



AWK Group

Enabling digital performance.

Cyber Resilienz in unsicheren Zeiten
Risiken und Nebenwirkungen von Covid-19

Netzwerk Risikomanagement, 24. November 2020
Adrian Marti, Partner

Die Entwicklung der Corona-Pandemie und ihre Konsequenzen sind schwer zu prognostizieren

«It's going to disappear»
US Präsident Trump
27. Feb 2020



«Uns stehen schwere Monate bevor»
Deutsche Kanzlerin Angela Merkel
26. Okt 2020



«Wir können jetzt Corona»
Schweizer Bundesrat A. Berset
20. Mai 2020



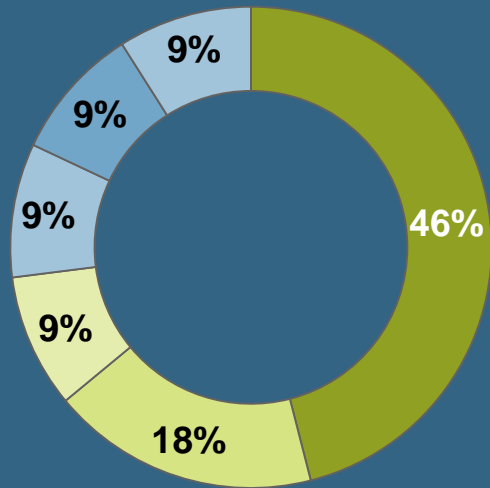
Wo sind all die Mitarbeitenden?



Risiko Manager sind mit einer Vielzahl von Herausforderungen konfrontiert

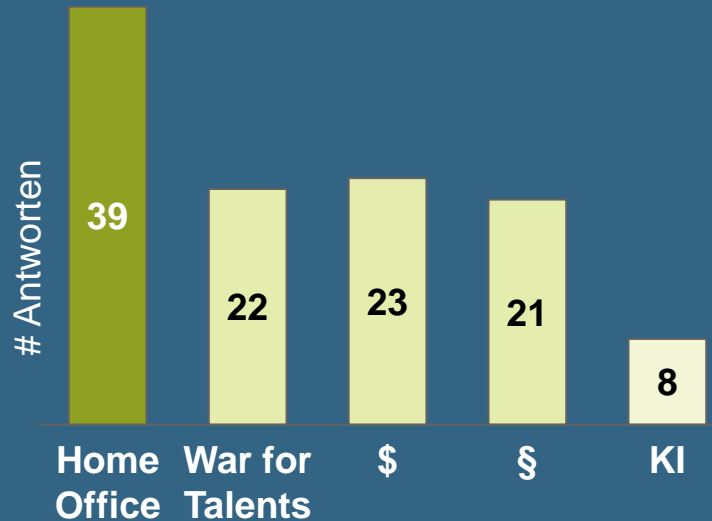


COVID-19 verstärkt die Cyber Security Herausforderungen



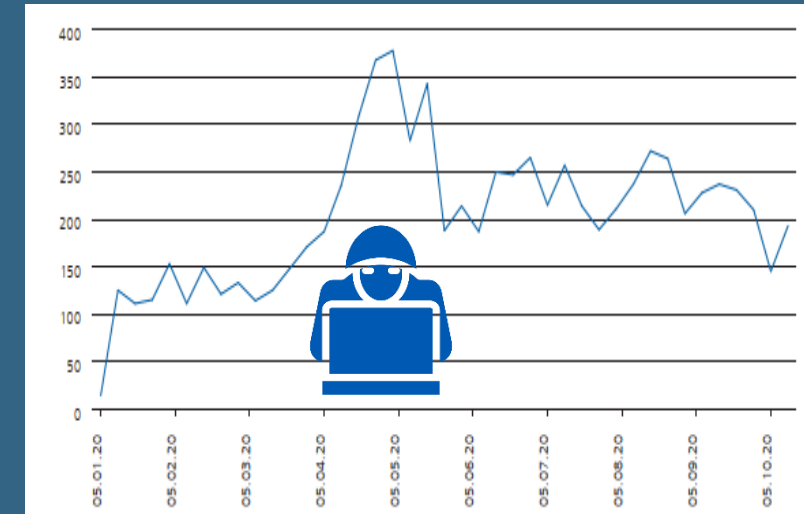
Beobachtete Angriffsvektoren

- E-Mails mit bösartigen Anhängen (46%)
- E-Mails mit Links zur Verbreitung von Malware (18%)
- Mobile Anwendungen (9%)
- Lieferkette (9%)
- Missbrauch von Anwendungen (9%)



Neue Herausforderungen im Vergleich zu 2019

- Neue Bedrohung Nr. 1: Zunahme der Arbeit im Home-Office auf Grund von COVID-19
- Knappheit an Fachkräften, Budget, Künstliche Intelligenz verschärften sich

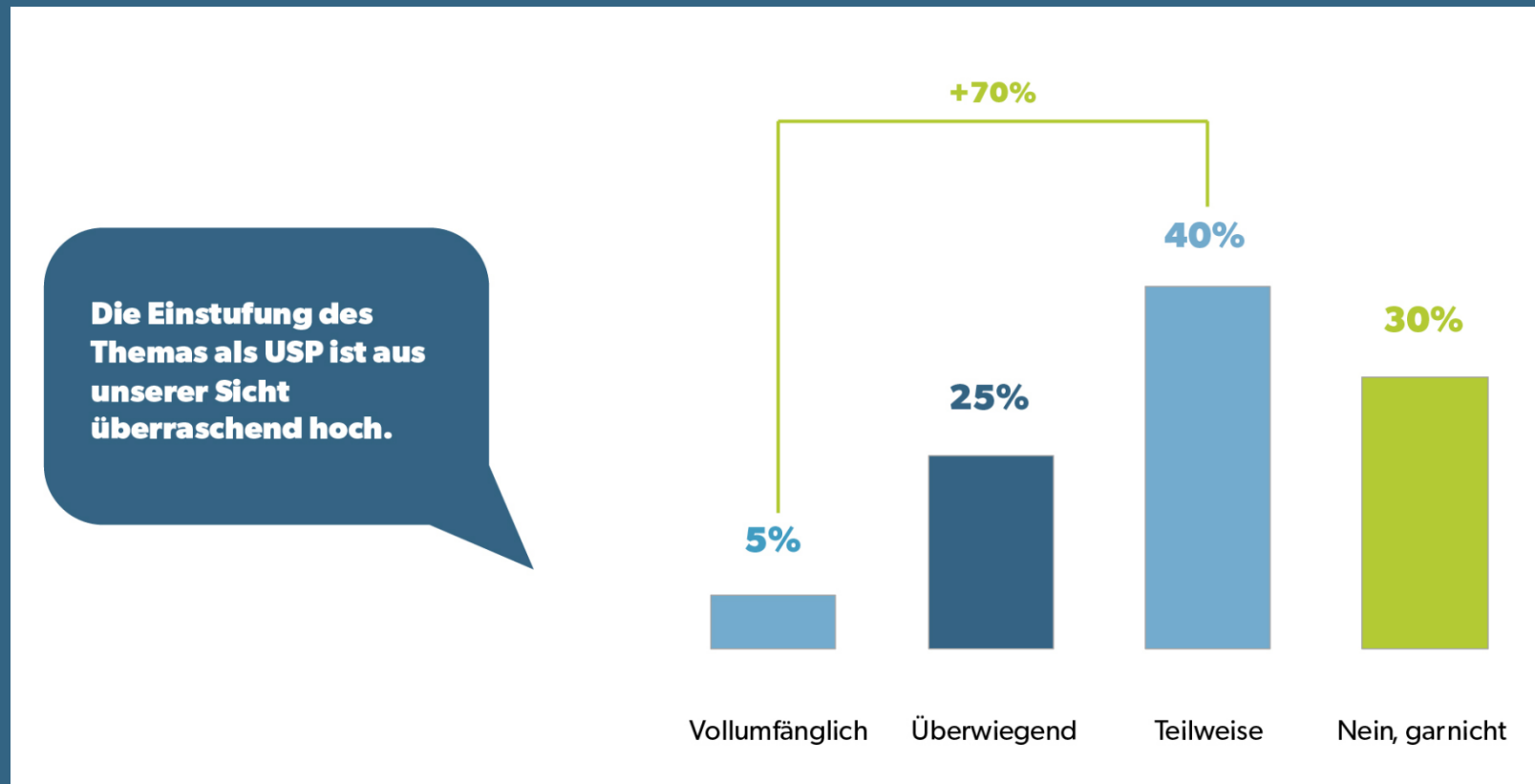


Monatlich beobachtete Cyber Angriffe

- COVID-19 zwang Unternehmen zu
 - Anpassung Sicherheitsstrategien
 - Durchsetzung Sicherheit erschwert
 - Lockerung von Sicherheitsrichtlinien?
- Angreifer versuchten die Schwachstelle auszunutzen

Cyber Security ist für 70% der Unternehmen ein Differenzierungsmerkmal am Markt.

Ist das Thema Cyber Security für Ihr Unternehmen ein Differenzierungsmerkmal am Markt?



Höchste Relevanz für

- ICT (100%)
- Banken (92%)
- öffentliche Verwaltung (80%)

Tiefste Relevanz für

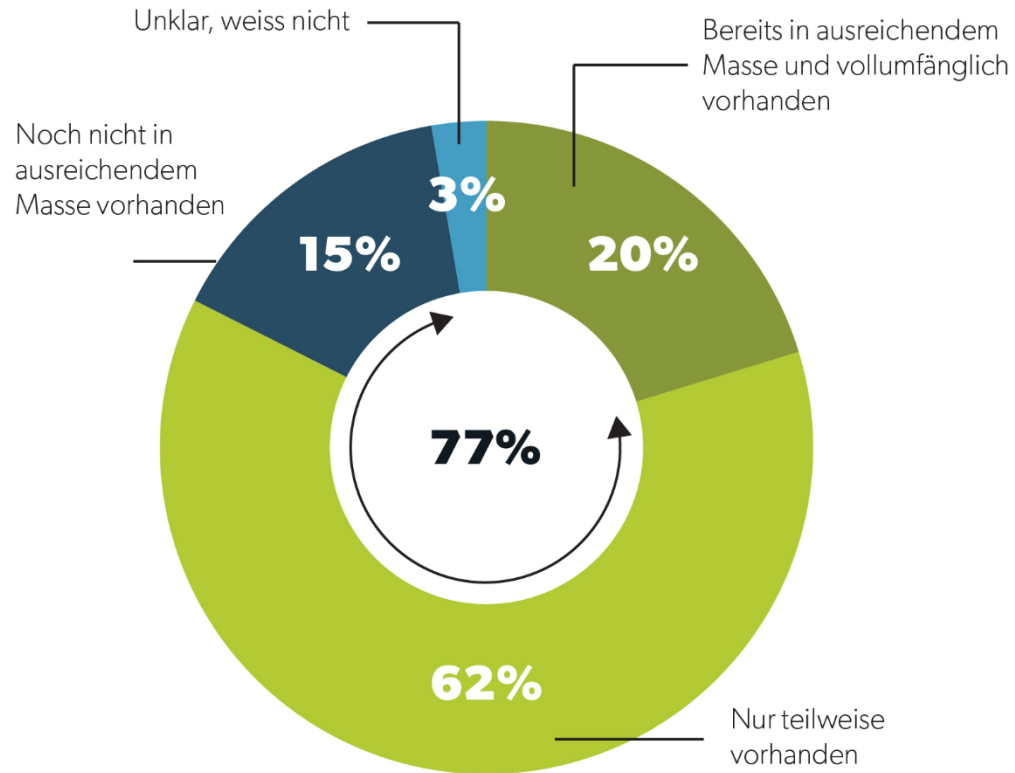
- Dienstleister (50%)
- Industriebetriebe (50%)
- Health Science (40%)

Einstufung 2018: 63%

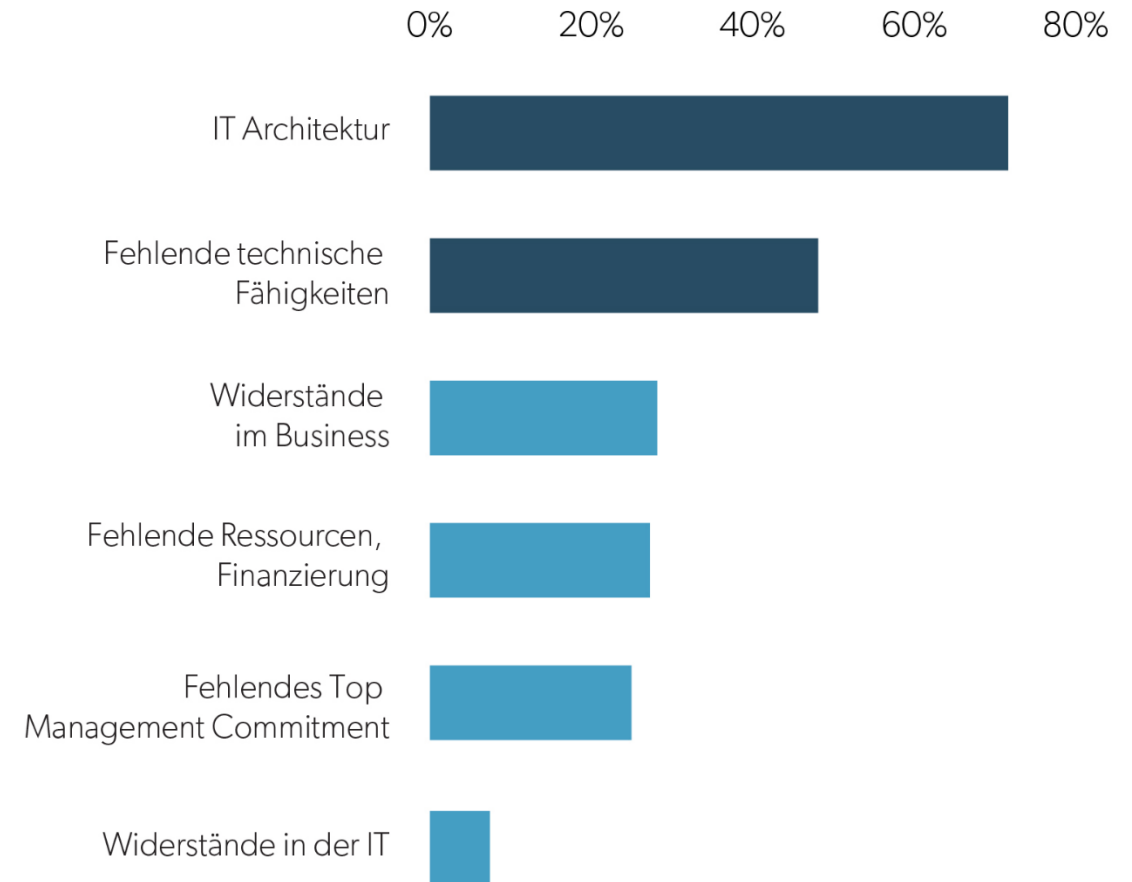
Viele Unternehmen stehen bezüglich ihrer Cyber-Resilienz vor grossen Herausforderungen.

Nur 20% der befragten Unternehmen beurteilen ihre Cyber-Resilienz als ausreichend

Verfügt Ihr Unternehmen bereits über **die notwendigen Cyber-Resilienz Fähigkeiten?**

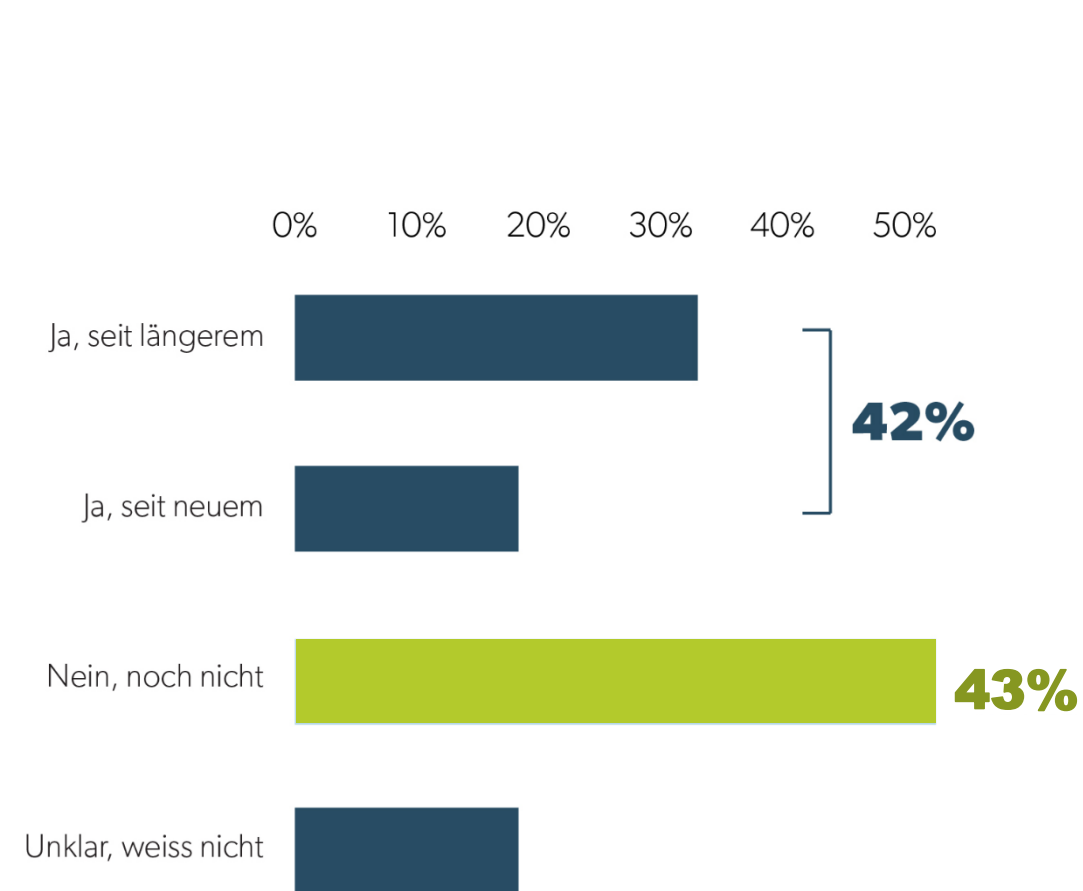


Was sind die **grössten Hürden**, für den Aufbau der erforderlichen Cyber-Resilienz?

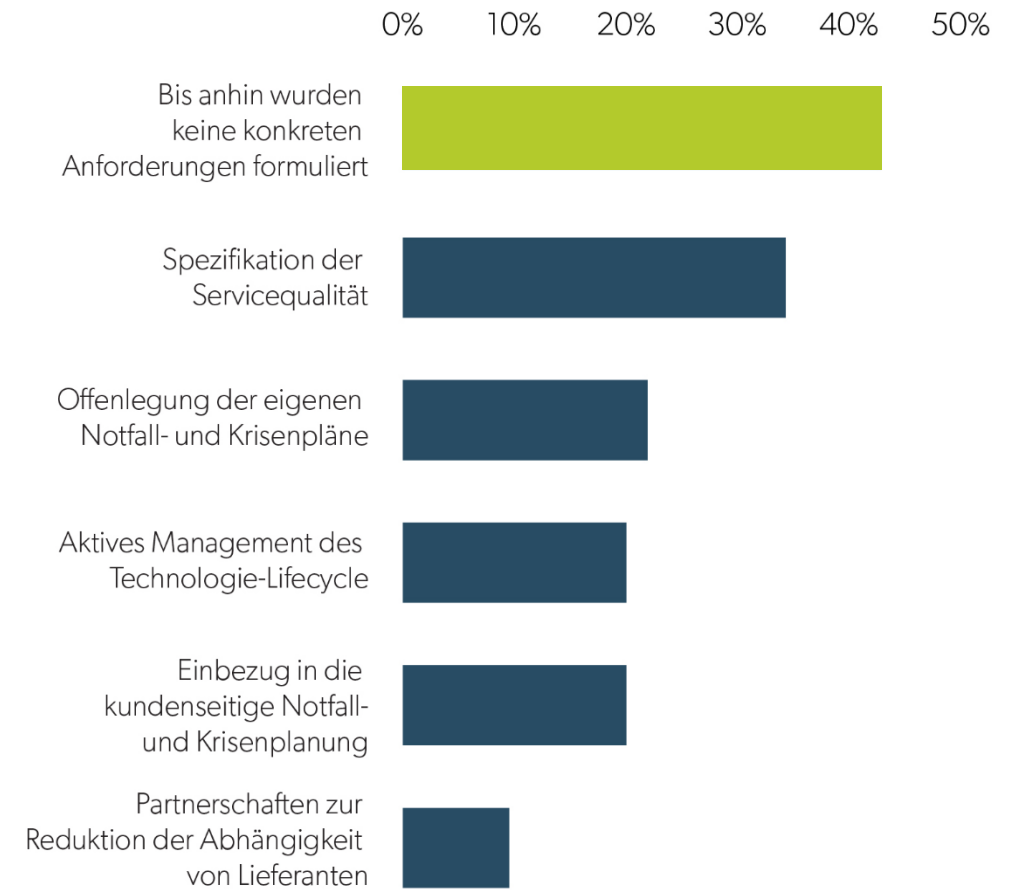


Wird Cyber-Resilienz über die gesamte Wertschöpfungskette zu einem Kundenbedürfnis?

Übernehmen Sie die **Verantwortung für die Cyber-Sicherheit Ihrer Kunden oder Partner**, um die Resilienz der gemeinsamen Wertschöpfungskette zu steigern?



Welche **konkreten Anforderungen** stellen Ihre **Kunden** und/oder **Leistungsbezüger** an eine resiliente Ausgestaltung der Geschäftsbeziehung?



Third Party Risk Management

Risk Metrics & Reporting

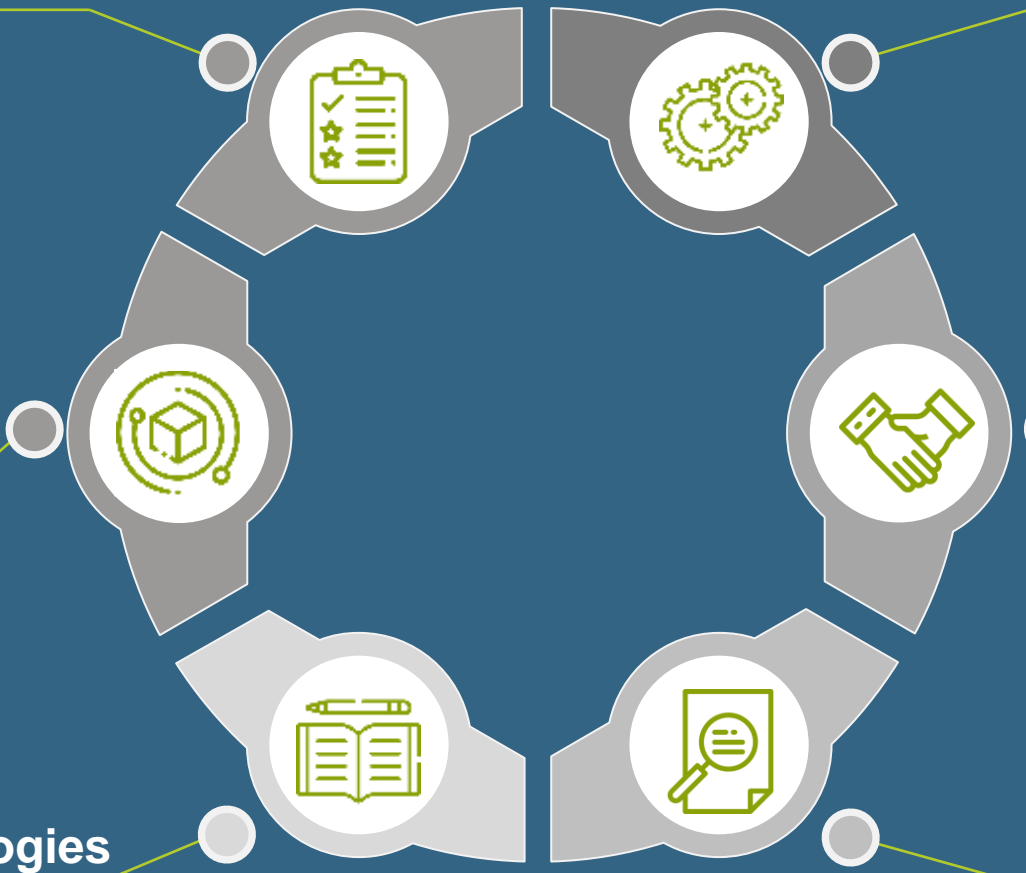
Tools & Technology

Third Party Risk Management Lifecycle Processes

Risk Culture & Awareness

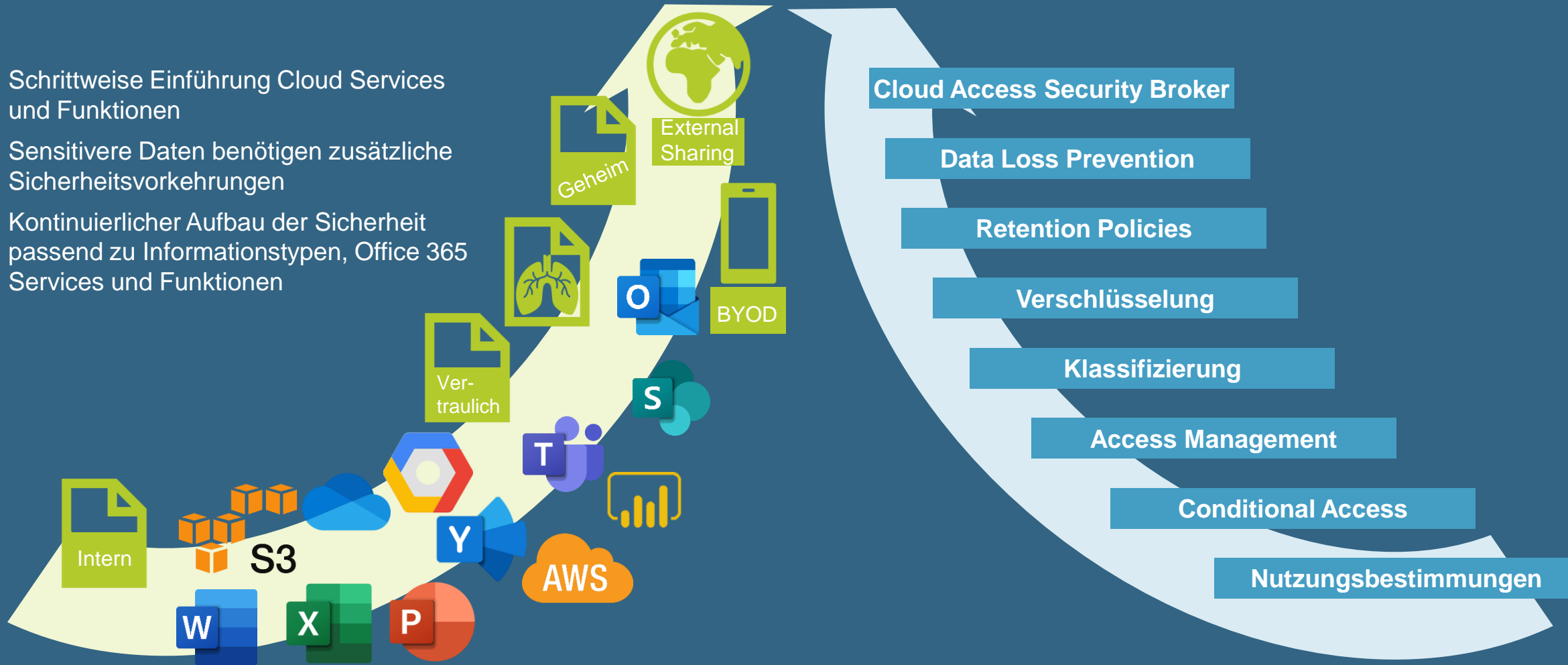
Policies & Risk Methodologies

Governance & Oversight






















Kontinuierlicher Ausbau Cloud Services und Sicherheitsmassnahmen

- Schrittweise Einführung Cloud Services und Funktionen
- Sensitivere Daten benötigen zusätzliche Sicherheitsvorkehrungen
- Kontinuierlicher Aufbau der Sicherheit passend zu Informationstypen, Office 365 Services und Funktionen



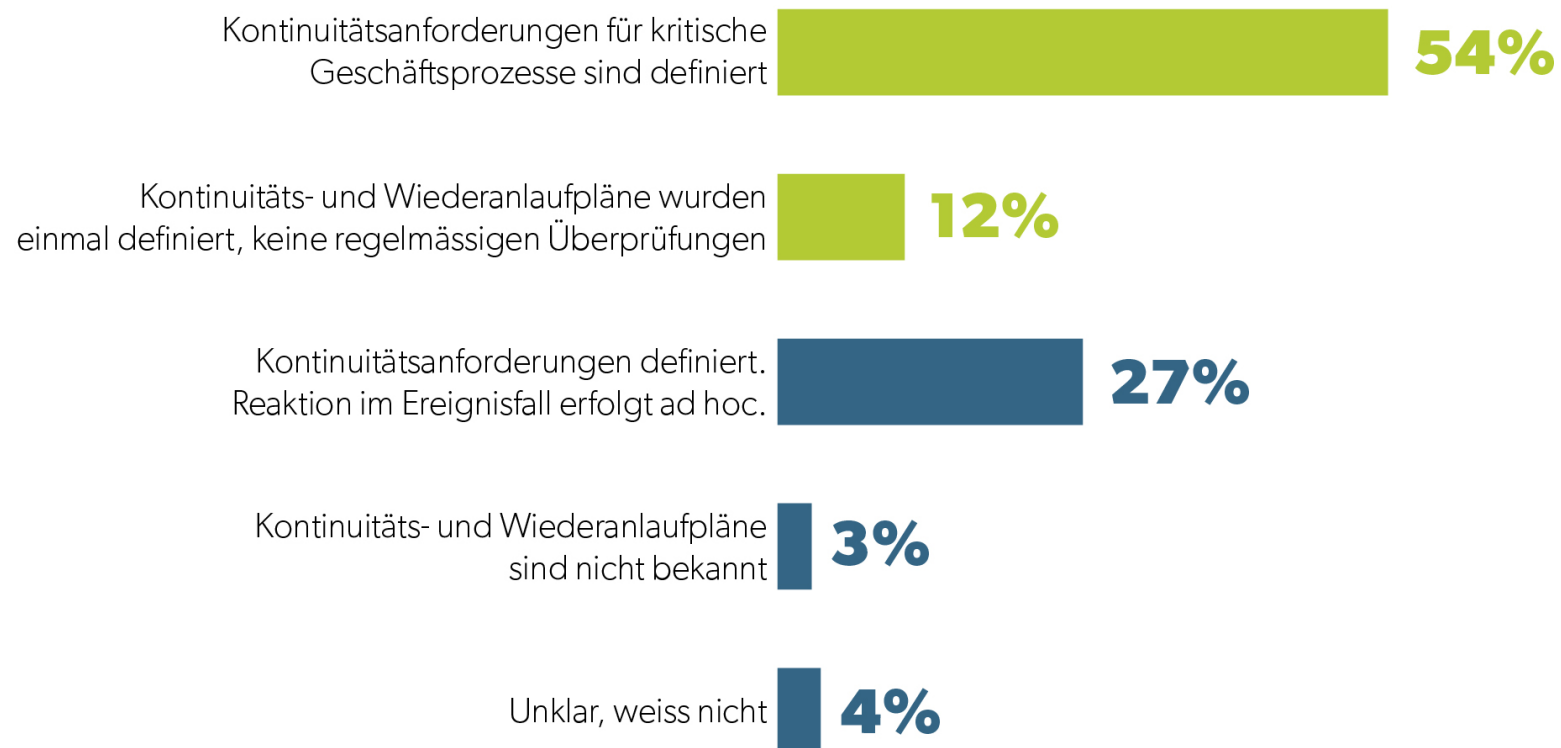
Massnahmen in allen Handlungsfeldern benötigen IT Fähigkeiten

Handlungsfelder	Handlungsbedarf		Wichtige Massnahmen	
	Kurzfristig (2020)	Mittel- & Langfristig (ab 2021)	Kurzfristig (2020)	Mittel- & Langfristig (ab 2021)
 IT			 <p>Artikel «Massnahmen plan für CIOs, CTOs und CDOs» LINK</p>	<ul style="list-style-type: none"> Überführen ad-hoc eingeführten Lösungen in ein nachhaltiges Setup (Fokus Digitaler Arbeitsplatz, digitale Kollaboration, IT Continuity Management) Digitalisierung im Unternehmen fördern
 Supply Chain Mgmt.				<ul style="list-style-type: none"> Supply Chain Resilienz durch Supply Chain Digitalisierung erhöhen Supply Chain Szenarien Planen
 Verkauf & Marketing				<ul style="list-style-type: none"> Auf- und Ausbau der digitalen Kundenschnittstelle (z.B. digitale Verkaufskanäle) CRM-Systeme zur Steigerung der Verkaufseffizienz
 Service				<ul style="list-style-type: none"> Automatisierung Serviceprozesse Fernzugriff auf Maschinen und Anlagen Self-Service Sites zur Entlastung des Servicepersonals
 Produktion				<ul style="list-style-type: none"> Automatisierung Produktion durch Robotics Vorausschauende Wartung Papierlose Fertigung
 Technik & Produktentwicklung				<ul style="list-style-type: none"> Digitale, innovative Produkterweiterungen Digitale Produkte, Services und Geschäftsmodelle

Und wenn es trotzdem passiert

Sind in Ihrer Unternehmung Kontinuitäts- und Wiederanlaufpläne für die Gewährleistung kritischer Geschäftsprozesse im Ausnahmefall definiert?

Wenn der Eintritt eines Cyber-Ereignisses nicht verhindert werden kann, wird die rasche Erholungsfähigkeit immer mehr zu einem kritischen Erfolgsfaktor.



Cyber Resilienz in unsicheren Zeiten



3 prioritäre Handlungsfelder:

Third Party Risk Management

Cloud Services & Sicherheitsmassnahmen

Business Continuity Management

Unsere Vision weist uns den Weg in die Zukunft.

Enabling Digital Performance



**Gemeinsam den
digitalen Wandel
gestalten!**

Wir verstehen die Bedürfnisse von Kunden aus unterschiedlichsten Branchen und sind vertraut mit den Technologien der Zukunft.

- Wir erarbeiten uns das Vertrauen unserer Kunden, indem wir ihre Anliegen in den Mittelpunkt unseres Denkens und Handelns stellen.
- Wir sind der bevorzugte Partner für unsere Kunden, weil wir als unabhängiges IT-Beratungsunternehmen aus einer neutralen Perspektive beraten.
- Wir helfen unseren Kunden, innovative Informationstechnologie zielführend und im Einklang mit ihren Geschäftszielen zu nutzen.
- Unsere Mitarbeitenden überzeugen durch Kompetenz, Engagement und als Menschen.

Cyber Security & Privacy – Schaffen Sie Vertrauen in Ihre digitalen Prozesse.

Strategie & Governance

- **Informationssicherheit** übergeordnet im Unternehmen **verankern**
- Mit dem richtigen **Framework** zur **effektiven Steuerung** der **Informationssicherheit** gelangen
- Wissen, was wann und mit wem zu tun ist

«Vertraulichkeit, Integrität und Verfügbarkeit von Informationen sicherstellen»

Cloud Security & IAM

- **Daten** auch in der **Cloud sicher** und **überwacht** aufbewahren
- **Jederzeit wissen, wer auf was Zugriff hat** – im eigenen Datacenter und in der Cloud
- Mit uns den richtigen Ansatz für **Identity und Access Management** finden und umsetzen

«Die Cloud sicher nutzen»

Resilience

- Auch **unbekannte Einflussfaktoren & Risiken abschätzen** und darauf reagieren
- **Geschäftsgefährdende Ereignisse absorbieren** und sich neuen Umständen anpassen
- **Business Continuity Management** aufbauen und erhalten

«Widerstandsfähigkeit gegenüber Gefahren stärken»

Privacy & Compliance

- Gegenwärtige und zukünftige **Anforderungen an gesetzliche Vorgaben und Regulatorien meistern**
- Durch **massgeschneiderte Prozesse** den **Überblick** behalten und angemessen und effektiv **auf Ereignisse reagieren**

«Datenschutz im Griff haben»

Herzlichen Dank für Ihr Interesse!



AWK Group

Enabling digital performance.



Adrian Marti
Dr. phil. nat., EMBA, CISM, CRISC
Partner, Head of Cyber Security & Privacy

+41 58 411 97 67
adrian.marti@awk.ch

<https://www.awk.ch/cyber-security-privacy>

AWK Cyber Security & Privacy

- Ihr produkteneutraler Spezialist für Informationssicherheit
- Unterstützt von der Strategie bis zur Umsetzung
- 50 Spezialisten für Cyber Security & Datenschutz
- >75 Sicherheitszertifizierungen
- 100 laufende Mandate (aktueller Stand)
- Unabhängig, produkt- und lösungsneutral
- In allen Branchen tätig
 - Banking
 - Manufacturing
 - Insurance
 - Utilities
 - Retail
 - Pharma
 - Public Services
 - Service Provider
 - Mobility
 - Health