Fraud Newsletter

January 2017

EY
Building a better working world

Fraud Newsletter

How certain are you that your employees are not taking company data with them when they leave?

Despite all that has been done and all the various security measures that have been implemented with regards to preventing data theft, we are still seeing more and more companies falling victim to the phenomenon known as 'insider threat', where data theft, amongst other things, from 'trusted employees' are occurring and having to deal with its' consequences. Recent research shows that the theft of confidential company information by employees is wide spread, with **more than 80 percent of employees who have taken sensitive data when they left.**[1] This is a staggering amount as Intellectual Property (IP) sets your business apart from competitors and is possibly among the most important valuable asset you company possesses. It is surprising that not more is done to prevent this IP theft. Despite all that is undertaken to prevent data theft, many companies are still losing data when employees leave the company.

We've seen one recent case that involved an employee taking with him upon his departure, all the customer data that was then used to set-up an own business. And even more surprising was a recent case involving an employee taking data from their past employer at the request of their new employer. Losing valuable company data causes direct and indirect monetary loss and can also result in damage to brand and reputation. No one is immune to data theft. Over the last few years, companies in every industry sector around the globe have seen their sensitive internal data lost, stolen or leaked to the outside world. However, this newsletter is not about data theft caused by a hack or cybercrime, but addresses instead the simple question of **what about data theft from departing employees?**

1. http://www.darkreading.com/vulnerabilities---threats/survey-when-leaving-company-most-insiders-take-data-they-created/d/d-id/1323677

Dans quelle mesure avez-vous la certitude que vos employés n'emportent pas de données de l'entreprise avec eux lorsqu'ils quittent l'entreprise ?

Malgré tous les efforts déployés dans ce domaine et les différentes mesures de sécurité mises en place pour prévenir le vol de données, un nombre croissant d'entreprises sont victimes du phénomène de « menace interne » (Insider Threat), notamment le vol de données par des employés « de confiance » de l'entreprise, et doivent en gérer les conséquences. Une récente étude montre que le vol d'informations confidentielles internes à l'entreprise par des employés est largement répandu : **plus de 80 % des collaborateurs emportent avec eux des données sensibles lorsqu'ils quittent l'entreprise.**[1] Un chiffre ahurissant, étant donné que la propriété intellectuelle (« PI ») est un moyen de se démarquer de la concurrence et fait probablement partie des actifs les plus importants de votre entreprise. Etonnamment, aucune mesure n'est réellement mise en œuvre pour prévenir ce vol de propriété intellectuelle. En dépit de tous les efforts déployés pour prévenir le vol de données, de nombreuses entreprises continuent de perdre des données lors du départ de leurs employés.

Récemment, un collaborateur a emporté, au moment de son départ, l'intégralité des données client qui ont été ensuite utilisées pour créer une entreprise propre. Autre cas récent encore plus surprenant : celui d'un employé emportant des données de son ancien employeur à la demande du nouveau. La perte de données d'entreprise précieuses entraîne une perte financière directe et indirecte et peut également être dommageable à la marque et à la réputation.

1. http://www.darkreading.com/vulnerabilities---threats/survey-when-leaving-company-most-insiders-take-data-they-created/d/d-id/1323677

Wie sicher sind Sie, dass Ihre Mitarbeitenden keine Unternehmensdaten entwenden, wenn sie das Unternehmen verlassen?

Trotz aller Anstrengungen und aller Sicherheitsmassnahmen, die zur Verhütung von Datendiebstahl umgesetzt wurden, fallen weiterhin immer mehr Unternehmen einem Phänomen zum Opfer, welches man als «Insider-Bedrohung» bezeichnet. Hierbei handelt es sich unter anderem um Datendiebstahl durch «vertrauenswürdige Mitarbeitende», mit dessen Folgen sich die Unternehmen auseinandersetzen müssen. Neueste Studien zeigen, dass der Diebstahl vertraulicher Unternehmensdaten durch Mitarbeitende weit verbreitet ist: **Mehr als 80 Prozent der Mitarbeitenden haben beim Ausscheiden aus einem Unternehmen sensible Daten entwendet.**[1] Diese Zahl ist schwindelerregend, ist es doch das geistige Eigentum das Ihr Unternehmen von seinen Wettbewerbern abhebt, und somit möglicherweise das wertvollste Gut Ihres Unternehmens darstellt. Erstaunlich ist, dass nicht mehr zur Verhinderung des Diebstahls von geistigem Eigentum unternommen wird. Trotz aller Massnahmen zur Vorbeugung von Datendiebstahl verlieren viele Unternehmen noch immer Daten, wenn Mitarbeitende aus dem Unternehmen ausscheiden.

In einem unserer jüngsten Fälle hat ein Mitarbeiter bei seinem Ausscheiden aus dem Unternehmen alle Kundendaten mitgenommen und diese dann zur Gründung seines eigenen Unternehmens verwendet. Noch erstaunlicher ist ein weiterer Fall bei dem ein Mitarbeiter auf Bitten des neuen Arbeitgebers Daten von seinem bisherigen Arbeitgeber entwendete. Der Verlust wertvoller Unternehmensdaten verursacht sowohl direkten als auch indirekten finanziellen Schaden und

1. http://www.darkreading.com/vulnerabilities---threats/survey-when-leaving-company-most-insiders-take-data-they-created/d/d-id/1323677

Data is likely one of your organization's most valuable assets, protecting it and keeping it not only out of the public domain, but also keeping it away from your competitors is of paramount importance. There are numerous reports and statistics on data theft / data breaches. Cyber security is becoming if not already, an increasingly hot topic and on everyone's agenda. However, surprisingly little is done to address the notion of 'insider threat', an example which includes data theft perpetrated by employees leaving the firm. Companies need to address `insider threat' on the next level, by taking a closer look when employees voluntarily or involuntarily leave the firm, and companies need to monitor and investigate when red flags present themselves.

Data Theft Common by Departing Employees

It appears that when leaving a company, employees seem to feel entitled to information they create on the job. Perhaps this is due to more and more employees who are working from remote locations, perhaps even on home computers, rendering the notion of who really owns the data to be quite ambiguous. Additionally, with an increase in mobility in the workforce, many employees don't have a lasting relationship with their employers. Data may be physically or logically removed from the organization either intentionally or unintentionally. Email, cloud storage, flash drives and personal handheld devices are making it easy to carry, transfer and take data outside of the workplace. In today's world where more and more employees are storing their business and customer contacts online in various platforms, some employees may not believe they are doing anything wrong when they take customer lists and other internal company data when they move on to a new job. Some signs of potential data theft by employees are quite obvious after the fact, and some can only be found using digital forensic techniques.

Personne n'est à l'abri du vol de données. Ces dernières années, des entreprises de tous les secteurs d'activité, partout dans le monde, ont été victimes de pertes, de vols ou de fuites de leurs données internes sensibles. Cependant, cette newsletter ne porte pas sur le vol de données lié au piratage ou à la cybercriminalité, mais sur le **vol de données d'employés qui quittent l'entreprise.** Les données font probablement partie des actifs les plus précieux de votre entreprise. Il est donc essentiel de les protéger et de les préserver de tout accès du public et de la concurrence. Il existe de nombreux rapports et statistiques sur le vol / la violation de données. La cybersécurité est un sujet d'une brûlante actualité, qui focalise l'attention de tous. Néanmoins, on constate avec surprise que peu d'efforts sont déployés contre la « menace interne », notamment le vol de données perpétré par des employés qui quittent l'entreprise. Les entreprises se doivent de passer à la vitesse supérieure dans ce domaine en surveillant davantage les collaborateurs qui quittent, volontairement ou involontairement, l'entreprise, en étant attentives aux signaux d'alerte et, le cas échéant, en menant à bien des enquêtes.

Le vol de données, un mal répandu parmi les employés qui quittent l'entreprise

Il apparaît que lorsqu'ils quittent une entreprise, les employés ont l'impression d'avoir des droits sur les informations qu'ils ont générées dans le cadre de leur activité. Ceci est peut-être lié au fait que de plus en plus d'employés travaillent à distance, parfois même sur leurs ordinateurs personnels à domicile, ce qui rend la notion de « propriétaire réel » des données relativement ambiguë. En outre, en raison de la mobilité croissante de la main-d'œuvre, de nombreux employés n'entretiennent pas de relation durable avec leurs employeurs. Les données peuvent être physiquement ou logiquement supprimées de l'entreprise, volontairement ou non. Les e-mails, le stockage en nuage (cloud), les clés USB et

kann zudem die Marke und den Ruf des Unternehmens schädigen. Niemand ist gegen Datendiebstahl gefeit. In den letzten Jahren haben Unternehmen weltweit und branchenübergreifend Datenverlust, Datendiebstahl oder die Weitergabe vertraulicher interner Daten an Dritte erfahren. In diesem Newsletter befassen wir uns allerdings nicht mit Datendiebstahl durch Hacker oder Cyber-Kriminalität, sondern mit der einfachen Frage: **Wie sieht es mit Datendiebstahl durch scheidende Mitarbeitende aus?** Daten sind wahrscheinlich der wertvollste Besitz Ihres Unternehmens. Sie vor Weitergabe an die Öffentlichkeit und an ihre Wettbewerber zu schützen, ist äusserst wichtig. Die Berichte und Statistiken zu Datendiebstahl/ Datenschutzverletzungen sind zahlreich. Cyber-Sicherheit ist ein heisses Thema, das immer drängender wird und mit dem sich jeder befassen sollte. Gegen das Phänomen der «Insider-Bedrohung» – d.h. Datendiebstahl durch ausscheidende Mitarbeitende – wird dagegen erstaunlich wenig unternommen. Unternehmen müssen die «Insider-Bedrohung» auf der nächsten Ebene angehen in dem sie genau hinsehen, wenn Mitarbeitende freiwillig oder unfreiwillig aus dem Unternehmen ausscheiden. Treten hier Alarmsignale auf, sind Überwachung und Untersuchung erforderlich.

Datendiebstahl durch ausscheidende Mitarbeitende

Anscheinend haben Mitarbeiter, die ein Unternehmen verlassen, das Gefühl, Anspruch auf die Daten zu haben, die sie im Rahmen ihrer Tätigkeit erstellt haben. Dies liegt vielleicht daran, dass immer mehr Mitarbeitende ausserhalb des Unternehmens arbeiten, ggf. am heimischen Computer, und dadurch eine unklare Auffassung über das Eigentum der Daten besteht. Hinzu kommt, dass mit zunehmender Mobilität des Personals viele Mitarbeitende keine dauerhafte Beziehung mehr zu ihren Arbeitgebern aufbauen. Daten können zudem physisch

Common indicators that data theft may have occurred or that data is at risk include:

- Employee printing large quantities of documents or copying/scanning of specific documents
- Employee using the internal systems at odd hours of the day (after typical business hours or while on leave)
- Employee copying data to USB drives or to cloud platforms
- Accessing & sending personal email from company devices, particularly email with attachments
- Asking co-workers to provide them with confidential information outside of their responsibility

Typically, these behaviors take place shortly before the employee resigns or leaves.

So what can be done?

It all starts with hiring the right people. As everyone knows, getting the right people to work for you will make or break your business. Being offered confidential information from a candidate during a job interview or within the first weeks after hiring can be considered a definite red flag that you may have just become involved in a data theft incident – and should also serve as a warning that this person will most probably do the same thing when they leave your company.

With everyone clear on theft being wrong and that stealing laptops or office furniture is illegal, why do so many companies disregard the threat of data theft when employees leave the firm? **Few firms are investing the time and resources** to assess and implement policies, procedures & technical monitoring solutions (Data Loss Prevention - DLPs) to address the risks found by departing employees. Employers should include members of the management team, human resources and information technology professionals to develop and implement an effective confidential information security plan – whilst also taking into account local labour and employment regulations and laws.

les appareils personnels portatifs facilitent le transport, le transfert et l'acheminement de données à l'extérieur du lieu de travail. Dans le monde actuel, où les employés sont de plus en plus nombreux à stocker leurs contacts professionnels et clients en ligne sur différentes plates-formes, certains d'entre eux peuvent ne pas avoir conscience de mal faire quand ils emportent des listes de clients et autres données internes de l'entreprise quand ils changent d'employeur. Certains signes de vol de données potentiel par des employés sont parfaitement évidents a posteriori, et d'autres ne sont décelables qu'à l'appui de techniques d'enquêtes numériques. Les indicateurs courants du vol ou du risque de vol de données par un employé sont les suivants :

- Impression de grandes quantités de documents ou copie/numérisation de documents spécifiques
- Utilisation des systèmes internes à des horaires inhabituels (en dehors des heures ouvrables classiques ou au moment de la sortie des bureaux)
- Copie de données sur des clés USB ou sur des plates-formes de cloud
- Accès et envoi d'e-mails personnels, contenant notamment des pièces jointes, depuis des appareils de l'entreprise
- Demande à des collègues d'informations confidentielles sortant du cadre de leurs responsabilités

En règle générale, ces comportements se produisent juste avant la démission ou le départ de l'employé.

Quelles sont les mesures à mettre en œuvre ?

Il faut d'abord recruter les bonnes personnes. Comme chacun sait, ce sont les collaborateurs qui font l'échec ou le succès d'une entreprise. La fourniture d'informations confidentielles par un candidat pendant un entretien d'embauche ou dans les premières semaines après son recrutement peut être considérée comme un indice clair d'un incident potentiel lié à un vol de données – et doit également vous alerter

oder logisch aus dem Unternehmen entnommen werden – beabsichtigt oder unbeabsichtigt. E-Mail, Cloud-Speicherung, Speichersticks und persönliche mobile Geräte machen es einfach, Daten vom Arbeitsplatz zu entwenden bzw. zu übertragen. In der heutigen Welt, in der immer mehr Mitarbeitende ihre Geschäfts- und Kundenkontakte online auf diversen Plattformen speichern, ist es durchaus denkbar, dass manchem Mitarbeitenden gar nicht bewusst ist, dass er etwas Falsches tut, wenn er bei einem Jobwechsel Kundenlisten oder andere interne Unternehmensdaten mitnimmt. In manchen Fällen gibt es ganz offensichtliche Zeichen für einen potenziellen Datendiebstahl, in anderen ist ein solcher nur mit Hilfe digitaler Kriminaltechnik festzustellen. Die häufigsten Anzeichen für einen möglichen Datendiebstahl oder eine entsprechende Gefahr sind:

- Mitarbeitende drucken grosse Mengen an Dokumenten aus oder kopieren/scannen bestimmte Dokumente
- Mitarbeitende nutzen die internen Systeme zu ungewöhnlichen Tageszeiten (ausserhalb der normalen Arbeitszeiten oder im Urlaub)
- Mitarbeitende kopieren Daten auf USB-Speicher oder Cloud-Plattformen
- Über den Firmencomputer wird auf persönliche E-Mails zugegriffen bzw. werden persönliche E-Mails versendet, insbesondere E-Mails mit Anhängen
- Kolleginnen oder Kollegen werden um vertrauliche Informationen ausserhalb ihres Verantwortungsbereichs gebeten

In der Regel treten diese Verhaltensweisen kurz vor der Kündigung oder dem Ausscheiden des Mitarbeitenden auf.

Was kann man tun?

Es beginnt damit, die richtigen Leute einzustellen. Bekanntlich steht und fällt der Erfolg Ihres Unternehmens damit, dass die richtigen Leute für Sie arbeiten. Wenn ein Kandidat in einem Vorstellungsgespräch oder in den ersten Wochen nach seiner

Intentional security breaches by employees are extremely difficult to prevent, but a few suggestions that can help:

- Conduct a data assessment to understand which data you need to protect most, where it is stored, what is currently implemented to tackle this issue and what further measures could be adopted
- Determine and assess the need of a dedicated Data Loss Prevention solution, enabling the real time monitoring, detection and blocking of sensitive/ confidential data while in use, in motion, as well as at rest
- When logged onto the company network, apply internet use restrictions on services (for example, email & cloud storage providers) not needed for working purposes and have policies in place to address the use of personal devices at work
- Include a training in the exit interview to make employees aware of regulations regarding IP/data theft and inform them that the company would take legal action if theft was suspected – and have the departing employee sign an acknowledgement form

Unfortunately, no matter how diligent the effort, no data protection policies or systems can prevent all risk of employee information theft. Therefore, when theft is suspected, the following is suggested:

- Quickly assess and determine what happened, what data has been exposed and what the magnitude of the potential risk is
- Contact your legal department or outside legal counsel
- Take steps to forensically collect and preserve evidence: devices (like laptops and phones), data locations (like network shares), and, perhaps most importantly, available access records and log files
- Contact a company experienced in data risk analysis, forensic investigation & mitigation solutions

sur le fait que cette personne risque fort de faire la même chose lorsqu'elle quittera votre entreprise.

Il est de notoriété publique que le vol est répréhensible et que le fait de dérober des ordinateurs portables ou du matériel de bureau est illégal. Alors pourquoi les entreprises sont-elles aussi nombreuses à négliger la menace liée au vol de données par des collaborateurs qui quittent l'entreprise ? **Peu d'entre elles consacrent le temps et les ressources nécessaires** à l'évaluation et à la mise en œuvre de politiques, de procédures et de solutions de surveillance technique dans le domaine de la prévention de la perte de données (DLP) pour remédier aux risques dans ce domaine. Toute entreprise devrait regrouper des membres de l'équipe de direction et des ressources humaines ainsi que des professionnels des technologies de l'information pour développer et mettre en œuvre un plan de sécurisation efficace des informations confidentielles, dans le respect des lois et règlements locaux en vigueur en matière d'emploi et de droit du travail. Les infractions volontaires à la sécurité de la part d'employés sont extrêmement difficiles à prévenir, mais voici quelques conseils :

- Réalisez une analyse des données pour comprendre quelles données vous avez besoin de protéger en priorité, où celles-ci sont stockées, les mesures actuellement mises en œuvre dans ce domaine et les autres mesures qui pourraient être adoptées
- Déterminez et évaluez la nécessité d'une solution de prévention de la perte de données dédiée permettant la surveillance, la détection et le blocage en temps réel des données sensibles/ confidentielles en cours d'utilisation, en circulation ou dormantes
- Dans le cadre de la connexion au réseau d'entreprise, appliquez des restrictions à l'utilisation de services sur Internet (par exemple, fournisseurs de messageries électroniques et de stockage en ligne) non nécessaires à l'usage professionnel

Einstellung vertrauliche Informationen anbietet, ist dies definitiv als Alarmsignal zu werten, gerade in einen Datendiebstahl verwickelt zu werden – und es sollte Ihnen eine Warnung sein, dass diese Person wahrscheinlich dasselbe tun wird, wenn sie Ihr Unternehmen verlässt.

Wenn aber doch jeder weiss, dass Diebstahl falsch und das Stehlen von Laptops oder Büromöbeln eine Straftat ist, warum ignorieren so viele Unternehmen die Gefahr des Datendiebstahls beim Ausscheiden von Mitarbeitenden aus dem Unternehmen? **Nur wenige Unternehmen investieren Zeit und Ressourcen**, um zur Verhütung von Datenverlusten Richtlinien, Verfahrensanweisungen und technische Überwachungslösungen zu prüfen und einzuführen (Data Loss Prevention – DLPs) und so die von ausscheidenden Mitarbeitenden ausgehenden Risiken zu mindern. Arbeitgeber sollten gemeinsam mit Mitgliedern des Management-Teams, der Personalabteilung und IT-Spezialisten einen effektiven Sicherheitsplan für vertrauliche Informationen entwickeln und dabei die lokalen arbeitsrechtlichen Vorschriften und Bestimmungen berücksichtigen. Absichtliche Sicherheitsverletzungen durch Mitarbeitende sind äusserst schwer zu verhindern, aber folgende Massnahmen können hilfreich sein:

- Klassifizierung der Daten, um festzustellen, welche Daten am meisten geschützt werden müssen, wo diese gespeichert werden, welche Vorkehrungen bisher getroffen wurden, um dem Problem des Datendiebstahls zu begegnen, und welche weiteren Massnahmen ergriffen werden könnten
- Feststellung und Beurteilung des Bedarfs einer gezielten «Data Loss Prevention»-Lösung, die eine Überwachung, Identifizierung und Sperrung sensibler/vertraulicher Daten in Echtzeit ermöglicht, während diese in Geschäftsprozessen verarbeitet (data in use), übertragen (data in motion) oder gespeichert werden (data in rest)

The concept of 'Insider Threat' is a very real threat to all businesses, in all sectors and of all sizes. But by pro-actively taking the necessary steps, business are limiting the risks that they may face by departing or malicious employees. Whilst trusting your employees is important, equally important is to have the necessary controls and measures in place to verify this trust. The corporate culture should reflect the **"trust but verify"** mantra, with your data security protocols and relevant policies adapted accordingly. **Being transparent to employees about their organization's monitoring of their systems and potentially taking a deeper look into their activity when they are leaving the firm is also a good if not best deterrent possible to preventing the intentional or unintentional incident of data theft.** These easy preventative measures can minimize the amounts of data loss incidents and can therefore reduce the cost & resources needed for any civil litigation and investigation needed when faced with your valuable data leaving the company along with your resigning employees.

et instaurez des politiques de gestion de l'utilisation des appareils personnels au travail

- Incluez une formation à l'entretien de départ pour sensibiliser les collaborateurs aux dispositions relatives au vol de données/PI et les informer qu'ils risquent des poursuites judiciaires en cas de vol; faites signer un formulaire d'attestation aux employés qui quittent l'entreprise

Malheureusement, aussi rigoureux que soient les efforts déployés, aucun système ou politique de protection des données ne peut prévenir entièrement le risque de vol d'informations par les collaborateurs. Par conséquent, en cas de suspicion de vol, la procédure conseillée est la suivante :

- Analysez et déterminez rapidement le déroulement des faits, les données qui ont été exposées et l'ampleur du risque potentiel
- Contactez votre service juridique ou votre conseiller juridique externe
- Prenez des mesures pour collecter et conserver des preuves judiciaires: appareils (ordinateurs portables, téléphones…), emplacements des données (partages de réseaux) et enfin et surtout, enregistrements des accès et fichiers-journaux disponibles
- Contactez une entreprise spécialisée dans l'analyse des risques liés aux données et dans les solutions d'atténuation et d'enquête criminelle

Le concept de « menace interne » est une menace bien réelle pour les entreprises de toute taille et de tout secteur. Mais en prenant les mesures nécessaires de manière proactive, les entreprises limitent les risques auxquels des collaborateurs malveillants ou qui quittent l'entreprise risqueraient de les exposer. Il est important de faire confiance à vos employés, mais il l'est tout autant d'instaurer les contrôles et les mesures requis pour vérifier cette confiance. La devise **« faire confiance, mais vérifier »** doit être ancrée dans la culture d'entreprise, et vos protocoles de sécurité des données ainsi que les politiques pertinentes, adaptées de manière correspondante. **Communiquer en toute transparence auprès des**

- Anwendung von Internet-Nutzungsbeschränkungen für die im Unternehmensnetzwerk eingeloggten Benutzer für bestimmte Dienste (wie E-Mail oder Cloud-Speicheranbieter), die nicht für Arbeitszwecke benötigt werden, und Bereitstellung von Richtlinien über die Nutzung privater Geräte am Arbeitsplatz
- Aufnahme einer Belehrung in das Kündigungsgespräch, in der die Mitarbeitenden auf Bestimmungen zum Diebstahl von geistigem Eigentum und Daten hingewiesen werden, und die Mitteilung, dass das Unternehmen im Verdachtsfall rechtliche Schritte einleiten wird – anschliessend wird der scheidende Mitarbeiter aufgefordert, eine entsprechende Anerkenntniserklärung zu unterschreiben

Leider kann keine Datenschutzrichtlinie und kein System die Gefahr des Datendiebstahls durch Mitarbeitende gänzlich eliminieren – mögen die entsprechenden Massnahmen auch noch so umfangreich sein. Für den Fall eines Verdachts auf Diebstahl wird daher Folgendes empfohlen:

- Prüfen und ermitteln Sie rasch, was geschehen ist, welche Daten betroffen sein können und wie hoch das potenzielle Risiko ist
- Wenden Sie sich an Ihre Rechtsabteilung bzw. Ihren externen Rechtsberater
- Leiten Sie Schritte ein, um Beweise zu sammeln und zu sichern: Geräte (wie Laptops oder Telefone), Datenspeicherorte (wie gemeinsame Bereiche im Netzwerk) und – vielleicht am wichtigsten – verfügbarer Zugang zu Aufzeichnungen und Protokolldateien
- Kontaktieren Sie ein Unternehmen, das Erfahrung in der Datenrisikoanalyse hat und Lösungen für kriminaltechnische Untersuchungen und Schadensbegrenzung anbietet

Das Thema «Insider-Bedrohung» ist eine sehr reale Bedrohung für Unternehmen jeder Branche und jeder Grösse. Unternehmen können jedoch die Risiken, die ihnen durch ausscheidende oder böswillige Mitarbeitende entstehen,

employés au sujet de la surveillance de leurs systèmes et analyser de manière détaillée leur activité lorsqu'ils s'apprêtent à quitter l'entreprise sont des facteurs de dissuasion efficaces, sinon optimaux, pour prévenir l'incident volontaire ou involontaire lié au vol de données. Ces mesures préventives simples peuvent contribuer à réduire le nombre d'incidents liés à la perte de données et, partant, le coût et les ressources associés à toute enquête et procédure civile en cas de vol de vos données sensibles par des collaborateurs qui quittent l'entreprise.

proaktiv durch Einleitung der erforderlichen Massnahmen begrenzen. Es ist wichtig, dass Sie Ihren Mitarbeitenden vertrauen. Genauso wichtig ist es aber auch, über die erforderlichen Kontrollen und Massnahmen zu verfügen, um dieses Vertrauen zu überprüfen. Die Devise **«Vertrauen ist gut, Kontrolle ist besser»** sollte sich in Ihrer Unternehmenskultur widerspiegeln, und Sie sollten Ihre Datensicherheitsprotokolle und -richtlinien entsprechend anpassen. **Seien Sie Ihren Mitarbeitenden gegenüber transparent, was die Überwachung der Systeme durch das Unternehmen betrifft. Und nehmen Sie die Aktivitäten eines scheidenden Mitarbeitenden unter Umständen genauer unter die Lupe – das ist eine gute, wenn nicht die beste Abschreckung, mit der sich ein absichtlicher oder unabsichtlicher Datendiebstahl verhindern lässt.** Diese leicht umzusetzenden Präventivmassnahmen können die Datenverlustvorfälle minimieren und damit die Kosten und Ressourcen reduzieren, die für zivilrechtliche Streitigkeiten und Untersuchungen aufgewendet werden müssen, wenn wertvolle Daten gemeinsam mit scheidenden Mitarbeitenden das Unternehmen verlassen.

Contacts

Michael Faske
Partner, Head of Fraud Investigation & Dispute Services Switzerland
+41 58 286 3292
michael.faske@ch.ey.com

Paul Wang
Partner, Regional Head Swiss Romandie of Fraud Investigation & Dispute Services
+41 58 286 5826
paul.wang@ch.ey.com

Matthias Grossenbacher
Executive Director, Fraud Investigation & Dispute Services Schweiz
+41 58 286 4338
matthias.grossenbacher@ch.ey.com

EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

ED None

ey.com