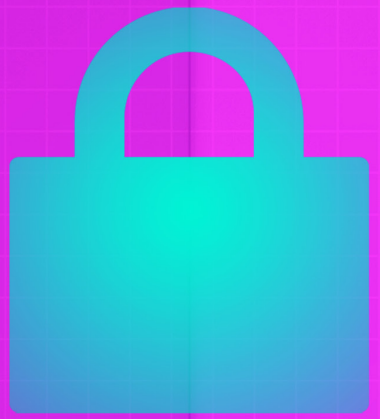
e-bok

datto
A Kaseya COMPANY



Dattos rapport om cybersäkerhet för små och medelstora företag för leverantörer av hanterade tjänster

En värld av möjligheter för leverantörer av hanterade tjänster

Små och medelstora företag står inför ökande cybersäkerhetsutmaningar, vilket resulterar i att många små och medelstora företag ökar sitt engagemang för säkerhet och sina säkerhetsbudgetar. Det finns utrymme för leverantörer av hanterade tjänster att realisera resurstillväxt inom många områden, inklusive säker identitets- och åtkomsthantering, slutpunktssäkerhet, verksamhetskontinuitet och katastrofåterställning (Business Continuity and Disaster Recovery, BCDR) och nätfiskeskydd. Dagens värld av växande cyberhot för små och medelstora företag är en värld av ökade affärsmöjligheter inom säkerhet för leverantörer av hanterade tjänster överallt.

Vi pratade med 2 913 IT-beslutsfattare för att få reda på deras säkerhetsproblem och vi delar dessa data med dig för att hjälpa dig att utveckla din leverantör av hanterade tjänster.

7 Viktiga upptäckter

IT-proffsen är oroade över säkerheten och redo att göra investeringar för att hålla sina organisationer säkra.

Små och medelstora företag fortsätter att uppleva betydande säkerhetsutmaningar och inser att de måste göra investeringar för att lösa dem. Ungefär hälften av våra undersökningssvarande planerar att spendera medel på e-postsäkerhet, säkerhetskopiering och antivirusskydd.

Många små och medelstora företag behöver hjälp med att förbereda sig för att återhämta sig från säkerhetsincidenter.

Mer än hälften av våra svarande medgav att en framgångsrik nätfiske-attack eller ännu värre, en ransomware-attack, allvarligt skulle skada deras organisation med några som säger att det kan vara ett dödligt slag.

Få små och medelstora företag minskar sina säkerhetsutgifter. Istället investerar de i säkerhet.

Fyra av tio av våra deltagare i undersökningen sa att deras organisation ökar sina cybersäkerhetsutgifter, och de flesta förväntar sig att fortsätta – utmärkta nyheter för leverantörer av hanterade tjänster om dagens utmanande ekonomi.

Nätfiske är det största säkerhetsproblemet som små och medelstora företag står inför.

IT-ledare för företag är oroliga för nätfiske och den fara det medför. Detta skapar möjligheter till resurstillväxt för leverantörer av hanterade tjänster kring e-postsäkerhet och säkerhetsutbildning med nätfiskesimuleringar.

Driftstopp är kostsamt, men många företag har inte rätt verktyg på plats för att minimera detta.

Leverantörer av hanterade tjänster har en gyllene möjlighet att utöka intäkterna och hjälpa sina kunder att minska dyra driftstopp med lösningar som BCDR, hanterade säkerhetsoperationscenter (SOC) och incidentresponsplanering.

Små och medelstora företag tenderar att förlita sig på outsourcad IT-säkerhet.

Företag behöver hjälp utifrån med att upprätthålla och förbättra sin säkerhet. Nästan hälften av de IT-specialister som vi undersökte sa att deras organisation förlitar sig på en leverantör av hanterade tjänster eller leverantör av hanterad säkerhetstjänst för att få jobbet gjort.

Ett stort antal små och medelstora företag är inte nöjda med sin nuvarande defensiva uppbyggnad.

En tredjedel av våra svarande sa att de är missnöjda med sin nuvarande uppsättning av säkerhetslösningar, vilket indikerar att det finns utrymme för leverantörer av hanterade tjänster att röra sig på marknaden.

Cybersäkerhetslösningar

NIST är inte det mest populära ramverket

Zero-trust rekommenderas starkt av experter, men endast 14 % av svarande sa att deras organisationer använder det ramverket och bara 7 % var bekymrade över det, vilket innebär att det finns gott om utrymme för tillväxt (och möjligheter för leverantörer av hanterade tjänster) inom detta område.

Ramverk eller förordning	Användningsnivå	Orosnivå
CIS	34 %	26 %
CMMC	30 %	26 %
COBIT	27 %	23 %
NIST	22 %	19 %
ISO 27001	21 %	15 %
NCSC (National Cyber Security Centre)	18 %	20 %
HIPAA	18 %	13 %
Zero Trust	14 %	7 %
ASD Essential 8	14 %	13 %
PCI-DSS	12 %	10 %
SOC II	11 %	7 %
MITRE ATT&CK	9 %	9 %
Övrigt	5 %	-
Inga	3 %	27 %

CIS och CMMC används oftast och är de mest oroande cybersäkerhetsramverken.

Små och medelstora företag är proaktiva när det gäller att bedöma sårbarheter

Majoriteten av små och medelstora företag i alla regioner är intresserade av att hålla ett öga på sina sårbarheter i IT-säkerheten i ett så pass ombytligt cyberbrottsklimat. Det gör dem särskilt angelägna om att ha användarvänliga lösningar som gör sårbarhetsbedömningsprocessen snabb och enkel.

Frekvens av bedömningar	Svar
Mer än 4 gånger om året	13 %
3–4 gånger per år	24 %
Två gånger per år	25 %
En gång per år	21 %
En gång vartannat till vart fjärde år	12 %
En gång vart femte år eller längre	3 %
Aldrig	1 %
Vet inte	2 %

Över en tredjedel av de tillfrågade utför sårbarhetsbedömningar av IT-säkerhet tre eller fler gånger per år.

Små och medelstora företag minskar inte sina säkerhetsutgifter, utan budgetarna ökar istället

Mot bakgrund av stigande cyberbrottslighet och en växande medvetenhet om de skador som en cyberattack kan göras av icke-tekniska beslutsfattare har IT-säkerhetsbudgetarna ökat under det senaste året. Små och medelstora företag är optimistiska om att de förblir stabila eller ökar under 2023. Detta ger leverantörer av hanterade tjänster möjlighet att uppmuntra kunder att göra omfattande säkerhetsförbättringar och uppgraderingar.

IT-budgetar	Svar
Ökade	42 %
Förblev densamma	40 %
Minskade	6 %

Fyra av tio (42 %) av de tillfrågade rapporterade en ökad IT-säkerhetsbudget i år.

Säkerhet utgör en stor del av de flesta IT-budgetar

Små och medelstora företag har pengar att spendera på säkerhet

% av den totala IT-budgeten	Svar
Mindre än 1 %	1 %
1 % –5 %	10 %
6 % –10 %	19 %
11 %–15 %	19 %
16 %–20 %	20 %
21 %–30 %	15 %
31 %–40 %	8 %
41 % –50 %	5 %
Mer än 50 %	3 %

Nästan en tredjedel av små och medelstora företag ägnar 20 % till 50 % av sin IT-budget åt säkerhet.

Små och medelstora företag finns på marknaden för IT-säkerhetshjälp

Medan många små och medelstora företag hanterar säkerhet internt finns det gott om företag som vill ha leverantörer av hanterade tjänster och leverantörer av hanterade säkerhetstjänster för sina IT-säkerhetsbehov. Bristen på teknisk kompetens är en bidragande faktor, men brist på expertis är också en viktig drivkraft för företag att outsourca sitt tekniska arbete. Leverantörer av hanterade tjänster kan dra nytta av att positionera sig som kunniga, uppdaterade experter för kunder och potentiella kunder.

En av fyra outsourcar sin säkerhet till en leverantör av hanterade tjänster och en av sex till en leverantör av hanterad säkerhetstjänst.

Vem hanterar din IT-säkerhet?	Svar
Delvis intern IT	47 %
Dedikerad intern IT	50 %
Individuell outsourcing av IT	28 %
Företaget outsourcar IT som är IT-tjänsteleverantör eller leverantör av hanterade tjänster	26 %
Företaget outsourcar IT som är en leverantör av hanterad säkerhetstjänst	16 %
Företaget outsourcar IT, men är inte säker på vilken typ det anses vara	5 %

Det finns utrymme för leverantörer av hanterade tjänster att manövrera på marknaden

Endast 31 % av respondenterna säger att de är helt nöjda med sina säkerhetslösningar, vilket skapar möjligheter för leverantörer av hanterade tjänster att växa.

Nöjdhetsnivå	Svar
Helt nöjd	31 %
Ganska nöjd	54 %
Neutral	12 %
Ganska missnöjd	2 %
Helt missnöjd	1 %

Endast 54 %

av företagen är något nöjda med sina säkerhetslösningar.

De flesta företag har anammat budskapet att en återhämtningsplan är nödvändig för verksamheten

När det gäller att ha en återhämtningsplan på plats sa över hälften av svarande att de har en standard återhämtningsplan redo. Vissa företag behöver dock fortfarande mycket hjälp med att skapa en återhämtningsplan, vilket innebär möjligheter för leverantörer av hanterade tjänster att hjälpa dem att vara redo för problem. Det är också en klar möjlighet för leverantörer av hanterade tjänster att vägleda kunder till att investera i resurser de behöver för att anta den planen, som BCDR eller verktyg för identitets- och åtkomsthantering på distans.

Åtta av tio deltagare i undersökningen (81 %) uppgav att deras företag har en återhämtningsplan på plats.

Status för återhämtningsplan	Svar
Vi har en förstklassig återhämtningsplan på plats	29 %
Vi har en standard återhämtningsplan på plats	52 %
Vi har lösningar för att skydda oss, men har ingen formell återhämtningsplan på plats	14 %
Vi har ingen återhämtningsplan på plats	2 %
Jag tror att min tjänsteleverantör har en återhämtningsplan på plats, men jag känner inte till detaljerna	3 %

Säkerhetsprodukter

Ett starkt försvar mot ransomware leder SMB-prioriteringslistan

I ransomware-eran är det ingen överraskning att antivirusprogram 57 % och e-postsäkerhet 53 % står högst upp på företagens implementeringslistor.

Säkerhetslösningarna som organisationer ska implementera under de kommande 12 månaderna

Lösning	Respondenter
Antivirusprogram	57 %
Skydd mot e-post/spam	53 %
Säkerhetskopiering av filer	49 %
Hanterad brandvägg	49 %
Cybersäkerhetsutbildning för anställda	43 %
Identitets- och åtkomsthantering	38 %
Center för säkerhetsverksamhet	28 %
Hanterad detektion och svar (managed detection and response, MDR)	27 %
Business Continuity and Disaster Recovery (BCDR)	27 %
Incidentrespons	27 %
Slutpunktsdetektion och svar	25 %
Automatiserad programfix	25 %
Plattform för mobil hantering	23 %
Hotjakt	20 %
Penetrationstestning	14 %
Kriminalteknik	12 %

Endast 43 % av svarande genomför utbildning i säkerhetsmedvetenhet.

Små och medelstora företag är redo att investera i molnet

Cyberbrottsligheten de senaste åren innebär att företag är redo att investera i molnsäkerhet.

De främsta IT-säkerhetsområdena som små och medelstora företag planerar att investera under de kommande 12 månaderna

Investeringsområde	Svar
Nätverkssäkerhet	47 %
Molnsäkerhet	45 %
Cyberförsäkring	36 %
Säkerhet för e-post-/samarbetsverktyg	29 %
Slutpunktssäkerhet	27 %
Sårbarhetsbedömning	26 %
Business Continuity and Disaster Recovery (BCDR)	25 %
Vet inte	5 %

Nätverkssäkerhet och molnsäkerhet är de främsta områdena som planeras för investeringar under 2023.

Cyberhot

Små och medelstora företag har en bred omfattning av säkerhetsfaror

En titt bakom luckan på de faktorer som små och medelstora företag skyller sina säkerhetsproblem på kan hjälpa dig att tala till deras smärtpunkter med förtroende.

Huvudorsaker till att små och medelstora företag känner att de har haft cybersäkerhetsproblem

Problem	Svar
Nätfiskande e-post	37 %
Skadliga webbplatser/webbannonser	27 %
Svaga lösenord/åtkomsthantering	24 %
Dåliga användarrutiner/svaghet	24 %
Brist på utbildning i cybersäkerhet för slutanvändare	23 %
Brist på utbildning i cybersäkerhet för administratörer	19 %
Nätfiskande telefonsamtal	19 %
Brist på försvarslösningar (antivirus)	19 %
Otillräckligt säkerhetsstöd för olika typer av användarenheter	18 %
Föråldrade säkerhetskorrigeringar	18 %
Brist på finansiering för IT-säkerhetslösningar	17 %
Förlorade/stulna medarbetaruppgifter	17 %
Brist på verkställande stöd för att anta säkerhetslösningar	16 %
Öppen tillgång till fjärrskrivbordsprotokoll	15 %
Shadow IT	13 %

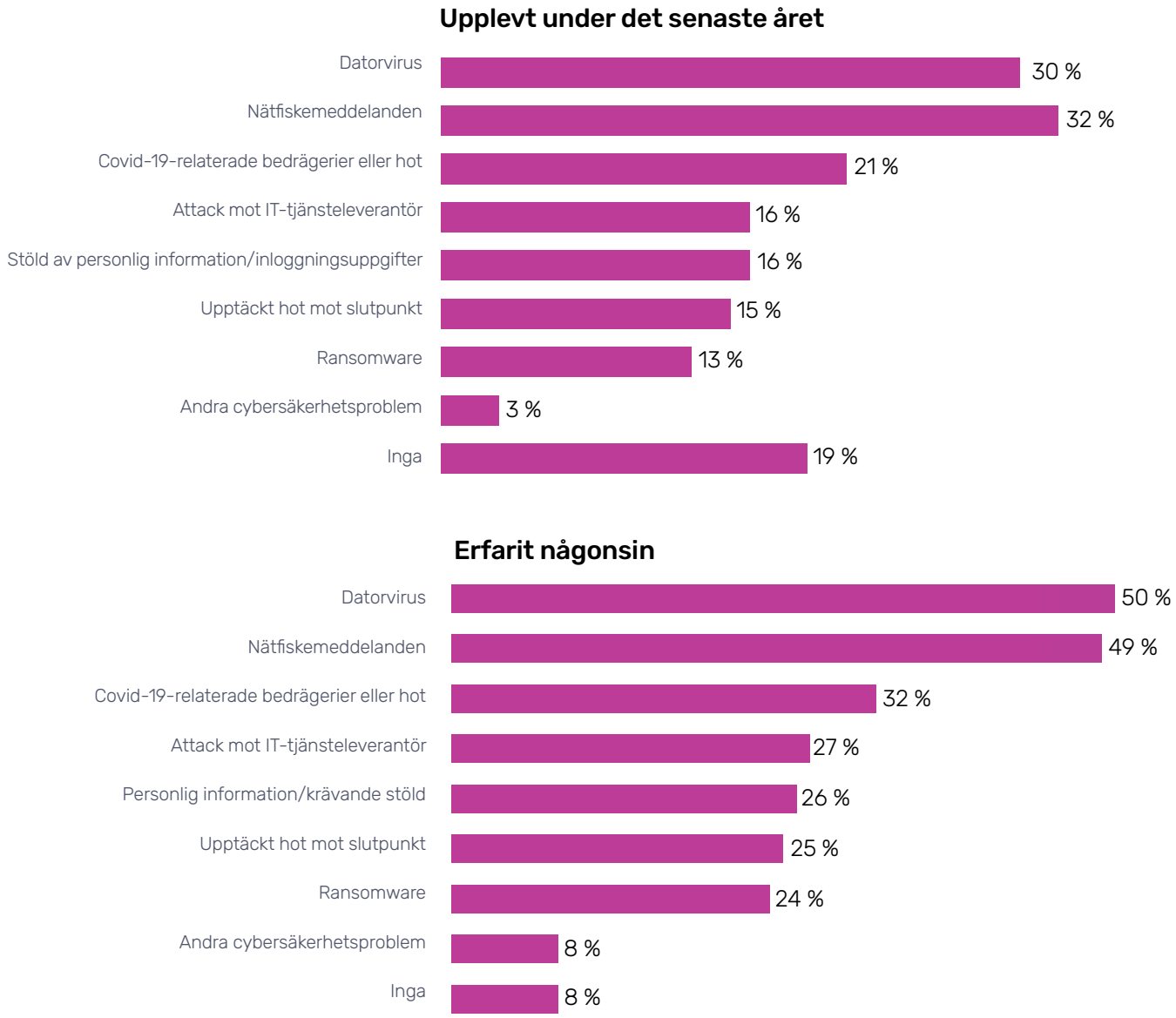
Cirka 42 % av små och medelstora företag skyller sina säkerhetsfrågor på brist på utbildning.

Små och medelstora företag plågas av nätfiske

Många av våra svarande såg nätfiske som huvudmisstänkt för säkerhetsfrågor, och mer än en fjärdedel av respondenterna har upplevt en attack mot sin IT-leverantör (16 % under det senaste året). Detta är en möjlighet för leverantörer av hanterade tjänster att tillhandahålla mycket säker service.

Cybersäkerhetsfrågor som har påverkat små och medelstora företag under de senaste 12 månaderna.

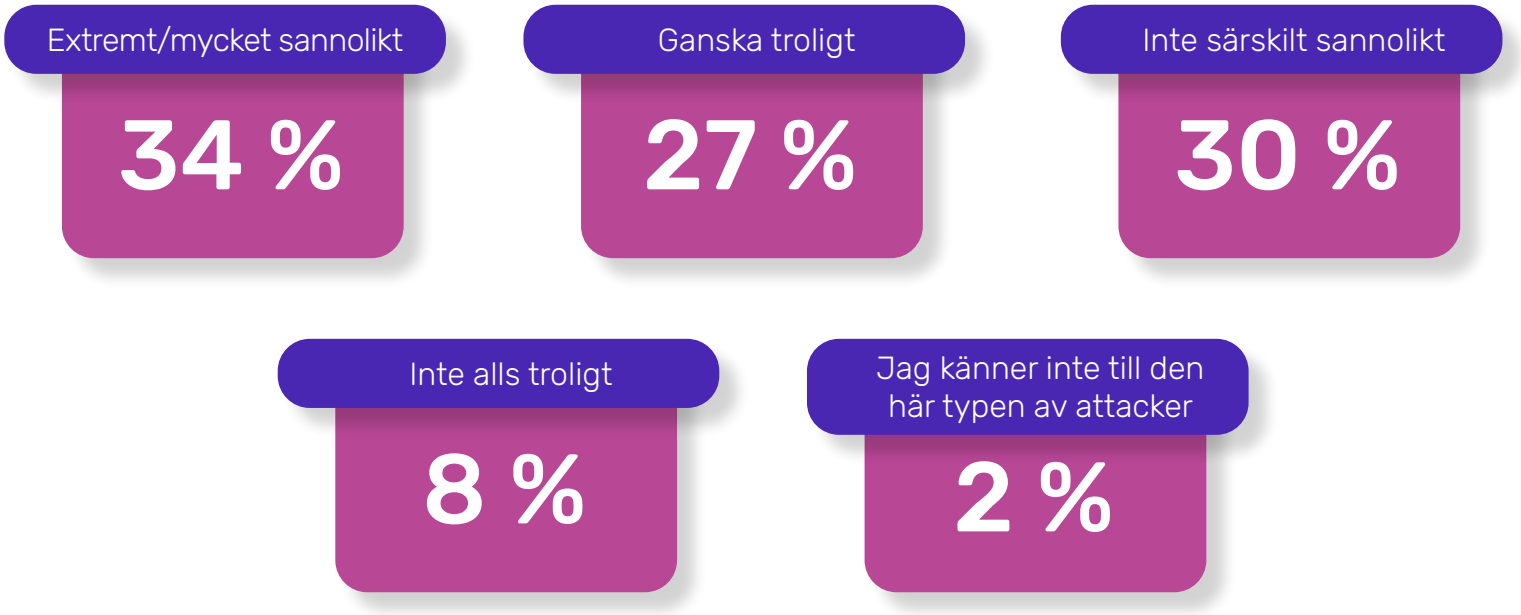
Nästan en tredjedel av respondenterna hanterade nätfiske och virus förra året.



Nästan tre fjärdedelar av företagen säger att en ransomware-attack skulle vara ett dödsslag

Företag vet att en ransomware-attack kan förstöra dem och de letar efter sätt att förhindra det.

Omkring 60 % av respondenterna ansåg att deras organisation kan drabbas av en framgångsrik ransomware-attack under de närmaste 12 månaderna.



Omkring 70 % av små och medelstora företag medgav att effekten av en ransomware-attack skulle vara extrem eller betydande.

Extrem inverkan - det skulle vara svårt att återhämta sig

17 %

Betydande inverkan

53 %

Minimal inverkan

28 %

Ingen inverkan

3 %

Ransom-krav varierar kraftigt

Att visa kunder och framtida klienter en tydlig bild av lösenbegäran de kan komma att erfara kan hjälpa dem att inse det faktiska slaget mot deras bankkonton.

Nästan en tredjedel av små och medelstora företag stod inför 10 000–50 000 dollar i lösenkostnad.

Lösenbelopp	Svar
Mindre än 100 USD	2 %
100 till mindre än 500 USD	4 %
500 till mindre än 1 000 USD	10 %
1 000 till mindre än 5 000 USD	21 %
5 000 till mindre än 10 000 USD	25 %
10 000 till mindre än 25 000 USD	20 %
25 000 till mindre än 50 000 USD	11 %
50 000 USD eller mer	6 %

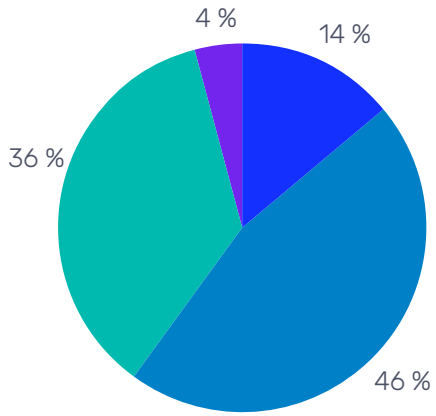
De flesta små och medelstora företag förväntar sig att bli nätfiskade

Strax under tre fjärdedelar av respondenterna tror att det är sannolikt att deras organisation kommer att uppleva en nätfiske-attack under det kommande året. Här letar de också efter sätt att mildra den risken.

Cirka 72 % av respondenterna förväntar sig en nätfiske attack under det kommande året.

Sannolikhet	Svar
Extremt/mycket sannolikt	41 %
Ganska troligt	31 %
Inte särskilt sannolikt	22 %
Inte alls troligt	7 %

Fler respondenter kände att de skulle falla offer för nätfiske under det kommande året än ransomware, men de trodde att effekten av en framgångsrik ransomware-attack skulle vara större för deras organisation än effekten av en nätfiske-attack.



Nästan hälften av respondenterna tror att en nätfiske-attack skulle ha en betydande inverkan på deras verksamhet.

- Minimal inverkan
- Betydande inverkan
- Extrem inverkan – det skulle vara svårt att återhämta sig
- Ingen inverkan

Små och medelstora företag har förtroende för sin förmåga att återhämta sig från en cybersäkerhetsincident

Trots detta förtroende finns det gott om möjligheter för leverantörer av hanterade tjänster inom detta område att föreslå nya lösningar som minskar risker eller uppgraderingar av en kunds eller framtida klients säkerhetsutbyggnad för att göra den ännu starkare - 16 % av svarande sa att deras organisation skulle dömas i händelse av en framgångsrik cyberattack eller en annan skadlig cybersäkerhetsincident och 47 % sa att de tror att återhämtning skulle vara svår.

Framgångsrik katastrofåterställning är lättare sagd än gjord

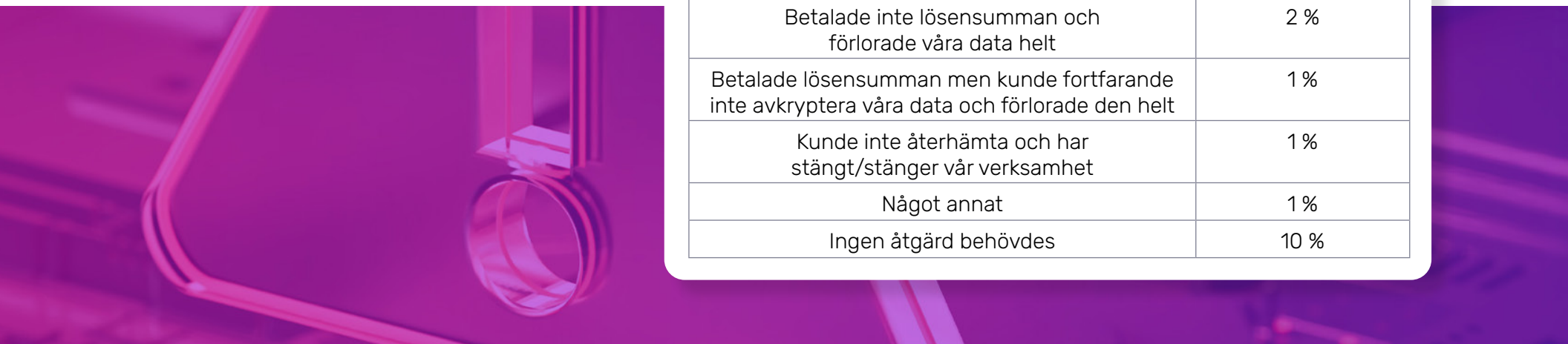
Leverantörer av hanterade tjänster kan ge små och medelstora företag den hjälp de behöver för att förbättra sina säkerhetskopierings- och återställningsprocesser.

En femtedel av respondenterna tvingades ominstallera och omkonfigurera om alla system från grunden för att komma tillbaka till arbetet.

Drygt hälften av respondenterna i undersökningen (47 %) sa att deras företag sannolikt skulle återhämta sig från en cyberattack eller cybersäkerhetsincident, men det skulle vara smärtsamt.

Resultat	Svar
Återhämtning skulle vara lätt	**37 %**
Återhämtning skulle vara svårt	**47 %**
Vi skulle inte återhämta oss	**16 %**

Vidtagen åtgärd för att återgå till baslinjen	Svar
Utförde katastrofåterställning (DR) och återställde allt från fullständiga säkerhetskopior	30 %
Återställde en del av systemen och ominstallerade och omkonfigurerade resten	29 %
Ominstallerade och omkonfigurerade alla våra system från grunden	21 %
Betalade lösensumman för att få våra data avkrypterade	2 %
Betalade inte lösensumman och förlorade våra data helt	2 %
Betalade lösensumman men kunde fortfarande inte avkryptera våra data och förlorade den helt	1 %
Kunde inte återhämta och har stängt/stänger vår verksamhet	1 %
Något annat	1 %
Ingen åtgärd behövdes	10 %



Driftstopp kostar i genomsnitt 126 000 USD

Driftstopp är ett dyrt problem som nästan hälften av våra svarande kämpade med under det senaste året. Inverkan på verksamheten och skadande kostnader för driftstopp ger leverantörer av hanterade tjänster ett sätt att rekommendera lösningar, som BCDR, vilka kommer att minska driftstoppen i händelse av en säkerhetsincident. Kostnaden för driftstopp är även ett faktum som kan användas när man talar om utbildning i säkerhetsmedvetenhet och andra förebyggande åtgärder.

126 000 USD är den genomsnittliga kostnaden för driftstopp, inklusive förlorade intäkter.

Kostnad för driftstopp	Svar
1 000 till mindre än 250 000 USD	84 %
1 000 till mindre än 250 000 USD	8 %
1 000 till mindre än 250 000 USD	4 %
750 000 till mindre än 1 miljon USD	3 %
1 miljon USD eller mer	1 %

Manuell säkerhetskopiering är den främsta återställningsmetoden

Drygt hälften av respondenterna i undersökningen (49 %) sa att deras organisationer förlitade sig på manuell säkerhetskopiering för att återställa data i sin senaste cybersäkerhetsincident. Det innebär att hälften av de företag vi undersökte måste uppdatera till säkerhetskopiering i molnet och lära sig fördelarna med BCDR - en stor möjlighetspoäng för leverantörer av hanterade tjänster.

Topplösningar eller metoder som används för att återställa data.

Metod för återställning	Svar
Manuell säkerhetskopiering	49 %
Kopiera från gamla system	36 %
Kontinuerlig tillgänglighet	36 %
Tredje parts BCDR	32 %
Något annat	11 %
Vi gjorde ingenting och återställde inte våra data	2 %
Vi förlorade inga data	13 %

Ungefär hälften av de små och medelstora företag som hade ett cybersäkerhetsproblem var igång inom en dag

Idag är det inte om du har en incident, utan när. Lösningar som minskar återhämtningstiden kommer att vara tilltalande för företag.

Omkring 45 % av företagen genomgick mer än två dagars driftstopp.

Återställningstid	Svar
Ingen – vi hade inga driftstopp	12 %
Mindre än 1 dag	23 %
1 dag	20 %
2–3 dagar	31 %
4–6 dagar	10 %
En vecka eller mer	3 %
Vet inte	1 %
Föredrar att inte svara	1 %

Cyberförsäkring

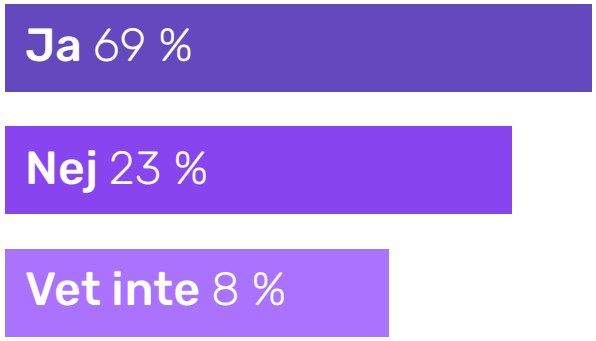
De flesta små och medelstora företag har eller är på marknaden för cyberförsäkringar Svarande med cyberförsäkringar kommer också sannolikt att engagera sig i andra smarta säkerhetsmetoder.

De har i allmänhet mer IT-stöd, fler ramverk för cybersäkerhet och fler säkerhetslösningar. De har också mer sannolikt upplevt en cybersäkerhetsincident tidigare.

Nästan tre fjärdedelar av de tillfrågade har cyberförsäkring.

En tredjedel av dem utan cyberförsäkring är mycket benägna att investera i det inom de närmaste 12 månaderna.

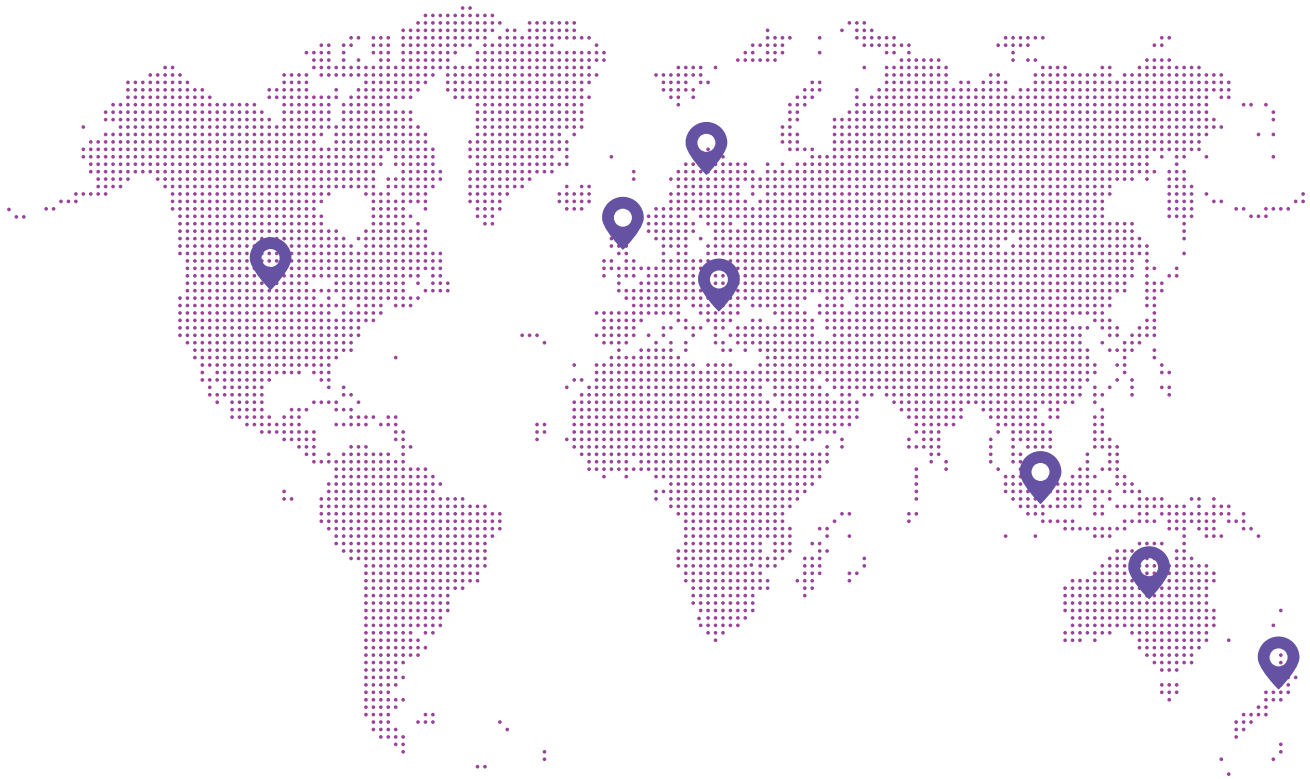
Har du någon cyberförsäkring?



Sannolikhet	Svar
Extremt/mycket sannolikt	37 %
Ganska sannolikt	38 %
Inte särskilt sannolikt	22 %
Inte alls troligt	4 %

Undersökningsmetodik

Datto SMB Cybersecurity Survey for MSPs Report skapades från en delmängd data som samlades in i en undersökning av 2 913 IT-beslutsfattare som genomfördes i juli och augusti 2022. Respondenterna var tvungna att vara beslutsfattare för IT på små eller medelstora företag med 10–300 anställda. Marknaderna som valdes för analys var Nordamerika (USA och Kanada), Storbritannien, Tyskland, Nederländerna, Australien och Nya Zeeland och Singapore.



Om Datto

Datto, ett Kaseya-varumärke, tillhandahåller branschledande molnbaserade programvaru- och tekniklösningar som levereras av leverantörer av hanterade tjänster. Datto erbjuder Unified Continuity, Networking och Business Management-lösningar och har skapat ett unikt ekosystem av partners som är leverantörer av hanterade tjänster. Dessa partners tillhandahåller Datto-lösningar till över en miljon företag över hela världen. Sedan Datto grundades 2007 har företaget vunnit otaliga priser varje år för sin snabba tillväxt, sina framstående produkter, överlägsna tekniska support och för att skapa en enastående arbetsplats. Datto har sitt huvudkvarter i Norwalk, Connecticut och globala kontor i Storbritannien, Nederländerna, Danmark, Tyskland, Kanada, Australien, Kina och Singapore. Läs mer på datto.com.