GLOBAL PERSPECTIVES & INSIGHTS

Cybersicherheit im Jahr 2022

TEIL 1: Wie die neuen SEC-Vorschläge das Spiel verändern könnten

TEIL 2: Kritische Partner – Interne Revision und der CISO

TEIL 3: Reaktion auf Cybervorfälle und Wiederherstellung

The Institute of Internal Auditors

INHALT

Teil 1

Wie die neuen SEC-Vorschläge das Spiel verändern könnten

Über die Experten

Andy Watkin-Child

Watkin-Child ist seit 20 Jahren in den Bereichen Cybersicherheit, Risikomanagement und Technologie tätig und Mitbegründer der Augusta Group, einem Anbieter von Lösungen für Management, Überwachung und Prüfung von Cybersicherheit und Cyberrisiken. Er hatte internationale Führungspositionen in der 1. und 2. Verteidigungslinie für Cybersicherheit, Cyber-Risikomanagement, operationelle Risiken und Technologie inne und arbeitete mit Führungsteams von Unternehmen mit einer Bilanzsumme von über 1 Billion Euro in den Bereichen Maschinenbau und Fertigung, Finanzdienstleistungen sowie Verlagswesen und Medien. Er ist ein erfahrenes Mitglied von Boards, globalen Risiko-Führungsteams und Komitees für Cybersicherheit, operationellen Risiken und und DSGVO.

Manoj Satnaliwala

Satnaliwala ist Chief Audit Executive und SVP of Internal Audit bei Caliber Home Loans. Er ist für alle Prüfungsaktivitäten verantwortlich und arbeitet direkt mit dem Audit Committee zusammen. Vor seiner jetzigen Tätigkeit leitete er die Revisionsfunktion bei Radian Group Inc., dem drittgrößten börsennotierten Hypothekenversicherer in den Vereinigten Staaten, und war Direktor für Interne Revision bei PwC, wo er die Validierung der Kontrollen für die Interne Revision als Teil des CCAR-Projekts für eine große Bankholdinggesellschaft leitete.

Einführung

Neue Regulierungsvorschläge könnten große Auswirkungen haben

Die Nachrichtenlage im Jahr 2022 und in den letzten Jahren war wenig positiv. Cyber-Bedrohungen spielten eine große Rolle in einem Mix aus Ukraine-Krise, anhaltenden COVID-19-Bedrohungen und wachsenden Spannungen zwischen den USA und China. Diese und weitere Faktoren haben dazu geführt, dass das Thema Cybersicherheit auf der Risikolandkarte der Internen Revision einen bedeutenden – und sogar einen führenden – Platz einnimmt.

Das Jahr 2022 war jedoch auch von Entwicklungen im Bereich der Cybersicherheit geprägt, die sich auf ein breites Spektrum von Organisationen auswirken werden, deren Verständnis mehr Aufwand erfordert und deren Auswirkungen erst nach einiger Zeit vollständig erfasst werden können. Dazu gehören vor allem zwei Regulierungsvorschläge der US-Börsenaufsichtsbehörde SEC (Securities and Exchange Commission). Der zweite Vorschlag ist besonders erwähnenswert, da er von börsennotierten Unternehmen, die in den USA tätig sind, verlangt, dass sie ihre Cybersicherheitsrichtlinien, -verfahren und -strategien sowie die Kenntnisse und Erfahrungen des Board – sofern vorhanden – im Bereich der Cybersicherheit offenlegen. Wenn sie umgesetzt werden (was wahrscheinlich in irgendeiner Form der Fall sein wird), werden alle börsennotierten Unternehmen, unabhängig von ihrer Branche oder Größe, diesen neuen Vorschriften unterliegen. Ohne zu übertreiben, stellen diese Entwicklungen ein neues Kapitel für die Cybersicherheit und ein neues Thema für die Interne Revision dar, die eine entscheidende Rolle dabei spielen wird, ihre Organisationen durch diese Herausforderung zu navigieren.

Obwohl dies keine Herausforderung ist, die man auf die leichte Schulter nehmen sollte, verfügt die Interne Revision glücklicherweise über die Instrumente und Fähigkeiten, die sie benötigt, um Prüfungssicherheit in diesem sich entwickelnden Risikobereich zu bieten. Teil 1 der dreiteiligen Global Knowledge Brief-Reihe des IIA zum Thema Cybersicherheit gibt einen Überblick über die neuen Vorschläge der SEC, einschließlich der Auswirkungen auf die Regulierung der Cybersicherheitsberichterstattung in den USA und im Ausland. Außerdem wird untersucht, wie Interne Revisorinnen und Revisoren eine wichtige Rolle dabei spielen können, ihre Organisationen bei der Bewältigung einer veränderten Compliance-Landschaft zu unterstützen, die durch die neuen Vorschriften bald entstehen könnte.

Die Bühne frei machen

Cybersicherheit dominiert die Risikolandschaft

Das größte Risiko unserer Zeit

Cybersicherheit bleibt auch im Jahr 2022 auf allen Ebenen aller Organisationen in allen Branchen ein wichtiges Thema, und diese Besorgnis spiegelt sich deutlich in den Daten des *nordamerikanischen Pulse of Internal Audit* (*Pulse*) des IIA für *2022 wider.*[1] Auf die Frage, wie hoch das Risiko für ihr Unternehmen unter 13 Hauptrisiken ist, stuften die Revisionsleitungen, die an der Pulse-Umfrage teilnahmen, technologiebezogene Risiken als die drei wichtigsten ein: Cybersicherheit, IT und Beziehungen zu Dritten (zu denen häufig IT-Dienstleistungen gehören). Selbst unter diesen drei Spitzenreitern nimmt die Cybersicherheit mit Abstand den ersten Platz ein: 85 % der Befragten stuften sie als hohes oder sehr hohes Risiko ein, 24 Prozentpunkte höher als die Bewertungen für die IT, das zweithöchste eingestufte Risiko.

Diese Sorge ist gerechtfertigt. Im Jahr 2021 nahmen Cyberangriffe fast aller Art in alarmierendem Ausmaß zu. Laut dem *SonicWall Cyber Threat Report 2022*[2] stieg die Zahl der verschlüsselten Bedrohungen im Jahr 2021 um 167 % (10,4 Millionen Angriffe), Ransomware um 105 % (623,3 Millionen Angriffe), Cryptojacking (Angriffe auf Computer, um Kryptowährung zu schürfen) um 19 % (97,1 Millionen Angriffe), Einbruchsversuche um 11 % (5,3 Billionen Angriffe) und auf das Internet der Dinge (IoT) gerichtete Malware um 6 % (60,1 Millionen Angriffe).

Hinzu kommt, dass all diese Angriffe mit erheblichen Kosten für den Schaden verbunden sind, den sie anrichten. Laut der neuesten Version des Cybersecurity Almanac 2022 von Cisco/Cybersecurity Ventures[3] werden die jährlichen Gesamtkosten von Cyberangriffen bis 2025 voraussichtlich 10,5 Billionen US-Dollar erreichen, was einem durchschnittlichen Wachstum von 15 % im Vergleich zum Vorjahr entspricht.

Und dabei sind die dramatischen Veränderungen in der geopolitischen Landschaft, die sich auf die Cybersicherheit auswirken, noch gar nicht berücksichtigt. Schon vor dem Einmarsch Russlands in der Ukraine gab es reichlich Beweise dafür, dass mutmaßlich staatlich geförderte Cyberangriffe mit einem hohen Grad an Raffinesse in ihrer Wirkung und Häufigkeit zunehmen. Beim Einbruch in die Systeme des texanischen Unternehmens SolarWind im Jahr 2020, der von einer Hackergruppe durchgeführt wurde, die Berichten zufolge[4] vom russischen Auslandsgeheimdienst gesteuert wurde, wurde die digitale Infrastruktur von bis zu 18.000 Kunden[5] – darunter Microsoft, Cisco, Intel, Deloitte, Teile des Pentagon, das US-Ministerium für Heimatschutz, das Energieministerium und die Nationale Behörde für nukleare Sicherheit – kompromittiert und blieb monatelang unentdeckt.

Im Jahr 2021 gab es einen weiteren großen, mutmaßlich staatlich geförderten Angriff auf ein US-Unternehmen: die Colonial Pipeline Co.[6] Durch den Angriff wurde vorübergehend fast die Hälfte der Benzin- und Flugzeugtreibstofflieferungen an die Ostküste unterbrochen. Letztendlich zahlte Colonial ein Lösegeld von fast 5 Millionen Dollar an die Hackergruppe DarkSide, um das Netzwerk wiederherzustellen und die Daten zu retten.

---

[1]. The IIA, *2022 North American Pulse of Internal Audit*, March 2022, https://www.theiia.org/en/content/research/pulse-of-internal-audit/2022/2022-north-american-pulse-of-internal-audit/

[2]. SonicWall, *2022 SonicWall Cyber Threat Report*, 2022, https://www.sonicwall.com/2022-cyber-threat-report/.

[3]. Steve Morgan, "2022 Cybersecurity Almanac: 100 Facts, Figures, Predictions And Statistics," Cybersecurity Ventures, Cisco, January 19, 2022, https://cybersecurityventures.com/cybersecurity-almanac-2022/.

[4]. Joe Hernandez, The Russian Hacker Group Behind the SolarWinds Attack Is At It Again, Microsoft Says," NPR, updated October 25, 2021, https://www.npr.org/2021/10/25/1048982477/russian-hacker-solarwinds-attack-microsoft.

[5]. [5]. Isabella Jibilian and Katie Canales, "The US Is Readying Sanctions Against Russia Over the SolarWinds Cyber Attack. Here's a Simple Explanation of How the Massive Hack Happened and Why It's Such a Big Deal," Business Insider, updated April 15, 2021, https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12.

[6]. Andrew Marquardt, "As Biden Warns of a Russian Cyberattack, What Are the Precedents? Here's What Happened When a Major Oil Pipeline Was Hacked Last Year," Fortune, March 22, 2022, https://fortune.com/2022/03/22/biden-warns-russian-cyber-attack-pipeline/.

Geopolitische Sollbruchstelle

Seit diesen Angriffen ist die Besorgnis gegenüber Russland nur noch größer geworden und hat mit dem Einmarsch in die Ukraine einen Höhepunkt erreicht. Russlands Aggression gegen die Ukraine umfasst neben der traditionellen Kriegsführung auch die Cyber-Kriegsführung – ein groß angelegter Angriff auf das ukrainische Stromnetz[7] – und es wird zunehmend befürchtet, dass Russland Vergeltung für die unzähligen Wirtschaftssanktionen üben könnte, die ihm von der NATO und den USA auferlegt wurden. Nur eine Woche vor dem offiziellen Einmarsch Russlands in die Ukraine gab die Cybersecurity and Infrastructure Security Agency (CISA) eine seltene Erklärung mit dem Titel "Shields Up"[8] heraus, in der US-Unternehmen aller Größenordnungen ermahnt werden, eine verstärkte Haltung in Bezug auf die Cybersicherheit und den Schutz kritischer Anlagen einzunehmen. "Kürzlich von der CISA und anderen nicht klassifizierten Quellen veröffentlichte Hinweise zeigen, dass russische, staatlich unterstützte Bedrohungsakteure die folgenden Branchen und Organisationen in den Vereinigten Staaten und anderen westlichen Ländern ins Visier nehmen: COVID-19-Forschung, Regierungen, Wahlkampforganisationen, Gesundheitswesen und Pharmazie, Verteidigung, Energie, Videospiele, Nuklearindustrie, kommerzielle Einrichtungen, Wasserwirtschaft, Luftfahrt und kritische Produktionsanlagen", schrieb die CISA in einer Erklärung vom März 2022[9] zur Bewertung der russischen Cyber-Bedrohungen.

Im Mai 2021 unterzeichnete Präsident Biden eine Durchführungsverordnung[10] zur Verbesserung der nationalen Sicherheit in den USA. Die Verordnung befasste sich insbesondere mit der Notwendigkeit für Regierungsbehörden, Richtlinien und Standards für die Cybersicherheit zu überprüfen und neue zu entwickeln, und für Organisationen, sich auf die Verbesserung der Sicherheit der Software-Lieferkette und den Austausch von Bedrohungsinformationen zu konzentrieren. Kürzlich gab der Präsident auch eine Erklärung ab, in der er erneut auf die russische Bedrohung der Cybersicherheit hinwies und die entstehenden Leitlinien des CISA[11] zu diesem Thema hervorhob.

Russland ist nicht der einzige staatliche Akteur, der angeblich hinter destabilisierenden Cyberangriffen steht. Laut einem Bericht[12] der Evanina Group aus dem Jahr 2021 ist China an der Cyberfront zunehmend aggressiver geworden, insbesondere im Hinblick auf die Beschaffung persönlicher Daten und den Datenschutz.

"Chinas Fähigkeit, sich unser geistiges Eigentum und unsere Geschäftsgeheimnisse durch illegale, legale und ausgeklügelte hybride Methoden zu beschaffen, ist mit nichts zu vergleichen, was wir je erlebt haben", sagte William Evanina, ehemaliger Direktor des National Counterintelligence and Security Center.

Evanina verwies auf zahlreiche Cybervorfälle, die mit der Kommunistischen Partei Chinas in Verbindung gebracht werden, darunter der Cyberangriff auf Equifax im Jahr 2017, eine Kampagne von vier chinesischen Staatsangehörigen in den Jahren 2011-2018, die sich in Dutzende von Unternehmen, Universitäten und Regierungseinrichtungen einhackten, sowie eine staatlich geförderte Cyberkampagne in den Jahren 2011-2013, die US-amerikanische Öl- und Erdgaspipeline-Unternehmen angriff. (Das DOJ veröffentlichte im Juli 2021 einen Bericht zu diesem Vorfall.) Er verwies auch auf einen Bericht der National Security Agency (NSA), des Federal Bureau of Investigation (FBI) und der CISA vom Juli 2021, in dem mehr als 50 Cyber-Taktiken und -Werkzeuge aufgeführt sind, die von chinesischen, staatlich gesponserten Hackern gegen die USA eingesetzt werden.

In diesem komplexen und insgesamt gefährlichen Cyber-Umfeld hat die SEC historische Schritte unternommen, um die Cyber-Gesundheit und die Prävention in der gesamten Unternehmenslandschaft zu verbessern, insbesondere im Hinblick auf die Berichterstattung an die SEC und (in einigen Fällen) an die Öffentlichkeit. Diese Schritte sind die ersten ihrer Art und könnten nicht nur für börsennotierte US-Unternehmen, sondern für Unternehmen auf der ganzen Welt erhebliche Auswirkungen haben.

---

[7]. IANS, Ukraine Foils Russia-backed Cyber Attack on Power Grid," April 14, 2022, https://www.nationalheraldindia.com/international/ukraine-foils-russia-backed-cyber-attack-on-power-grid.
[8]. Cybersecurity and Infrastructure Security Agency (CISA), "Shields Up," accessed April 22, 2022, https://www.cisa.gov/shields-up.
[9]. Cybersecurity and Infrastructure Security Agency (CISA), "Russia Cyber Threat Overview and Advisories," Department of Homeland Security, accessed April 22, 2022, https://www.cisa.gov/uscert/russia.
[10]. U.S. General Services Administration (GSA), "Executive Order 14028: Improving the Nation's Cybersecurity," May 12, 2021, https://www.gsa.gov/technology/technology-products-services/it-security/executive-order-14028-improving-the-nations-cybersecurity.
[11]. Cybersecurity and Infrastructure Security Agency (CISA), "Shields Up."
[12]. William Evanina, "Statement of William R. Evanina, CEO, The Evanina Group, Before the Senate Select Committee on Intelligence, at a Hearing Concerning the Comprehensive Threat to America Posed by the Communist Party of China (CCP), The Evanina Group, August 4, 2021, https://www.intelligence.senate.gov/sites/default/files/documents/os-bevanina-080421.pdf.

Die große Veränderung

Ein historischer erster Schritt zur Offenlegung von Cybervorfällen

Die Vorschläge

Innerhalb von zwei Monaten hat die SEC zwei lange erwartete Vorschläge zur Cybersicherheit im Unternehmenssektor vorgelegt. Der erste Vorschlag,[13] der im Februar 2022 veröffentlicht wurde, konzentriert sich auf registrierte Anlageberater, registrierte Investmentgesellschaften und Unternehmensentwicklungsgesellschaften oder -fonds. Nach den vorgeschlagenen Regeln wären Berater und Fonds verpflichtet:

- Schriftliche Cybersicherheitsrichtlinien und -verfahren einzuführen und umzusetzen, um Cybersicherheitsrisiken zu begegnen, die Kunden und Fondsanlegern schaden könnten.
- Erhebliche Cybersicherheitsvorfälle, die den Berater oder seine Fondskunden betreffen, an die SEC auf einem neuen, vertraulichen Formular zu melden.
- Cybersicherheitsrisiken und bedeutende Cybersicherheitsvorfällen, die in den letzten zwei Geschäftsjahren aufgetreten sind, in ihren Broschüren und Registrierungserklärungen offenzulegen.

Darüber hinaus sieht der Vorschlag neue Aufzeichnungspflichten für Berater und Fonds vor, um die Verfügbarkeit von sicherheitsrelevanten Informationen zu verbessern und die Kontroll- und Durchsetzungsmöglichkeiten der SEC zu erleichtern.

"Cyber-Risiken stehen mit jedem Teil der dreiteiligen Aufgabe der SEC in Verbindung, insbesondere mit unseren Zielen des Anlegerschutzes und der Aufrechterhaltung geordneter Märkte", sagte der SEC-Vorsitzende Gary Gensler in einer Presseerklärung.[14] "Die vorgeschlagenen Regeln und Änderungen sollen die Bereitschaft zur Cybersicherheit verbessern und könnten das Vertrauen der Anleger in die Widerstandsfähigkeit von Beratern und Fonds gegen Cybersicherheitsbedrohungen und -angriffe stärken."

Während diese Vorschriften – wenn auch nur implizit – die Erwartungen der SEC in Bezug auf den Umgang mit Cybersicherheitsrisiken und die Meldung von Cybersicherheitsvorfällen widerspiegeln, werden diese Erwartungen im zweiten Vorschlag explizit gemacht. Der zweite Vorschlag,[15] der sich an alle börsennotierten Unternehmen richtet und im März 2022 veröffentlicht wurde, zielt darauf ab, "die Offenlegung in Bezug auf Cybersicherheits-Risikomanagement, -Strategie und -Governance sowie die Berichterstattung über Cybersicherheitsvorfälle durch börsennotierte Unternehmen, die den Berichtspflichten des Securities Exchange Act von 1934 unterliegen, zu verbessern und zu standardisieren". Um dies zu erreichen, würden die neuen Regeln von börsennotierten Unternehmen verlangen, Angaben zu folgenden Punkten zu machen:

- Strategien und Verfahren des Unternehmens zur Identifizierung und Verwaltung von Cybersicherheitsrisiken. Die Vorschriften enthalten eine umfangreiche, aber nicht vollständige Liste von Risikomanagementstrategien, -richtlinien und -verfahren, die der Offenlegung unterliegen können, darunter:
    - Ob das Unternehmen über ein Programm zur Beurteilung der Cybersicherheitsrisiken verfügt.
    - Ob das Unternehmen Beurteiler, Berater, Prüfer oder andere Dienstleister in Verbindung mit einem Programm zur Beurteilung von Cybersicherheitsrisiken einsetzt.
    - Ob das Unternehmen über Strategien und Verfahren verfügt, um die Cybersicherheitsrisiken im Zusammenhang mit der Inanspruchnahme von externen Dienstleistern zu überwachen und zu identifizieren.

[13]. U.S. Securities and Exchange Commission (SEC), "Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies," February 9, 2022, https://www.sec.gov/rules/proposed/2022/33-11028.pdf.
[14]. U.S. Securities and Exchange Commission (SEC), "SEC Proposes Cybersecurity Risk Management Rules and Amendments for Registered Investment Advisers and Funds," press release, February 9, 2022, https://www.sec.gov/news/press-release/2022-20.
[15]. U.S. Securities and Exchange Commission (SEC), "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure," March 9, 2022, https://www.sec.gov/rules/proposed/2022/33-11038.pdf.

- Ob das Unternehmen Aktivitäten zur Verhinderung, Erkennung und Minimierung der Auswirkungen von Cybersicherheitsvorfällen unternimmt.
- Ob das Unternehmen über Geschäftskontinuitäts-, Notfall- und Wiederherstellungspläne für den Fall eines Cybersicherheitsvorfalls verfügt.
- Ob frühere Cybersicherheitsvorfälle zu Änderungen in der Unternehmensführung, den Richtlinien und Verfahren oder den Technologien des Unternehmens geführt haben.
- Ob sich Risiken und Vorfälle im Zusammenhang mit der Cybersicherheit auf das Geschäftsergebnis oder die Finanzlage des Unternehmens ausgewirkt haben oder mit hinreichender Wahrscheinlichkeit auswirken werden.
- Ob Cybersicherheitsrisiken im Rahmen der Geschäftsstrategie, der Finanzplanung und der Kapitalzuweisung des Unternehmens berücksichtigt werden.

- Die Rolle des Managements bei der Umsetzung von Cybersicherheitsrichtlinien und -verfahren, einschließlich:
  - Ob bestimmte Führungspositionen oder Komitees für die Messung und das Management von Cybersicherheitsrisiken zuständig sind.
  - Ob das Unternehmen einen Chief Information Security Officer oder eine Person in einer vergleichbaren Position benannt hat.
  - Ob es Verfahren gibt, mit denen diese Personen oder Komitees über die Verhinderung, Minderung, Aufdeckung und Behebung von Cybersicherheitsvorfällen informiert werden und diese überwachen.
  - Ob diese Personen oder Komitees dem Board oder einem Ausschuss des Boards über Cybersicherheitsrisiken berichten und wie häufig sie dies tun.
  - Ob das gesamte Board, bestimmte Mitglieder oder ein Ausschuss des Boards für die Beaufsichtigung von Cybersicherheitsrisiken zuständig ist.
  - Ob das Boards über Cybersicherheitsrisiken informiert ist und wie häufig es solche Risiken diskutiert.
  - Ob und wie das Board oder ein Komitee Cybersicherheitsrisiken im Rahmen der Geschäftsstrategie, des Risikomanagements und der Überwachung der Finanzen berücksichtigt.

- Die Fachkenntnisse des Boards im Bereich der Cybersicherheit, falls vorhanden, und seine Aufsicht über die Cybersicherheitsrisiken. Dazu gehören folgende Informationen:
  - Ob das Board über Berufserfahrung im Bereich der Cybersicherheit verfügt.
  - Ob das Board eine Zertifizierung oder einen Abschluss in Cybersicherheit erworben hat.
  - Ob das Board über Kenntnisse, Fähigkeiten oder einen anderen Hintergrund im Bereich der Cybersicherheit verfügt.

Darüber hinaus sieht der Vorschlag eine Änderung des Formulars 8-K vor, wonach börsennotierte Unternehmen verpflichtet wären, Cybersicherheitsvorfälle innerhalb von vier Arbeitstagen zu veröffentlichen, so wie sie dies bereits bei anderen unvorhergesehenen wichtigen Ereignissen tun müssen. Diese Offenlegungen würden Folgendes umfassen:

- Wann der Vorfall entdeckt wurde und ob er noch andauert.
- Eine kurze Beschreibung von Art und Umfang des Vorfalls.
- Ob Daten gestohlen, verändert, abgerufen oder zu einem anderen unbefugten Zweck verwendet wurden.
- Die Auswirkungen des Vorfalls auf den Betrieb des Unternehmens.
- Ob das Unternehmen den Vorfall behoben hat oder derzeit behebt.

Nach Ansicht der SEC würden diese Angaben den Anlegern "einheitliche, vergleichbare und entscheidungsnützliche" Informationen liefern. "Die Cybersicherheit ist heute ein bedeutender werdendes Risiko, mit dem sich öffentliche Emittenten

zunehmend auseinandersetzen müssen", so Gensler.[16] "Die starke Vernetzung, der Einsatz von prädiktiven Datenanalysen und der unersättliche Wunsch nach Daten nehmen immer mehr zu und gefährden unsere Finanzkonten, Investitionen und privaten Informationen. Die Anleger wollen mehr darüber wissen, wie die Emittenten mit diesen wachsenden Risiken umgehen."

Die historische Bedeutung

In vielerlei Hinsicht spiegelt die Struktur dieser beschriebenen Regeln andere Offenlegungsregeln der SEC wider, wie z. B. jene, die sich auf finanzielle Bedingungen und Betriebsergebnisse (Sarbanes-Oxley), Insiderinformationen und organisatorische Stärken, Schwächen, Chancen und Bedrohungen beziehen. Der jetzige Schritt, Cybersicherheitsrisiken zu einem Thema zu erheben, an dem eine Offenlegung erforderlich ist, ist jedoch weitgehend beispiellos.

"Die USA sind wahrscheinlich das erste und einzige Land der Welt, das die Cybersicherheit reguliert", sagt Andy Watkin-Child, Gründungspartner von The Augusta Group und Parava Security Solutions und Gründer von Cybersecurity Maturity Model Certification Europe (CMMC Europe). "Unternehmen in den USA sind vielleicht mit der Datenschutzgrundverordnung (GDPR) der EU vertraut und werden diese Vorschläge schnell in einen Topf werfen, aber Datenschutz und Cybersicherheit sind zwei verschiedene Paradigmen. Es gibt einen großen Unterschied. Abgesehen von der Financial Management Regulation des Verteidigungsministeriums, die dazu führen könnte, dass selbst ausländische Auftragnehmer vom Justizministerium auf Schwachstellen in der Cybersicherheit untersucht werden, gibt es im Bereich der Cybersicherheit nichts Vergleichbares."

Watkin-Child erklärt auch, dass die Bedeutung der neuen Regeln starke Auswirkungen auf das Ausland haben könnte. "Die Ukraine-Krise hat bewiesen, dass Cybersicherheit eine Waffe ist, und in der Tat hat die NATO sie seit 2016 als eine Art von Operation betrachtet", sagt er. "Cybersicherheit ist ein offensives Werkzeug, gleich neben Atomwaffen. Das Problem dabei ist, dass es sich um einen Einsatzbereich handelt, der eine ernste Bedrohung für nationale Infrastrukturen darstellt. Der Vorschlag der SEC trifft zuerst die großen Akteure, die Handelsunternehmen, aber ich glaube, dass dies hoffentlich auch auf Organisationen außerhalb des Zuständigkeitsbereichs der SEC übergreifen wird, weil die Unternehmenslandschaft und die föderale Landschaft auf globaler Ebene so eng miteinander verflochten sind."

Im Krieg, so Watkin-Child, kann man die Cybersicherheit nicht nur innerhalb eines einzelnen Militärs betrachten. Wenn ein Verbündeter verwundbar ist, hat das direkte Auswirkungen auf die gesamte gemeinsame Operation. Der Schutz der Cybersicherheit für öffentliche – und private – Unternehmen ist nicht unterschiedlich. "Wenn amerikanische Waffensysteme nicht gehackt werden können, britische aber schon, ist es sinnlos, überhaupt einen Schutz zu haben", sagt er. "Es gibt einen Grund, warum der [US-]Präsident mit der NATO unter anderem über gemeinsame Cybersicherheitsstandards gesprochen hat. Das ist richtig, denn wenn eine Macht wie Russland den Unternehmenssektor nutzt, um beispielsweise Stromerzeuger anzugreifen, sind Wasser, Strom, Gas und Gesundheitsversorgung weg."

Solche potenziellen Folgen sind natürlich makroökonomischer Natur, aber es ist wichtig, auch die Folgen auf Unternehmensebene nicht außer Acht zu lassen. Und obwohl man angesichts der umfangreichen Listen von Elementen, die eine Aufnahme in die Cybersicherheitsoffenlegung rechtfertigen könnten, den Eindruck haben könnte, sind nicht alle Folgen negativ.

"Natürlich gibt es die rechtliche Seite der Offenlegung", sagt Watkin-Child, "aber wie es in den Vorschlägen heißt, erstatten Sie nicht nur der SEC Bericht. Sie erstatten allen Marktteilnehmern Bericht, die einen Einfluss auf Ihr Geschäft haben könnten. Die Anlegergemeinschaft, die Rating-Agenturen, die Versicherungsgesellschaften: Sie alle werden zusammen mit der SEC sehen, wie gut Sie es mit der Cybersicherheit meinen, oder eben nicht. Eine solche Transparenz birgt Risiken, aber sie ist auch eine Chance."

[16]. Gary Gensler, "Statement on Proposal for Mandatory Cybersecurity Disclosures," U.S. Securities and Exchange Commission (SEC), March 9, 2022, https://www.sec.gov/news/statement/gensler-cybersecurity-20220309.

Die Rolle der Internen Revision bleibt konsistent

Identifizieren, beurteilen, kommunizieren

Die Werkzeuge sind vorhanden

Der Sarbanes-Oxley Act von 2002 (SOX) brachte zusätzliche Verantwortlichkeiten mit sich und eröffnete der Internen Revision neue Möglichkeiten, einen Mehrwert für ihre Organisation zu schaffen. Als die Unternehmen die neuen Gesetze umsetzten, wurde die Interne Revision für viele zum Synonym für die Einhaltung des SOX. Aufgrund der Art der neuen SEC-Vorschläge besteht Grund zu der Annahme, dass dies auch im Bereich der Cybersicherheit geschehen könnte.

Auf den ersten Blick mag dies aufgrund der Komplexität des Themas Cybersicherheit zumindest kurzfristig als unmöglich erscheinen. Laut der Pulse-Umfrage[17] entfallen in börsennotierten Unternehmen durchschnittlich nur 9 % des Prüfungsplans auf die Cybersicherheit, was gegenüber den 7 % der letzten drei Jahre einen Anstieg darstellt, aber weit unter den 35 % liegt, die für die Finanzberichterstattung vorgesehen sind. Dafür gibt es mehrere Gründe, wie z. B. Budgetbeschränkungen, Mangel an ausreichenden Ressourcen und fehlende Kenntnisse oder Erfahrungen.

Der wirkliche Wert, den die Interne Revision bieten kann, liegt jedoch nicht unbedingt im Wissen über Cybersicherheit, sondern im Wissen über die Identifizierung von Risiken, die Kommunikation von Risiken und die Bewertung von Kontrollen zur Bewältigung von Risiken. In der Tat sind dies genau die Dinge, die die SEC-Vorschläge für ein bestimmtes Risiko hervorheben wollen.

"Es ist wichtig zu erkennen, dass es bei diesen Vorschlägen nicht wirklich um Cybersicherheit geht, sondern um das Risikomanagement im Bereich der Cybersicherheit", sagt Watkin-Child. "Wenn die Leute an Cybersicherheit denken, denken sie alle an die Implementierung von Kontrollen und das Reparieren von Dingen. Die SEC will aber etwas ganz anderes: Sie will, dass Unternehmen ihre Cybersicherheitsrisiken beurteilen. Sie wollen, dass die Boards der Unternehmen über die nötigen Governance-Strukturen verfügen, um ihr Cybersicherheit-Risikomanagementprogramm – in welcher Form auch immer – zu bewerten und die Beaufsichtigung sicherzustellen."

"Die SEC möchte, dass die Boards die Verantwortung für die Aufsicht übernehmen und den Rest absichern", sagt Manoj Satnaliwala, Chief Audit Executive von Caliber Home Loans, Inc. "Die Lücke liegt nicht wirklich bei den Cybersicherheitsstandards. Es gibt bereits Rahmenwerke, die Unternehmen als Leitfaden dienen, wie z. B. das NIST Cybersecurity Framework. Die wirkliche Lücke liegt in der Rechenschaftspflicht, die schnell zu einer Verantwortungsschaukel werden kann."

Die Rolle der Internen Revision kann dazu beitragen, diese Wippe ins Gleichgewicht zu bringen. "Boards und Management brauchen Hilfe. Die Interne Revision gewährleistet durch ihre Prüfung die Rechenschaft und fördert durch eine bessere Sichtbarkeit im gesamten Unternehmen die gemeinsame Verantwortung für Risiken", sagt Satnaliwala. "Das Risiko ist anders, aber die Rolle der Internen Revision bleibt gleich. Revisionsfunktionen müssen nicht neu anfangen, und es ist unvernünftig zu erwarten, dass sich jede Interne Revision mit den Feinheiten eines Cybersicherheitsprogramms befasst. Im Hinblick auf diese Herausforderung ist es nicht viel mehr als ein Blick auf die Vorschläge der SEC und die Frage nach deren Erwartungen. Solange zumindest einige Ressourcen für die Cybersicherheit vorhanden sind, glaube ich nicht, dass in der durchschnittlichen Internen Revision irgendwelche Änderungen erforderlich sind, außer der Anpassung der Ansätze, um eine angemessene Risikoabdeckung zu gewährleisten."

Der Zugang zu solchen Ressourcen im Bereich der Cybersicherheit ist jedoch oft leichter gesagt als getan. Der Aufbau eines gewissen Maßes an Fachwissen im Bereich Cybersicherheit durch Schulungen und Zertifizierungen geschieht nicht über Nacht, und insbesondere für kleine Interne Revisionen mit begrenzten Budgets für die Einstellung teurer, gefragter Talente sind die Möglichkeiten, eine über die prozessgesteuerte Einhaltung von Vorschriften hinausgehende Rolle zu übernehmen, begrenzt. In

[17]. The IIA, “2022 North American Pulse of Internal Audit”.

diesen Fällen muss die Interne Revision ein umfassendes Verständnis dafür haben, wo das Wissen am besten abgerufen werden kann. Dies kann sein:

- **Innerhalb der eigenen Talentbasis der Organisation.** Diejenigen, die Erfahrung in einer eher traditionellen IT-Revisionsfunktion haben, verfügen oft über die Wissensbasis, um technische Cybersicherheitsschulungen relativ schnell zu absolvieren. Darüber hinaus können bestimmte Cybersicherheitsgrundlagen in Bereiche wie Änderungsmanagement, Zugangskontrollen, IT-Betrieb und Notfallwiederherstellung integriert werden, was langfristig den Bedarf an Outsourcing verringern könnte.
- **Durch die Zusammenarbeit sowohl mit der zweiten Linie als auch mit vertrauenswürdigen externen Prüfungsfunktionen.** Unter Wahrung der Unabhängigkeit und Objektivität der Internen Revision in Übereinstimmung mit den *Internationalen Standards für die berufliche Praxis der Interne Revision* (IPPF) kann der Aufbau einer engeren Zusammenarbeit mit relevanten Funktionen wie der IT den Prüfern einen indirekten Zugang zu technischen Kompetenzen verschaffen, die andernfalls nur schwer oder zu hohen Kosten zu erhalten wären.

Schlussfolgerung

Zeit zur Vorbereitung

Das Thema Cybersicherheit entwickelt sich ständig weiter, da die bösartigen Akteure ihre Methoden immer wieder erneuern und die Unternehmen immer wieder neue Wege beschreiten, um sie zu bekämpfen. Da die Geschichte der Cybersicherheit weitergeschrieben wird, wird das Jahr 2022 für die Meilensteine in Erinnerung bleiben, die in dem Bemühen erreicht wurden, den schlimmen Trends in der Unternehmenslandschaft entgegenzuwirken. Obwohl die beide Vorschläge der SEC eine 60-tägige Konsultationsfrist durchlaufen müssen, bevor die Regeln offiziell werden, dürfte es für börsennotierte Unternehmen und ihre Internen Revisionen kaum Überraschungen geben.

Die Interne Revision kann und sollte die ihr zur Verfügung stehende Zeit nutzen, um sich einen Überblick über den gesamten Umfang der Vermögenswerte ihrer Organisation zu verschaffen, die in einer Cybersicherheitsstrategie berücksichtigt werden sollten, sofern dies noch nicht geschehen ist. Ohne dieses Wissen ist es für Revisorinnen und Revisoren schwierig zu beurteilen, ob die derzeitigen Kontrollen, Richtlinien und Governance-Strategien im Bereich der Cybersicherheit ausreichend sind. Solche Bewertungen sind nicht nur für die Sicherheit des Unternehmens wichtig, sondern für die gesamte Marktgemeinschaft. Die Welt wird von Tag zu Tag vernetzter, und das bedeutet, dass die Verantwortung für Risiken wie Cybersicherheit weitgehend geteilt wird. Schließlich hat die Geschichte immer wieder gezeigt, dass die Verletzung einer Organisation einen sehr realen Einfluss auf die Sicherheit einer anderen haben kann.

Eine Kette ist nur so stark wie ihr schwächstes Glied.

TEIL 2

Kritische Partner – Interne Revision und der CISO

Über die Experten

Jerry Perullo

Jerry Perullo ist der Gründer von Adversarial Risk Management, einer Firma für Cybersicherheits-Programmstrategie und -Governance, die es wachsenden Unternehmen ermöglicht, schnell ausgereifte Cybersicherheitsprogramme zu entwickeln. Vor der Gründung von Adversarial zog Perullo sich als Chief Information Security Officer von IntercontinentalExchange (NYSE:ICE) zurück, nachdem er 20 Jahre lang das Cybersicherheitsprogramm für eine globale Familie kritischer Wirtschaftsinfrastrukturen, darunter die New Yorker Börse, aufgebaut und geleitet hatte. Perullo, der als NACD-Direktor zertifiziert ist, war außerdem sechs Jahre lang im Board des Financial Services Information Sharing and Analysis Center (FS-ISAC) tätig, zuletzt als Vorsitzender. Perullo hält außerdem Vorlesungen am Georgia Institute of Technology, wo er als Professor für die Praxis an der School of Cybersecurity and Privacy tätig ist, und teilt seine Erfahrungen mit Führungskräften im Bereich Technologierisiken über seinen lifeafterCISO.com-Podcast.

Hassan NK Khayal, CIA, CRMA, CFE

Hassan NK Khayal ist ein Internal Audit Manager mit Sitz in Dubai. Hassan wurde vom Institute of Internal Auditors (IIA) als einer der 15 weltweit führenden Nachwuchskräfte unter 30 Jahren ausgezeichnet. Hassan Khayal besitzt einen BBA, einen MBA und ein Zertifikat in Nahoststudien. Hassan ist CIA, CRMA und CFE. Hassan verfügt außerdem über professionelle Zertifizierungen in den Bereichen Robotic Process Automation (RPA), Datenanalyse, Internet der Dinge (IoT), Qualitätsmanagement, Gesundheit und Sicherheit, Umweltmanagement und Risikomanagement.

Alan Maran

Alan ist Head of Internal Audit (CAE) bei Chewy, Inc. Er ist seit Januar 2019 für das Unternehmen tätig. In dieser Rolle ist er für die Überwachung der gesamten strategischen und ausführenden Aktivitäten der Internen Revision verantwortlich, einschließlich der Durchführung von agilen Unternehmensrisikobeurteilungen, der kontinuierlichen und zeitnahen Beratungsunterstützung für verschiedene Aktivitäten, die von der Geschäftsleitung gefördert werden, und der Prüfungssicherheit über die Angemessenheit der Kontrollen für die wichtigsten Risiken, die für das Unternehmen identifiziert wurden, der Abstimmung mit den Betriebsabläufen, Unternehmenssystemen und der IT-Governance, dem Risiko und der Compliance (GRC) im gesamten Unternehmen und der kontinuierlichen Fokussierung auf die Entwicklung der Mitglieder des Revisionsteams mit verstärktem Fokus auf Datenanalyse, Cybersicherheit und Datenschutz. Alan ist eine erfahrene Audit-Führungskraft mit mehr als 22 Jahren Erfahrung in den Bereichen eCommerce, Fintech, Technologie und Fertigungsunternehmen, die sich weiterhin leidenschaftlich für das Lernen interessiert. Bevor er zu Chewy kam, war er in verschiedenen Führungspositionen tätig, zunächst bei Ernst & Young, LLC, und dann in verschiedenen Positionen der Internen Revision in multinationalen Fortune-500-Unternehmen. Er hat einen MBA und einen Master in Finance von der Washington State University, ist Certified Fraud Examiner (CFE), Certified Blockchain Expert und Mitglied der lokalen Sektionen des Institute of Internal Auditors.

Srini Srinivasan, PMP, CBIP

Srini Srinivasan ist der Chief Information Security and Data Officer bei Chewy, Inc. Er ist seit Oktober 2019 für das Unternehmen tätig, als er als Head of Security, Data and Corporate Systems einstieg. In dieser Funktion ist er für die Überwachung der Informationssicherheit, die Verwaltung von Daten- und Analyseplattformen, Unternehmenssysteme und IT-Governance, Risiko und Compliance (GRC) im gesamten Unternehmen verantwortlich. Srini ist eine erfahrene Technologie-Führungskraft mit mehr als 25 Jahren Erfahrung in den Bereichen eCommerce, Bank- und Finanzdienstleistungen, Einzelhandel und Marketing. Bevor er zu Chewy kam, war er in Führungspositionen bei der Citizens Financial Group tätig. Er verfügt über einen Master-Abschluss in Informatik der Bharathidasan University und einen MBA der Bentley University.

Einführung

Partnerschaften im Bereich der Cybersicherheit sind entscheidend für den Erfolg

Cybersicherheit gehört nach wie vor zu den größten Risiken für alle Unternehmen. Umfragen zeigen immer wieder, dass Cyber-Kriminelle unablässig und dreist versuchen, sensible Daten zu hacken oder ungeschulte und ahnungslose Personen dazu zu verleiten, sensible Informationen preiszugeben oder böswilligen Akteuren Zugang zu gewähren.

So zeigt der Verizon Data Breach Investigations Report 2022, dass die Zahl der Ransomware-Verstöße im Jahr 2021 um erschreckende 13 % gestiegen ist – mehr als in den vergangenen fünf Jahren zusammen. Die erfolgreichsten Methoden für Ransomware-Angriffe bleiben dem Bericht zufolge jedoch gleich: Missbrauch von Desktop-Sharing- und Remote-Access-Software (40 %) und E-Mail (35 %).[18]

Der neue Leitfaden des IIA, Auditing Cybersecurity Operations: Prevention and Detection (GTAG), soll Organisationen helfen, die Sicherheit von Cybersicherheit-Operationen zu prüfen und zu priorisieren. Er soll Internen Revisorinnen und Revisoren helfen, Cybersicherheitsvorgänge zu definieren, ihre Komponenten zu identifizieren, relevante Kontrollrichtlinien in IT-Kontrollrahmen zu berücksichtigen und Ansätze zur Prüfung von Cybersicherheitsvorgängen zu verstehen.

Ein Schlüssel zur Verbesserung der Cybersicherheit, der in den Leitlinien nicht behandelt wird, ist eine gesunde Beziehung zwischen den Revisionsleitungen und den Chief Information Security Officers (CISOs). Diese potenziell symbiotische Beziehung kann dazu beitragen, die Interne Revision und die Informationssicherheit in Bezug auf Rahmenbedingungen, Risiken und Kontrollen aufeinander abzustimmen und gleichzeitig das steigende Risikoprofil im Bereich der Cybersicherheit zu managen.

In diesem Global Knowledge Brief werden die Vorteile einer engen Beziehung zwischen den Revisionsleitungen und ihren Kollegen aus dem Bereich der Informationssicherheit untersucht, Wege zum Aufbau und zur Pflege solcher Beziehungen bei gleichzeitiger Gewährleistung der Unabhängigkeit der Internen Revision aufgezeigt und beurteilt, wie diese Partnerschaften einen Mehrwert für das Unternehmen schaffen können.

[18]. "Takeaways From the 2022 Verizon Data Breach Investigations Report," J. Mack, Rapid7, May 31, 2022, https://www.rapid7.com/blog/post/2022/05/31/3-takeaways-from-the-2022-verizon-data-breach-investigations-report/.

Kollektive Cybersicherheit

Cyberrisiken erfordern einen unternehmensweiten Ansatz

Die Cybersicherheit ist nach wie vor ein wachsender und sich weiterentwickelnder Risikobereich, da die Machenschaften der Cyberkriminellen jedes Jahr raffinierter und zahlreicher werden. Es gibt keinen Mangel an Statistiken, die zeigen, dass Unternehmen weiterhin anfällig für Cyberangriffe sind. Gleichzeitig wächst der Druck auf Unternehmen aller Branchen, datengesteuerte Geschäftsstrategien einzuführen, die sich in hohem Maße auf die Erfassung, Verwaltung, Analyse und Nutzung von Daten stützen und gleichzeitig neue Technologien zur Verbesserung der Leistung und des Endergebnisses einsetzen.

Wie bei anderen bedeutenden Risikobereichen sollte auch das Cyberrisiko im gesamten Unternehmen verstanden und verwaltet werden. Laut dem Bericht "The State of Cyber Resilience" von Microsoft und dem Versicherungsmakler und Risikomanagementunternehmen Marsh verfolgen jedoch nur wenige Unternehmen einen unternehmensweiten Ansatz zur Verwaltung der Cybersicherheit. Auf der Grundlage einer Umfrage[19] unter mehr als 600 Entscheidungsträgern für Cyberrisiken ergab der Bericht, dass nur etwa 4 von 10 Unternehmen die Rechtsabteilung, die Unternehmensplanung, die Finanzabteilung, den Betrieb oder das Lieferkettenmanagement in die Planung von Cyberrisiken einbeziehen.[20]

"Eine Sache, die das Vertrauen bremst, ist die Tatsache, dass die meisten Unternehmen keinen unternehmensweiten Ansatz für Cyberrisiken gewählt haben, der im Kern auf eine breit angelegte Kommunikation abzielt und die Zusammenarbeit und den Abgleich zwischen den Beteiligten in den entscheidenden Momenten der Wahrheit auf ihrem Weg zur Cyberresilienz fördert", heißt es in dem Bericht.[21].

Zu den wichtigsten Risikotrends, die in dem Bericht genannt werden, gehört:

"Cyberspezifische unternehmensweite Ziele – einschließlich Cybersicherheitsmaßnahmen, Versicherungen, Daten und Analysen sowie Reaktionspläne auf Vorfälle – sollten auf den Aufbau von Cyberresilienz und nicht nur auf die Verhinderung von Vorfällen ausgerichtet sein, da jedes Unternehmen mit einem Cyberangriff rechnen muss."[22]

Um einen wirksamen unternehmensweiten Ansatz zu unterstützen, können die Revisionsleitungen einen wichtigen Beitrag leisten, indem sie Beziehungen zu den CISOs aufbauen und pflegen. Solche Beziehungen müssen auf gegenseitigem Verständnis, Zielen und Respekt beruhen.

Der erfahrene CISO und Gründer von Adversarial Risk Management, Jerry Perullo, der früher bei der NYSE-Muttergesellschaft Intercontinental Exchange (NYSE:ICE) tätig war, sagte, dass eine schlechte Kommunikation oder ein unklares Verständnis der Rollen von Informationssicherheit und Interner Revision die Abstimmung im Bereich Cybersicherheit beeinträchtigen kann. Eine gute Beziehung zwischen den Revisionsleitungen und der Informationssicherheit hingegen ermöglicht ein tieferes Verständnis der Ziele, der Strategie, der Abläufe und der Richtlinien, wodurch die Interne Revision – und damit auch ihre Ergebnisse und Empfehlungen – für die Verantwortlichen für Cyberrisiken, die Geschäftsleitung und das Board relevanter werden, sagte er. Darüber hinaus erweitert eine enge Beziehung zwischen der Internen Revision und den Informationssicherheitsteams das Wissen über die kritischen Aufgaben der beiden Bereiche und darüber, wie sie beide die allgemeine Cybersicherheit unterstützen.

"Letzten Endes will die Interne Revision etwas über Informationssicherheit lernen", sagte Perullo. "Es gibt viele Möglichkeiten, dies zu tun, aber es geht nichts über das Lernen vom (Informationssicherheits-)Team selbst."

Bei seiner Beratungstätigkeit mit Start-ups beginnt Perullo häufig mit der Einrichtung von Governance-Programmen für die Cybersicherheit. Dazu gehört in der Regel die Einrichtung eines funktionsübergreifenden Governance-Komitees für Cybersicherheit, dem Geschäftsleitung, Finanzabteilung, Rechtsabteilung und Informationssicherheit angehören können. Oft sind auch leitende Mitarbeiterinnen und Mitarbeiter der Internen Revision als Beobachter dabei, sagt er.

---

19. "2022 Marsh und Microsoft Cyber Risk Survey"
20. "The state of cyber resilience," Marsh Microsoft, 2022, https://www.marsh.com/us/services/cyber-risk/insights/the-state-of-cyber-resilience.html?utm_source=forbes&utm_medium=referral-link&utm_campaign=gl-cyber-risk-2022-the-state-of-cyber-resilience.
21. Ibid.
22. ibid.

Fünf Schlüssel zum Erfolg

Vorteile einer soliden Beziehung zwischen Interner Revision und CISO

Die Interne Revision und die CISOs sehen zahlreiche Vorteile einer gut durchdachten Partnerschaft. Die Details und die Ausgereiftheit solcher Partnerschaften können je nach Größe der Organisation, dem Grad der Regulierung in der jeweiligen Branche oder dem Risikoprofil einer Organisation im Bereich der Cybersicherheit variieren. Es gibt jedoch fünf Bereiche, in denen Zusammenarbeit und Kooperation unabhängig von der Größe des Unternehmens oder der Branche, in der es tätig ist, klare Vorteile bringen können.

Verständnis des Cyberrisikoprofils des Unternehmens und Abstimmung darauf

Ein Risikoprofil ist eine quantitative Analyse der Arten von Bedrohungen, denen eine Organisation ausgesetzt ist. Aus der Perspektive der Cybersicherheit identifiziert eine solche Analyse Vermögenswerte und Cyberrisiken, untersucht Richtlinien und Praktiken, die zur Bewältigung dieser Risiken entwickelt wurden, und bemüht sich um ein Verständnis der möglicherweise vorhandenen Schwachstellen. Das Verständnis des Cyberrisikoprofils durch die Interne Revision bietet eine Grundlage für die Erstellung eines Prüfungsplans, der nicht nur den Gesamtansatz der Organisation in Bezug auf die Cybersicherheit unterstützt, sondern auch die Relevanz und den Wert der Internen Revision in diesem wichtigen Bereich verbessern kann.

Alan Maran, Leiter der Internen Revision bei Chewy, Inc., hat in den drei Jahren seit dem Börsengang des Online-Händlers für Tiernahrung und andere Produkte für Haustiere eine enge Beziehung zum CISO des Unternehmens, Srini Srinivasan, aufgebaut. Srinivasan sagte, dass die Informationssicherheit mit der Internen Revision, der Rechtsabteilung und anderen Beteiligten zusammenarbeitete, um das Cyberrisikoprofil des Unternehmens auf der Grundlage des NIST Cybersecurity Framework umfassend zu bewerten und zu messen.

"Das ist unsere Ausgangsbasis", sagte Srinivasan. "Wir haben dann einen Drei-Jahres-Fahrplan für Cybersicherheit und Governance aufgestellt, den wir auf der Grundlage der von uns durchgeführten Bewertung des Cybersicherheitsrahmens angepasst und verbessert haben. Wir führen nun jedes Jahr eine Beurteilung durch, um zu sehen, ob wir in den Bereichen, in denen wir Chancen sehen, Verbesserungen erzielen, und um zu beurteilen, wie unsere Gesamtrisikobewertung ausfällt."

Dieser kooperative Ansatz, der die Interne Revision von Anfang an involviert hat, ermöglichte eine gemeinsame Strategie, die die Prüfungs- und Beratungsdienste der Internen Revision mit dem Ziel einbezieht, die allgemeine Cybersicherheitslage von Chewy kontinuierlich zu verbessern.

"Es geht nicht darum, zu sagen: Ich muss immer die IT und die Sicherheit prüfen. Wir müssen sie auch unterstützen", sagte Maran. "Von Seiten der Internen Revision sehen wir uns als Partner mit einer starken Mentalität zur Unterstützung von Srini und seinem Team bei der Entwicklung einer Gesamtstrategie."

Ein zusätzlicher Vorteil der Zusammenarbeit besteht darin, dass die Informationssicherheit und die unabhängige Prüfungssicherheit bereits in einem frühen Stadium in neue Projekte einbezogen werden. Mit anderen Worten: Informationssicherheit, Interne Revision und Governance-Kontrollen sind keine nachträglichen Überlegungen mehr, so Srinivasan.

"Wenn die Projektinitiativen in Gang kommen, beteiligen sich unsere beiden Teams und arbeiten mit den Ingenieur-, Produkt- und Unternehmensteams zusammen… Was sind die Sicherheitsüberlegungen? Befolgen wir die Best Practices?", so Srinivasan.

Dieser Ansatz hilft dabei, Cyberrisiken zu erkennen, zu minimieren und, wenn möglich, zu beseitigen, indem geeignete Prozesse und Kontrollen während der Projektentwicklung aufgebaut werden, so Srinivasan. "Wenn das Projekt in Betrieb geht, ist es für unsere beiden Teams sehr einfach, weil wir ein solides Verständnis haben. Wenn wir dann Kontrollberuteilungen der Revision, Zugriffsüberprüfungen oder Governance-Kontrollen durchführen, haben wir viel mehr Einblicke."

Verständnis der Rollen

Die von Maran und Srinivasan aufgebaute Beziehung wurde in hohem Maße dadurch begünstigt, dass Chewy ein relativ neues börsennotiertes Unternehmen war, was die Möglichkeit bot, die Beziehung von Grund auf zu gestalten. Dies schuf auch die Erwartung einer offenen und häufigen Kommunikation zwischen Maran, Srinivasan und ihren Teams.

"Es war ein idealer Weg, um diese Transparenz und das Vertrauen zwischen den wichtigsten Interessengruppen herzustellen, deshalb wollten wir diese Gelegenheit nicht verstreichen lassen", sagte Srinivasan.

Das heißt nicht, dass es nie Meinungsverschiedenheiten gibt. Aber wenn es doch zu Konflikten kommt, macht es die Beziehung einfacher, sie zu diskutieren und eine Lösung zu finden, die beiden Seiten dient, so Srinivasan.

"Es gibt für mich keinen Vorteil, wenn ich der Internen Revision etwas vorenthalte", sagte er. "Je mehr sie darüber wissen, was wir tun, desto größer ist ihre Wertschätzung. Auch aus der Sicht der Internen Revision kann ich Ihnen sagen, dass es meiner Meinung nach hier keine 'Schlupflöcher' gibt.“ Letztlich ermöglicht der kollaborative Ansatz ein agiles Vorgehen, bei dem die Interne Revision Teil eines Prozesses ist, in dem Mängel früher erkannt und behoben werden können, so Srinivasan.

Maran fügt hinzu, dass das offene Zusammenspiel das gegenseitige Rollenverständnis bekräftigt und stärkt. "Srini geht nicht davon aus, dass wir alles wissen, aber gleichzeitig respektiert er unsere Bedenken und unsere Sichtweise", sagte er.

Relevanz

Eine der größten Herausforderungen für die Interne Revision in allen Risikobereichen ist es, zum richtigen Zeitpunkt Erkenntnisse und Feststellungen zu kritischen Themen zu liefern, insbesondere aber im Bereich der Cybersicherheit. Dieses sich ständig weiterentwickelnde und schnelllebige Risiko verlangt, dass die Prüfung relevant und zeitnah erfolgt.

Perullo warnte davor, dass Aufträge der Internen Revision und damit verbundene Empfehlungen, die nicht auf die Cybersicherheitsmission des Unternehmens abgestimmt sind, mehr schaden als nützen können. Sie können innerhalb der Informationssicherheit Verwirrung darüber stiften, was die Interne Revision sehen will, insbesondere, wenn sie sich nicht sicher ist.

"Die Interne Revision hat anfangs vielleicht keine gute Vorstellung davon, was sie sehen will", sagte er. "Es ist besser, vor der Prüfung zusammenzuarbeiten und den Cyber-Governance-Prozess zu beobachten, um sicherzustellen, dass die Audits mit der Mission übereinstimmen.

Hassan Khayal, ein Berater für Interne Revision mit Fachkenntnissen im Bereich Cyber, sagte, dass dies ein Bereich sei, in dem die Interne Revision besonders anfällig für Kritik sei. Allzu oft weigern sich Revisorinnen und Revisoren unter dem Vorwand, die Unabhängigkeit der Internen Revision zu schützen, Mitglieder der IT- oder Informationssicherheitsteams kennenzulernen und mehr über dieses Thema zu erfahren.

"Bei meinen ersten Aufträgen sagte ich dem IT-Mitarbeiter schamlos: Ich bin vor allem hier, um von Ihnen zu lernen. Ich würde die Person mit Prozess- oder technischen Verständnis zu einem freundschaftlichen Gespräch beim Mittagessen mitnehmen, um zu erfahren, was diese Person im Detail macht."

Dieser Aufklärungsprozess hilft der Revisorin oder dem Revisor auch, den Reifegrad der Cybersicherheit des Unternehmens zu verstehen, was für die Erteilung relevanter Empfehlungen entscheidend ist, so Khayal.

"Wenn es sich um ein kleines bis mittelgroßes Unternehmen oder sogar eine größere Organisation handelt, die nicht börsennotiert ist, kann oder sollte man nur bestimmte Dinge tun", sagte er. "Ab einem bestimmten Punkt können die Empfehlungen zu aggressiv sein, sodass sie nicht realistisch sind."

Der Aufbau einer engen Beziehung zwischen der Internen Revision und den Informationssicherheitsteams verringert die Wahrscheinlichkeit irrelevanter oder fehlgeleiteter Prüfungsaufträge und Empfehlungen. Dieser Vorteil hat sich bei Chewy bestätigt.

"Alans Team und Alan selbst sind sehr gut damit vertraut, wie unsere allgemeine Sicherheitsstrategie aus technologischer Sicht aussieht, was wir in diesem Bereich tun und was einige unserer Hauptrisiken sind", sagte Srinivasan. "Wir haben also keine große Lücke zwischen den Risikobewertungen und unseren internen Fähigkeiten. Dies wird uns weiterhin dabei helfen, das Wissen unseres Teams oder unserer Teammitglieder bei Chewy sowie unseres Führungsteams insgesamt zu verbessern."

Kommunikation mit Board und Geschäftsleitung

Die Unternehmenskultur von Chewy bietet eine breitere Risikobetrachtung, die durch offene Gespräche unterstützt wird. Maran und Srinivasan haben die Aufgabe übernommen, die Stakeholder – Geschäftsleitung und Board – über ihre Zusammenarbeit und die daraus resultierenden Vorteile zu informieren.

"In vielen Unternehmen gibt es Leute, die einen isolierten Ansatz verfolgen. Nach dem Motto: Oh, es geht um IT-Sicherheit, also werden wir mit dem CISO sprechen, und der CISO wird sich darum kümmern. Aber im Rahmen eines integrierten Risikomanagements oder einer unternehmensweiten Risikomanagementperspektive kann jedes Risiko, das wir für das Unternehmen sehen, auf das gesamte Unternehmen zurückwirken", so Maran. "Ein Cyberangriff kann sich auf Ihre Abläufe, Ihre Ergebnisse und Ihre Finanzen auswirken. Srini hat auch gute Arbeit geleistet, indem er die Führungskräfte darüber informiert hat, was wir tun und welche Risiken wir mindern. In dieser Hinsicht war es also eine gute Zusammenarbeit."

Dies bedeutet auch, dass das Unternehmen rechtzeitig und flexibel auf sich ändernde Risiken und aufsichtsbehördliche Vorschriften im Cyberbereich reagieren kann. Maran und Srinivasan sind zum Beispiel zuversichtlich, dass das Unternehmen auf die vorgeschlagenen Cybersicherheit-Berichtsregeln der U.S. Securities and Exchange Commission des ersten Quartals 2022 reagieren kann.

Diese Zusammenarbeit geht auch über die Informationssicherheit und die Interne Revision hinaus. "Sie ist nicht auf die Sicherheit des Unternehmens beschränkt", sagte Srinivasan. "Wir haben andere wichtige Stakeholder, mit denen wir in ähnlicher Weise zusammenarbeiten, darunter das Buchhaltungsteam und das Team der Rechtsabteilung. Ich denke, dass wir durch den Aufbau dieser transparenten Beziehungen sehr gut gerüstet sind, wenn diese sich entwickelnden Vorschriften und zusätzlichen Anforderungen ins Spiel kommen."

Während die Führungsebene von Chewy von einer konsistenten und einheitlichen Kommunikation profitiert, warnt Khayal vor erheblichen Gefahren, wenn die Führungsebene nicht über den Status und die Bedürfnisse der Cybersicherheit im Unternehmen auf dem Laufenden gehalten wird. IT und Cybersicherheit können schnell als reine Kostenstellen betrachtet werden, wenn die Führungskräfte nicht darüber informiert und geschult sind, so Khayal. Wenn die Interne Revision sich scheut, die Informationssicherheit zu verstehen, ist es unwahrscheinlicher, dass sie wertvolle und relevante Sicherheit in diesem Bereich bietet, so Khayal. Und dies wirkt sich auf die Ansichten der Geschäftsleitung und des Boards zum Thema Cybersicherheit aus.

Wahrung und Achtung der Unabhängigkeit

Khayal, der sich auf seine CISA-Prüfung vorbereitet, sagte, dass sein Engagement für die Zertifizierung bereits seine Glaubwürdigkeit unter IT- und Informationssicherheitsexperten erhöht hat. Es hat ihm auch ermöglicht, mit diesen Mitarbeiterinnen und Mitarbeitern auf ihrem Niveau zu interagieren, was es wahrscheinlicher macht, dass sie Informationen preisgeben, die für einen Prüfer, der nur bei der Durchführung eines Prüfungsauftrags dabei ist, als zu fortgeschritten oder zu komplex angesehen werden könnten. Darüber hinaus sieht er diese Interaktion nicht als Bedrohung für seine Fähigkeit, einen unabhängigen und objektiven Prüfungsauftrag durchzuführen.

"Am Ende des Tages ist man am Arbeitsplatz", sagte er. "Wenn wir den Prüferinnen und Prüfern sagen, dass sie unabhängig sein sollen, meine ich persönlich nicht: Du darfst keine Freunde bei der Arbeit haben; du solltest immer alleine zum Mittagessen gehen."

Khayal sagte, er verfolge diesen Ansatz in allen Bereichen der Organisation. Er spricht über Linux mit dem Computerpersonal oder über soziale Medien mit dem Marketingpersonal.

"Es ist eine gute Gelegenheit, sich beruflich weiterzuentwickeln und gleichzeitig Beziehungen zu pflegen", sagte er. "Es ist so, wie wenn wir unseren Prüfungskunden sagen: Wir sehen uns den Prozess und die Transaktionen an, wir haben es nicht auf die Menschen abgesehen. Wenn man Leute zum Mittagessen einlädt, geht es nicht um den Prozess oder die Transaktion".

Bei Chewy unterstütze die enge Arbeitsbeziehung zwischen Maran und Srinivasan das gegenseitige Verständnis für die Notwendigkeit einer unabhängigen Überprüfung, sagte Maran.

"Es liegt in der Natur unseres Berufs zu vertrauen, aber zu überprüfen. Vom Standpunkt der Objektivität gesehen, bin ich dazu verpflichtet", sagte er. "Wir vertrauen also bis zu einem gewissen Grad, vor allem auf Dinge, die wir inkrementell getestet haben. In den meisten Fällen stellen wir fest, dass sich die Dinge nicht geändert haben. Aber ich prüfe auch weiterhin die Integrität der vom Management bereitgestellten Informationen. Wir sehen uns einen Bericht nicht nur für bare Münze an, sondern gehen zur Quelle zurück, um sicherzustellen, dass wir dieselben Ergebnisse erhalten wie sie, um zu gewährleisten, dass er vollständig und genau ist."

Letztendlich ist es einfacher, wenn man die Rolle des anderen in der Organisation versteht, so Maran.

"Es gibt hier eine Vereinbarung. Hier ist, was ich tun muss. Das ist die Prüfungssicherheit, die ich der Führungsebene – dem Board, den Interessengruppen und dem Audit Committee – geben muss", sagte er. "Wir stimmen uns über die Prüfungen ab, die wir im Laufe des Jahres durchführen werden. Wir stimmen uns über den Umfang ab. Ja, wir haben manchmal Diskussionen über unseren Standpunkt und die Sichtweise des anderen, aber in den Risikobereichen, in denen wir Prüfungssicherheit bieten müssen, sind wir uns selten uneinig.

Srinivasan fügt hinzu, dass die Konzentration auf einen datengesteuerten Ansatz für die Cybersicherheit voraussetzt, dass zwischen der Informationssicherheit und der Interne Revision Einigkeit über die Fakten besteht.

"Wenn es Meinungsverschiedenheiten gibt, müssen wir uns durcharbeiten und zu denselben Fakten kommen", sagte er. "Dann kann man ein gewisses Maß an Subjektivität zulassen und individuell sagen: Okay, ich halte das für mittelkritisch, hochkritisch oder niedrigkritisch. Ich denke, das führt zu einer gesunden Diskussion und zu einem gesunden Ergebnis, anstatt dass man sich die Köpfe einschlägt, ohne einen gemeinsamen Bezugsrahmen zu haben."

Mehrwert schaffen

Verbesserung der Cybersicherheitsresilienz

Srinivasan sagte, dass sein Ansatz von Anfang an darin bestand, der Mission von Chewy treu zu bleiben. Das bedeutete, drei Dinge zu erreichen: die internen Betriebsprinzipien des Unternehmens anzuwenden, die Abstimmung zwischen Informationssicherheit und interner Revision zu gewährleisten und durch Transparenz Vertrauen aufzubauen.

"Ich denke, wir haben einen weiten Weg zurückgelegt, und es zahlt sich wirklich aus, dass die Teammitglieder und die Führungskräfte sich gegenseitig auf dem Laufenden halten müssen", sagte er.

Wie bereits erwähnt, unterstützt das hohe Maß an Kommunikation, Zusammenarbeit und Kooperation einen agilen Ansatz, der die Interne Revision kontinuierlich in den Cybersicherheitsprozess einbezieht. Srinivasan weist darauf hin, dass wichtige Faktoren wie der zunehmende Fokus auf Nachhaltigkeit, Überlegungen zur Lieferkette, Marktbedingungen, geopolitische Entwicklungen und vieles mehr belastbare Ansätze für die Cybersicherheit und die damit verbundene Sicherheit erfordern.

"Ich denke, das zwingt uns dazu, wachsam und flink zu sein, schnell zu reagieren und relevant zu sein", sagte er. "Wenn wir einen klassischen Wasserfall-Ansatz mit längeren Vorlaufzeiten verfolgen, werden wir den Anschluss verpassen. Deshalb bin ich froh über das hohe Maß an Engagement, das wir haben."

Erweiterung des Wissens

Ein weiterer wesentlicher Vorteil der Partnerschaft besteht darin, dass beide Teams ihr Verständnis und ihre Wertschätzung für die Ansätze des jeweils anderen zur Erreichung desselben Ziels – der Gewährleistung der Cybersicherheit des Unternehmens – weiterentwickelt haben.

"Wir überprüfen immer gegenseitig unser technisches Wissen: Haben wir uns das angeschaut? Denkst du darüber nach? Hier ist mein Standpunkt zu dieser Risikoanalyse. Stimmt er auch mit deiner Sichtweise überein?'", sagte Maran. "Wir haben also von Anfang an darüber nachgedacht, wo wir suchen werden, und Srini nimmt an den Kickoff-Meetings teil. Er ist schon im Gespräch, bevor wir mit der Prüfung beginnen. Es gibt wirklich keine Überraschungen."

Der eigentliche Mehrwert ergibt sich jedoch aus der Zusammenarbeit, sobald die Prüfungsaufträge ausgeführt sind und die Interne Revision direkt mit dem IT- und Sicherheitspersonal zusammenarbeitet.

"Aus der Perspektive der Karriereentwicklung, insbesondere in den Bereichen IT und Cybersicherheit, ist es wirklich lohnend, denn man tut sehr viel mehr als nur Häkchen setzen und zu fragen: Haben Sie das getan?", sagte Maran. "Es geht um viel mehr. Es geht um Interpretation, es geht um technisches Fachwissen, das richtig angewendet werden muss, und ich denke, dass mein Team dabei viel lernt."

Schlussfolgerung

Eine gesunde Beziehung zwischen der Internen Revision und der Informationssicherheit bietet dem Unternehmen zahlreiche Vorteile, vor allem bei der Abstimmung und dem Verständnis des Cyberrisikoprofils des Unternehmens – von Schwachstellen und Chancen bis hin zu Reifegrad und Penetrationstests.

Darüber hinaus kann eine solide Beziehung die Resilienz und Flexibilität erhöhen, wenn das Unternehmen auf Cybervorfälle, Änderungen bei den Faktoren, die die Cybersicherheit beeinflussen, oder die sich entwickelnde regulatorische Landschaft reagieren muss. Sie trägt dazu bei, der Geschäftsleitung und dem Board eine konsistente und einheitliche Botschaft über Risiken, Bedürfnisse, Prioritäten und den Zustand der Cybersicherheit zu übermitteln. Die Unabhängigkeit der Internen Revision kann erfolgreich geschützt und sogar verbessert werden, wenn beide Seiten ein tieferes Verständnis und eine größere Wertschätzung der Rollen, Ansätze und Pflichten entwickeln. Letztendlich kann eine solide Beziehung zwischen den Leitungen der Internen Revision und den CISOs die IT-Sicherheit stärken, indem sie einen unternehmensweiten Ansatz zur Cybersicherheit unterstützt.

"Die Denkweise ändert sich von der einfachen Prüfung (Ich muss hingehen, beurteilen und aussagekräftige Feststellungen treffen.) hin zu der Aussage: Das ist mein Unternehmen, das ist mir wirklich wichtig, und so werde ich diesem Team helfen, erfolgreich zu sein", so Maran.

TEIL 3

Reaktion auf Cybervorfälle und Wiederherstellung

Über die Experten

Brian Tremblay

Brian Tremblay leitet Compliance Practice bei Onapsis, wo er dafür verantwortlich ist, Kunden dabei zu helfen, die Herausforderungen und Chancen zu verstehen und zu bewältigen, die durch die zunehmende Überschneidung von Compliance, Cybersicherheit und Geschäftskontinuität im Zusammenhang mit allgemeinen IT-Kontrollen und regulatorischen und Compliance-Angelegenheiten wie Sarbanes-Oxley (SOX) und der Datenschutzgrundverordnung (GDPR) entstehen. Vor seiner Tätigkeit bei Onapsis war er CAE beim Hightech-Halbleiterunternehmen Acacia Communications. Neben der Gründung und Leitung aller Aktivitäten der Internen Revision half er bei der Vorbereitung des Unternehmens auf den Börsengang (einschließlich der Implementierung von SOX) und erleichterte die Implementierung von Enterprise Risk Management (ERM). Zuvor war Tremblay Direktor der Internen Revision bei Iron Mountain und beaufsichtigte alle Prüfungen und Projekte in Nordamerika sowie die Zusammenarbeit mit den globalen Qualitätsmanagern. Davor baute er als Senior Manager bei Houghton Mifflin Harcourt eine Abteilung für Interne Revision auf und führte eine SOX-Implementierung durch. In seiner früheren Laufbahn war er bei Raytheon und Deloitte tätig.

DaMon Ross Sr.

Im Jahr 2020 gründete DaMon Ross Sr. Cyber Defense International, wo er und sein Team Elite-Cybersicherheitsoperationen und Fähigkeiten zur Aufklärung von Cyberbedrohungen einsetzen, um erschwingliche Cybersicherheitslösungen und -dienstleistungen für Organisationen bereitzustellen, die nicht über die Mittel verfügen, diese Fähigkeiten selbst aufzubauen. Bevor er Cyber Defense International gründete, war Ross als Senior Vice President für Cybersicherheitsoperationen bei der SunTrust Bank tätig. In dieser Funktion war er mit dem Aufbau des 24/7/365-Cybersicherheitsbetriebszentrums von SunTrust beauftragt. Ross baute Ros Teams auf, die sich auf die Bereiche Cyber Intelligence, Überwachung von Cyberbedrohungen, Reaktion auf Cybervorfälle und Cyberkriminalität spezialisierten. Darüber hinaus arbeitete er erfolgreich mit Partnern aus den Bereichen Recht, Personalwesen, Unternehmenssicherheit sowie Unternehmensethik und -risiko zusammen, um das erste Programm zur Überwachung von Insider-Bedrohungen in der Bank zu etablieren. Ross förderte auch den Aufbau zahlreicher Partnerschaften zum Informationsaustausch, darunter mit der United States Secret Service Electronic Crimes Task Force und dem Department of Homeland Security.

Einführung

Zurück zu den Grundlagen

XXX **Die Cybersicherheit ist seit langem ein wichtiges Thema** für Unternehmen und ihre Interne Revisionsfunktionen, und mit der Einführung der neuen Vorschläge der Securities and Exchange Commission (SEC) zu Risikomanagement, Strategie, Governance und Offenlegung von Vorfällen im Bereich der Cybersicherheit war das Jahr 2022 keine Ausnahme. Der Anstoß für diese und andere Regulierungsvorschläge ist gerechtfertigt. Einem Bericht des Identity Theft Resource Center zufolge wurden im Jahr 2021 1.862 öffentlichkeitswirksame Datenschutzverletzungen registriert, eine Zahl, die die Gesamtzahl des Jahres 2020 um 68 % übertrifft und auch den Rekord aus dem Jahr 2017 übertrifft. Keine Branche ist von diesem Trend verschont geblieben.[23]

In diesem Umfeld wünschen sich Unternehmen klare, robuste Cybersicherheit-Kontrollen und -Prozesse, die auf zentralen Grundlagen aufbauen. Dazu gehören kontinuierliches Lernen über das Risiko und die damit verbundenen Vorschriften sowie die Kommunikation und Abstimmung zwischen Vorstand, Management und interner Revision. Teil 1 Teil 1 der dreiteiligen Serie Cybersicherheit in 2022 des IIA konzentriert sich auf die potenziellen Auswirkungen von Vorschriften, während Teil 2 die Vorteile einer symbiotischen Beziehung zwischen Chief Information Security Officers (CISOs) und ihren Kollegen aus der Interne Revision untersucht. In diesem letzten Teil geht es um die Entwicklung und Umsetzung der Strategie eines Unternehmens zur Reaktion auf Cybervorfälle und insbesondere um die Frage, wo die Interne Revision bei der Bewertung der Kontrollen, die für eine rasche Wiederherstellung nach einem Verstoß gegen die Cybersicherheit entscheidend sind, einen organisatorischen Mehrwert bieten kann.

[23]. Identify Theft Resource Center, "Identify Theft Resource Center's 2021 Annual Data Breach Report Sets New Record for Number of Compromises," January 24, 2022, https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises/.

Schlüsselkontrollen

Stärkung der Rolle der Interne Revision bei der Reaktion auf Cyberrisiken

Der Irrtum der Reaktion auf Vorfälle

Obwohl die Begriffe "Reaktion auf Cybervorfälle" und "Reaktion und Wiederherstellung im Bereich der Cybersicherheit" zutreffende und nützliche Definitionen **sind**, implizieren sie auch eine etwas unvollständige Vorstellung davon, was solche Pläne benötigen, um wirksam zu sein.

Die Interne Revision hat die wichtigste Aufgabe, den Unternehmen unabhängige Sicherheit für das Risikomanagement zu bieten. Dazu gehört nicht nur die Gewährleistung einer angemessenen Reaktion auf Cyber-Vorfälle, sondern auch die ordnungsgemäße Bewertung von Kontrollen, um sicherzustellen, dass das Risiko und seine Auswirkungen gemindert oder im Idealfall verhindert werden. Um einen solch hohen Standard für ein bestimmtes Risiko zu erreichen, sollte die Aufmerksamkeit nicht nur auf die Reaktion auf ein Risiko gerichtet sein. Stattdessen ist es effektiver, die Reaktion auf Cybervorfälle ganzheitlich und zyklisch zu betrachten, wobei sowohl präventiven Kontrollen als auch aktiven Reaktionsmaßnahmen Priorität eingeräumt wird.

"Das Risikomanagement ist wie ein Rad", sagt Brian Tremblay, Leiter der Compliance-Praxis bei Onapsis, Inc. "Am Anfang des Rades haben wir die richtigen Kontrollen, und die Prozesse sind so, wie sie unserer Meinung nach sein sollten. Wenn dann etwas passiert, stellt sich sofort die Frage: Haben die Kontrollen wie erwartet funktioniert, und ist das, was wir erwartet haben, auch eingetreten? Daraus lernen wir dann, was wir ändern müssen, und der Kreislauf beginnt von neuem. Wenn Sie nur im Nachhinein auf ein Ereignis reagieren, gehen Sie wahrscheinlich ineffizient mit Ihrer Zeit und Ihren Ressourcen um. Die Gegenwart und die Zukunft sollten gleichwertig berücksichtigt werden, denn wir bauen nicht nur das Unternehmen von heute auf, sondern auch das Unternehmen der Zukunft. Da Unternehmen so oft damit zu kämpfen haben, ist dies ein wirklich wichtiger Punkt, auf den sich die Interne Revision konzentrieren sollte. "

Unveränderte Grundlagen

Risiken werden selten weniger komplex, und da die Cybersicherheit von Natur aus hochtechnisch ist, ist die Lernkurve zum Verständnis sowohl des Risikos selbst als auch der zur Risikominderung erforderlichen Systeme mit jedem weiteren technologischen Fortschritt nur noch steiler geworden. Dies bedeutet jedoch nicht zwangsläufig, dass sich die grundlegende Struktur eines Reaktionsplans für Cybervorfälle und die darin enthaltenen Kontrollen drastisch ändern.

Diese Kontrollen werden in der neuesten ergänzenden Anleitung des IIA, *Auditing Cyber Incident Response and Recovery*, beschrieben und können in vier übergeordnete Geschäftsziele eingeteilt werden:

- **Planung der Reaktion auf einen Zwischenfall.** Es sollten Richtlinien und Verfahren festgelegt werden, anhand derer festgestellt werden kann, ob ein Zwischenfall eingetreten ist und wie darauf zu reagieren ist. Die Planung sollte die wichtigsten Beteiligten einbeziehen, Rollen und Verantwortlichkeiten festlegen und gegebenenfalls getestet werden, um das Bewusstsein und die Ausführung zu fördern.
- **Identifizierung von Vorfällen.** Prozesse zur Analyse von Daten aus detektivischen Kontrollen führen zur Feststellung des Vorliegens eines Cybervorfalls, der in der Regel der Auslöser für die Durchführung eines oder mehrerer Reaktionspläne ist.
- **Kommunikation.** Bei Cybervorfällen gibt es viele potenzielle Beteiligte, daher sollte jeder Reaktionsplan eine Kommunikationsstrategie für eine angemessene und rechtzeitige Benachrichtigung über die Auswirkungen und die Lösungsbemühungen enthalten.

- **Technische Reaktion und Wiederherstellung.** Die Art des Vorfalls bestimmt weitgehend die erforderlichen technischen Sanierungs- und Wiederherstellungskontrollen, die häufig eine Koordinierung der internen und externen Bemühungen erfordern.[24]

Die Erreichung dieser Geschäftsziele und die Einhaltung eines etablierten Rahmens für die Reaktion auf Cybervorfälle, wie z. B. des National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity, erfordert technisches Wissen in Bezug auf die Implementierung, Wartung und Verbesserung, das Informationssicherheits- und Informationstechnologie-Teams bereitstellen können - Wissen, das interne Revisionsteams möglicherweise nicht besitzen. Auf ist jedoch gleichzeitig viel Platz für andere, weniger technische, aber ebenso wertvolle Disziplinen, die einen wichtigen Beitrag leisten können. Die Interne Revision ist mit ihrem einzigartigen Zugang zu und ihrem Verständnis von organisatorischen Funktionen in allen Abteilungen sowie ihrer unabhängigen Perspektive, die für die Bereitstellung objektiver Sicherheit entscheidend ist, genau so eine Disziplin.

"Aus Sicht der Interne Revision unterscheidet sich der Ansatz zur Reaktion auf Cybervorfälle nicht von anderen Risiken, da der Schwerpunkt auf dem eigentlichen Prozess und dem Ergebnis dieses Prozesses liegt", so DaMon Ross Sr. "Selbst bei der technischen Natur der Materialien wird jeder interne Prüfer, der es gewohnt ist, in einem Prozessbereich zu arbeiten, ziemlich schnell erkennen, worauf es ankommt. "

Ein solcher Prozess ähnelt mehr als nur dem, was die Interne Revision in den Programmen zur Einhaltung des Sarbanes-Oxley-Gesetzes (SOX), in den Krisenreaktionsplänen oder in jeder etablierten Risikomanagementstrategie sehen kann. "Verschiedene Organisationen haben unterschiedliche Terminologien, aber ein Plan für Cybervorfälle ist im Wesentlichen eine Richtlinie, die festlegt, wann ein Cybervorfall eintritt, welche Rollen und Verantwortlichkeiten alle betroffenen Parteien haben und wer bei der Entscheidungsfindung mit am Tisch sitzen muss", so Ross.

Tremblay äußerte eine ähnliche Meinung. Kontrollen, die sich auf Cyber-Risiken beziehen, sind auch Teil von Rahmenwerken, die für das Management von Compliance-Risiken im Zusammenhang mit Sarbanes-Oxley verwendet werden, sagte er.

Einer der ersten Schritte, die Hacker unternehmen, wenn sie in eine Technologie eindringen, besteht darin, sich die erforderlichen Rechte und Privilegien zu verschaffen, um ihr Ziel zu erreichen. Im großen Schema der Risiken fällt dies unter das Risiko des unbefugten Zugriffs. Es macht keinen Unterschied, ob es sich um ein SOX- oder ein Cyber-Risiko handelt, so Tremblay. "Die Risiken, wenn man sie auf ihre einfachsten Formen herunterbricht, und die Kontrollen zur Minderung dieser Risiken sind im Wesentlichen identisch. "

Kontrollen der Dokumentation

Wie Tremblay erwähnte, gibt es bei den Kontrollen, die in einer solchen Richtlinie enthalten sind, auch erhebliche Überschneidungen mit den Kontrollen, die bei anderen organisatorischen Risiken durchgeführt werden. Ein Beispiel ist ein effektiver Dokumentationsprozess. Ross stimmt dem zu. Unternehmen müssen verstehen, wie Arbeitsabläufe aussehen, die Cyber-Vorfälle ordnungsgemäß dokumentieren, und wie all die parallel laufenden Teile zusammenwirken, sagte er.

"Das gilt nicht nur für große Vorfälle. Jede Organisation sollte über eine Funktion verfügen, die sich täglich damit befasst. Nehmen wir an, auf einem Computer befindet sich Malware. Solche kleinen Vorfälle können sich zu größeren Ereignissen auswachsen, und im schlimmsten Fall hilft eine ordnungsgemäße Dokumentation, um zu verstehen, wie es zur Eskalation kam. Diese Funktion ist eine Kontrolle in sich selbst. "

Erkennung und Kontrolle der physischen Infrastruktur

Eine weitere kritische Kontrolle, die unter die Rubrik der Risiken durch unbefugten Zugriff fällt, ist die physische Infrastruktur. Auch wenn man beim Thema Cybersicherheit nicht sofort an solche Kontrollen denkt, war der unbefugte Zugriff auf Festplatten oder Server, auf denen sensible Daten gespeichert sind, im Jahr 2020 für 10 % aller böswilligen Sicherheitsverletzungen verantwortlich, die Unternehmen im Durchschnitt 4,36 Millionen US-Dollar pro Sicherheitsverletzung kosteten, so eine Studie des Ponemon Institute, die von IBM Security veröffentlicht wurde.

[24]. The IIA, *Auditing Cyber Incident Response and Recovery*, Supplemental Guidance, Practice Guide, https://www.theiia.org/globalassets/documents/content/articles/guidance/gtag/2022/gtag_auditing_cyber_incident_response_and_recovery_final.pdf.

Eine solche Infrastruktur kann sichere Serverräume mit eingeschränktem Zugang sowie einfachere Sicherheitsmaßnahmen wie verschlossene Türen in den Einrichtungen umfassen. Die Sicherheit der Infrastruktur ist zwar wichtig, aber noch wichtiger ist es, über Kontrollen zu verfügen, um potenziell verdächtige Aktivitäten zu erkennen und zu dokumentieren.

"Wenn ich von physischer Infrastruktur spreche, meine ich nicht so sehr verschlossene Türen, sondern vielmehr die Sicherstellung, dass es eine Benachrichtigung und Dokumentation der Aktion gibt, die das eigentliche Risiko darstellt. Das ist wie der Hauptgang einer Mahlzeit und nicht die Vorspeise", sagte Tremblay.

Die Identifizierung und Überprüfung solcher Systeme fällt genau in den Kompetenzbereich der Interne Revision", so Ross und fügte hinzu: "Die Interne Revision ist in der Lage, Systeme zu identifizieren, die besonders risikoreich oder kritisch für die Existenz der Organisation sind. Es ist sogar wahrscheinlich, dass die Interne Revision diese Systeme bereits identifiziert hat, um die Einhaltung von Bundesgesetzen und -vorschriften in Bezug auf andere Risiken zu gewährleisten. Alles, was nötig ist, ist, dieses Denken zu erweitern, um neue Arten der Bereitstellung einzubeziehen, die einen erhöhten Zugang bieten können. "

Angleichung der Einziehungserwartungen

Eine wirksame Dokumentation in allen Phasen eines Reaktionsplans auf Cybervorfälle ist von entscheidender Bedeutung. Ebenso wichtig ist jedoch die Kommunikation der Daten, die diese Dokumentation liefert, und die Abstimmung der Erwartungen der Organisation an die Erkennung und Wiederherstellung.

Laut Tremblay ist dies eine der größten Lücken, die er in den Cyber-Response-Plänen von Unternehmen festgestellt hat - und wo die Interne Revision den größten Nutzen bieten kann. "Die Rolle der Interne Revision bei der Wiederherstellung von Cyber-Katastrophen ist eine doppelte", sagte er. "Erstens: Sicherstellen, dass der Vorfall existiert, und dass Sie ihn durch Dokumentation oder durch die von Ihnen verwendete Technologie oder den Prozess nachweisen können. Zweitens, und das wird meines Erachtens nicht oft genug getan, muss man sich mit allen wichtigen Beteiligten zusammensetzen, um einen realistischen Zeitplan für die Wiederherstellung auf der Grundlage der Risikobereitschaft des Unternehmens festzulegen. "

Der Zeitplan, so Tremblay, wird vom "Eigentümer" der fraglichen Anwendung im Unternehmen festgelegt, also dem CISO, dem Leiter der Lieferkette oder einer anderen Führungskraft, je nachdem, wo der Vorfall auftritt. Der Schlüssel für die Interne Revision liegt darin, als Bindeglied zwischen dieser Partei und allen anderen Parteien zu fungieren, die für ihre täglichen Aufgaben von dieser Anwendung abhängig sind.

"Der CISO kann zum Beispiel sagen, dass eine Wiederherstellungszeit von 48 Stunden akzeptabel ist, aber wenn man sich nicht an den CFO oder andere Führungskräfte oder Funktionen wendet, die darauf angewiesen sind, dass die Technologie wieder funktioniert, und deren Meinung einholt, kann es zu einem Chaos kommen", so Tremblay. "Der CFO kann zum Beispiel sagen, dass 48 Stunden in Ordnung sind, aber nur, wenn wir die Bücher nicht abschließen. Wenn wir aber die Bücher abschließen, ist keine Ausfallzeit akzeptabel, weil das Unternehmen dann eine Fristverlängerung beantragen müsste, was auf den öffentlichen Märkten sehr schlecht aussehen würde. "

Bei solchen Gesprächen muss sich nicht unbedingt eine Partei über die andere hinwegsetzen. Vielmehr kann die Interne Revision durch eine solche Kommunikation einen Konsens im Einklang mit der Risikobereitschaft des Unternehmens herbeiführen. "In Fällen, in denen eine Diskrepanz besteht", so Tremblay, "kann die Interne Revision fragen: 'Lohnt es sich wirklich, dass das passiert? Der CEO könnte sagen: 'Ja, das ist es, denn es wird eine Million Dollar kosten, dieses Problem zu lösen. ' Was wir wirklich tun, ist sicherzustellen, dass der Plan wirklich um die Interessengruppen und die Technologie herum entwickelt wurde. "

Er fährt fort: "Ich denke, das ist ein Bereich, in dem wir als Berufsgruppe nicht besonders gut sind. Ich glaube, wir versuchen, bestimmte Dinge zu validieren, ohne wirklich zu sagen: 'Hey, im Rahmen der Überprüfung der Kontrollen im Zusammenhang mit der Reaktion auf Vorfälle haben wir eine Lücke in den Anforderungen der Beteiligten an bestimmte Technologien festgestellt. ' Das ist sehr berechtigt. Damit wird ein zuvor nicht erkanntes Geschäftsrisiko identifiziert, das für das Unternehmen wertvoll ist. "

Funktionsübergreifende Zusammenarbeit

Es ist ein weit verbreiteter Irrglaube, dass der CISO und das Sicherheitsteam die Hauptverantwortung für die Cybersicherheitsmaßnahmen tragen. Dies ist nur teilweise richtig. Obwohl die Erfahrung und das Fachwissen, die für die Umsetzung der eher technischen Aspekte einer Cyberstrategie erforderlich sind, höchstwahrscheinlich in dieser Abteilung zu finden sind, ist es gefährlich anzunehmen, dass die Abteilung die Bandbreite - oder den Wunsch - hat, die Last allein zu schultern.

"Die Reaktion auf Cybervorfälle ist ein funktionsübergreifender Prozess, zumindest sollte sie das sein", so Ross. "Der Hauptgrund für Verzögerungen bei den Reaktionszeiten in Unternehmen liegt meiner Meinung nach nicht an den Kenntnissen der Abteilung für Informationssicherheit selbst, sondern an der Festlegung von funktionsübergreifenden Rollen und Verantwortlichkeiten mit Abteilungen, die nicht primär für die Sicherheit zuständig sind. Sie haben andere Dinge zu tun. "

Ross zufolge sollte die Korrektur dieses Missverständnisses und die Förderung des Gedankens der gemeinsamen Verantwortung aller Beteiligten ein Hauptschwerpunkt der internen Revision sein. "Der Schwerpunkt muss nicht unbedingt auf dem Sicherheitsteam liegen und auf dem, was es tut, sondern vielmehr darauf, wie sein Prozess von anderen Stellen im Unternehmen, die daran beteiligt sind, unterstützt wird. Das Sicherheitsteam weiß, was es zu tun hat, aber es kann die IT-Teams und Back-End-Entwickler nicht zwingen, in entscheidender Weise zu helfen. Es ist viel Organisationspolitik im Spiel, und als ich in dieser Position war, habe ich in der Interne Revision einen wertvollen Partner gefunden. Sicherheitsteams können diese Kämpfe nicht allein ausfechten. Wenn eine einigermaßen neutrale Partei dabei helfen kann, die Lücken im Unternehmen zu identifizieren, ist das für alle hilfreich. "

Eine nützliche Strategie, um diese Lücken aufzuzeigen und die Rollen zu klären, besteht laut Ross darin, dass die Interne Revision - in der Regel in Zusammenarbeit mit einem externen Berater - Tischsimulationen durchführt. "Sobald Sie Ihren Plan für die Reaktion auf Cybervorfälle an einem Ort haben, an dem er getestet werden kann, bringt eine Tabletop-Simulation den CIO, den CISO, die IT-Führungskräfte, den CEO, die Interne Revision - also alle relevanten Interessengruppen - in einem Konferenzraum oder per Zoom-Anruf zusammen, um ein plausibles Szenario durchzuspielen. Auch ohne technisches Fachwissen kann die Interne Revision die Diskussion erleichtern, indem sie fragt, wer welche Aufgaben hat, und bewertet, wie diese Verantwortlichkeiten mit der Realität übereinstimmen. Sie könnten sagen: "Zu diesem Zeitpunkt sollte Ihr Team X und Y gemäß unserem Plan ausführen, aber in Wirklichkeit könnten Sie Z tun. Die meisten Unternehmen müssen diese Prüfungen mindestens einmal im Jahr durchführen, aber die Interne Revision sollte diese Aufgabe wirklich übernehmen. "

Schlussfolgerung

Mit dem Risikoumfeld mitwachsen

Die Interne Revision verdient aufgrund ihrer einzigartigen Stellung im Unternehmen einen Platz am Tisch, wenn es um die Reaktionspläne eines Unternehmens auf Cybervorfälle geht. Dieser Erfolg entbindet die Interne Revision jedoch nicht von ihrem Streben nach einer tieferen Erforschung und einem besseren Verständnis der Cybersicherheit. In einer Zukunft, in der physische Infrastrukturen schnell zugunsten von Cloud-basierten Technologien aufgegeben werden, wird von der Interne Revision unweigerlich mehr Fachwissen verlangt und erwartet.

"Als ich meine Laufbahn in der Interne Revision begann, war eines der Hauptargumente, dass es sich um eine sehr allgemein gehaltene Aufgabe handelt", so Tremblay. "Man bekam viel zu sehen und lernte viel über viele Dinge, für die man kein Experte sein musste. Aber die Technologie hat sich so stark verändert, dass ich mich langsam frage, ob die Tage des Generalisten in der Interne Revision nicht gezählt sind. Vielleicht wird die Interne Revision stattdessen eines Tages mehr zu einem Fachexperten (SME) für Dinge, die von Natur aus kritisch für Unternehmen sind. Anstelle von Prüfungsteams, die aus 8-10 Betriebs-, Compliance- und Jahresabschlussprüfern bestehen, werden Unternehmen dann einen Cybersicherheitsprüfer, einen ESG-Prüfer usw. haben. "

Ross stimmt dem zu. "Wie soll man bei neuen Technologien die Lücken im Reaktionsprozess wirklich verstehen, wenn man nicht so tief eindringen kann? Das würde man nie wirklich können. "

Mit dem vorhandenen Wissen und den vorhandenen Ressourcen kann viel erreicht werden, aber es steht eine aufregende und radikal neue Zukunft bevor. Die Interne Revision muss ein Teil davon sein.

Frühere Ausgaben

Frühere Ausgaben von Global Perspectives and Insights finden Sie unter www.theiia.org/GPI.

Feedback der Leser

Senden Sie Fragen oder Kommentare an globalperspectives@theiia.org.

Über die IIA

Das Institute of Internal Auditors (IIA) ist ein internationaler Berufsverband, der weltweit mehr als 215.000 Mitglieder betreut und 180.000 Zertifizierungen zum Certified Internal Auditor (CIA) vergeben hat. Das IIA wurde 1941 gegründet und ist weltweit als führend in den Bereichen Normen, Zertifizierung, Ausbildung, Forschung und technische Anleitung für den Berufsstand der Innenrevisoren anerkannt. Weitere Informationen finden Sie unter theiia.org.

Haftungsausschluss

Urheberrecht

August 2022

The Institute of Internal Auditors

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101