kan ertoe leiden dat ik voor een andere zorgverlener (arts, verpleegkundige of ander medisch personeel) in het ziekenhuis kies**

   Helemaal eens / eens / neutraal / oneens / helemaal oneens

9. **Een datalek of datadiefstal zou ertoe kunnen leiden dat ik voor een ander ziekenhuis kies**

   Helemaal eens / eens / neutraal / oneens / helemaal oneens

10. **Een datalek of datadiefstal kan ervoor zorgen dat ik minder persoonlijke (gevoelige) informatie deel met een zorgverlener (arts, verpleegkundige of medisch personeel) van het ziekenhuis**

    Helemaal eens / eens / neutraal / oneens / helemaal oneens

11. **Een datalek of datadiefstal kan ervoor zorgen dat ik minder persoonlijke (gevoelige) informatie deel met een ziekenhuis**

    Helemaal eens / eens / neutraal / oneens / helemaal oneens

Casus 2 Ransomware aanval

Inleiding
Een opkomende dreiging voor zorginstellingen is ransomware. Bij een ransomware aanval worden de gegevens op een systeem versleuteld, waardoor medewerkers er niet meer bij kunnen. In de meeste gevallen worden de gegevens gegijzeld en pas weer vrijgegeven als er losgeld wordt betaald. Vaak gaat het om een hoog bedrag. Als een ziekenhuis geraakt wordt door een ransomware aanval kan dit grote impact hebben en ertoe leiden dat operaties en behandelingen uitgesteld moeten worden.

Stel u heeft een medisch probleem waarvoor u naar het ziekenhuis moet om hulp te krijgen van een zorgverlener. En zeer recent heeft er een ransomware aanval op een ziekenhuis plaatsgevonden waardoor operaties niet konden doorgaan en uitgesteld moesten worden, en patiënten naar andere ziekenhuizen moesten worden doorverwezen. Hoe zou dit u beïnvloeden? Om deze impact en invloed te kunnen meten vragen wij u de onderstaande stellingen te beantwoorden, met het bovenstaande voorbeeld in gedachte.

1. **Een ransomware aanval vermindert mijn vertrouwen in de deskundigheid* van de zorgverleners (arts, verpleegkundige of ander medisch personeel) van een ziekenhuis**

   Helemaal eens / eens / neutraal / oneens / helemaal oneens

   * Bij de deskundigheid van een zorgverlener kunt u aan de volgende dingen denken; de zorgverlener heeft goede (medische) kennis, is bekwaam in het uitvoeren van (medische) behandelingen, de zorgverlener luistert en communiceert goed met de patiënt, de zorgverlener geeft duidelijke voorlichting over de diagnose en behandelmogelijkheden, de zorgverlener doet altijd wat het beste is voor de patiënt en de zorgverlener gaat professioneel om met de persoonlijke informatie van de patiënt.

2. **Een ransomware aanval vermindert mijn vertrouwen in de deskundigheid* van een ziekenhuis**

   Helemaal eens / eens / neutraal / oneens / helemaal oneens

   * Bij de deskundigheid van een zorginstelling kunt u aan de volgende dingen denken; de zorginstelling heeft voldoende en deskundige zorgverleners in dienst, de zorginstelling heeft goede kwalitatieve faciliteiten voor medische zorg (bijvoorbeeld de nieuwste medische apparatuur en operatiekamers), de zorginstelling luistert en communiceert goed met de patiënt, de zorginstelling doet altijd wat het beste is voor de patiënt en de zorginstelling gaat professioneel om met de persoonlijke informatie van de patiënt.

3. **Een ransomware aanval vermindert mijn vertrouwen in de kwaliteit van de aangeboden zorg van een ziekenhuis.**

   Helemaal eens/ eens / neutraal / oneens / helemaal oneens

4. **Een ransomware aanval kan er voor zorgen dat ik wacht met zoeken van hulp voor een (medisch) probleem**

   Helemaal eens / eens / neutraal / oneens / helemaal oneens

5. **Een ransomware aanval kan er voor zorgen dat ik niet de medische adviezen en (medicatie) voorschriften volg zoals aangegeven door de zorgverlener (arts, verpleegkundige of ander medisch personeel) van een ziekenhuis**

   Helemaal eens / eens / neutraal / oneens / helemaal oneens

6. **Een ransomware aanval kan er voor zorgen dat ik een (medische) behandeling of afspraak bij een ziekenhuis uitstel**

   Helemaal eens / eens / neutraal / oneens / helemaal oneens

7. **Een ransomware aanval kan er voor zorgen dat ik van een (medische) behandeling of afspraak in een ziekenhuis af zie**

   Helemaal eens / eens / neutraal / oneens / helemaal oneens

8. **Een ransomware aanval kan er toe leiden dat ik voor een andere zorgverlener (arts, verpleegkundige of ander medisch personeel) in het ziekenhuis kies**

   Helemaal eens / eens / neutraal / oneens / helemaal oneens

9. **Een ransomware aanval zou er toe kunnen leiden dat ik voor een ander ziekenhuis kies**

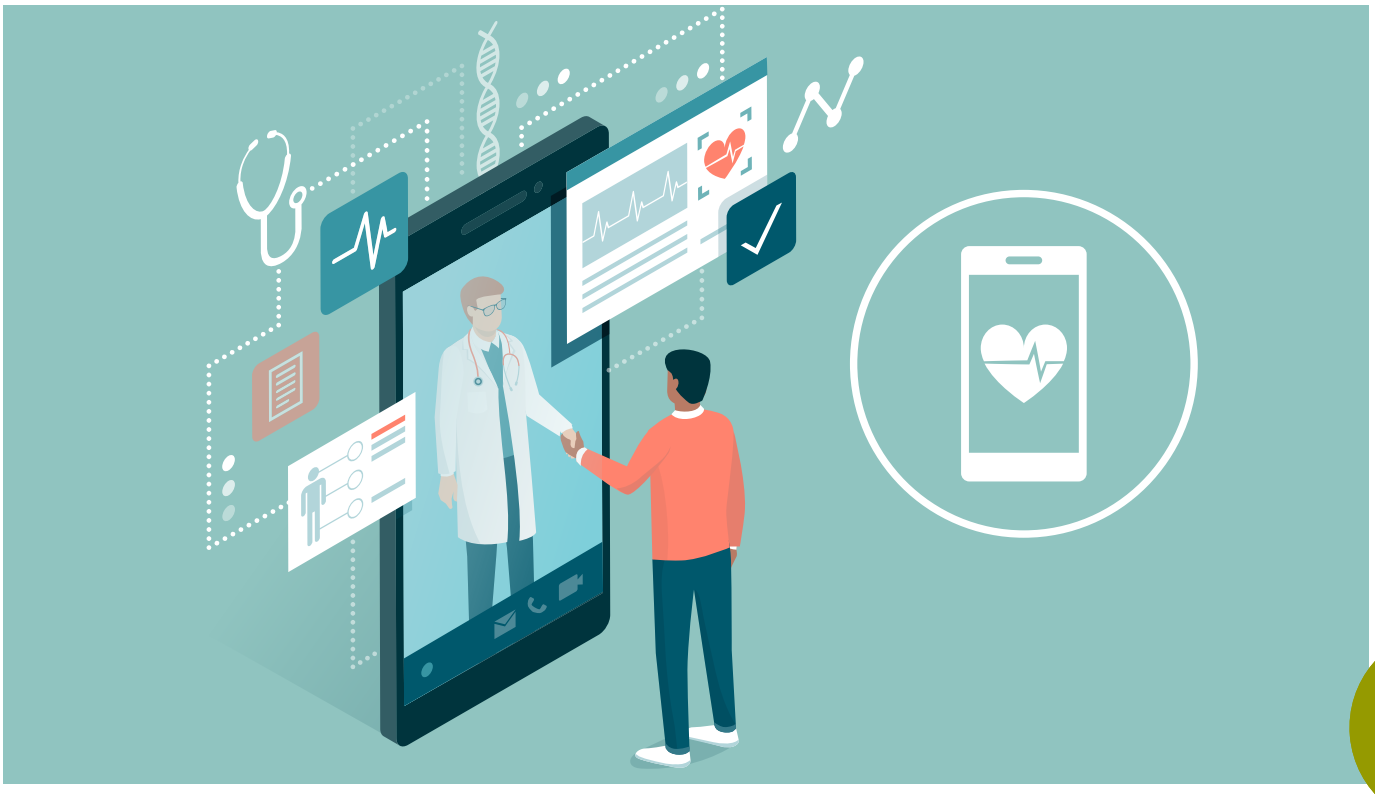
   Helemaal eens / eens / neutraal / oneens / helemaal oneens

10. **Een ransomware aanval kan er voor zorgen dat ik minder persoonlijke (gevoelige) informatie deel met een zorgverlener (arts, verpleegkundige of medisch personeel) van het ziekenhuis**

    Helemaal eens / eens / neutraal / oneens / helemaal oneens

11. **Een ransomware aanval kan er voor zorgen dat ik minder persoonlijke (gevoelige) informatie deel met een ziekenhuis**

    Helemaal eens / eens / neutraal / oneens / helemaal oneens



Meer informatie

www.dehaagsehogeschool.nl

cybersecurity@hhs.nl

Johanna Westerdijkplein 75
2521 EN Den Haag

let's change
YOU. US. THE WORLD.