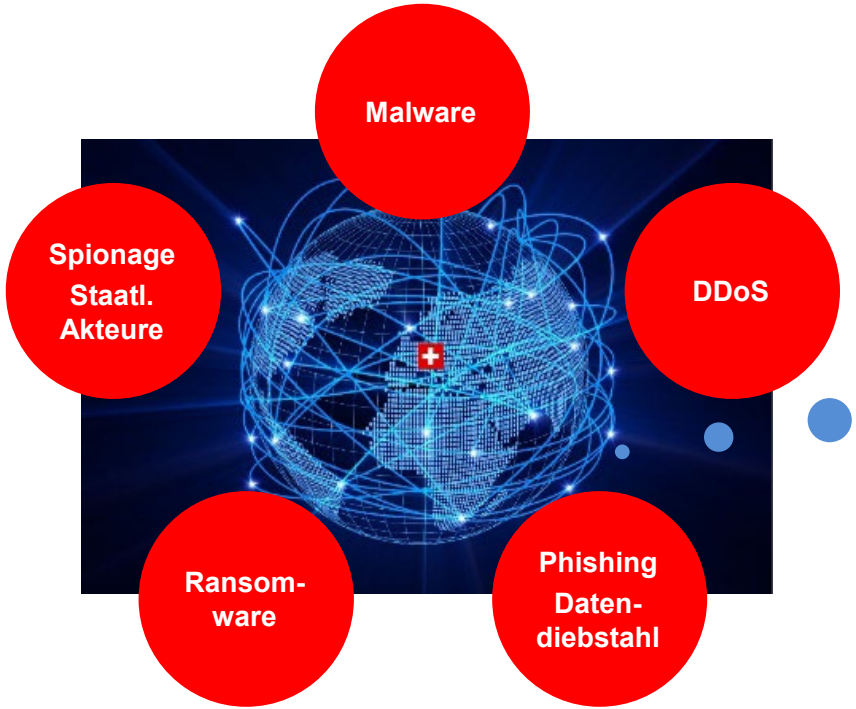
Herausforderungen durch Cybersecurity in der modernen Unternehmensrealität

Oliver M. Brupbacher

Dr. iur., LL.M., Rechtsanwalt, Partner
Kellerhals Carrard

Die Bedrohungslage verschärft sich



Managed Service Providers

Cloud Anbieter

Nach Pascal Lamia, Leiter
Operative Cybersicherheit NCSC

Agenda

1. Cybersecurity Risiken im geltenden Recht
2. Cybersecurity Untersuchungen im Unternehmen
3. Meldepflichten und Kommunikation
4. Cybersecurity Preparedness

1. Cybersecurity Risiken im geltenden Recht

Vielfalt der Risiken

Regulatorische Anforderungen und Sanktionen, z.B.

- Mindestanforderungen an die Datensicherheit (*Art. 8 revDSG*)
- Finanzinstitute und Versicherungen (z.B. Art. 14, 23 FinfraG; Art. 3f Abs. 2 BankG)
- Telekommunikation (z.B. Art. 48a FMG)
- Gesundheitswesen (z.B. Art. 12 Abs. 1 lit. b EPDG; Art. 6 Abs. 1, 2 MepV)

Strafuntersuchungen, z.B.

- Verletzung der Datensicherheit (*Art. 61 lit. c revDSG*)
- Geheimnisverletzung (z.B. Art. 35 DSG; *Art. 62 revDSG*; Art. 320 ff. StGB; Art. 47 BankG; Art. 43, 53 FMG; Art. 16 ff. PrSG)

Haftung, z.B.

- der Gesellschaft (z.B. Art. 97 ff.; 41ff. OR; Art. 1, 4 PrHG; Art. 15 DSG / *Art. 32 revDSG*; Art. 28 ff. ZGB)
- der Organe (Art. 754, 827 OR)

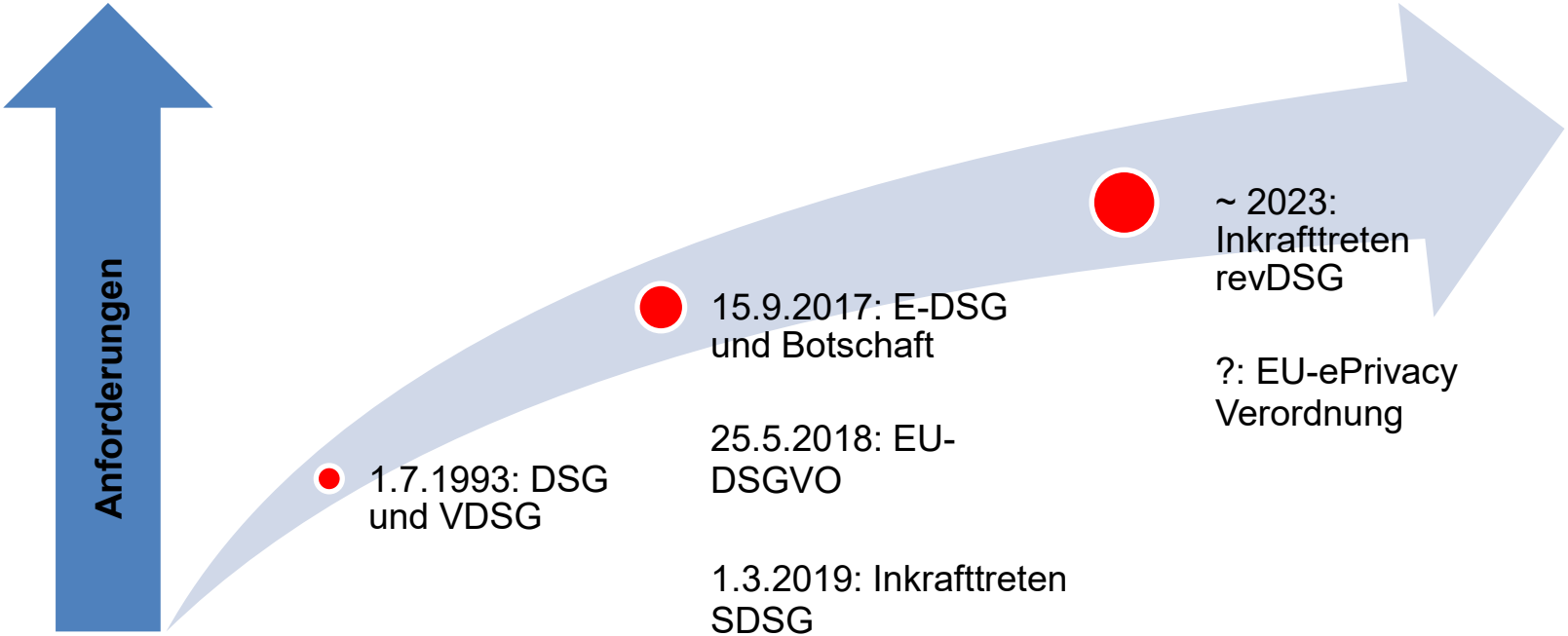
Ausländische Risiken, z.B.

- "*For too long, companies have chosen silence under the mistaken belief that it is less risky to hide a breach than to bring it forward and to report it. Well that changes today.*" (Deputy Attorney General Lisa O. Monaco, 6.10.2021; Biden Administration EO on Cybersecurity)

Dazu kommen u.U.

- Datenschäden
- Verlust von geistigem Eigentum, Fabrikations- und Geschäftsgeheimnissen
- Reputationsverlust
- Sach- und Personenschäden
- Supply Chain- / Betriebsunterbruch

Verschärfung der Datenschutz-Anforderungen



EU-DSGVO: Geltung in der Schweiz

- Grds. Anknüpfung am **Ort der Niederlassung** (Art. 3(1) DSGVO)
- **Aber** auch Geltung, wenn der Verarbeiter (Art. 3(2) DSGVO):
  - (1) Ggü. Personen in der EU Waren oder Dienstleistungen **anbietet** (Sprache, Währung, lokale Domain, Versand an lokale Kunden, etc.)
  - (2) das Verhalten von Personen in der EU **beobachtet** (Profiling, Tracking, etc.)

Cybersecurity: Datenschutz-Compliance

Bearbeitung grds. erlaubt

- Sofern die Grundsätze eingehalten werden

(Art. 12 Abs. 1 DSG / *Art. 30 Abs. 1 revDSG*)

Bearbeitungsgrundsätze

- Rechtmässig, nach Treu und Glauben, verhältnismässig
- Zweckgebunden und transparent
- Datenrichtigkeit

(Art. 4 f. DSG / *Art. 6 revDSG*)

Datensicherheit

- Angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten

(Art. 7 DSG / *Art. 8 revDSG*)

Datenschutz-Folgeabschätzung

- Im Rahmen der Vorbereitung von Projekten

(*Art. 22 revDSG*)

Meldung von Data Breaches

- Bei Verletzungen der Datensicherheit

(*Art. 24 revDSG*)

Dokumentationspflicht

- Verzeichnis der Bearbeitungstätigkeiten (als Ersatz der heute geltenden Verpflichtung zur Anmeldung einer Datensammlung)

(*Art. 12 revDSG*)

Sanktionen

Aktuell

- EDÖB gibt Empfehlungen ab
- Bei Nichtbefolgung oder Ablehnung: Bundesverwaltungsgericht
- Busse von max. CHF 10'000 für vorsätzliche Verletzung bestimmter Pflichten nach DSG

revDSG

- *EDÖB hat Kompetenz zu*
  - *Untersuchung von Bearbeitungsvorgängen*
  - *Verfügungen zur Einstellung, Einschränkung oder Anpassung einer Bearbeitung*
- *Kantonale Strafbehörden haben Kompetenz zur Verhängung persönlicher Bussen bis CHF 250k für Verletzung bestimmter DSG-Bestimmungen (insb. für vorsätzliche Nichteinhaltung der Mindestanforderungen an die Datensicherheit; Art. 61 lit. c revDSG) und mangelnde Kooperation mit EDÖB*
- *Bussen nicht versicherbar*

EU-DSGVO

- Aufsichtsbehörden mit Kompetenz zu
  - Untersuchung von Bearbeitungsvorgängen
  - Verfügungen zur Einstellung, Einschränkung oder Anpassung einer Verarbeitung
  - Für die meisten Verstösse: Verhängung von Bussen bis EUR 10m/20m oder 2%/4% des weltweiten Jahresumsatzes (insb. für Verletzungen der Datensicherheit; Art. 83(5)(a) DSGVO)
  - Auch bei Fahrlässigkeit
- Ev. weitere Bussen nach lokalem Recht

2. Cybersecurity Untersuchungen im Unternehmen

Am Anfang

From: Peter
To: CEO
Date: Dec 30, 2020 5:30pm CET
Subject: Data Breach Detected

Good Afternoon (and Happy New Year)!

I am an outside consultant, and I have identified what appears to be a serious data breach involving your company's information. This facebook post links to a Google Sheet containing first and last names, social security numbers, email addresses, phone numbers, dates of birth, home addresses, and other identifying information regarding your employees. As you can see, there are over 250k rows of data.

I don't think this should be the type of data that should be publicly available, don't you agree?

As an experienced outside consultant in the cybersecurity field, I am more than happy to help your company in responding to this sensitive situation. Of course, I would expect to be compensated for my time. I have already uncovered more information that I can tell you about once my retainer is paid. My standard retainer is $ 10,000. Additional payment information to follow.

Szenario entwickelt mit Morrison & Foerster LLP (John P. Carlin, David A. Newman und Alex Iftimie)

Mi. 30.12.2020 | Mi. 06.01.2021 | Do. 07.01.2021 | Fr. 08.01.2021

De quoi s’agit-il?

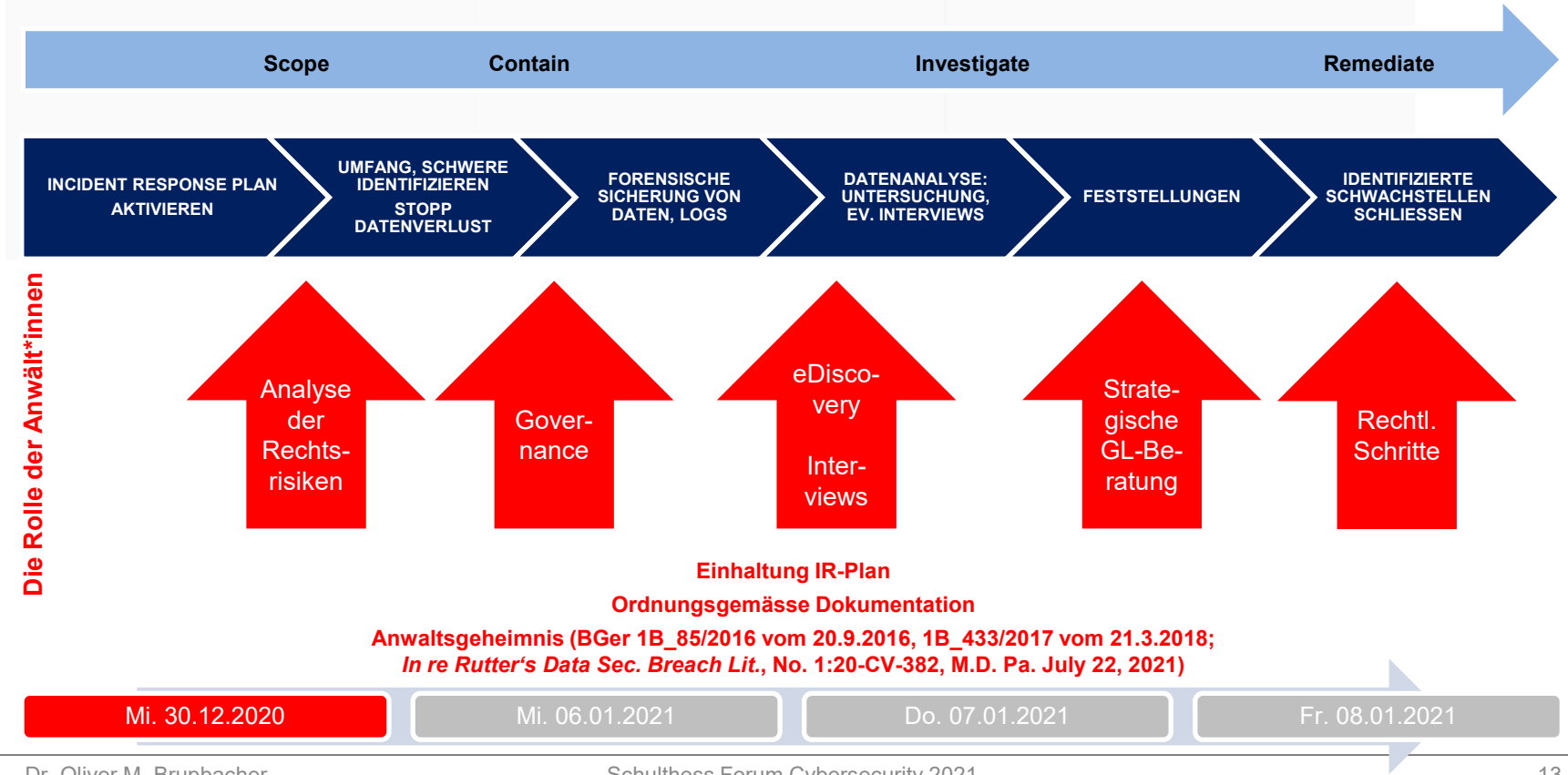
Ein Mitarbeiter Ihrer Firma teilt Ihnen mit, dass er auf den Link zu dem facebook-Post geklickt hat und dass Peter Recht hat: Ein facebook-Post von "Streetfighter" enthält einen Link zu einem Google Sheet, das alle Kategorien von Informationen enthält, die Peter beschrieben hat.

Wahrscheinlich hätten auch andere Besucher der facebook-Seite auf den Link klicken und auf dieses Dokument zugreifen können. Der Link wurde kurz vor Weihnachten gepostet.

- **Welche Fragen müssen Sie beantworten, um Entscheidungen zu treffen?**
- **Wer trifft Entscheidungen?**
- **Wer muss an der Reaktion beteiligt werden?**
- **Ist angesichts des Vorfalls eine Benachrichtigung der Mitarbeiter oder der Öffentlichkeit erforderlich?**
- **Müssen Aufsichtsbehörden informiert werden?**

Mi. 30.12.2020 | Mi. 06.01.2021 | Do. 07.01.2021 | Fr. 08.01.2021

Cybersecurity Untersuchung



3. Meldepflichten und Kommunikation

Meldepflichten im In- und Ausland (Auswahl)

Bei Betroffenheit personenbezogener Daten

- Benachrichtigung der **Betroffenen** (Art. 4 Abs. 1, 2 DSG / *Art. 6 Abs. 1, 2 revDSG*), insb. falls zum Schutz erforderlich oder vom EDÖB verlangt (*Art. 24 Abs. 4 revDSG*)
- **Ausnahmen** bei überwiegenden Drittinteressen, wo die Information unmöglich ist / einen unverhältnismässigen Aufwand erfordert (*Art. 24 Abs. 5 lit. a, b revDSG*)
- Benachrichtigung des **EDÖB** bei einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen (*Art. 24 Abs. 1, 2 revDSG*)
- Keine allg. Pflicht zur Information der **Öffentlichkeit** (aber Art. 4 Abs. 1, 2 DSG / *Art. 6 Abs. 1, 2 revDSG; Art. 24 Abs. 5 lit. c revDSG*)

Aufsichtsbehörden – branchenspezifische Meldepflichten

- **Finanzinstitute** und **Versicherungen** (Art. 29 Abs. 2 FINMAG; FINMA Aufsichtsmitteilung 05/2020; FINMA Rundschreiben 08/25)
- **Telekommunikation** (Art. 96 Abs. 1 FDV)
- **Gesundheitswesen** (Art. 12 Abs. 3 EPDV; Art. 66 MepV)

Mi. 30.12.2020 | Mi. 06.01.2021 | Do. 07.01.2021 | Fr. 08.01.2021

Meldepflichten im In- und Ausland (Auswahl)

Offenlegung	– **Rückstellungen** im Geschäftsbericht (z.B. Art. 960e OR; Art. 49 ff. KR) – **Ad hoc**-Publizität (Art. 53 KR)
Freiwillige Meldung	– **Strafverfolgungsbehörden** – Nationales Zentrum für Cybersicherheit (**NCSC**) – Koordinationsstelle zur Bekämpfung der Internetkriminalität (**KOBIK**)
Vertragliche Meldepflichten	– **Auftragsverarbeiter** von Personendaten (*Art. 24 Abs. 3 revDSG*) – Gegenüber **Versicherern** – Gegenüber **Geschäftspartnern**
Ausländische Meldepflichten	– Im Einzelfall abzuklären

Mi. 30.12.2020 | Mi. 06.01.2021 | Do. 07.01.2021 | Fr. 08.01.2021

Kommunikation

Telefonkonferenz um 9.00 Uhr CET: Das von Ihnen beauftragte externe Forensikteam hat einen grossen, unbekannten Dateitransfer gefunden, der in den Datenbanken Ihrer Firma ablief und auch Mitarbeiterdaten betrifft, und stoppte ihn. Die Dateien sind verschlüsselt, und ihr Inhalt kann nicht geöffnet werden. Das Team hat keine Hinweise darauf gefunden, dass dieses Problem mit den Mitarbeiterdaten auf facebook zusammenhängt. Die Experten untersuchen gegenwärtig noch, ob der Zugriff und Transfer von Ihrer Firma aus stattgefunden haben könnte.

Anruf um 14:00 Uhr CET: Ein Blogger kündigt an, morgen um 9:00 Uhr CET einen Artikel über eine Datenschutzverletzung betreffend Mitarbeiterdaten bei Ihrer Firma zu veröffentlichen, unabhängig davon, ob Sie einen Kommentar dazu abgeben oder nicht. Ihr CEO möchte der Sache zuvorkommen und eine Pressemitteilung herausgeben. Ihre PR-Firma entwirft ein kurzes Statement:

"*We are aware of an intrusion relating to employee information, and our investigation remains ongoing, but at this time, we have no evidence that any information of our customers has been compromised.*"

- **Was ist Ihre Reaktion auf das Statement?**
- **Wie reagieren Sie auf die Anfrage des Bloggers?**

Mi. 30.12.2020 | **Mi. 06.01.2021** | Do. 07.01.2021 | Fr. 08.01.2021

Kommunikation

- **Herausforderungen** an die Kommunikation bei Cyber Incidents sind erheblich
  - → Daher: **Frühzeitig** Experten einschalten und Prozesse etablieren
- Ausgangspunkt der Kommunikationsstrategie: **Rechtliche** Strategie

Verhalten, das die Reputationsrisiken erhöht und zu vermeiden ist:

- Aussagen als **gesichert** erscheinen lassen, die tatsächlich ungesichert sind
- **Widersprüche** zwischen SBS und Handeln des Unternehmens
- "PR-**Reinwaschung**" und "**scheibchenweise** Information"
- **Inkonsistente** Kommunikation (bei Pressemitteilungen, Behörden, FAQs, öffentliche Erklärungen, Call-Center-Antworten auf Kundenanfragen, etc.)

Phishing

From: CISO
To: CEO
Date: Jan 7, 2021 6:30pm CET
Subject: Cyber threat

Bad news. The forensics team has now found artifacts of exfiltration of client data – and indications that the same intruder is elsewhere on the broader company network.

We now think that the bad actor's point of entry into our systems wasn't through a vulnerability of our systems, but through our own staff clicking the link to the facebook post in Peter's first email. So Peter appears connected to the bad actor (or possibly is the bad actor).

In certain emails, the link was doctored to be identical to the actual facebook post link but contained hidden scripts that launched when clicked. We don't know how it got past our phishing filters.

Ransomware

From: Peter
To: CEO
Date: Jan 8, 2021 11:30pm CET
Subject: Re: Data Breach Detected

Uh oh, looks like you found me! It's unfortunate that you terminated the exe I was running, but no worries- there's plenty more where that came from :-) I already have over 1TB of data from you! If only you managed to find my exe and terminate it sooner... I even gave you a hint earlier!

I guess I can tell you now about the other information I alluded to in my first email. Your client relationships are really interesting. I'm sure the world would like to know more about them! Of course, you might be able to convince me otherwise by paying my retainer fee... And I would much prefer to deal with you privately instead of all those fake news outlets.

Also, I did leave something behind that I thought you would appreciate...

Mi. 30.12.2020 | Mi. 06.01.2021 | Do. 07.01.2021 | Fr. 08.01.2021

Ransomware

This machine has been encrypted with the strongest encryption. The ONLY decryption key is stored on a secret Internet server. Nobody can decrypt your files until you pay and obtain the decryption key. Time is money. You have 48 hours to submit payment of $25,000 in Bitcoin. If you do not send money in that time, your files will be permanently encrypted and the decryption key will be destroyed.

Click on this link to connect to the secret server and follow instructions.

Mi. 30.12.2020 | Mi. 06.01.2021 | Do. 07.01.2021 | Fr. 08.01.2021

4. Cybersecurity Preparedness

Cybersecurity Compliance by Design

RISIKO-, KRISEN- UND KONTINUITÄTSMANAGEMENT

Datensicherheit Privacy by Design & Default	– Technische und organisatorische Massnahmen für ein dem Risiko angemessenes Datenschutzniveau – Massnahmen zur Einhaltung anderer Datenschutz-Vorschriften – Standardmässige Minimierung der Datenverarbeitung
Incident Response (IR) Plan	– Asset Discovery & Assessment – Identifikation von Typen potentieller Incidents – Identifikation von internen und externen Stakeholders – Festlegung von Rollen und Verantwortlichkeiten
Kommunikationsplan	– Schlüssiges und widerspruchsfreies Standby Statement (SBS) – Q&A
Business Continuity Plan	– Business Impact Analyse – BCM Massnahmen

Lessons Learned

Danke für Ihre Aufmerksamkeit

Kontakt
Dr. Oliver M. Brupbacher
Rechtsanwalt, Partner
Kellerhals Carrard
Henric Petri-Strasse 35
4010 Basel
058 200 30 47
oliver.brupbacher@kellerhals-carrard.ch