Neue Zürcher Compliance-Konferenz 2021

Cybersecurity Untersuchungen – Einsichten von der Frontlinie. Eine Planübung

Dr. iur. Claudia Götz Staehelin
LL.M., CIPP/E, Advokatin, Partnerin
Kellerhals Carrard

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

Agenda

Neue Zürcher Compliance-Konferenz 2021

1. Beginn und Krisenmanagement
2. Cyber Security Untersuchung
3. Kommunikation
4. Risiken
5. Ransomware
6. Corporate Governance
7. Lessons Learned

Neue Zürcher Compliance-Konferenz 2021

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

1. Beginn und Krisenmanagement

Neue Zürcher Compliance-Konferenz 2021

- 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

1. Beginn und Krisenmanagement

Neue Zürcher Compliance-Konferenz 2021

Meldepflichten im In- und Ausland

- 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, 6 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, z.B.
  - Finanzinstitute und Versicherungen (Art. 29 Abs. 2 FINMAG; FINMA Aufsichtsmitteilung 05/2020; FINMA Rundschreiben 08/25)
  - Gesundheitswesen (Art. 12 Abs. 3 EPDV; Art. 66 revMepV)
  - Telekommunikation (Art. 96 Abs. 1 FDV)
- Offenlegung
  - Rückstellungen im Geschäftsbericht (z.B. Art. 960e OR; Art. 49 ff. KR)
  - Ad hoc-Publizität (Art. 53 KR)
- Freiwillige Meldung an Strafverfolgungsbehörden; alternativ an
  - Nationales Zentrum für Cybersicherheit (NCSC) oder Koordinationsstelle zur Bekämpfung der Internetkriminalität (KOBIK)
- Vertragliche Meldepflichten, insb. auch
  - Auftragsverarbeiter von Personendaten (Art. 24 Abs. 3 revDSG)
  - Gegenüber Versicherern
- Ausländische Meldepflichten

Hauptthemen:
- Ob und an wen
- Zeitpunkt

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

1. Beginn und Krisenmanagement

Neue Zürcher Compliance-Konferenz 2021

Die Rolle des Anwalts

- Identifikation und Analyse rechtlicher Risiken
- Strategische Beratung der Geschäftsleitung
- Governance:
  - Einhaltung des Incident Response Plan des Unternehmens und anderer Prozesse
  - Ordnungsgemässe Dokumentation aller Vorgänge
  - Kommunikationsstrategie und Überprüfung der Statements
- Einleitung einer vom Anwaltsgeheimnis geschützten internen Untersuchung
  - I.d.R. unter Beauftragung externer Forensiker und IT-Experten
  - Beweissicherung / eDiscovery
- Ggf. Einleitung rechtlicher Schritte (Strafanzeige, Zivilklagen, Verteidigung)

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

2. Cyber Security Untersuchung

Neue Zürcher Compliance-Konferenz 2021

VOR ANGRIFF: VORBEREITUNG

- Incident Response Plan, inkl. Kommunikationsplan
- Training für Response Team Members
- Bewusstsein für Risiken innerhalb der Belegschaft schaffen

WÄHREND ANGRIFF: KOORDINIERTES UND EINHEITLICHES HANDELN

- Cyber-Bedrohung identifizieren
- Umfang und Schwere der Cyber-Bedrohung bestimmen
- Cyber-Bedrohung eindämmen
- Entscheiden, ob und wann Verbraucher, Kunden, Geschäftspartner oder Behörden informiert werden sollen/müssen
- Kommunikationsstrategie definieren

CYBER SECURITY INVESTIGATION & KRISENMANAGEMENT

- Strukturierter Prozess, in dem forensisch digitale Daten aus am Angriff beteiligten Netzwerken (Internet und/oder lokales Netzwerk) untersucht, analysiert und ggf. wiederhergestellt werden (*root cause analysis*)
- Cyber-Krisenmanagement

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

2. Cyber Security Untersuchung

Neue Zürcher Compliance-Konferenz 2021

Vorbereitung | **Durchführung** | **Nachbereitung**

INCIDENT RESPONSE PLAN AKTIVIEREN → UMFANG, SCHWERE IDENTIFIZIEREN STOPP DATENVERLUST → FORENSISCHE SICHERUNG VON DATEN, LOGS → DATENANALYSE: UNTERSUCHUNG, EV. INTERVIEWS → FESTSTELLUNGEN → IDENTIFIZIERTE SCHWACHSTELLEN SCHLIESSEN

Anwaltsgeheimnisses / Vertraulichkeit: Beauftragung von forensischen Cyber-Experten durch externe Anwälte, Kommunikations-Protokolle

Scope → Contain → Investigate → Remediate

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

Neue Zürcher Compliance-Konferenz 2021

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

3. Kommunikation

Neue Zürcher Compliance-Konferenz 2021

- ☑ Herausforderungen an die Kommunikation bei Cyber Incidents sind erheblich
  - ☑ Daher: Frühzeitig Experten einschalten und Prozesse etablieren
- ☑ Ausgangspunkt der Kommunikationsstrategie: Rechtliche Strategie
- ☑ Zur Vorbereitung auf Cyber Incidents gehört ein schlüssiges und widerspruchsfreies Standby Statement (SBS) und ein Q&A
- ⊘ 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.)

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

Neue Zürcher Compliance-Konferenz 2021

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.

- **Was sollten Sie jetzt tun?**
- **Sollten Sie die Strafverfolgungsbehörden einschalten?**
- **Was sind die Risiken und der Nutzen des jeweiligen Vorgehens?**

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

4. Risiken

Neue Zürcher Compliance-Konferenz 2021

- Datenschäden
- Verlust von geistigem Eigentum, Fabrikations- und Geschäftsgeheimnissen
- Reputationsverlust
- Sach- und Personenschäden
- Betriebsunterbruch
- Regulatorische Untersuchungen und Sanktionen, insb.
  - Mindestanforderungen an die Datensicherheit (Art. 8 revDSG)
  - Finanzinstitute und Versicherungen (z.B. Art. 14, 23 FinfraG; Art. 3f Abs. 2 BankG)
  - Gesundheitswesen (z.B. Art. 12 Abs. 1 lit. b EPDG; Art. 6 Abs. 1, 2 revMepV)
  - Telekommunikation (z.B. Art. 48a revFMG)
- 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 PrHG)
- Haftung, z.B.
  - der Gesellschaft (z.B. Art. 97 ff.; 41ff. OR; Art. 1, 4 PrHG; Art. 15 Abs. 1 DSG / Art. 31 Abs. 2 revDSG; Art. 28 ff. ZGB)
  - der Organe (Art. 754, 827 OR)
- Ausländische Risiken, z.B.
  - "*Companies should avoid generic cyberscurity-related disclosure and provide specific information that is useful to investors.*" (SEC Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 21.2.2018)

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

Neue Zürcher Compliance-Konferenz 2021

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

Neue Zürcher Compliance-Konferenz 2021

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

5. Ransomware

Neue Zürcher Compliance-Konferenz 2021

Bezahlen oder nicht bezahlen?

- "*Demand for ransomware payments has increased during the COVID-19 pandemic as cyber actors target online systems that U.S. persons rely on to continue conducting business. Companies that facilitate ransomware payments to cyber actors on behalf of victims, including financial institutions, cyber insurance firms, and companies involved in digital forensics and incident response, not only encourage future ransomware payment demands but also may risk violating OFAC regulations.*"
  (OFAC Advisory on Potential Sanctions Risks for Facilitating Ransomware Payment, 1.10.2020)
- Risiken:
  - Verletzung von Wirtschaftssanktionen
  - Materielle Unterstützung des Terrorismus
  - Reputationsrisiken
  - Wiederholungsrisiken

Cyber Risk Versicherung

- Breite Verfügbarkeit
- Grundvoraussetzung i.d.R. Implementierung eines Cyber Risk Managements
- Deckungsbedingungen teilw. umstritten, z.B. *war exclusion* (*Mondelez Int., Inc. v. Zurich American Insurance Co.*, No. 2018L011008, 2018 WL 4941760, Ill. Cir. Ct., Oct. 10, 2018), *sanction limitation*

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

6. Corporate Governance

Neue Zürcher Compliance-Konferenz 2021

Incident Response Plan (IR-Plan)

- Ein Incident Response Plan enthält Anweisungen, die dem Unternehmen helfen sollen, sich auf einen Cyber Incident vorzubereiten, diesen zu erkennen und angemessen zu reagieren
- Wer macht was, wann?
- Hauptelemente des IR-Plans:
  - Asset Discovery/Assessment
    - Analyse von Daten und IT assets, zwecks Identifikation derselben und Risiko-Analyse
  - Typen von potentiellen Incidents festlegen
    - Koordination mit Business Continuity Plan
  - Rollen und Verantwortlichkeiten des Response Teams festlegen
    - Interne und externe Mitglieder und Leader festlegen (mit Befugnissen); Kontaktliste erstellen; Eskalationsprozesse festlegen
  - Interne und externe Stakeholders identifizieren
    - Kunden, Mitarbeiter, Verbraucher, Behörden, Öffentlichkeit
  - IR-Plan gestützt auf identifizierte potentielle Szenarien testen

Kommunikationsplan

7. Lessons Learned

Neue Zürcher Compliance-Konferenz 2021

- Expertise und Koordination des internen und externen Response Teams
- Schnelligkeit und Entscheidungsbefugnis
- Strategischer Ansatz
- Vorbereitung (IR-Plan, Kommunikationsplan)
- Einübung des IR-Plans
- Business Continuity Plan (z.B. Back-up Systeme)
- Reibungsloser Informationsfluss im Unternehmen

Neue Zürcher Compliance-Konferenz 2021

Danke für Ihre Aufmerksamkeit

Kontakt
Dr. Claudia Götz Staehelin
Kellerhals Carrard
Henrci-Petri-Strasse 35
4051 Basel
058 200 30 65
claudia.goetz@kellerhals-carrard.ch

Dr. Claudia Götz Staehelin, Head der Praxisgruppe Investigations bei Kellerhals Carrard, ist Partnerin im Bereich Litigation und Investigations und spezialisiert auf Dispute Resolution sowie interne Untersuchungen in verschiedenen Branchen. Sie berät ihre Klienten in den Bereichen Compliance, interne Untersuchungen, grenzüberschreitende Verfahren, internationale Rechtshilfe und Datenschutz und unterstützt ihre Klienten im Krisenmanagement. Claudia Götz Staehelin kombiniert Dispute Resolution Expertise mit umfangreicher Business-Erfahrung. Bevor sie in die Kanzlei eintrat, war Claudia Head Litigation bei Novartis, wo sie grosse grenzüberschreitende Streitigkeiten und Untersuchungen leitete und die Geschäftsleitung zu Prozessrisiken des Unternehmens sowie zu den finanziellen und reputationsbezogenen Auswirkungen beriet.

Kontakt
Dr. Oliver M. Brupbacher
Kellerhals Carrard
Henric Petri-Strasse 35
4051 Basel
058 200 30 47
oliver.Brupbacher@kellerhals-carrard.ch

Dr. Oliver M. Brupbacher ist Partner bei Kellerhals Carrard. Zuvor war er Senior Litigation Counsel, Head Global Discovery und global produktverantwortlicher Anwalt bei Novartis. Oliver Brupbacher berät und vertritt Parteien in Verfahren vor staatlichen Gerichten und Schiedsgerichten in allen Bereichen des Wirtschaftsrechts sowie in internen und regulatorischen Untersuchungen. Als Teil seiner Tätigkeit befasst er sich regelmässig mit der Prävention und dem Krisenmanagement von Cybersecurity Vorfällen. Darüber hinaus ist er spezialisiert auf Healthcare und Life Sciences, grenzüberschreitende Verfahren, internationale Rechtshilfe sowie Datenschutz und Information Governance. Oliver Brupbacher verbindet fachliche Expertise mit tiefgehender Kenntnis des Gesundheitssektors und der Unternehmenswelt auf allen Ebenen und in nationalen wie internationalen Verhältnissen.