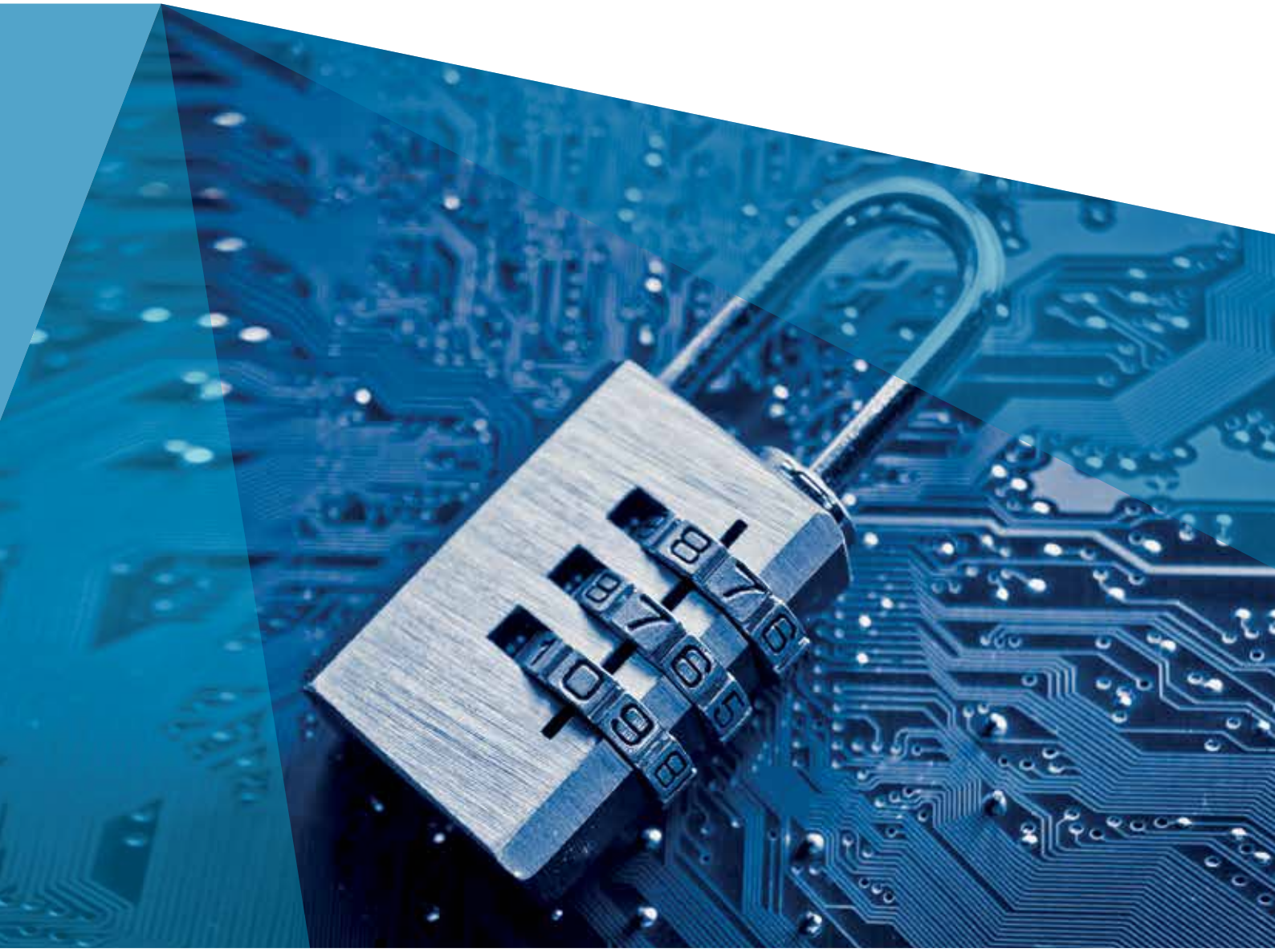
OLIVER WYMAN

CYBER-ATTACKEN KEINE CHANCE GEBEN

WIE UNTERNEHMEN UMFASSENDE INFORMATIONSSICHERHEIT UMSETZEN KÖNNEN



CYBER-ATTACKEN KEINE CHANCE GEBEN

Cyber-Sicherheit und Informationsschutz werden für Unternehmen aller Branchen weltweit zur zentralen Herausforderung. Ob Datendiebstahl oder -fälschung, ob Computersabotage oder Cyber-Spionage, ob unsachgemäßer Umgang mit Unternehmensinformationen durch Mitarbeiter, Lieferanten oder andere Geschäftspartner: Cyber-Kriminalität nimmt immer mehr und immer neue Formen an, ist aber nur ein Teil des Problems. Sich auf das bestehende Corporate Risk Management oder die Kompetenz der IT-Abteilung zu verlassen, reicht bei Weitem nicht aus. Wirkungsvolle Informationssicherheit ist vielmehr Aufgabe des gesamten Unternehmens und gehört auf die Vorstandsagenda. Die Anforderungen sind mehrdimensional – entsprechend muss die Risikobewertung einem ganzheitlichen Ansatz folgen. Oliver Wyman hat Schlüsselkriterien identifiziert, die erfolgsentscheidend für ein nachhaltiges Information Security Management sind.

Die Abhängigkeit von Informationstechnologie und Internet ist für Unternehmen weltweit und über alle Branchen hinweg immens. Im „Global Risks"-Report 2014 des World Economic Forum[1] rangiert der Zusammenbruch der grundlegenden Informationsinfrastruktur auf dem fünften Platz der Risiken mit den potenziell größten Auswirkungen für die Weltwirtschaft. Auf Rang fünf der weltweit wahrscheinlichsten Risiken wiederum finden sich im gleichen Report Cyber-Attacken. Tatsächlich zählt Cyber-Kriminalität längst zu den zentralen Bedrohungen für Unternehmen.

Gerade Hightech-Nationen wie Deutschland oder USA sind massives Ziel von Cyber-Angriffen, die noch dazu immer aggressiver und raffinierter werden. Laut Center for Strategic and International Studies belief sich allein in Deutschland der Schaden durch Cyber-Kriminalität 2013 auf 43 Milliarden Euro, weltweit waren es bis zu 575 Milliarden US-Dollar. Seit 2010 wächst die Zahl registrierter Cyber-Attacken weltweit um mehr als 20 Prozent pro Jahr. Bei Weitem nicht alle Angriffe werden bemerkt oder von Unternehmen gemeldet.

VIELSCHICHTIGES THEMA

In vielen Unternehmen wächst zunehmend das Bewusstsein, dass Cyber-Kriminalität eine ernsthafte Bedrohung ist und sogar existenzgefährdende Ausmaße annehmen kann. Noch wird dieses Thema aber zu fragmentiert behandelt. Bei der Betrachtung der Risiken stehen vornehmlich Hacker-Aktivitäten im Vordergrund. Daher erschöpfen sich Abwehrmaßnahmen häufig in der Anpassung der Firewall in der IT. Doch Informationssicherheit ist weitaus vielschichtiger.

Umfassender Schutz von Unternehmensdaten und -werten vor dem Zugriff Unberechtigter macht es erforderlich, mehrere Dimensionen von Bedrohungsszenarien in Erwägung zu ziehen, die externer wie interner Natur sein können. Berücksichtigt werden muss darüber hinaus die zunehmende digitale Transformation. So sehr die Digitalisierung wichtiger Treiber für Wachstum ist, so sehr erhöht sie die Anfälligkeit der Unternehmen für Cyber-Kriminalität.

1 Der Global Risks-Report wird jährlich vom World Economic Forum in Zusammenarbeit mit Marsh & McLennan Companies und weiteren Partnern erstellt. Die Studienergebnisse des Global Risks-Report 2014 beruhen auf einer Befragung von über 700 Experten und beleuchten 31 Risiken mit weltweiter Bedeutung für das nächste Jahrzehnt.

BEISPIELE FÜR BEDROHUNGSARTEN

SABOTAGE UND TERRORISMUS

- Ziel: maximaler Schaden
- Angreifer versucht nicht unbedingt, sich zu tarnen
- Wunsch nach starker Aufmerksamkeit der Öffentlichkeit

SPIONAGE UND KRIMINALITÄT

- Ziel: persönliche Bereicherung oder Vorteilsschaffung
- Täter konzentriert sich darauf, nicht oder so spät wie möglich entdeckt zu werden
- Verfügbarkeit möglicherweise signifikanter finanzieller und technischer Ressourcen

OPERATIVE RISIKEN

- Indirektes Risiko durch den Verlust von Daten oder entsprechende Schäden (z.B. finanzieller Schaden, Wettbewerbsnachteil, Imageschaden)
- Häufig durch eigene Mitarbeiter oder externe Partner verursacht
- Eher ein opportunistisches Risiko – kein absichtliches Ausnutzen von Schwachstellen

WEITREICHENDE SCHÄDEN

Mehrdimensional ist auch das Ausmaß der Schäden: Imageverlust durch Datenlecks, finanzielle Einbußen durch Produktionsstillstand oder Diebstahl von Geschäftsgeheimnissen, operative Einschränkungen durch Manipulation von technischen Geräten. Betroffen sind nicht nur die Unternehmen. Bei Verstößen und nachweisbaren Sicherheitsmängeln können Vorstände und Führungskräfte zur Verantwortung gezogen und in die Pflicht genommen werden. In einer aktuellen Studie unserer Schwestergesellschaft Marsh nennen Risikomanager großer Unternehmen dementsprechend vor allem den Missbrauch von Kundeninformationen, den Verlust von Intellectual Property, Rufschädigung und – zunehmend – aufsichtsrechtliche Konsequenzen als Punkte, die ihnen die meisten Sorgen bereiten[2].

Vor diesem Hintergrund gehört das Thema Informationssicherheit zwingend auf die Vorstandsagenda. Erforderlich sind Sicherheitsmaßnahmen, die die gesamte Organisation einschließen. In technischer Hinsicht ist beispielsweise zu gewährleisten, dass kein unberechtigter Zugriff auf die Systeme im Unternehmen möglich ist.

Im Zuge erweiterter Schulungsmaßnahmen müssen Mitarbeiter für das Thema Informationssicherheit sensibilisiert werden. Mit der Einführung nachhaltiger Führungsstrukturen und -mechanismen ist für die Sicherheit der Organisation zu sorgen. Prozesse wiederum sind so zu gestalten, dass sich Dritte keine Unternehmensdaten beschaffen können.

2 Marsh ist der größte Versicherungsbroker der Welt und Teil von Marsh & McLennan Companies. Das Unternehmen ist führend bei der Absicherung von Cyber-Risiken und erstellt regelmäßig die Cyber Risk Survey.

ERKENNTNISSE IN DER SCHWERINDUSTRIE

In einem sicherheitsrelevanten Sektor der Schwerindustrie entwickelte Oliver Wyman eine Informationssicherheitsstrategie für einen Zulieferer. Das Projekt wurde unter Verantwortung der IT-Abteilung durchgeführt, im Scope befand sich die gesamte Prozesslandschaft des Unternehmens. Oliver Wyman leitete gemeinsam mit dem Kunden die wichtigsten Schutzbedarfe und notwendigen Maßnahmen ab. Im Ergebnis wurde deutlich, dass die wesentlichen Stellhebel zur Verbesserung des Schutzniveaus nur gemeinsam mit den Partner- und Kundenunternehmen des Zulieferers umsetzbar waren. Der Grund: Dessen Produkte werden im weiteren Produktionsprozess in höherwertige Produkte verbaut, an die weiterführende Informationsschutzanforderungen zu stellen sind. Um diese erfüllen zu können, musste die Programmverantwortung aus der IT auf die Geschäftsführungsebene verlagert werden.

Lessons learned:

- Der Grad der vertikalen Integration in der Wertschöpfungskette ist entscheidend für die Bestimmung des Informationsschutzniveaus. In vielen Fällen ist eine Abstimmung mit zuliefernden und/oder abnehmenden Unternehmen erforderlich.
- Die Allokation der Durchführungsverantwortung für ein Informationssicherheitsprojekt bei der IT-Organisation greift in vielen Fällen zu kurz, weil oftmals wesentliche Risiken und Schutzbedarfe außerhalb der IT zu verorten sind. Die Allokation als unternehmensweites Programm mit direkter Berichtslinie an Geschäftsführung beziehungsweise Vorstand empfiehlt sich.

ERKENNTNISSE IN DER ENERGIEBRANCHE

Ein Unternehmen der Energiebranche beauftragte Oliver Wyman mit der Bewertung des aktuellen Informationsschutzniveaus inklusive Ableitung korrespondierender Maßnahmen. Im Rahmen der Projektdurchführung waren branchenspezifische Regularien zu berücksichtigen. Oliver Wyman brachte neben der fachlichen Expertise auch regulatorisches Know-how in das Projekt ein. Im Ergebnis wurden Maßnahmen definiert und dokumentiert, die auch der Prüfung durch Dritte standhalten.

Lessons learned:

Die Definition von Informationssicherheitsstrategien in regulierten Branchen erfordert tiefe Kenntnisse des regulatorischen Umfelds. In vielen Branchen ist der gesetzliche Rahmen für Informationssicherheit im Wandel. Normen und Standards wie ISO 2700x oder NIST bieten wichtige Anhaltspunkte und Vorschläge, müssen aber an die jeweils spezifische Situation, die Branche und an etwaige regulatorische Besonderheiten angepasst werden.

ERKENNTNISSE IN DER FINANZBRANCHE

Für ein führendes Finanzinstitut hat Oliver Wyman die Cyber-Security-Roadmap bewertet und überprüft. In diesem Zusammenhang wurden unter anderem Schwachstellen in den Bereichen „Prevention“ und „Detection“ identifiziert.

Lessons learned:

Für eine umfassende Vorbeugung und möglichst rasche Identifikation von Schwachstellen ist die Implementierung weitreichender Früherkennungsindikatoren und gezieltes Sammeln und Auswerten bekannter Risikodaten notwendig. In solchen Cyber-Intelligence-Analysis-Teams laufen Datenströme externer Dienstleister (zum Beispiel Monitoring von Dark-Web-/Deep-Web-Seiten), die Überwachung interner Systeme und Prozesse sowie die Koordination der Aktivitäten mit Sicherheitsbehörden zusammen. Um dies zielgerichtet umzusetzen, ist es wichtig, die schützenswerten Assets und hauptsächlichen Schutzbedarfe des Unternehmens zu kennen, zu priorisieren und Schutzmaßnahmen regelmäßig zu überprüfen und zu aktualisieren.

HOHER NACHHOLBEDARF

Noch mangelt es vielerorts an der Erkenntnis, dass die Anforderungen an eine weitreichende Informationssicherheit mehrdimensional sind und die Risikobewertung einen ganzheitlichen Ansatz erfordert. Hauptgrund dafür ist aus Sicht von Oliver Wyman, dass in Unternehmen zu wenig Transparenz darüber besteht, welche Informationen tatsächlich schützenswert sind. Diese variieren je Unternehmen und Branche. Sind es bei einem Hersteller von Maschinen Baupläne oder Zugriffsdaten für Produktionsanlagen, können es bei Industriedienstleistern oder Marketingagenturen Kundendaten oder vertrauliche Projektinformationen sein.

Entsprechend groß ist der Nachholbedarf, was umfassende Sicherheit angeht. Sich allein auf die technische Kompetenz der IT-Abteilung oder ein funktionierendes Corporate Risk Management zu verlassen, reicht nicht aus. Letzteres kann angesichts der Vielschichtigkeit möglicher Bedrohungen und der daraus resultierenden komplexen Fragestellungen lediglich Basis für ein wirkungsvolles Information Security Management sein, das Prozesse und Strukturen ebenso anpasst wie technische Rahmenparameter, Unternehmenskultur und den Umgang mit Mitarbeitern.

ERFOLGSENTSCHEIDENDE FAKTOREN

Für nachhaltige Informationssicherheit sind laut Oliver Wyman verschiedene Erfolgskriterien entscheidend. Dazu gehört in erster Linie die ganzheitliche Risikobewertung über alle Funktionen und Ebenen hinweg, die potenzielle Ziele ebenso berücksichtigt wie Bedrohungen und Maßnahmen. Von Bedeutung ist zudem, sich Klarheit über die wichtigsten Informationswerte und Daten des Unternehmens zu verschaffen. Damit sind die Informationen, Produkte, Bereiche, Prozesse oder Systeme gemeint, die für das Unternehmen von strategischer Relevanz und daher unbedingt zu schützen sind. Zugleich führt kein Weg daran vorbei, im Blick zu haben, wie sich deren Stellenwert durch die digitale Transformation oder die Entwicklung des Geschäftsmodells verändern wird.

Abbildung 1: Ein unternehmensweiter Rahmen für das Information Security Management

- Entwicklung einer ganzheitlichen **IS-Strategie**, die Risikobereitschaft, Umwelt und Fähigkeiten berücksichtigt
- Einführung von **Governance-Strukturen**, um Sicherheit im gesamten Unternehmen zu gewährleisten
- Ableitung von **Sicherheitsrichtlinien**, um Compliance gemäß Branchenstandards (PCI, ISO, FISMA etc.) zu garantieren
- Auswahl von **geeignetem Personal** und dessen Schulung, Etablierung einer Risikokultur
- Abstimmung der **Sicherheitsprozesse** mit der Information-Security-Strategie und den Sicherheitsrichtlinien
- Implementierung einer **Technologieinfrastruktur** zur Unterstützung der Sicherheitsprozesse
- Design und Installation einer **physischen Infrastruktur** mit Zugangskontrollen, Überwachung und Krisenmanagement
- Durchführung **regelmäßiger Audits**, um Compliance und Wirksamkeit der definierten Prozesse zu gewährleisten

Quelle: Oliver Wyman

Darüber hinaus gilt es, sich infrage kommende Schädigungsszenarien zu vergegenwärtigen, die Risikobereitschaft festzulegen und zentrale Maßnahmen für den Informationsschutz zu verankern. Diese reichen von der Definition einer klaren Strategie zum Schutz aller relevanten Unternehmensinformationen über den Aufbau entsprechender Governance-Strukturen bis hin zu regelmäßigen Audits sowie Prozesskontrollpunkten, die es ermöglichen, das Ausmaß der Bedrohungen jederzeit abschätzen zu können.

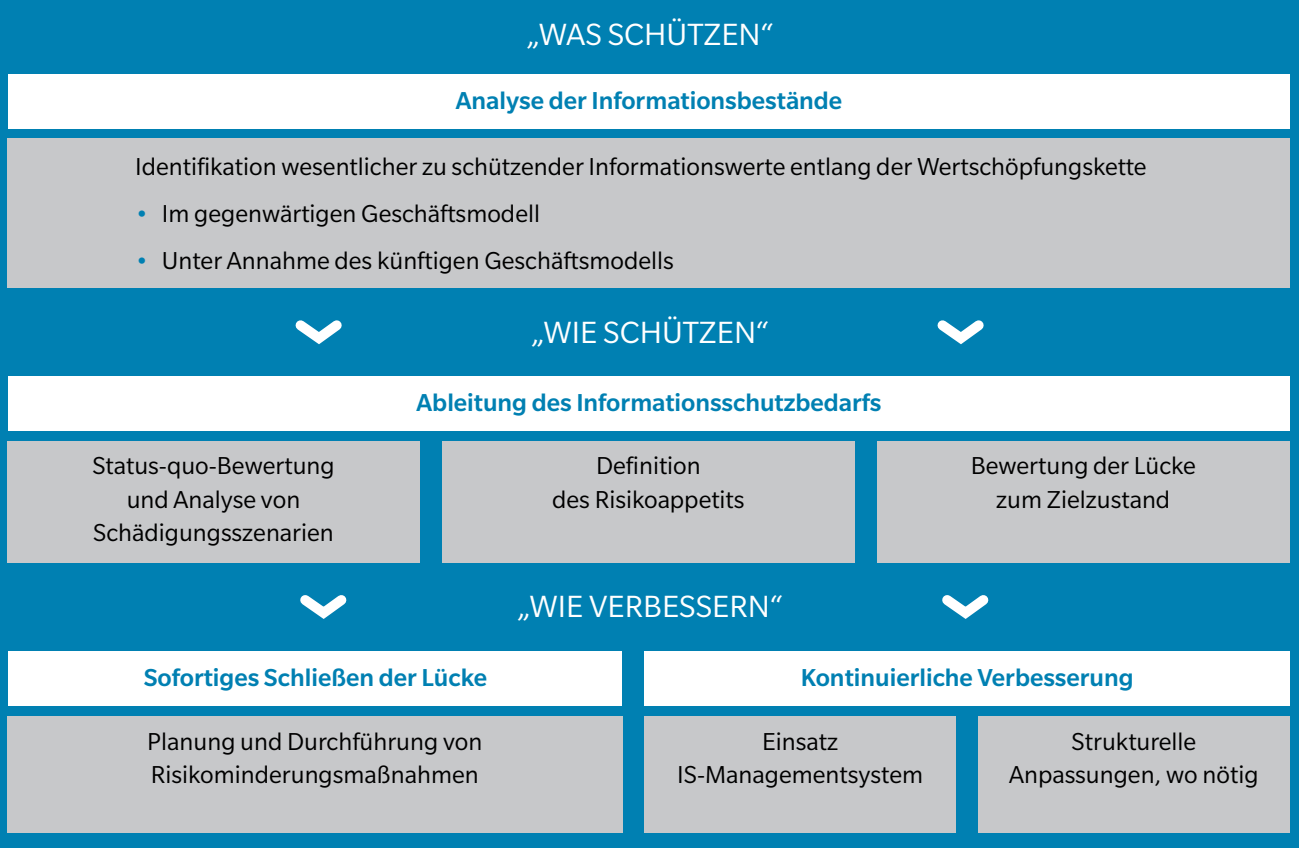
KONTINUIERLICHER PROZESS

Informationssicherheit heißt nicht, von heute auf morgen die perfekte Sicherheit zu erreichen. Während sich eine technische Verbesserung oftmals relativ rasch erzielen lässt, können organisatorische und prozessuale Veränderungen bis zu einem Jahr dauern. Am zeitintensivsten ist es in der Regel, die Mitarbeiter zu sensibilisieren.

Steht das Fundament, wird moderne Informationssicherheit zu einem fortlaufenden Prozess, der je nach Ausprägung und Unternehmensgröße unterschiedlich aufwendig ist. Diesen gezielt zu steuern erfordert eine übergeordnete Sicherheitsinstanz. Das kann ein Chief Information Security Officer sein, ein erweiterter Datenschutzbeauftragter oder ein Vorstandsmitglied, dessen Aufgabenbereich entsprechend aufgestockt wird.

Für alle Unternehmen ist es jetzt an der Zeit zu handeln. Cyber-Kriminalität wird weiter zunehmen und noch vielfältiger werden. In der Folge werden auch die Schäden für die Unternehmen ein noch größeres Ausmaß annehmen. Dem gilt es Vorschub zu leisten – mit einem ganzheitlichen Information Security Management.

Abbildung 2: Vorgehen Informationssicherheit



Quelle: Oliver Wyman

ÜBER OLIVER WYMAN

Oliver Wyman ist eine international führende Managementberatung mit weltweit 3.700 Mitarbeitern in mehr als 50 Büros in 26 Ländern. Das Unternehmen verbindet ausgeprägte Branchenspezialisierung mit hoher Methodenkompetenz bei Strategieentwicklung, Prozessdesign, Risikomanagement und Organisationsberatung. Gemeinsam mit Kunden entwirft und realisiert Oliver Wyman nachhaltige Wachstumsstrategien. Wir unterstützen Unternehmen dabei, ihre Geschäftsmodelle, Prozesse, IT, Risikostrukturen und Organisationen zu verbessern, Abläufe zu beschleunigen und Marktchancen optimal zu nutzen. Oliver Wyman ist eine hundertprozentige Tochter von Marsh & McLennan Companies (NYSE: MMC).

Weitere Informationen finden Sie unter www.oliverwyman.de.

KONTAKT

DR. CLAUS HERBOLZHEIMER

Partner, Strategic IT & Operations
claus.herbolzheimer@oliverwyman.com
+49 30 399 945 63

DR. KAI BENDER

Partner, Strategic IT & Operations
kai.bender@oliverwyman.com
+49 30 399 945 61

RAJ BECTOR

Partner, Strategic IT & Operations
raj.bector@oliverwyman.com
+1 646 364 8519

SILVIO SPERZANI

Partner, Strategic IT & Operations
silvio.sperzani@oliverwyman.com
+39 23 057 7449

OLIVER WYMAN