GLOBAL PERSPECTIVES & INSIGHTS

Keamanan Siber Pada Tahun 2022

BAGIAN 1: Bagaimana Usulan Perubahan Peraturan SEC (Stock Exchange Committee) Baru Dapat Mengubah Permainan

BAGIAN 2: Mitra Penting – Audit Internal dan CISO

BAGIAN 3: Respons dan Pemulihan Insiden Siber

The Institute of Internal Auditors

CONTENT

BAGIAN 1:

Bagaimana Usulan Perubahan Peraturan SEC (Stock Exchange Committee) Baru Dapat Mengubah Permainan

Tentang Para Ahli

Andy Watkin-Child

Watkin-Child merupakan praktisi veteran dengan 20 tahun pengalaman di bidang keamanan siber, teknologi dan manajemen risiko, dan mitra pendiri The Augusta Group, sebuah perusahaan yang menyediakan solusi untuk manajemen, pengawasan, dan assurance terhadap keamanan dan risiko siber. Ia memegang posisi pimpinan internasional pada lini pertahanan pertama dan kedua atas kemanan siber, manajemen risiko siber, risiko operasional, dan teknologi, yang bekerja dengan tim *leadership* pada perusahaan – perusahaan dengan nilai neraca lebih dari €1 triliun, yang tersebar di industri rekayasa dan manufaktur, layanan finansial, publishing, dan media. Ia berpengalaman sebagai anggota Direksi, tim leadership risiko global, dan komite kemanan siber, risiko operasional, dan GDPR.

Manoj Satnaliwala

Satnaliwala merupakan Chied Audit executive dan SVP Audit Internal dari Caliber Home Loans dan bertanggung jawab atas seluruh aktivitas audit, serta bekerja langsung dengan komite audit. Sebelum di posisinya saat ini, ia memimpin fungsi audit pada Radian Group Inc., sebuah perusahaan terbuka di bidang asuransi hipotek terbesar ketiga dan menjadi Direktur Audit Internal di PwC, dimana ia mengelola proses validasi pengendalian untuk Audit Internal sebagai bagian dari proyek CCAR untuk perusahaan holding perbankan besar.

Pengantar

Usulan peraturan baru dapat memiliki implikasi yang besar

Dalam siklus pemberitaan di tahun 2022, dan faktanya selama beberapa tahun belakangan ini, kita melihat sedikit hal positif, dan ancaman siber terus membayangi, bercampur dengan krisis Ukraina, ancaman COVID-19 yang berkepanjangan, dan meningkatnya tensi antara Amerika Serikat dan China. Secara bersama-sama, variabel–variabel ini dikombinasikan dengan faktor-faktor lainnya telah memberikan tempat yang signifikan – dan tentunya yang utama – bagi isu kemanan siber, dalam peta risiko auditor internal.

Namun demikian, tahun 2022 juga menjadi tahun munculnya banyak perkembangan terkait dengan kemanan siber yang pasti akan berdampak luas bagi organisasi, membutuhkan upaya yang lebih untuk dapat memahaminya, dan implikasinya akan memakan waktu untuk dapat benar – benar dimengerti. Di antara perkembangan - perkembangan tersebut, yang paling signifikan adalah dua usulan peraturan dari Securities and Exchange Commission (SEC) Amerika Serikat. Secara khusus, usulan yang kedua layak untuk dicermati karena akan mewajibkan perusahaan – perusahaan terbuka yang beroperasi di Amerika Serikat untuk menyajikan informasi mengenai kebijakan, prosedur, dan strategi tata kelola terkait dengan kemanan siber, dan juga pengalaman serta pengetahuan Dewan Komisaris dan Direksi – jika ada – terhadap dunia kemanan siber. Jika diterapkan (yang kemungkinan besar akan diterapkan dalam suatu bentuk tertentu), perusahaan-perusahaan terbuka, tidak memandang jenis industri maupun ukuran organisasinya, akan masuk dalam lingkup peraturan baru tersebut. Tanpa melebih – lebihkan, perkembangan ini menunjukkan babak baru dunia kemanan siber dan sebuah topik yang baru bagi komunitas audit internal, yang akan memainkan peran yang kritikal dalam menavigasi perusahaannya melalui tantangan ini.

Walaupun hal ini bukan tantangan yang dapat dianggap enteng, audit internal untungnya memahami alat dan keahlian yang dibutuhkan untuk memberikan keyakinan atas area risiko yang terus berkembang ini. Bagian pertama dari tiga bagian seri kemanan siber pada Global Knowledge Brief yang diterbitkan oleh IIA, menyajikan sebuah gambaran umum atas usulan SEC yang baru, mencakup implikasinya terhadap peraturan atas pelaporan kemanan siber baik di Amerika Serikat maupun di negara lainnya. Usulan SEC tersebut juga mengeksplorasi bagaimana auditor internal dapat memiliki peran penting dalam membantu organisasi dalam mengelola perubahan tatanan kepatuhan yang akan tercipta akibat regulasi baru tersebut.

Menyiapkan Panggung

Keamanan siber mendominasi tatanan risiko

Risiko utama di zaman kita

Di tahun 2022, **keamanan siber tetap menjadi hal yang terpenting** pada setiap tingkatan di seluruh organisasi dan di seluruh industri, dan kekhawatiran tersebut terefleksikan secara jelas dalam data dari *2022 North American Pulse of Internal Audit* (*Pulse*)[1] yang diterbitkan oleh IIA. Saat diminta untuk memberikan rating terhadap tingkat risiko dari organisasinya, para pimpinan audit internal menempatkan risiko terkait dengan teknologi ke dalam tiga risiko teratas – kemanan siber, Teknologi Informasi (TI), dan hubungan dengan pihak ketiga (yang seringkali mencakup jasa TI). Bahkan diantara tiga risiko utama tersebut, kemanan siber dengan mudahnya menempati posisi teratas, dengan 85% responden memberikan rating risiko tinggi atau sangat tinggi, lebih tinggi 24% daripada rating untuk TI, yang menempati posisi risiko tertinggi kedua

Kekhawatiran tersebut dapat dibenarkan. Di tahun 2021, hampir setiap jenis serangan siber telah meningkat dengan tingkat yang mengkhawatirkan. Berdasarkan *2022 SonicWall Cyber Threat Report*[2], jumlah ancaman terenkripsi menanjak 167% (10,4 juta serangan), *ransomware* meningkat 105% (623,3 juta serangan), *cryptojacking* (serangan pada komputer untuk menambang *cryptocurrency*) meningkat 19% (97,1 juta serangan), percobaan intrusi meningkat 11% (5,3 juta serangan), dan malware yang ditujukan ke Internet Untuk Segala (IoT) meningkat 6% (60,1 juta serangan).

Terlebih lagi, semua serangan-serangan ini membawa biaya yang signifikan atas kerugian yang ditimbulkan. Total biaya per tahun dari serangan-serangan siber diperkirakan mencapai $10,5 triliun pada tahun 2025, dengan rata-rata peningkatan sebesar 15% dari tahun ke tahun, menurut versi terbaru dari 2022 Cybersecurity Almanac[3] yang diterbitkan Cisco/Cybersecurity Ventures.

Dan hal ini bahkan belum mempertimbangkan perubahan dramatis atas tatanan geopolitik yang berdampak pada keamanan siber. Bahkan sebelum invasi Rusia atas Ukraina, terdapat banyak bukti yang menunjukkan bahwa dugaan serangan siber yang disponsori negara, dengan tingkat kerumitan tinggi, telah meningkat baik dari frekuensi maupun dampaknya. Serangan ke sistem SolarWind di Texas, yang dilakukan oleh kelompok peretas yang menurut laporan[4] diarahkan oleh Foreign Intelligence Service Rusia, telah melihat infrastruktur digital hingga 18,000 pelanggan[5] – termasuk Microsoft, Cisco, Intel, Deloitte, beberapa bagian dari Pentagon, Department of Homeland Security, Department of Energy, dan National Nuclear Security Administration Amerika Serikat – berhasil ditembus dan tidak terdeteksi selama berbulan-bulan.

Di tahun 2021, serangan besar lainnya yang disponsori suatu negara terhadap perusahaan Amerika Serikat terjadi pada Colonial Pipeline Co.[6] Serangan tersebut secara temporer mengganggu hampir setengah aliran bensin dan persediaan bahan bakar jet ke Pantai Timur Amerika Serikat. Pada akhirnya, Colonial Pipeline Co membayar tebusan sebesar $5 juta kepada kelompok peretas DarkSide untuk memulihkan jaringan dan mengembalikan data yang diretas.

---

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. 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/.

Titik henti (*breaking point*) geopolitik

Sejak serangan-serangan ini, kekhawatiran terhadap Rusia terus meningkat, dan mencapai puncaknya dengan invasi ke Ukraina. Tentu saja, agresi Rusia ke Ukraina termasuk perang siber – sebuah serangan berskala besar terhadap jaringan listrik[7] Ukraina – selain perang tradisional, dan terdapat kekhawatiran yang meningkat bahwa Rusia dapat membalas beragam sanksi ekonomi yang ditetapkan oleh NATO dan Amerika Serikat. Hanya dalam satu minggu sebelum pergerakan resmi Rusia ke Ukraina, Cybersecurity and Infrastructure Security Agency (CISA) Amerika Serikat menerbitkan pernyataan "*Naikkan Perisai*[8]" yang jarang diterbitkan, yang memperingatkan seluruh perusahaan-perusahaan Amerika Serikat, untuk menerapkan keamanan siber dan perlindungan aset kritikal, dengan tingkat yang lebih tinggi. Dalam pernyataan[9] CISA di bulan Maret 2022 yang menilai ancaman siber Rusia, CISA menulis "Saran-saran terkini yang dipublikasi oleh CISA dan sumber-sumber rahasia lainnya menunjukkan bahwa aktor-aktor ancaman yang disponsori negara Rusia sedang menargetkan industri-industri dan organisasi-organisasi berikut di Amerika Serikat dan negara barat lainnya: riset COVID-19, pemerintah, organisasi pemilihan, kesehatan dan obat-obatan, pertahanan, energi, video game, nuklir, fasilitas komersial, air, penerbangan, dan manufaktur kritikal."

Di bulan Mei 2021, Presiden Biden menandatangani sebuah executive order[10] yang dirancang untuk meningkatkan keamanan nasional di Amerika serikat. Perintah tersebut secara spesifik menyebutkan perlunya agensi-agensi pemerintahan untuk mereviu dan mengembangkan pedoman dan standar baru untuk keamanan siber, dan agar organisasi-organisasi fokus untuk meningkatkan keamanan rantai pasokan perangkat lunak dan penyebaran informasi ancaman. Baru-baru ini, Presiden Amerika Serikat juga menerbitkan sebuah pernyataan yang menekankan kembali ancaman keamanan siber dari Rusia dan menyorot panduan[11] CISA yang terus berkembang atas persoalan tersebut.

Rusia bukan satu-satunya aktor negara yang dituduh mendukung serangan-serangan siber yang menimbulkan ketidakstabilan. Menurut laporan[12] di tahun 2021 dari Evanina group, Cina telah menjadi semakin agresif pada siber, khususnya terkait dengan akuisisi data terhadap informasi personal dan privasi data.

"Kemampuan Cina untuk mendapatkan Kekayaan Intelektual dan Rahasia dagang kita secara holistik dengan menggunakan metode yang illegal, legal, dan metode campuran yang rumit tidak seperti yang pernah kita saksikan sebelumnya," kata William Evanina, mantan Direktur National Counterintelligence and Security Center.

Evanina merujuk pada berbagai insiden siber yang terhubung dengan Partai Komunis Cina, termasuk serangan siber Equifax di tahun 2017; kampanye empat warga negara Cina di tahun 2011 – 2018 untuk meretas lusinan perusahaan, universitas, dan entitas pemerintah; dan kampanye siber yang disponsori negara di tahun 2011 – 2013 yang menyerang perusahaan penyalur minyak dan gas alam Amerika serikat (Department of Justice Amerika Serikat merilis sebuah laporan atas insiden ini di bulan juli 2021). Ia juga merujuk pada sebuah laporan di bulan Juli 2021 dari National Security Agency (NSA), Federal Bureau of Investigation (FBI), and CISA yang merilis lebih dari 50 taktik siber dan alat yang digunakan oleh peretas Cina yang disponsori negara, terhadap Amerika Serikat.

Dalam lingkungan siber yang kompleks dan umumnya berbahaya ini, yang mana SEC telah mengambil langkah historis untuk menekankan kesiapan dan kesehatan siber pada tatanan organisasi, khususnya terkait dengan pelaporan kepada SEC dan (pada kasus-kasus tertentu) kepada publik. Langkah-langkah ini merupakan yang pertama kali diterapkan dan dapat memiliki implikasi yang signifikan tidak hanya kepada perusahaan-perusahaan publik Amerika Serikat namun juga perusahaan-perusahaan di seluruh dunia.

---

[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.

Perubahan Besar

Langkah pertama yang bersejarah terhadap pengungkapan insiden siber

Usulan

Dalam rentang waktu dua bulan, SEC mengungkapkan dua usulan yang sudah lama ditunggu-tunggu atas keamanan siber di sektor bisnis. Usulan pertama[13], yang diungkapkan di bulan Februari 2022, fokus pada perusahaan jasa konsultan investasi beregister, perusahaan investasi beregister, dan perusahaan pengembangan bisnis atau pengelola dana. Dalam peraturan yang diusulkan, perusahaan jasa konsultan dan pengelola dana akan diwajibkan untuk:

- Menerapkan kebijakan dan prosedur keamanan siber tertulis yang dirancang untuk merespon risiko-risiko siber yang dapat merugikan para klien dan investor.
- Melaporkan insiden-insiden signifikan yang mempengaruhi perusahaan jasa konsultan atau klien dari pengelola dana publik atau privat, kepada SEC dalam format baru yang rahasia.
- Mengungkapkan kepada publik risiko siber dan insiden keamanan siber signifikan yang terjadi sepanjang dua tahun belakangan dalam brosur dan pernyataan registrasi.

Sebagai tambahan, usulan tersebut akan menetapkan persyaratan baru bagi para perusahaan jasa konsultan dan pengelola dana dalam menyimpan catatan yang dirancang untuk meningkatkan ketersediaan informasi terkait dengan kemanan siber, dan juga membantu memfasilitasi kemampuan SEC dalam melakukan inspeksi dan penegakan peraturan.

“Risiko siber berhubungan dengan ketiga bagian misi SEC, dan secara khusus berhubungan dengan tujuan kami untuk melindungi investor dan menjaga stabilitas pasar.” Kata Ketua SEC Gary Gensler dalam sebuah konferensi pers[14]. “Usulan peraturan dan perubahannya dirancang untuk meningkatkan kesiapan terhadap serangan keamanan siber dan dapat menaikkan kepercayaan diri investor atas ketahanan para perusahaan jasa konsultan dan pengelola dana terhadap ancaman dan serangan keamanan siber.”

Sementara peraturan-peraturan ini secara implisit mencerminkan ekspektasi SEC atas bagaimana entitas seharusnya mengelola risiko kemanan siber dan melaporkan insiden keamanan siber, Usulan yang kedua membuat ekspektasi-ekspektasi tersebut menjadi eksplisit, Usulan kedua[15], yang ditujukan kepada semua perusahaan terbuka dan diterbitkan di bulan Maret 2022, ingin “meningkatkan dan menstandarisasi pengungkapan informasi terkait dengan manajemen risiko, strategi, dan tata kelola keamanan siber, serta pelaporan insiden keamanan siber oleh perusahaan terbuka yang masuk ke dalam lingkup persyaratan pelaporan dalam Securities Exchange Act tahun 1934.” Untuk menjalankan hal tersebut, peraturan baru tersebut akan mengharuskan perusahan-perusahaan terbuka untuk mengungkapkan:

- Kebijakan dan prosedur perusahaan untuk mengidentifikasi dan mengelola risiko kemanan siber. Peraturan tersebut mencakup daftar yang ekstensif namun tidak secara komprehensif, yang berisi strategi manajemen risiko, kebijakan, dan prosedur yang dapat mengungkapkan:
    - Apakah perusahaan memiliki program penilaian risiko kemaanan siber
    - Apakah perusahaan melibatkan para penilai, konsultan, auditor, atau pihak ketiga lainnya sehubungan dengan program penilaian risiko kemanan siber

[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.

- Apakah perusahaan memiliki kebijakan dan prosedur untuk mengawasi dan mengidentifikasi risiko-risiko keamanan siber yang terkoneksi dengan program penilaian risiko kemanan siber
- Apakah perusahaan melakukan aktifitas untuk mencegah, mendeteksi, dan meminimalisir dampak dari insiden kemanan siber.
- Apakah perusahaan memiliki rencana keberlangsungan, kontigensi, dan pemulihan bisnis dari kejadian insiden keamanan siber.
- Apakah insiden keamanan siber sebelumnya telah memberikan informasi kepada perusahaan untuk merubah tata Kelola, kebijakan dan prosedur, atau teknologi
- Apakah risiko-risiko dan insiden terkait kemanan siber telah mempengaruhi atau kemungkinan besar mempengaruhi kondisi operasional dan finansial perusahaan

- Peran manajemen dalam menerapkan kebijakan dan prosedur kemanan siber, termasuk;
  - Apakah terdapat komite atau posisi manajemen tertentu yang bertanggung jawab untuk mengukur dan mengelola risiko keamanan siber
  - Apakah perusahan telah menunjuk Chief Information Security Officer atau seseorang dengan posisi yang setara.
  - Apakah komite atau pihak yang ditunjuk tersebut telah mengetahui proses-proses di perusahaan dan memonitor pencegahan, mitigasi, deteksi, dan remediasi atas insiden keamanan siber
  - Apakah komite atau pihak yang ditunjuk tersebut melaporkan ke Dewan Komisaris/Direksi atau komite Dewan Komisaris/Direksi atas risiko-risiko keamanan siber, dan juga seberapa sering mereka melaporkan.
  - Apakah seluruh Dewan Komisaris/Direksi, direktur tertentu, atau dewan komite bertanggung jawab atas pengawasan risiko kemanan siber
  - Apakah Dewan Komisaris/Direksi terinformasikan mengenai risiko kemanan siber dan frekuensi dilakukannya diskusi-diskusi membahas risiko-risiko tersebut.
  - Apakah dan Bagaimana Dewan Komisaris/Direksi atau dewan komite mempertimbangkan risiko kemanan siber sebagai bagian dari strategi bisnis, manajemen risiko, dan pengawasan finansial.

- Keahlian Dewan Komisaris/Direksi, jika ada, dan pengawasannya atas risiko kemanan siber, yang mencakup informasi:
  - Apakah Dewan Komisaris/Direksi memiliki pengalaman kerja di bidang kemanaan siber
  - Apakah Dewan Komisaris/Direksi memiliki sertifikasi atau gelar terkait dengan kemanan siber
  - Apakah Dewan Komisaris/Direksi memiliki pengetahuan, skill, atau latar belakang terkait dengan keamanan siber

Sebagai tambahan, usulan tersebut mengikutsertakan perubahan atas *form* 8-K, yang akan mewajibkan perusahaan-perusahaan terbuka untuk mengungkapkan insiden-insiden keamanan siber dalam waktu 4 hari kerja, sebagaimana mereka juga diharuskan untuk menginformasikan hal-hal lainnya yang di luar rencana. Pengungkapan ini termasuk:

- Kapan insiden diketahui dan apakah saat ini sedang terjadi
- Deskripsi singkat atas sifat dan lingkup insiden
- Apakah ada data yang dicuri, diubah, diakses, atau digunakan untuk tujuan lain yang tidak diperbolehkan
- Dampak insiden terhadap operasional perusahaan
- Apakah perusahaan telah memperbaiki atau saat ini sedang proses memperbaiki insiden tersebut

Pengungkapan ini, menurut SEC, akan memberikan investor informasi yang "konsisten, dapat dibandingkan, dan berguna untuk pengambilan keputusan". "Saat ini, kemanan siber merupakan risiko yang terus berkembang di mana perusahaan terbuka harus dapat terus bersaing." Kata Gensler[16]. "Keterhubungan dari jaringan kita, penggunaan data analisis prediktif, dan hasrat yang tinggi atas data hanya akan terus bertambah cepat, menempatkan akun-akun finansial, investasi, dan informasi pribadi kita dalam risiko. Investor ingin lebih mengetahui mengenai bagaimana perusahaan terbuka mengelola risiko-risiko yang terus berkembang tersebut."

Sejarah Penting

Dalam banyak hal, struktur dari preaturan-peraturan ini mirip dengan peraturan SEC lainnya terkait dengan kewajiban pengungkapan informasi mengenai kondisi keuangan dan hasil operasional (Sarbanes-Oxley), informasi orang dalam (insider), dan kekuatan, kelemahan, peluang, dan ancaman organisasi. Namun demikian, mengambil langkah tambahan dalam mengelevasi risiko kemanan siber sampai pada titik tertentu yang mewajibkan pengungkapan informasi, belum pernah terjadi sebelumnya.

"AS mungkin menjadi negara pertama, dan saya katakan satu-satunya negara di dunia yang meregulasi keamanan siber," kata Andy Watkin-Child, mitra pendiri the Augusta Group dan Parava Security Solutions, serta pendiri Cybersecurity Maturity Model Certification Europe (CMMC Europe). "Perusahan-perusahaan di Amerika Serikat mungkin familiar dengan General Data Protection Regulation (GDPR) yang diterbitkan Europe Union, dan mungkin akan menggabungkan kedua Usulan ini menjadi satu, tetapi proteksi data dan keamanan siber merupakan dua paradigma yang berbeda. Ada sebuah perbedaan besar, dan selain Financial Management Regulation dari Department of Defense (DoD) Amerika Serikat – yang mana menyebabkan kontraktor asing bahkan juga diinvestigasi oleh Department of Justice Amerika Serikat atas kelemahan kemanan siber – tidak ada yang seperti ini di dunia kemanan siber."

Watkin-Child juga menjelaskan pentingnya peraturan baru ini dapat memiliki efek riak yang kuat ke negara-negara lainnya. Krisis ukraina telah membuktikan bahwa keamanan siber merupakan senjata, dan NATO telah mempertimbangkannya sebagai suatu bentuk derajat operasi, sejak tahun 2016," katanya. "Keamanan siber merupakan sebuah alat yang ofensif di samping senjata nuklir. Permasalahannya adalah karena itu merupakan domain operasi, dan memberikan ancaman besar bagi infrastruktur nasional. Usulan SEC berdampak pada pemain besar lebih dulu – perusahaan jual beli – namun saya meyakini bahwa ini semoga akan menurun ke organisasi-organisasi diluar pengaruh SEC karena tatanan bisnis, dan juga tatanan federal, sangat saling terkait pada tingkat global."

Dalam kondisi perang, kata Watkin-Child, seseorang tidak dapat mempertimbangkan keamanan siber dalam satu militer saja; jika salah satu sekutu mengalami kerentanan, maka itu akan berdampak langsung pada keseluruhan operasi gabungan. Perlindungan keamanan siber untuk perusahaan publik – dan privat – tidak berbeda. "Jika sistem senjata Amerika tidak dapat diretas sementara sistem negara Inggris dapat diretas, tidak ada gunanya memiliki perlindungan," ungkapnya. "Ada alasannya presiden Amerika Serikat telah berbicara dengan NATO mengenai standar keamanan siber umum. Ini merupakan tindakan yang tepat, karena jika sebuah entitas seperti Rusia menggunakan sektor bisnis untuk menyerang pembangkit listrik, contohnya, air, listrik, gas, dan layanan kesehatan anda – semuanya sirna."

Potensi konsekuensi tersebut tentu saja bersifat makro, namun penting untuk juga tidak merendahkan konsekuensi pada tingkat organisasi. Meskipun kita melihat daftar yang ekstensif atas elemen-elemen yang dapat memastikan pengungkapan kemanan siber, tidak semua konsekuensi adalah negatif.

"Tentu saja, ada sisi legal dari pengungkapan-pengungkapan tersebut," kata Watkin-Child, "Namun, seperti yang dikatakan dalam usulan, anda tidak hanya melapor ke SEC. Anda juga melapor ke seluruh partisipan pasar yang mungkin memiliki pengaruh ke bisnis anda. Komunitas investasi, Lembaga pemeringkat kredit, perusahaan asuransi – mereka semua bersama dengan SEC akan melihat seberapa baik tidaknya anda dalam keamanan siber. Transparansi tersebut memiliki risiko, tetapi juga membawa peluang."

[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.

Peran Audit Internal Tetap Konsisten

Mengidentifikasi, Menilai, Mengkomunikasikan

Peralatannya telah ada

Sarbanes-Oxley Act tahun 2022 (SOX) memberi tanggung jawab tambahan dan membuka peluang baru bagi fungsi audit internal untuk memberikan nilai tambah bagi organisasi mereka. Tentunya, saat organisasi menyesuaikan dengan peraturan baru tersebut, banyak audit internal yang dianggap sinonim dengan kepatuhan terhadap SOX. Oleh karena sifat dasar dari usulan baru SEC tersebut, hal yang sama dapat terjadi di dalam dunia keamanan siber.

Awalnya, hal ini terlihat setidaknya sangat mustahil dalam jangka pendek, karena sifat dasar dari dunia kemanan siber yang kompleks. Menurut responden dari Pulse survey[17], secara rata-rata kemanan siber dialokasikan dalam rencana audit hanya sebesar 9% pada perusahaan terbuka, meningkat dari sebesar 7% pada tiga tahun sebelumnya namun jauh dibawah alokasi untuk pelaporan keuangan sebesar 35%. Ada beberapa alasan mengapa hal ini terjadi, seperti anggaran yang terbatas, tidak adanya sumber daya yang cukup, dan kurangnya pengalaman atau pengetahuan.

Nilai sebenarnya yang dapat dibawa oleh audit internal, tidak hanya melalui pengetahuan atas keamanan siber, namun juga pengetahuan mengenai identifikasi risiko, komunikasi risiko, dan evaluasi pengendalian untuk merespon risiko. Tentunya, hal inilah yang ingin ditekankan oleh Usulan SEC untuk satu risiko yang spesifik.

“Penting untuk disadari bahwa usulan-usulan ini tidak benar-benar tentang keamanan siber, namun tentang manajemen risiko keamanan siber,” kata Watkin-Child. “Saat orang-orang berfikir tentang keamanan siber, mereka semua berfikir tentang menerapkan pengendalian dan memperbaiki sesuatu. Apa yang ingin dicari oleh SEC adalah sesuatu yang benar-benar berbeda; mereka ingin melihat organisasi untuk menilai risiko keamanan siber. Mereka ingin Dewan Komisaris/Direksi di organisasi-organisasi untuk memiliki struktur tata kelola untuk mengevaluasi dan meyakinkan adanya pengawasan terhadap program manajemen risiko kemaanan siber, entah dalam bentuk apapun.”

“Apa yang SEC inginkan adalah melihat Dewan Komisaris/Direksi mengambil tanggung jawab untuk mengawasi dan meyakini sisanya,” kata Manoj Satnaliwala, chief audit executive dari Caliber Home Loans, Inc. “celahnya bukan pada standar keamanan siber – ada kerangka-kerangka untuk memandu organisasi, seperti contohnya NIST Cybersecurity Framework. Celah yang sebenarnya adalah pada akuntabilitas, yang tanggung jawabnya dengan cepat dapat menjadi naik turun seperti jungkat jungkit.

Peran audit internal dapat membantu untuk membawa keseimbangan terhadap jungkat jungkit tersebut. “Dewan Komisaris/Direksi dan manajemen, mereka butuh bantuan. Audit internal melalui jasa asurans memastikan akuntabilitas dan, melalui visibilitas yang ditingkatkan di seluruh organisasi, mempromosikan kepemilikan bersama terhadap risiko.” Kata Satnaliwala. “Risiko tersebut berbeda, namun peran audit internal tetap konsisten. Fungsi audit tidak harus dimulai dari awal, dan tidak realistis jika berharap setiap fungsi audit internal untuk memahami seluk beluk program kemanan siber, namun terhadap tantangan ini, lebih dari sekedar melihat usulan SEC dan bertanya, ‘Apa yang diekspektasikan oleh SEC?’ Selama setidaknya tersedia beberapa sumber daya untuk keamanan siber, saya kira secara rata-rata fungsi audit internal tidak perlu diubah, selain merubah pendekatan untuk memastikan risiko telah tercakup secara memadai.”

Namun demikian, memiliki akses sumber daya kemanan siber seringkali mudah dikatakan namun sulit untuk dilakukan. Mengembangkan keahlian keamanan siber pada tingkatan apapun melalui pelatihan dan sertifikasi tidak akan terjadi seketika, dan bagi fungsi audit internal kecil dengan anggaran yang terbatas untuk merekrut talenta yang mahal dan sangat diminati, opsi untuk menjalankan peran apapun selain kepatuhan yang berbasis proses, sangat terbatas. Dalam kasus ini, audit internal harus memiliki pemahaman yang komprehensif mengenai di mana mereka dapat mengakses pengetahuan tersebut. Hal ini dapat melalui:

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

- **Di dalam basis talenta organisasi.** Mereka yang memiliki pengalaman audit TI yang lebih tradisional seringkali memiliki basis pengetahuan untuk menyelesaikan pelatihan teknis keamanan siber relatif cepat. Sebagai tambahan, fundamental keamanan siber tertentu dapat diterapkan pada area tertentu seperti manajemen perubahan, pengendalian akses, operasional TI, dan pemulihan bencana, yang dapat mengurangi kebutuhan untuk alih daya untuk jangka panjang
- **Melalui kolaborasi dengan lini kedua dan fungsi audit eksterdal yang dipercaya.** Sementara independensi dan obyektifitas audit internal harus dipertahankan sesuai dengan *International Standards for the Professional Practice of Internal Auditing* (IPPF), menerapkan hubungan kerja yang lebih kolaboratif dengan fungsi-fungsi lain yang relevan seperti TI dapat memberikan auditor akses secara tidak langsung terhadap kompetensi teknis yang sulit atau mahal untuk diperoleh.

Kesimpulan

Waktunya untuk bersiap

Kemanan siber, sebagai sebuah topik, terus berkembang sebagaimana para pelaku kejahatan terus menginovasi pendekatan mereka dan perusahaan terus berinovasi untuk menghalau mereka. Namun demikian, sejarah keamanan siber terus tercatat, tahun 2022 menjadi tahun yang akan diingat akan tonggak pencapaian terhadap upaya untuk melawan tren yang mengerikan di seluruh tatanan bisnis. Walaupun usulan SEC masih harus melewati periode 60 hari untuk mengumpulkan komentar sebelum diterbitkan secara resmi, akan ada sedikit kejutan bagi perusahaan-perusahaan terbuka dan fungsi audit internal mereka.

Audit internal dapat dan seharusnya menggunakan waktu yang ada, jika belum melakukan, untuk melihat secara menyeluruh aset-aset organisasi yang seharusnya dapat diperhitungkan untuk menerapkan strategi kemanan siber. Tanpa pengetahuan tersebut, auditor internal akan sulit untuk menilai kecukupan pengendalian yang ada saat ini, kebijakan, dan strategi tata kelola yang terkait dengan siber Penilaian tersebut tidak hanya penting bagi kemanan organisasi, namun tentunya juga untuk seluruh komunitas pasar. Setiap hari, dunia ini menjadi semakin saling terkoneksi, dan ini berarti tanggung jawab terkait risiko seperti kemanan siber sebagian besar dibagikan. Pada akhirnya, sejarah menunjukkan bahwa, penembusan keamanan atas suatu organisasi dapat memiliki dampak yang nyata bagi keamanan organisasi yang lain.

Sebuah rantai hanya sekuat mata rantai terlemahnya.

BAGIAN 2

Mitra Penting – Audit Internal dan CISO

Tentang para Ahli

Jerry Perullo

Jerry Perullo adalah pendiri Adversarial Risk Management, sebuah firma Cybersecurity Program Strategy and Governance yang mendukung perusahaan yang sedang tumbuh untuk secara cepat membentuk program keamanan siber yang matang. Sebelum mendirikan Adversarial, Perullo pensiun sebagai Kepala Departemen Keamanan Informasi (Chief Information Security Officer/CISO) di IntercontinentalExchange (NYSE:ICE) setelah 20 tahun membangun dan memimpin program keamanan siber pada berbagai infrastruktur ekonomi global termasuk New York Stock Exchange. Memiliki sertifikasi NACD Directorship Certified®, Perullo juga bertindak sebagai Dewan Komisaris pada Financial Services Information Sharing and Analysis Center (FS-ISAC) selama 6 tahun, terkini sebagai Ketua. Perullo juga mengajar di Georgia Institute of Technology sebagai profesor praktikum pada Sekolah Keamanan Siber dan Privasi dan membagikan pengalamannya kepada para pemimpin risiko teknologi melalui podcastnya lifeafterCISO.com.

Hassan NK Khayal, CIA, CRMA, CFE

Hassan NK Khayal adalah seorang Manajer Audit Internal di Dubai. Hassan ternasuk salah satu di dalam 15 dari 30 peringkat tertinggi pemimpin baru global. Hassan memegang gelar BBA, MBA, dan keahlian dalam studi timur tengah. Hassan juga seorang CIA, CRMA, dan CFE. Hassan juga memegang sertifikasi profesional di bidang otomasi proses robotik, analisis data, internet of things (IoT), manajemen mutu, kesehatan dan keamanan, manajemen lingkungan, dan manajemen risiko.

Alan Maran

Alan adalah seorang kepala audit internal pada Chewy, Inc. Dia telah bekerja di perusahaan tersebut sejak Januari 2019. Dalam perannya, ia bertanggung jawab untuk mengawasi aktivitas strategis dan pelaksanaan fungsi audit internal secara menyeluruh, termasuk penilaian risiko perusahaan, menyediakan dukungan berupa pemberian nasihat (advis) secara berkesinambungan dan tepat waktu untuk berbagai aktivitas yang didukung oleh manajemen, dan asurans terhadap ketepatan pengendalian atas risiko kunci yang telah diidentifikasi oleh manajemen selaras dengan operasi, sistem korporasi, dan tata kelola, risiko, dan kepatuhan TI pada keseluruhan perusahaan, dan melanjutkan fokus pada pengembangan anggota tim audit internal dengan fokus pada analisis data, keamanan siber, dan privasi data. Alan adalah eksekutif audit yang berpengalaman lebih dari 22 tahun di bidang perdagangan elektronis, teknologi keuangan, dan perusahaan teknologi dan manufaktur yang terus memiliki semangat untuk belajar. Sebelum bergabung di Chewy, dia membangun peran kepemimpinannya secara progresif dengan memulai karirnya di Ernst & Young, LLC dan kemudian meningkat ke berbagai posisi audit internal lain di organisasi multi-nasional Fortune 500. Dia bergelar MBA dan Magister Keuangan dari Washington State University, seorang Certified Fraud Examiner (CFE), Certified Blockchain Expert, dan berafiliasi dengan Institute of Internal Auditors chapter lokal.

Srini Srinivasan, PMP, CBIP

Srini Srinivasan adalah Kepala Keamanan Informasi dan Data pada Chewy, Inc. Dia telah bekerja di perusahaan tersebut sejak Oktober 2019, sebagai Kepala Keamanan, Data, dan Sistem Korporasi. Dalam perannya, dia bertanggung jawab untuk mengawasi keamanan informasi, manajemen data dan platform analisis, sistem korporasi dan tata kelola, risiko, dan kepatuhan TI pada perusahaan secara menyeluruh. Srini seorang eksekutif teknologi yang berpengalaman selama lebih dari 25 tahun pada bidang perdagangan elektonis, jasa perbankan dan keuangan, ritel, dan pemasaran. Sebelum bergabung dengan Chewy, dia berperan sebagai pimpinan pada Citizens Financial Group. Dia memegang gelar magister bidang ilmu komputer dari Bharathidasan University dan MBA dari Bentley University.

Pengantar

Kemitraan dalam kemanaan siber penting untuk mencapai kesuksesan

Keamanan siber bertahan di antara risiko-risiko utama bagi seluruh organisasi. Survei-survei secara konsisten merefleksikan upaya yang terus menerus dilakukan oleh penjahat siber untuk membajak data sensitif atau memancing mereka yang tidak terlatih atau tidak memiliki kecurigaan untuk membocorkan informasi sensitif atau memberikan akses kepada orang jahat.

Contohnya, Laporan Investigasi Kebocoran Data Verizon 2022 menunjukkan peningkatan yang menakjubkan sekitar 13% dalam pelanggaran terkait ransomware selama tahun 2021, lebih besar daripada kombinasi lima tahun sebelumnya. Namun demikian, laporan menemukan bahwa metode paling berhasil dalam serangan ramsomware tetap konsisten, yaitu penyalahgunaan komputer meja yang digunakan secara bersama dan perangkat lunak akses jarak jauh (40%) dan surat elektronik (35%), menurut laporan Verizon. [18]

Panduan baru dari IIA, Mengaudit Operasi Keamanan Siber: Pencegahan dan Pendeteksian (GTAG), didesain untuk membantu organisasi dalam memeriksa dan memprioritaskan asurans terhadap operasi keamanan siber. Panduan ini bertujuan untuk membantu auditor internal mendefinisikan operasional keamanan siber, mengidentifikasi komponennya, dan memertimbangkan pedoman pengendalian yang relevan untuk kerangka kerja TI, dan memahami pendekatan untuk mengaudit operasi keamanan siber.

Satu kunci untuk meningkatkan asurans keamanan siber yang tidak tercakup dalam panduan adalah adanya hubungan yang sehat antara kepala audit internal dan kepala petugas keamanan informasi (chief information security officer/CISO). Hubungan saling menguntungkan ini berpotensi dapat membantu menyelaraskan audit internal dan keamanan informasi dari aspek kerangka kerja, risiko, dan pengendalian, serta mendukung pengelolaan profil risiko keamanan siber yang semakin luas.

Perspektif dan Pandangn Global ini membahas manfaat hubungan yang kuat antara kepala audit internal dan mitra kerjanya di bidang keamanan informasi, melihat tahapan dalam membangun dan memelihara hubungan tersebut dengan tetap memastikan independensi audit, dan menilai bagaimana kemitraan tersebut dapat memberi nilai tambah kepada organisasi.

18. "3 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/.

Kasus untuk Keamanan Siber Kolektif

Risiko siber membutuhkan pendekatan secara luas dalam perusahaan

Keamanan siber tetap menjadi area risiko yang bertumbuh dan berkembang dengan setiap tahunnya menunjukkan skema kejahatan siber yang semakin canggih dan luas. Tidak kurang statistik yang menunjukkan organisasi tetap rentan terhadap serangan siber. Pada waktu yang sama, terdapat tekanan terhadap organisasi pada seluruh spektrum industri untuk menerapkan strategi bisnis yang sangat mengandalkan pada pengumpulan, pengelolaan, analisis, dan penggunaan data melalui pemanfaatan teknologi baru untuk meningkatkan kinerja dan laba.

Bersama area-area risiko signifikan lainnya, risiko siber harus dipahami dan dikelola oleh seluruh organisasi. Namun sedikit organisasi yang mengambil pendekatan perusahaan secara menyeluruh untuk mengelola keamanan siber, menurut "The State of Cyber Resilience", sebuah laporan dari Microsoft dan firma perantara asuransi dan manajemen risiko Marsh. Berdasarkan survei[19] kepada lebih dari 600 pengambil keputusan dalam risiko siber, laporan menemukan hanya 4 dari 10 organisasi yang melibatkan manajemen dari unit hukum, perencanaan korporasi, keuangan, operasi, atau rantai pasok dalam membuat rencana risiko siber[20].

"Satu hal yang membuat kurang yakin adalah kebanyakan perusahaan belum mengadopsi pendekatan perusahaan secara menyeluruh untuk risiko siber; yang salah satu intinya adalah tentang komunikasi secara luas dan mendorong kolaborasi dan keselarasan antarpemangku kepentingan pada saat pengambilan keputusan kunci pada perjalanan ketahanan siber mereka", menurut laporan[21].

Di antara tren risiko kunci yang diidentifikasi dalam laporan, disampaikan bahwa:

"Sasaran spesifik siber perusahaan secara luas – termasuk pengukuran keamanan siber, asuransi, data dan analisis, dan rencana tanggap insiden – harus selaras dalam membangun ketahanan siber untuk mencegah insiden, karena setiap organisasi dapat terkena serangan siber". [22]

Untuk mendukung pendekatan perusahaan secara luas yang efektif, kepala audit internal dapat berkontribusi secara signifikan dengan membangun dan memelihara hubungan dengan CISO. Hubungan tersebut harus didasarkan pada pemahaman, tujuan, dan respek yang saling menguntungkan.

CISO senior dan pendiri Adversarial Risk Management Jerry Perullo, secara formal bersama NYSE-parent Intercontinental Exchange (NYSE:ICE), mengatakan bahwa komunikasi yang buruk atau pemahaman yang tidak jelas akan keamanan informasi dan peran audit internal dapat merusak keselarasan manajemen risiko keamanan informasi. Sebaliknya, hubungan baik antara kepala audit internal dan keamanan informasi membuka pintu pemahaman yang lebih mendalam akan sasaran, strategi, operasi, dan kebijakan yang dapat membuat audit internal - dengan temuan dan rekomendasi yang dalam – lebih relevan bagi pemimpin risiko siber, manajemen eksekutif, dan dewan, katanya. Terlebih lagi, hubungan yang kuat antara audit internal dan tim keamanan informasi memperluas pengetahuan tentang misi penting pada area masing-masing dan bagaimana keduanya mendukung keamanan siber secara keseluruhan.

"Pada akhirnya, audit internal ingin teredukasi tentang keamanan informasi," kata Perullo. "Terdapat banyak cara untuk melakukannya, tapi tidak ada yang serupa dengan belajar langsung dari tim (keamanan informasi) itu sendiri".

Dalam pekerjaan konsultasinya dengan perusahaan rintisan, Perullo sering memulai dengan menyiapkan program tata kelola keamanan siber. Hal ini biasanya mencakup pembuatan komite tata kelola keamanan siber lintas fungsi yang dapat memuat

19 "2022 Marsh and 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

manajemen eksekutif, keuangan, hukum, dan keamanan informasi. Komite juga sering memasukkan eksekutif audit internal sebagai pengamat.

Lima Kunci untuk Keberhasilan

Manfaat hubungan yang solid antara audit internal dan CISO

Audit internal dan CISO memperoleh banyak manfaat dari kemitraan yang dirancang dengan baik. Tingkat kerincian dan kerumitan dari kemitraan tersebut dapat bervariasi bergantung pada ukuran organisasi, tingkat regulasi dalam masing-masing industri, atau profil risiko keamanan siber organisasi. Namun demikian, lima area dalam kolaborasi dan kerja sama dapat menghadirkan manfaat nyata terlepas dari ukuran organisasi atau di industri mana organisasi beroperasi.

Memahami dan menyelaraskan profil risiko organisasi

Profil risiko adalah analisis kuantitatif dari jenis ancaman yang dihadapi organisasi. Dari perspektif keamanan siber, analisis semacam itu dapat mengidentifikasi aset dan risiko siber, memeriksa kebijakan dan praktik yang dirancang untuk mengelola risiko tersebut, dan berupaya memahami setiap kerentanan yang mungkin ada. Pemahaman audit internal tentang profil risiko siber memberikan landasan untuk membangun rencana audit yang tidak hanya mendukung pendekatan keseluruhan organisasi terhadap keamanan siber, tetapi juga dapat meningkatkan relevansi dan nilai audit internal di area kritis ini.

Alan Maran, kepala audit internal di Chewy, Inc (pengecer produk makanan hewan dan produk terkait hewan peliharaan lainnya secara daring), telah mengembangkan hubungan yang kuat dengan CISO organisasi, Srini Srinivasan, selama tiga tahun sejak perusahaan ini memasuki bursa. Srinivasan mengatakan keamanan informasi bermitra dengan audit internal, unit hukum, dan pemangku kepentingan lainnya untuk menilai dan mengukur profil risiko siber perusahaan secara komprehensif berdasarkan Kerangka Keamanan Siber NIST.

“Itu adalah dasar kami,” kata Srinivasan. “Kami kemudian menetapkan peta jalan tiga tahun untuk keamanan dan tata kelola siber, dan kami menyesuaikannya dan meningkatkannya berdasarkan penilaian kerangka kerja keamanan siber yang kami lakukan. Kami sekarang melakukan penilaian setiap tahun untuk melihat apakah kami membuat peningkatan di area yang berpeluang tersebut dan menilai bagaimana skor risiko kami secara keseluruhan diukur.”

Pendekatan kolaboratif yang melibatkan audit internal sejak awal ini memungkinkan strategi saling menguntungkan yang menggabungkan asurans dan layanan konsultasi audit internal dengan tujuan untuk secara konsisten meningkatkan postur keamanan siber Chewy secara keseluruhan.

"Ini bukan perspektif, saya selalu perlu mengaudit TI dan keamanan. Kami juga perlu mendukungnya," kata Maran. “Dari sisi audit internal, kami melihat kami adalah mitra dengan mentalitas yang kuat untuk mendukung Srini dan timnya dalam mengembangkan strategi keseluruhan.”

Manfaat tambahan dari kolaborasi ini adalah keamanan informasi dan asurans yang independen dimuat ke dalam proyek-proyek baru sejak dini. Dengan kata lain, keamanan informasi, audit internal, dan pengendalian tata kelola tidak menjadi hal yang dipikirkan di kemudian hari, kata Srinivasan.

“Apa yang kami lakukan adalah, ketika inisiatif proyek sedang berjalan, kedua tim kami terlibat dan bermitra dengan tim teknik, tim produk, tim bisnis…. Apa pertimbangan keamanannya? Apakah kita mengikuti praktik terbaik?” kata Srinivasan.

Pendekatan ini membantu mengidentifikasi, meminimalkan, dan, jika mungkin, menghilangkan risiko siber dengan membangun proses dan pengendalian yang sesuai saat proyek dikembangkan, kata Srinivasan. “Jadi, ketika proyek itu berjalan akan menjadi sangat mudah bagi kedua (tim) kami karena kami mereka memiliki pemahaman yang kuat. Ketika kami menindaklanjuti baik dengan penilaian audit pada pengendalian, penelaahan pada akses, atau tata kelola, kami memiliki lebih banyak wawasan.”

Memahami peran

Hubungan yang dibangun oleh Maran dan Srinivasan sangat terbantu oleh Chewy sebagai perusahaan publik yang relatif baru, yang memberikan kesempatan untuk membentuk hubungan dari bawah ke atas. Hal ini juga membentuk harapan akan komunikasi yang terbuka dan sering antara Maran, Srinivasan, dan tim mereka.

“Ini adalah cara yang ideal untuk membangun transparansi dan kepercayaan di antara para pemangku kepentingan utama, jadi kami tidak ingin melewatkan kesempatan ini,” kata Srinivasan.

Ini bukan diartikan bahwa tidak pernah ada perbedaan pendapat. Tetapi ketika konflik muncul, hubungan tersebut memudahkan untuk memperdebatkannya dan menghasilkan solusi yang menguntungkan kedua belah pihak, kata Srinivasan.

“Tidak ada gunanya bagi saya untuk menjauhkan apa pun dari audit internal,” katanya. “Semakin mereka tahu tentang apa yang kita lakukan. . . semakin besar tingkat apresiasi yang mereka miliki. Dengan cara yang sama dari perspektif audit internal, saya dapat memberi tahu Anda bahwa saya pikir tidak ada unsur '*kena deh'* di sini.

Pada akhirnya, pendekatan kolaboratif memungkinkan untuk beroperasi secara gesit dengan audit internal adalah bagian tak terpisahkan dari proses ketika kekurangan dapat dideteksi dan diatasi lebih awal, kata Srinivasan.

Maran menambahkan bahwa interaksi yang jujur akan dapat menegaskan dan memperkuat pemahaman tentang peran masing-masing.

“Srini tidak berasumsi bahwa kita tahu semuanya, tetapi pada saat yang sama, dia menghormati kepentingan dan sudut pandang kami,” katanya.

Relevansi

Memberikan wawasan dan observasi dari penugasan asurans terkait isu-isu kritis pada waktu yang tepat adalah salah satu tantangan terbesar audit internal di area risiko apa pun, terutama untuk keamanan siber. Risiko yang terus berkembang dan serba cepat ini menuntut asurans yang relevan dan tepat waktu.

Perullo memperingatkan bahwa keterlibatan audit internal serta pemberian rekomendasi yang tidak selaras dengan misi keamanan siber organisasi dapat lebih merugikan daripada menguntungkan. Hal tersebut dapat membuat kebingungan unit keamanan informasi tentang apa yang ingin dilihat oleh audit internal, terutama jika audit internal tidak dapat meyakininya.

“Audit internal mungkin pada awalnya tidak memiliki pemahaman yang memadai tentang apa yang ingin dilihatnya,” katanya. “Lebih baik untuk berkolaborasi pada tahap pra-audit dan mengamati proses tata kelola siber untuk memastikan audit selaras dengan misi.”

Hassan Khayal, konsultan audit internal dengan keahlian siber, mengatakan bahwa keamanan siber adalah area audit internal yang sangat rentan terhadap kritik. Seringkali, auditor internal menolak untuk mengenal anggota tim TI atau tim keamanan informasi dan belajar lebih banyak tentang subjek audit tersebut dengan dalih melindungi independensi audit internal.

“Saya tanpa malu-malu akan pergi pada tugas pertama saya dan memberi tahu orang TI, 'Dengar, saya di sini untuk belajar dari Anda lebih dari apa pun. Saya akan mengajak orang dengan pemahaman proses atau pemahaman teknis dan melakukan percakapan ramah sambil makan siang sehingga saya tahu persis bagaimana seluk beluk pekerjaan yang mereka lakukan.”

Proses pendidikan ini juga membantu auditor internal memahami kematangan keamanan siber organisasi yang sangat penting untuk memberikan rekomendasi yang relevan, kata Khayal.

“Jika Anda berbicara tentang perusahaan kecil hingga menengah, atau bahkan organisasi yang lebih besar yang tidak diperdagangkan secara publik, maka sebenarnya terdapat begitu banyak hal yang dapat Anda lakukan atau harus lakukan,” katanya. “Pada titik tertentu, rekomendasi bisa terlalu agresif, sehingga rekomendasi yang Anda buat tidak realistis.”

Membangun hubungan yang kuat antara audit internal dan tim keamanan informasi mengurangi kemungkinan adanya penugasan dan rekomendasi audit yang tidak relevan atau salah arah. Manfaat itu telah ditegaskan di Chewy.

“Tim Alan dan Alan sendiri sangat paham dengan strategi keamanan kami secara keseluruhan, dari perspektif teknologi, apa yang kami lakukan, dan apa saja risiko utama kami,” kata Srinivasan. “Jadi, kami tidak memiliki kesenjangan besar antara peringkat risiko dan kemampuan internal kami. Ini akan terus membantu kami melakukan pekerjaan yang lebih baik dalam hal meningkatkan pengetahuan keseluruhan tim kami atau anggota tim kami di Chewy serta tim kepemimpinan kami.”

Komunikasi Terhadap Dewan Komisaris dan Dewan Direksi

Budaya organisasi yang diperkenalkan oleh Chewy memberikan pandangan yang lebih luas terhadap risiko yang didukung melalui percakapan terbuka. Maran dan Srinivasan telah mengambil peran dalam mengedukasi para pemangku kepentingan (stakeholders), yaitu Dewan Komisaris dan Dewan Direksi, sehubungan dengan kolaborasi dan keuntungan yang dihasilkan.

Maran menjelaskan, “Banyak organisasi maupun orang-orang di luar sana yang memiliki pendakatan tidak terintegrasi. Pendekatan seperti, ‘Oh, hal tersebut terkait dengan keamanan IT, sehingga ketika mendengar hal tersebut mereka akan langsung berbicara mengenai CISO, dan CISO akan menjalankan peran tersebut’. Akan tetapi dalam suatu perspektif terhadap manajemen risiko yang terpadu atau manajemen risiko perusahaan, risiko apapun yang akan berakibat terhadap perusahaan dapat Kembali ke keseluruhan bagian perusahaan”. Suatu serangan siber dapat mempengaruhi operasi, pelayanan, maupun keuangan. Srini juga telah melakukan pekerjaan yang baik dalam mengedukasi kepemimpinan terhadap apa yang sedang dilakukan dan bagaimana melakukan mitigasi terhadap risiko. Sehingga, melalui perspektif tersebut telah terjadi kolaborasi.

Hal ini tentunya telah menggambarkan respon yang tepat waktu dan gesit terhadap perubahan risiko dan pandangan terhadap regulasi siber. Sebagai contoh, Maran dan Srinivasan telah memilki keyakinan yang berkelanjutan bahwa organisasi dapat merespon usulan peraturan pelaporan keamanan siber yang diusulkan oleh Komisi Sekuritas dan Bursa Amerika Serikat yang diperkenalkan pada kuartal pertama tahun 2022.

Kolaborasi tersebut tentunya terjadi melebihi keamanan informasi dan audit internal. Disebutkan oleh Srinivasan bahwa “hal ini tidak terbatas terhadap keamanan dari suatu organisasi”. “Kita memiliki pemangku kepentingan utama yang lain dimana kita memiliki hubungan kemitraan yang sama, seperti tim akuntansi dan tim hukum. Saya berpendapat bahwa menciptakan hubungan yang transparan dan baik ketika peraturan-peraturan yang berkembang dan beberapa aturan tambahan berada dalam suatu pandangan yang sama.

Sementara kepemimpinan Chewy memperoleh manfaat dari pesan yang konsisten serta terpadu, Khayal memperingatkan bahwa bahaya yang signifikan terjadi ketika kepemimpinan tidak mengikuti perkembangan status dan kebutuhan keamanan siber dari suatu organisasi. TI dan keamanan siber dapat secara cepat dipandang sebagai pusat biaya ketika pemimpin tidak diinformasikan serta diedukasi mengenai hal tersebut. katanya. Khayal menyebutkan ketika audit internal menghindar terhadap keamanan informasi, maka mereka akan cenderung kurang menyajikan informasi berharga dan asurans yang relevan dalam area ini. Hal ini akan mempengaruhi pandangan terhadap keamanan siber dari sudut pandang dewan direksi dan dewan komisaris.

Melindungi dan Menghargai Independensi

Khayal, pekerja sekaligus Auditor Sistem Informasi yang bersertifikat (CISA) menyebutkan bahwa komitmennya dalam memperoleh sertifikasi telah meningkatkan kredibilitasnya di kalangan professional IT dan keamanan informasi. Hal tersebut juga telah membuat dia dapat berinteraksi dengan para rekan sejawat yang berada pada tingkatan level pekerjaan mereka masing-masing, membuat mereka cenderung untuk berpartisipasi dalam informasi secara terbuka yang mungkin dianggap terlalu canggih atau rumit bagi seorang auditor yang hanya datang ketika perikatan audit. Lebih lanjut, dia tidak memandang bahwa interaksi merupakan sebuah ancaman terhadap kemampuannya untuk melaksanakan kegiatan audit yang independent dan objektif.

“Pada suatu saat, anda akan berada di tempat kerja”, katanya. “Ketika kita mengatakan bahwa auditor akan bersikap independen, saya secara pribadi tidak percaya bahwa kita mengatakan hal tersebut ke mereka”. “Anda tidak dapat memiliki rekan-rekan di tempat kerja, anda seharusnya selalu pergi makan siang sendiri”.

Khayal menyebutkan bahwa dia mengambil pendekatan ini di seluruh area organisasi. Dia akan berbicara Linux dengan staf komputer atau media sosial dengan staf pemasaran.

“Merupakan suatu kesempatan yang baik untuk mengembangkan diri anda secara professional sambil membina hubungan”, menurutnya. Hal ini seperti ketika kita akan mengatakan pada klien audit atau auditi kami, bahwa “kita sedang melihat suatu proses dan transaksinya, kita tidak sedang mencari orang. Sehingga, ketika anda mengajak orang-orang untuk makan siang, maka anda tidak akan membawa mereka terhadap proses maupun transaksi”.

Maran menyebutkan bahwa terhadap Chewy, hubungan dekat tersebut antara Maran dan Srinivasan mendukung hubungan yang saling menguntungkan sehubungan dengan perlunya verifikasi independent.

“Secara alamiah, profesi kita adalah bukan untuk mempercayai tetapi melakukan verifikasi. Dari sudut pandang yang objectif, saya memiliki kewajiban untuk melaksanakan hal tersebut”, dia menyebutkan. “Ya dengan demikian, kita mempercayai hingga pada tingkatan tertentu, khususnya sesuatu hal tambahan yang telah kami periksa. Pada banyak kasus, kami melakukan validasi terhadap hal tersebut yang belum berubah. Akan tetapi saya juga tetap melanjutkan untuk melakukan pengecekan integritas dari informasi yang disajikan oleh manajemen. Kita tidak hanya sekedar melihat laporan dari nilainya, kami akan melihat sumber informasinya untuk memastikan bahwa kita akan memperoleh informasi yang sama, karena mereka ada untuk memastikan bahwa informasi tersebut lengkap dan akurat”.

Disebutkan oleh Maran, pada akhirnya mengerti peran satu sama lain dalam suatu organisasi membuat suatu hal menjadi mudah.

“Terdapat suatu kesepakatan di sini. Ini adalah hal yang perlu saya lakukan. Ini adalah jasa asurans yang perlu saya sediakan kepada kepemimpinan yang senior – dewan komisaris, pemangku kepentingan¸ dan kepada para komite audit”, sebutnya. Kita menyesuaikan terhadap kegiatan audit yang akan dilakukan tahun ini. Kita menyesuaikan ruang lingkup. Ya, kami kadang-kadang berbicara terkait sudut pandang kami dan bagaimana kami satu sama lain memandang hal tersebut, akan tetapi kami jarang untuk tidak setuju terhadap area risiko yang kami perlu berikan asurans.

Srinivasan menambahkan bahwa fokus terhadap pendekatan pengendalian data terhadap keamanan siber mengasumskan bahwa akan terdapat kesepakatan terhadap fakta antara informasi keamanan dan audit internal.

“Jika terdapat ketidaksepakatan, kita perlu untuk bekerja dan memperoleh kumpulan fakta yang sama,” dia menambahkan. Kemudian, jika kamu dapat memiliki beberapa level subjektivitas dimana setiap individu dapat mengatakan, “baiklah, ’saya merasa secara kritikal hal ini sedang atau secara kritikal ini tinggi atau secara kritikal ini rendah’. Saya merasa hal ini dapat menghasilkan diskusi serta hasli yang sehat, daripada saling berkeras tanpa memiliki pandangan referensi yang sama”.

Memberi Nilai Tambah

Meningkatkan ketahanan keamanan siber

Srinavasan menyebutkan bahwa pendekatannya sejak awal adalah sesuai dengan misinya Chewy. Hal tersebut berarti mencakup tiga hal: melaksanakan prinsip internal operasi perusahaan, memastikan kesesuaian antara keamanan informasi dan audit internal, dan membangun kepercayaan melalui transparansi.

“Saya berpendapat bahwa kita harus menempuh perjalanan jauh, dan ini tentunya akan membutuhkan banyak upaya dalam banyak hal yang diperlukan dari anggota tim dan kepemimpinan untuk memastikan satu sama lain selalu *up to date*”, katanya.

Sebagaimana disebutkan di bagian awal, tingkatan komunikasi yang tinggi, kolaborasi, dan dukungan kerja sama pendekatan yang tangkas untuk menggabungkan audit internal di dalam keamanan siber yang berkelanjutan. Srinivasan mencatat bahwa kekuatan utama, seperti perkembangan fokus terhadap keberlanjutan, pertimbangan jalur distribusi, kondisi pasar, perkembangan geopolitik, dan lebih membutuhkan pendekatan yang tangguh untuk keamanan siber dan asurans yang terkait.

“Saya rasa hal tersebut memaksa kita untuk lebih waspada, gesit dan responsif, dan relevan”, ujarnya. “Jika kita mengacu terhadap mekanisme *waterfall* klasik dengan waktu tunggu yang lebih lama, maka kita akan ketinggalan kapal. Dengan demikian, saya senang terhadap tingkatan keterlibatan yang sudah kami miliki”.

Memperluas Wawasan

Keuntungan intrinsik lain dari adanya kemitraan adalah bagaimana para tim telah berevolusi dan bertumbuh dalam suatu pengertian dan penghargaan terhadap pendekatan satu sama lain dalam mencapai tujuan yang sama – menjaga keamanan siber organisasi.

“Kita selalu mengecek pengetahuan teknis satu sama lain, dalam arti, ‘apakah kita melihat hal ini? Apakah anda berpikir tentang hal tersebut? Berikut adalah pandangan saya terhadap analisis risiko – apakah hal tersebut sejalan dengan pendapat anda juga?,” kata Maran. “Sehingga, dari hal tersebut kita telah memikirkan tentang apa yang akan kita cari, dan Srini berpartisipasi dalam rapat pembukaan. Dia ada di dalam percakapan sebelum kami memulai pelaksanaan audit. Hal ini tentunya bukan suatu kejutan.”

Tetapi nilai tambah yang nyata berasal dari kolaborasi ketika penugasan audit dilaksanakan dan audit internal secara langsung sepemahanan dengan personel TI dan keamanan.

“Dari sudut pandang pengembangan karir, khususnya dengan pola pikir IT dan keamanan siber, hal ini tentunya sangat memberikan manfaat karena anda dapat melihat banyak hal daripada sekedar melakukan centang terhadap hal yang telah dilakukan dan mengatakan, “apakah anda melakukan ini?,” Maran mengatakan. “Terdapat banyak kelebihan. Terdapat interpretasi bahwa terdapat keahlian teknikal yang harus dilaksanakan secara benar, sehingga hal tersebut terjadi ketika tim saya dapat belajar banyak.”

Kesimpulan

Hubungan yang baik antara audit internal dan keamanan informasi menawarkan banyak keuntungan terhadap organisasi, terutama dalam menyelaraskan dan memahami profil risiko siber suatu organsiasi – dari kerentanan dan kesempatan hingga pengujian terhadap maturitas dan uji peneterasi,

Hal lebih lainnya, dimana suatu hubungan dapat meningkatkan ketahanan dan kelincahan manakala suatu organisasi perlu untuk merespon kejadian siber, perubahan faktor-faktor yang mempengaruhi keamanan siber, atau pandangan terhadap peraturan yang berkembang. Hal ini membantu dalam menyajikan pesan yang konsisten dan terpadu terhadap C-Suite dan dewan komisaris sehubungan dengan risiko keamanan siber, kebutuhan, prioritas, dan kesehatan. Independensi audit internal dapat secara baik dilindungi, bahkan meningkatkan, ketika para pihak menumbuhkan pengertian yang lebih dalam dan pemahaman terhadap peran, pendekatan, dan tugasnya. Pada akhirnya, hubungan yang erat antara pimpinan audit dan CISO dapat memperkuat keamanan IT dengan mendukung pendekatan organsasasi yang menyeluruh terhadap keamanan siber.

“Pola pikir telah bergeser dari sekedar melakukan audit – ‘Saya butuh untuk masuk dan menilai, serta datang dengan pengamatan yang bermakna – dengan lebih mengatakan, ‘ini adalah perusahaan ku, inilah yang sangat saya pedulikan, dan inilah cara saya untuk membantu tim ini menjadi sukses,” kata Maran.

BAGIAN 3

Respons dan Pemulihan Insiden Siber

Tentang Pakar

Brian Tremblay

Brian Tremblay memimpin Praktik Kepatuhan di Onapsis, di mana dia bertanggung jawab untuk membantu pelanggan memahami dan menavigasi tantangan dan peluang yang diciptakan oleh meningkatnya tumpang tindihnya kepatuhan, keamanan siber, dan kelangsungan bisnis terkait dengan kontrol umum Teknologi Informasi (TI) serta masalah regulasi dan kepatuhan seperti *Sarbanes- Oxley* (SOX) dan *General Data Protection Regulation* (GDPR). Sebelum Onapsis, dia adalah Kepala Eksekutif Audit (CAE) untuk perusahaan semi konduktor teknologi tinggi Acacia Communications. Selain mendirikan dan memimpin seluruh aktivitas fungsi audit internal, beliau juga membantu mempersiapkan organisasi untuk masuk bursa (termasuk mengimplementasikan SOX) dan memfasilitasi penerapan manajemen risiko perusahaan (ERM). Sebelumnya, Tremblay adalah Direktur Audit Internal di Iron Mountain, mengawasi semua audit dan proyek di Amerika Utara serta berhubungan dengan Manajer Kualitas Global. Sebelumnya, sebagai manajer senior di Houghton Mifflin Harcourt, dia membangun Departemen Audit Internal dan menjalankan implementasi SOX. Di awal karirnya, dia bekerja di Raytheon dan Deloitte.

DaMon Ross Sr.

Pada tahun 2020, DaMon Ross Sr. memulai *Cyber Defense International*, di mana ia dan timnya memanfaatkan operasi keamanan siber elit dan kemampuan intelijen ancaman siber untuk memberikan solusi dan layanan keamanan siber yang terjangkau kepada organisasi yang tidak memiliki sarana untuk membangun kemampuan itu sendiri. Sebelum memulai *Cyber Defense International*, Ross menjabat sebagai Wakil Presiden Senior untuk Operasi Keamanan Siber di SunTrust Bank. Dalam peran ini, dia ditugaskan untuk membuat pusat operasi keamanan siber 24/7/365 SunTrust. Karena itu, Ross membangun tim yang berspesialisasi dalam intelijen siber, pemantauan ancaman siber, respons insiden siber, dan kejahatan siber. Khususnya, ia juga berhasil bermitra dengan hukum, sumber daya manusia, keamanan perusahaan, dan etika perusahaan dan mitra risiko untuk membentuk program pemantauan ancaman orang dalam pertama bank. Ross juga memfasilitasi pembentukan berbagai kemitraan berbagi informasi, termasuk dengan Satuan Tugas Kejahatan Elektronik Dinas Rahasia Amerika Serikat dan Departemen Keamanan Dalam Negeri.

Pengantar

Kembali ke dasar

Keamanan siber telah lama menjadi titik fokus utama organisasi dan fungsi audit internal mereka, dan dengan diperkenalkannya proposal baru Komisi Sekuritas dan Bursa (SEC) tentang manajemen risiko keamanan siber, strategi, tata kelola, dan pengungkapan insiden, Termasuk pada tahun 2022, dorongan untuk hal ini dan proposal peraturan lainnya diterbitkan. Menurut laporan dari Pusat Sumber Daya Pencurian Identitas , terdapat 1.862 pelanggaran data profil tinggi yang tercatat pada tahun 2021, angka yang melampaui total tahun 2020 sebesar 68%, serta rekor sepanjang masa yang ditetapkan pada tahun 2017. Tidak ada industri yang terhindar. dari tren.[23]

Dalam lingkungan ini, organisasi menginginkan, memang membutuhkan, kontrol dan proses keamanan siber yang jelas dan kuat yang dibangun di atas dasar-dasar inti, termasuk pembelajaran berkelanjutan tentang risiko dan peraturan terkaitnya, serta komunikasi dan keselarasan antara dewan, manajemen, dan audit internal. Bagian 1 dari seri tiga bagian The IIA, Keamanan Siber pada tahun 2022, berfokus pada potensi dampak peraturan, sementara Bagian 2 membahas manfaat dari hubungan simbiosis antara *Chief Information Security Officer* (CISO) dan rekan audit internal mereka. Bagian terakhir ini menekankan pada pengembangan dan implementasi strategi respons insiden siber organisasi, dan lebih khusus lagi, di mana audit internal dapat memberikan nilai organisasi dalam menilai kontrol yang penting untuk pemulihan cepat dari pelanggaran keamanan siber.

[23]. Pusat Sumber Pencurian Identitas, “Laporan Pelanggaran Data Tahunan 2021 dari Pusat Sumber Pencurian Identitas Menetapkan Rekor Baru untuk Jumlah Pelanggaran,” 24 Januari 2022, https://www.idtheftcenter.org/post/identity-theft-resource-center-2021 -annual-data-breach-report-sets-new-record-for-number-of-compromises/ .

Kontrol Utama

Memberikan audit internal untuk memainkan peran dalam respons siber

Kekeliruan respons insiden

Meskipun istilah "respons insiden siber" dan "respons dan pemulihan keamanan siber" adalah istilah yang akurat dan definisi yang berguna, mereka juga menyiratkan pandangan yang kurang begitu lengkap tentang rencana apa yang dibutuhkan agar menjadi efektif.

Audit internal dalam perannya yang paling penting memberi organisasi dengan asurans independen atas manajemen risiko. Ini mencakup tidak hanya asurans untuk respons yang tepat terhadap insiden siber, tetapi juga evaluasi kontrol yang tepat untuk memastikan bahwa risiko dan dampaknya termitigasi atau, idealnya, dicegah. Untuk mencapai standar yang begitu tinggi atas risiko apa pun, perhatian tidak boleh hanya dipersiapkan untuk sekadar menanggapi risiko. Sebaliknya, lebih efektif untuk melihat respons insiden siber secara menyeluruh, siklus yang memprioritaskan kontrol pencegahan serta tindakan respons aktif.

“Manajemen risiko seperti roda,” kata Brian Tremblay, pemimpin praktik kepatuhan di Onapsis, Inc. Dan kemudian, ketika sesuatu terjadi, percakapan segera menjadi, 'Apakah kontrol berjalan seperti yang diharapkan, dan apakah yang kita pikirkan akan terjadi terjadi?' Kemudian, dari sana, kita belajar apa yang perlu diubah, dan siklusnya dimulai lagi. Jika satu-satunya waktu Anda menanggapi suatu peristiwa adalah setelah kejadian, kemungkinan Anda tidak efisien dengan waktu dan sumber daya Anda. Masa kini dan masa depan harus diberikan bobot yang sama karena kita tidak hanya membangun bisnis hari ini, kita sedang membangun bisnis masa depan. Karena organisasi sering bergumul dengan hal ini, ini adalah tempat yang sangat penting bagi audit internal untuk fokus.”

Dasar-dasar yang tidak berubah

Risiko menjadi kompleks, dan karena keamanan siber secara inheren sangat teknis, kurva pembelajaran untuk memahami risiko itu sendiri dan sistem yang diperlukan untuk menguranginya hanya semakin curam dengan setiap kemajuan teknologi berikutnya. Namun, ini tidak berarti bahwa struktur dasar dari rencana respons insiden siber, dan kontrol di dalamnya, berubah secara dramatis.

Kontrol ini diuraikan dalam Panduan Tambahan terbaru, *Audit Respons dan Pemulihan Insiden Siber*, dan dapat dikelompokkan ke dalam empat tujuan bisnis tingkat tinggi:

- **Perencanaan Respons Insiden.** Kebijakan dan prosedur harus ditetapkan untuk memandu penentuan apakah suatu insiden telah terjadi dan apa yang harus dilakukan untuk mengatasinya. Perencanaan harus melibatkan pemangku kepentingan utama, menentukan peran dan tanggung jawab, dan diuji sebagaimana mestinya untuk meningkatkan kesadaran dan pelaksanaan.
- **Identifikasi Insiden.** Proses untuk menganalisis data dari kontrol detektif mengarah pada penentuan keberadaan insiden siber, yang biasanya merupakan pemicu untuk pelaksanaan satu atau lebih rencana respons.
- **Komunikasi.** Ada banyak pemangku kepentingan potensial dalam insiden siber, sehingga setiap rencana respons harus memasukkan strategi komunikasi untuk pemberitahuan dampak dan upaya penyelesaian yang tepat dan tepat waktu.

- **Respons Teknis dan Pemulihan.** Sifat insiden sangat menentukan kontrol perbaikan dan pemulihan teknis yang diperlukan, seringkali melibatkan koordinasi upaya internal dan eksternal.[24]

Mencapai tujuan bisnis ini dan mengikuti kerangka kerja respons insiden siber yang sudah mapan, seperti Kerangka untuk Meningkatkan Keamanan Siber Infrastruktur Kritis dari National Institute of Standards and Technology (NIST) memerlukan pengetahuan teknis yang berkaitan dengan implementasi, pemeliharaan, dan peningkatan yang dapat dilakukan oleh tim keamanan informasi dan teknologi informasi. menyediakan — pengetahuan yang mungkin atau mungkin tidak dimiliki oleh tim audit internal. Namun, ada banyak ruang secara bersamaan untuk orang lain dengan disiplin ilmu yang kurang teknis tetapi sama-sama berharga untuk memberikan nilai yang signifikan. Audit internal, dengan akses uniknya ke dan pemahaman tentang fungsi organisasi di semua departemen, serta perspektif independennya yang penting untuk memberikan jaminan objektif, adalah disiplin semacam itu.

“Dari perspektif audit internal, pendekatan terhadap respons insiden siber tidak berbeda dengan risiko lainnya karena fokusnya adalah pada proses aktual dan hasil dari proses tersebut,” kata DaMon Ross Sr., pendiri *Cyber Defense International, LLC*., dan mantan Wakil Presiden Senior, Kepala Operasi Keamanan Siber di SunTrust. “Bahkan dengan sifat teknis material, auditor internal mana pun yang terbiasa beroperasi di ruang proses akan mengambil apa yang penting dengan cukup cepat.”

Proses seperti itu lebih dari sekadar kemiripan dengan apa yang mungkin dilihat oleh audit internal dalam program kepatuhan *Sarbanes-Oxley* (SOX), rencana respons krisis, atau strategi manajemen risiko apa pun yang ditetapkan. “Organisasi yang berbeda memiliki terminologi yang berbeda, tetapi rencana insiden siber pada dasarnya adalah kebijakan yang menguraikan kapan insiden siber terjadi, apa peran dan tanggung jawab semua pihak yang berlaku, dan siapa yang perlu berada di meja untuk pengambilan keputusan,” kata Ross.

Tremblay mengungkapkan sentimen serupa. Kontrol yang relevan dengan risiko siber juga merupakan bagian dari kerangka kerja yang digunakan untuk mengelola risiko kepatuhan yang terkait dengan Sarbanes-Oxley, katanya.

Misalnya, salah satu langkah pertama yang diambil peretas ketika mereka membobol teknologi apa pun adalah mengakses hak dan hak istimewa yang diperlukan untuk mencapai tujuan mereka. Dalam skema risiko besar, ini termasuk dalam risiko akses yang tidak sah. Tidak ada perbedaan apakah itu berlaku untuk SOX atau risiko siber, kata Tremblay. “Risiko ketika diringkas menjadi bentuk paling sederhana, dan kontrol untuk mengurangi risiko tersebut, pada dasarnya identik.”

Kontrol terhadap dokumentasi

Seperti yang disebutkan Tremblay, kontrol yang terkandung dalam kebijakan semacam itu juga memiliki tumpang tindih yang signifikan dengan apa yang dapat dilihat dengan risiko organisasi lainnya. Salah satu contohnya adalah memiliki proses dokumentasi yang efektif. Ross setuju bahwa organisasi harus memahami seperti apa alur kerja yang mendokumentasikan insiden siber dengan benar, dan bagaimana semua bagian yang bergerak berjalan secara paralel, katanya.

“Ini bukan hanya untuk insiden besar. Setiap organisasi harus memiliki fungsi yang berhubungan dengan hal ini sehari-hari. Katakanlah komputer mendapat *malware* di dalamnya. Insiden kecil seperti itulah yang dapat berubah menjadi insiden yang lebih besar, dan jika yang terburuk terjadi, dokumentasi yang tepat membantu untuk memahami bagaimana hal itu meningkat. Fungsi itu adalah kontrol itu sendiri.”

Deteksi dan kontrol infrastruktur fisik

Kontrol penting lainnya, dan yang termasuk dalam rubrik risiko akses tidak sah, adalah infrastruktur fisik. Meskipun kontrol semacam itu mungkin tidak langsung terlintas dalam pikiran ketika membahas keamanan siber, akses tidak sah ke *hard drive* atau server tempat informasi sensitif disimpan bertanggung jawab atas 10% dari semua pelanggaran berbahaya pada tahun 2020, yang merugikan organisasi rata-rata $ 4,36 juta per pelanggaran, menurut penelitian dari *Ponemon Institute* yang diterbitkan oleh *IBM Security*.

[24]. IIA, *Audit Respons dan Pemulihan Insiden Siber*, Panduan Tambahan, Panduan Praktik, https://www.theiia.org/globalassets/documents/content/articles/guidance/gtag/2022/gtag_auditing_cyber_incident_response_and_recovery_final.pdf .

Infrastruktur tersebut bisa mencakup ruang *server* yang aman dengan akses terbatas, serta langkah-langkah keamanan yang lebih mendasar, seperti pintu terkunci di seluruh fasilitas. Meskipun keamanan infrastruktur itu penting, memiliki kontrol untuk mendeteksi dan mendokumentasikan aktivitas yang berpotensi mencurigakan dapat menjadi lebih relevan.

“Ketika saya berbicara tentang infrastruktur fisik, saya tidak sedang berbicara tentang pintu yang terkunci, tetapi memastikan ada notifikasi dan dokumentasi tindakan yang menimbulkan risiko nyata. Ini seperti hidangan makanan utama daripada makanan pembuka,” kata Tremblay.

Mengidentifikasi dan memberikan asurans untuk sistem semacam itu termasuk ke dalam keahlian mapan audit internal, kata Ross, menambahkan, “Audit internal memiliki kemampuan untuk mengidentifikasi sistem yang memiliki risiko tertinggi atau yang paling penting bagi kehidupan organisasi. Kemungkinan, pada kenyataannya, audit internal telah mengidentifikasi sistem-sistem ini sebagai bagian dari memberikan asurans kepatuhan terhadap undang-undang dan peraturan federal yang terkait dengan risiko lainnya. Hal yang diperlukan hanyalah memperluas pemikiran tersebut untuk memasukkan tipe penyediaan baru yang dapat menawarkan akses yang lebih tinggi.”

Penyelarasan harapan terhadap pemulihan

Dokumentasi yang efektif di setiap tahapan rencana atas respons insiden siber sangatlah penting. Hal yang sama pentingnya, adalah komunikasi data yang disediakan oleh dokumentasi tersebut dan penyelarasan atas deteksi organisasi dan harapan pemulihan terhadap insiden siber.

Menurut Tremblay, hal ini merupakan salah satu celah terbesar yang ia lihat di dalam rencana respons siber organisasi —dan dimana audit internal dapat memberikan nilai terbaiknya. "Ada dua peran audit internal dalam pemulihan bencana siber," katanya. "Yang pertama, pastikan insiden tersebut ada, dan anda dapat membuktikannya melalui dokumentasi, atau teknologi atau proses apapun yang Anda pakai. Kedua, dan hal yang menurut saya belum cukup dilakukan, adalah duduk bersama dengan seluruh pemngku kepentingan utama [untuk menentukan] kapan jadwal pemulihan yang realistis, yang didasarkan pada selera risiko organisasi."

Jadwal tersebut, kata Tremblay, akan ditetapkan oleh 'pemilik' aplikasi yang relevan di organisasi, yang bisa jadi CISO, kepala rantai pasokan, atau pemimpin lainnya, tergantung di mana insiden itu terjadi. Kunci audit internal adalah berfungsi sebagai penghubung antara pihak tersebut dan semua pihak lain yang bergantung pada aplikasi tersebut untuk melakukan pekerjaan sehari-hari.

"Misalnya, CISO mungkin mengatakan bahwa waktu penyelesaian selama 48 jam dapat diterima, tetapi jika anda tidak menyampaikannya kepada CFO atau pemimpin atau fungsi lain yang mengandalkan teknologi yang sedang dipakai tersebut dan meminta masukan dari mereka, berarti anda menyiapkan diri anda untuk sebuah potensi kekacauan," kata Tremblay. "Misalnya, CFO mungkin mengatakan bahwa 48 jam dapat diterima, tetapi hanya jika kita tidak sedang menutup pembukuan laporan keuangan. Tetapi jika CFO sedang menutup pembukuan, tidak ada waktu berhenti yang dapat diterima karena organisasi harus mengajukan perpanjangan, yang akan terlihat sangat buruk di pasar publik.”

Percakapan seperti ini tidak selalu mengharuskan satu pihak untuk mengesampingkan yang lain. Sebaliknya, melalui komunikasi tersebut, audit internal dapat memediasi konsensus sesuai dengan selera risiko organisasi. "Dalam kasus dimana ada ketidaksesuaian," kata Tremblay, "apa yang bisa ditanyakan internal [audit] adalah, 'Apakah itu benar-benar layak terjadi?' CEO mungkin berkata, 'Ya, benar, karena itu akan menghabiskan satu juta dolar untuk menyelesaikan masalah itu.' Apa yang sebenarnya kami lakukan adalah memastikan bahwa rencana tersebut benar-benar dikembangkan di sekitar pemangku kepentingan terkait teknologi tersebut.”

Ia melanjutkan, “Saya pikir ini adalah bidang dimana kita, sebagai sebuah profesi, belum kuasai dapat dengan baik. Saya pikir kita mencoba mencentang kotak untuk memvalidasi hal-hal tertentu tanpa benar-benar mengatakan, 'Hei, sebagai bagian dari tinjauan kami atas kontrol seputar respons insiden, kami mengidentifikasi kesenjangan dalam persyaratan antara pemangku kepentingan teknologi tertentu.' Itu sangat valid. Ini mengidentifikasi risiko bisnis yang berharga bagi organisasi namun sebelumnya tidak teridentifikasi.”

Fungsi Silang (Cross Function)

Ini adalah kesalahpahaman umum bahwa kepemilikan utama respons keamanan siber berada di tangan CISO dan tim keamanan. Sebagian besar memang betul. Sementara pengalaman dan keahlian yang dibutuhkan untuk menerapkan aspek

yang lebih teknis dari strategi siber kemungkinan besar akan ditemukan di departemen itu, berbahaya untuk berasumsi bahwa departemen tersebut akan memiliki *bandwidth* — atau keinginan — untuk memikul bebannya sendiri.

"Respons insiden siber, paling tidak, harus menjadi sebuah proses lintas fungsi," kata Ross. “Alasan terbesar dari kelambatan waktu respons organisasi yang saya lihat bukanlah departemen keamanan informasi itu sendiri dalam hal pengetahuan, melainkan penetapan peran dan tanggung jawab lintas fungsi dengan departemen dimana keamanan bukan tanggung jawab utama mereka. Mereka memiliki hal lain untuk dilakukan."

Menurut Ross, mengoreksi kesalahpahaman ini dan mengembangkan gagasan tanggung jawab bersama di seluruh pemangku kepentingan harus menjadi area utama fokus audit internal. "Penekanannya tidak boleh pada tim keamanan dan apa yang mereka lakukan, tetapi lebih kepada bagaimana proses mereka didukung oleh entitas lain di seluruh perusahaan yang berkepentingan dengan mereka. Tim keamanan tahu apa yang harus dilakukan, tetapi mereka tidak dapat memaksa tim TI dan pengembang *back-end* untuk membantu dengan cara yang kritis. Ada banyak politik organisasi yang terlibat, dan ketika saya berada di posisi itu, saya menemukan mitra yang berharga dalam audit internal. Tim keamanan tidak bisa bertarung sendirian. Jika Anda bisa mendapatkan pihak yang relatif netral untuk membantu mengidentifikasi dimana organisasi memiliki kesenjangan dalam prosesnya,

Satu strategi yang bermanfaat untuk menyoroti kesenjangan ini dan mengklarifikasi peran, kata Ross, adalah audit internal, untuk bekerja sama dengan konsultan eksternal, untuk memfasilitasi simulasi *tabletop*. “Begitu Anda memiliki rencana respons insiden siber yang dapat diuji, simulasi *tabletop* membawa CIO, CISO, pemimpin TI, CEO, audit internal —semua pemangku kepentingan terkait— bersama-sama di ruang konferensi atau panggilan Zoom untuk menelusuri skenario yang masuk akal. Bahkan tanpa keahlian teknis, audit internal dapat memfasilitasi diskusi dengan menanyakan siapa melakukan apa dan menilai bagaimana tanggung jawab tersebut selaras dengan kenyataan. Mereka dapat mengatakan, 'Pada titik ini, tim Anda harus menjalankan X dan Y sesuai dengan rencana kami, tetapi pada kenyataannya, Anda dapat melakukan Z.' Saat itulah Anda akan mendengar omong kosong yang sebenarnya. Sebagian besar organisasi harus melakukannya setidaknya setahun sekali, tetapi audit internal harus benar-benar bertanggung jawab untuk ini.”

Kesimpulan

Pengembangan lingkungan risiko

Audit internal, melalui posisinya yang unik di dalam organisasi, layak mendapat tempat duduk di meja ketika berbicara mengenai rencana respons insiden siber organisasi. Namun hal ini tidak menjadi alasan bagi audit internal untuk mengupayakan pemahaman yang lebih mendalam mengenai keamanan siber. Hal ini mengingat bahwa di masa depan, dimana infrastruktur fisik mulai ditinggalkan dan beralih ke teknologi berbasis *cloud*, keahlian yang lebih luas dari audit internal tentu akan dibutuhkan dan diharapkan.

"Ketika saya memulai karir saya di audit internal, salah satu nilai jual terbesar saya adalah memiliki peran yang sangat umum," kata Tremblay. "Anda harus melihat dan belajar tentang banyak hal yang tidak perlu anda kuasai. Tapi ada perubahan besar seputar teknologi, saya mulai bertanya-tanya apakah hari-hari auditor internal *generalist* sudah sudah akan berakhir. Sebaliknya, mungkin audit internal suatu hari nanti akan menjadi lebih dari sekadar ahli materi / *subject matter exper*t (SME) seputar hal-hal yang secara inheren penting bagi organisasi. Sehingga, alih-alih memiliki tim audit yang terdiri dari 8-10 auditor operasional, kepatuhan dan pelaporan keuangan, organisasi dapat memiliki auditor keamanan siber, satu auditor LST, dll."

Ross mengiyakan. "Pada titik tertentu dengan munculnya teknologi baru, bagaimana anda benar-benar memahami kesenjangan dalam proses respon di tingkat yang dalam jika Anda tidak berupaya bisa masuk sedalam itu? Anda tidak akan pernah benar-benar masuk."

Ada banyak hal yang dapat dicapai dengan pengetahuan dan sumber daya yang ada, tetapi masa depan baru yang menarik dan radikal akan datang. Audit internal perlu menjadi bagian dari masa depan itu.

Diterjemahkan dan diselaraskan oleh volunteer IIA Indonesia:

1. I Made Suandi Putra, CIA, CRMA
2. Dewi Andriati, CIA, CRMA
3. Octavian Abrianto, CIA
4. Fauzan Wahyuabdi Pratama, CIA
5. Armando Reagen Taruli Tua
6. I Gde Wiyadnya
7. Riani Nurainah Lisnasari, CIA

Isu Sebelumnya

Untuk mengakses terbitan Global Perspectives and Insights sebelumnya, kunjungi www.theiia.org/GPI.

Umpan Balik Pembaca

Kirim pertanyaan dan komentar ke globalperspectives@theiia.org.

Tentang IIA

The Institute of Internal Auditors (IIA) adalah asosiasi profesional internasional yang melayani lebih dari 215.000 anggota global dan telah memberikan 180.000 sertifikasi Certified Internal Auditor (CIA) di seluruh dunia. Didirikan pada tahun 1941, IIA diakui sebagai pemimpin profesi audit internal dalam standar, sertifikasi, pendidikan, penelitian, dan bimbingan teknis di seluruh dunia. Untuk informasi lebih lanjut, kunjungi theiia.org.

Disclaimer

Hak Cipta

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