KPMG

cutting through complexity

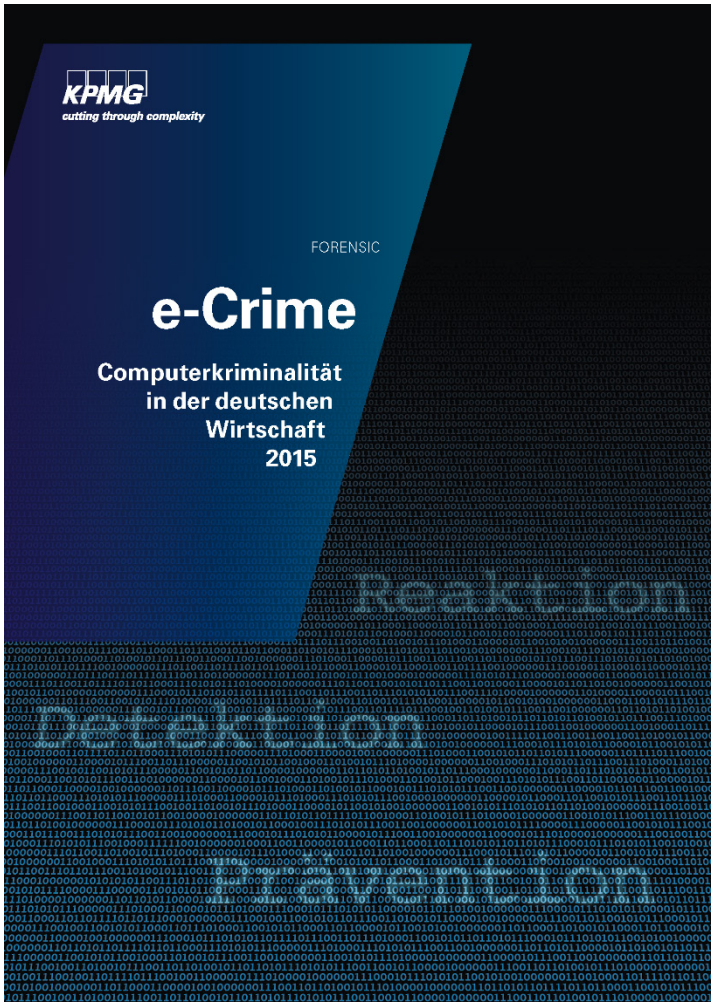
Cyber Insurance Service für Cyber-Versicherungen und Versicherungsnehmer

ALLES IM BLICK

FORENSIC. EINEN SPRUNG VORAUS.

www.kpmg.de/forensic

Cyber-Versicherungen können die Reaktionsfähigkeit von Unternehmen auf Cyber-Vorfälle sinnvoll ergänzen



Von e-Crime betroffen

2013 26 %

2015 40 %

e-Crime wird komplexer
ist schwerer aufzuspüren

2015 95 %

Keine Versäumnisse
bei der Reaktion

2013 99 %

2015 75 %

Risiko e-Crime ist
hoch/sehr hoch

2013 82 %

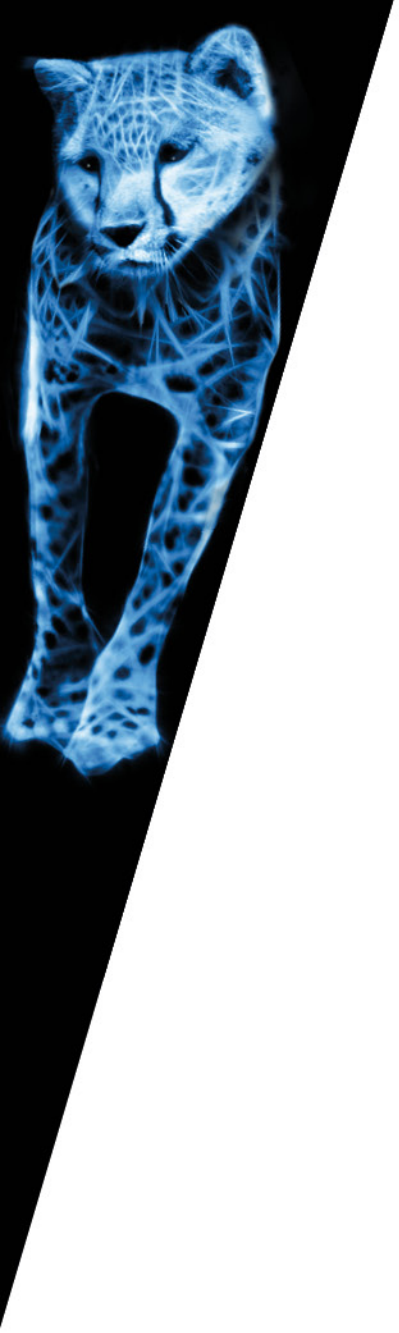
2015 89 %

Eigenes Risiko ist
hoch/sehr hoch

2013 34 %

2015 39 %

https://www.kpmg.com/DE/de/Documents/e-crime-studie-2015.pdf



Wie kann KPMG Cyber-Versicherungen und Versicherungsnehmer unterstützen?

- KPMG verfügt über langjährige und weltweite Erfahrungen in der Reaktion, Aufklärung und Aufarbeitung von Cyber-Vorfällen in Unternehmen aller Branchen.
- Zudem unterstützen wir Unternehmen dabei, sich risikoorientiert vor Angriffen zu schützen und im Ernstfall effizient und angemessen zu reagieren.
- Wissen und Erfahrungswerte haben wir in eine Methodik zur Beurteilung der Risikodisposition und Reaktionsfähigkeit von Unternehmen auf Cyber-Vorfälle überführt – KPMG CyberSAFE.

- Wir beurteilen die Praxistauglichkeit von Cyber-Versicherungen.
- Wir bereiten Underwriter gezielt auf Risikodialoge vor.
- Wir minimieren den Aufwand einer Risikobeurteilung von potenziellen Versicherungsnehmern.
- Unsere professionelle Unterstützung bei der Reaktion im Ernstfall ergänzt die Leistung von Cyber-Versicherungen und senkt die Kosten.

Dialog zur Praxistauglichkeit von Cyber-Versicherungen

Versicherer Schätzen unseren Dialog beim Design und der Weiterentwicklung von Cyber-Versicherungen. Unsere Expertise unterstützt Sie bei folgenden Fragestellungen:

- Was sollte eine Cyber-Versicherung abdecken?
  - Welche Szenarien sind abgedeckt?
  - Welche Schäden sind abgedeckt?
  - Wie können Schäden, Reaktionskosten und Selbstbeteiligung abgegrenzt werden?
- Wie kann die Risikodisposition des Versicherungsnehmers beurteilt werden?
  - Was ist ein sinnvolle Aufwand für eine Informationserhebung in Bezug auf den konkretem Nutzen zur Bestimmung von Deckungssumme und Versicherungsprämie?
  - Wie kann Vergleichbarkeit und Reproduzierbarkeit ermöglicht werden?
- Was muss im Schadensfall passieren?
  - Wie kann eine standardisierte und effiziente Reaktion ermöglicht werden?
  - Wie kann die Qualität des Reportings und der Schadensbemessung geprüft werden?

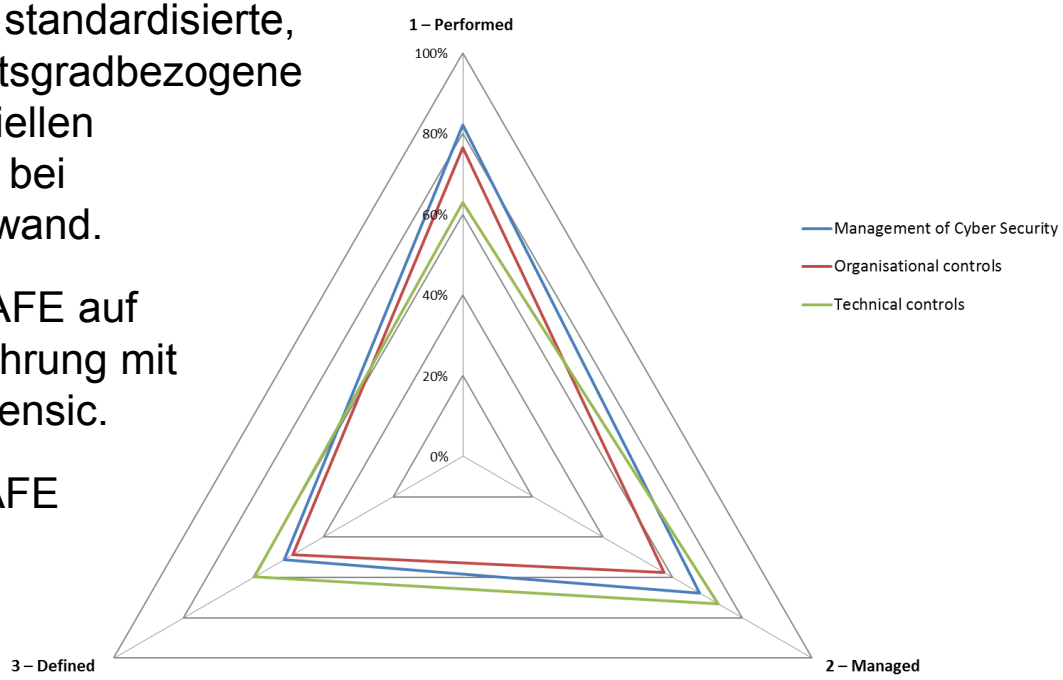
KPMG CyberSAFE

Eine vollständige Analyse der Risikodisposition und Reaktionsfähigkeit von Unternehmen auf Cyber-Vorfälle (Cyber Security) eines Unternehmens kann ein langer, aufwändiger Prozess sein.
Um Ihnen schnell einen Überblick zur Risikobeurteilung und Entscheidungsfindung zu ermöglichen,
hat KPMG CyberSAFE entwickelt.

CyberSAFE liefert eine standardisierte, gründliche und fähigkeitsgradbezogene Beurteilung von potenziellen Versicherungsnehmern bei geringstmöglichem Aufwand.

Wir setzen mit CyberSAFE auf unsere langjährige Erfahrung mit Cyber Security und Forensic.

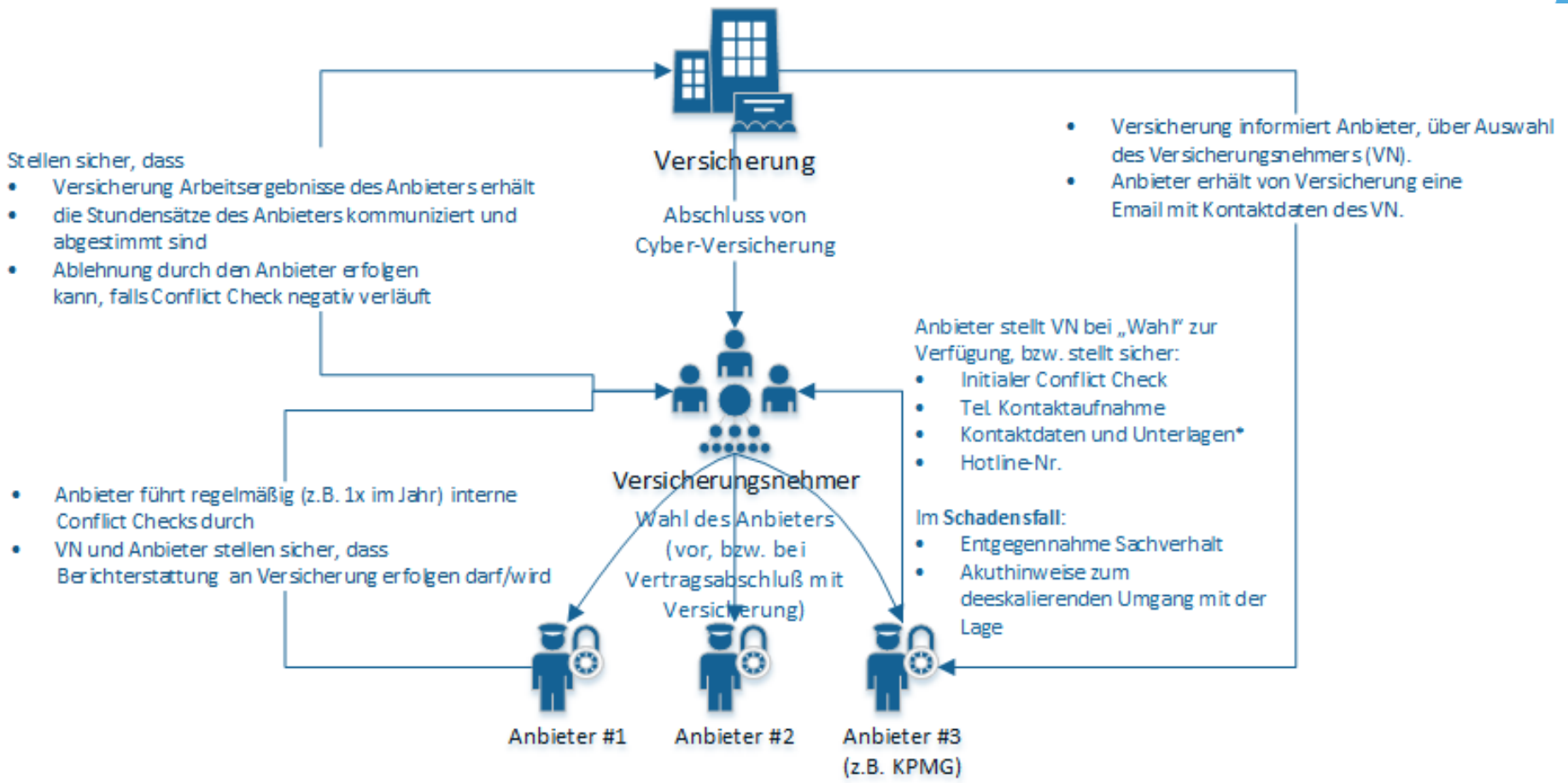
www.kpmg.de/CyberSAFE



KPMG CyberSAFE

- CyberSAFE ist eine webbasierte Anwendung, welche von KPMG entwickelt und betrieben wird. Sie erfüllt sehr hohe Ansprüche an Vertraulichkeit, Integrität und Verfügbarkeit der erfassten Informationen.
- Für die Umfeldanalyse und Recherche zur Schadenshistorie setzen wir neben einer Selbstauskunft auf ein globales Rechercheteam mit einem spezialisierten Portfolio öffentlich zugänglicher Quellen.
- Zudem arbeiten wir mit Better Practice-Anforderungen international anerkannter Standards (ISO 27001:2013/NIST/SANS 20 Critical Security Controls etc.).
- Zusätzlich berücksichtigen wir Umfeldanalysen und Schadenshistorien.
- Außerdem liefern wir Benchmarkinformationen und ermöglichen den Vergleich in der Peer Group.
- Mit einem qualitativen Überblick über die Fähigkeiten und Defizite eines potenziellen Versicherungsnehmers geben wir maßgeschneiderte Handlungsempfehlungen und senken somit die möglichen Kosten von Cyber-Vorfällen proaktiv.

Exemplarischer Prozess zur unabhängigen Beauftragung von KPMG für die Reaktion und Aufklärung im Ernstfall



* Unterlagen umfassen schriftliche Bestätigung zur Mandatierung inkl. Honorarstaffel, Standardset an generischen Erstinfos (u.a. Empfehlungen zur Ausarbeitung eines Basis-Krisenplans), Checkliste mit Erstmaßnahmen im Krisenfall

KPMG verfügt über eine globale Incident Response-Methodik

- Aktuell verfügt KPMG über weltweit 39 Forensic-akkreditierte Praxen mit 3.045 Forensic-Mitarbeitern – mehr als 500 Mitarbeiter mit der Spezialisierung auf Forensic Technology.
- Wir können bei unserer internationalen Tätigkeit auf Büros in 140 Ländern zurückgreifen. Damit sind wir bestens aufgestellt, um Versicherungsnehmer an den Unternehmenssitzen, Orten der Geschäftserbringung oder an den Standorten involvierter Geschäftspartner kurzfristig zu unterstützen.
- Bei Verdacht auf einen Cyber-Vorfall können uns Versicherungsnehmer über einen 24/7-Notruf kontaktieren: 0180 KPMG FOR* (+49 1805 764 367*)
- Versicherungsnehmern mit einem Incident Response-Rahmenvertrag bieten wir eine individuelle Hotline mit garantierten Reaktionszeiten.

* Telefonkosten: Festnetz 14 ct/min, Mobilfunknetze 42 ct/min

KPMG Incident Response-Methodik im Detail

1 Prepare and Train

- Assessment der aktuellen Fähigkeiten, um auf Sicherheitsvorfälle zu reagieren
- Bestimmung von Rollen, Verantwortlichkeiten und Points of Contact
- Definition der Anforderungen an interne und externe Krisenreaktion
- Training für Key Roles und Geschäftsführung (Notfallübung)
- Definierte Kontakte oder Rahmenverträge für zusätzliche Ressourcen

2 Initiate

- Beurteilung von technischen Alerts, Systemauffälligkeiten oder Störungen
- Bewertung von persönlich gemeldeten Auffälligkeiten
- Erste Erkennung von Zusammenhängen
- Bewertung des Gefahrenpotentials
- Information der Key Roles
- Vorbereitung interner und externer Krisenkommunikation
- Reaktionsplanung

3 Investigate

- Identifizierung kritischer Systeme und Netzwerke
- Risikobeurteilung
- Sicherung von Beweisdaten
- Individuelle Analyse von Beweisdaten zur Ermittlung des Schadensausmaß
- Ursachenanalyse
- Informationsmaßnahmen, sofern personenbezogene Daten betroffen sind
- Validierung technischer Indizien über forensische Interviews

KPMG Incident Response-Methodik im Detail

4 Contain and Recover

- Identifizierung von Schwachstellen und Gefahren
- Isolierung kompromittierter Syteme
- Priorisierte Beseitigung von Schwachstellen
- Wiederherstellung von sicheren Systemzuständen
- Begleitung von BCM-Maßnahmen
- Testing der Systemsicher-heit

5 Report and Monitor

- Abschließendes Reporting
- Präsentation der Ergebnisse gegenüber Dritten
- Moderation von Debriefings und Incident Closings
- Bestimmung und Priorisierung von technischen und organisatorischen Folgemaßnahmen
- Monitoring kritischer Systeme

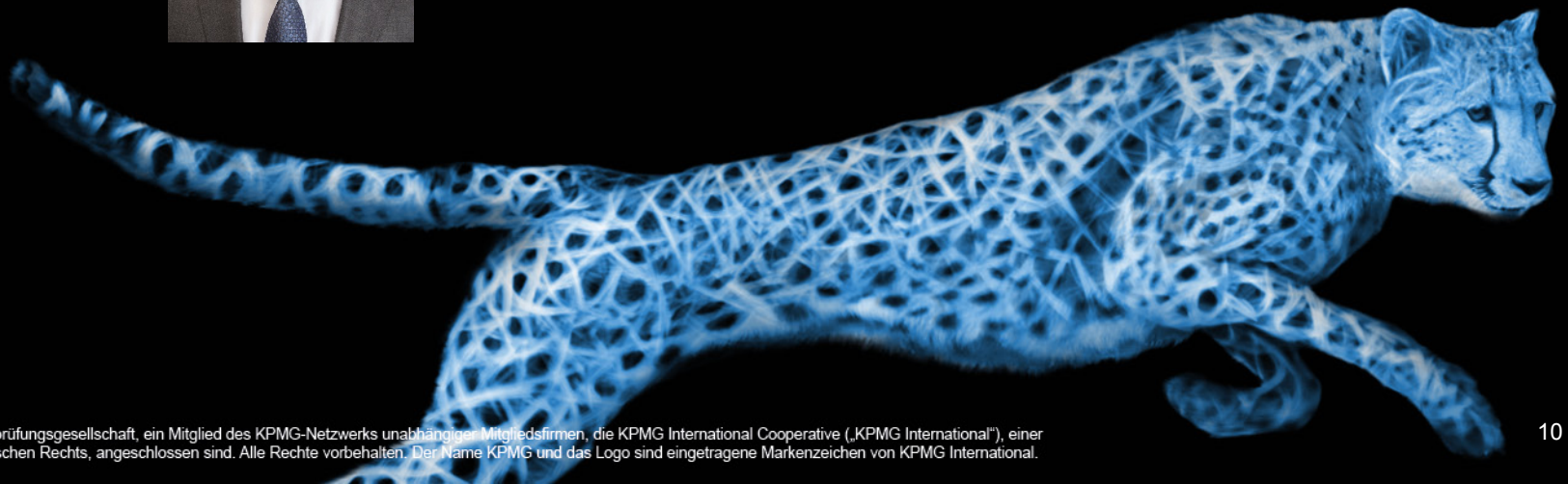
6 Post Incident Review

- Betrachtung der Effektivität von Prävention und Reaktion
- Identifizierung von Abweichungen zw. Vorgaben und Praxis
- Adjustierung der Risikoausrichtung
- Individuelle Optimierungsmaßnahmen
- Begleitung von Remediations

Ihre Ansprechpartner:

Alexander Geschonneck
Partner
Forensic
Klingelhöferstr. 18, 10785 Berlin
ageschonneck@kpmg.com
M +49 174 3201475

Thomas Fritzsche
Senior Manager
Forensic
Klingelhöferstr. 18, 10785 Berlin
tfritzsche@kpmg.com
M +49 173 5600557



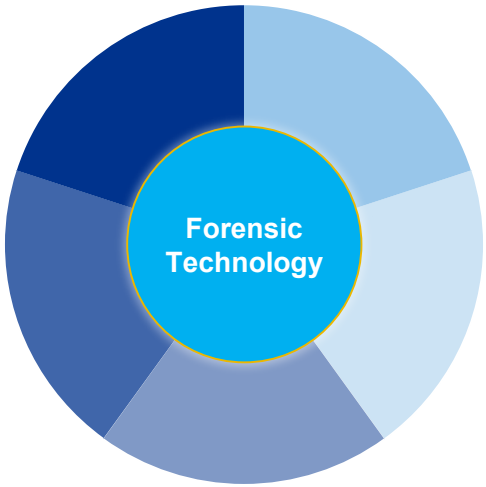
Leistungsspektrum Forensic Technology im Überblick

Incident Response and Cybercrime Investigation

Unterstützung bei der Erstreaktion- und -beurteilung, Eindämmung, Beweis-sicherung, Analyse und gerichtsfesten Aufbereitung unterschiedlicher Arten von informations- bzw. datenbezogenen Sicherheitsvorfällen.

Digital Evidence Recovery

Gerichtsverwertbare Sicherung digitaler Datenbestände. Soweit möglich werden nicht mehr direkt ansprechbare Daten wiederhergestellt, häufig ein unverzichtbares Element bei der Aufklärung wirtschaftskrimineller Handlungen.



Incident Readiness & Litigation Readiness

Unterstützung bei der Optimierung des Zusammenspiels von technologischen, organisatorischen und datenschutz-rechtlichen Herausforderungen im Zusammenhang mit Cyber Security Incidents und der Beweisführung anhand großer Datenmengen.

Forensic Data Analytics

Die Analyse umfangreicher Unternehmensdaten dient der Entdeckung von Schwachstellen in Kontrollsystemen sowie der Aufdeckung von unternehmensschädigenden Handlungen durch interne oder externe Personen oder Organisationen.

Evidence and Discovery Management

Die Bereitstellung digitaler Beweise und anderer Informationen durch zentral kontrollierte Portalsysteme mit umfassenden Such- und Analysesystemen.