PANDANGAN & WAWASAN GLOBAL

Keamanan Siber

BAGIAN I: *Staffing* dan Pengembangan untuk Generasi Berikutnya

BAGIAN II: Kecerdasan Buatan (AI) – Kawan dan Lawan Keamanan Siber

BAGIAN III: Manajemen Risiko Keamanan Siber Pihak Ketiga

AUDITBOARD

The Institute of Internal Auditors

Contents

Bagian 1: Staffing dan Pengembangan untuk Generasi Berikutnya **3**

PENDAHULUAN **5**

Sebuah Tantangan yang Jelas **6**

Upaya Keamanan Siber Audit Internal Semakin Berkembang 6

Tantangan **7**

Pemahaman yang Jernih tentang Lingkungan Siber Adalah Hal yang Mendasar 7

Penguatan Sumber Daya Audit Internal **9**

Mempekerjakan dan Mengembangkan Talenta Siber Audit Internal 9

Kesimpulan **11**

Bagian 2: Kecerdasan Buatan (AI) – Kawan dan Lawan Keamanan Siber **12**

PENDAHULUAN **14**

AI dalam Pekerjaan **15**

Audit Internal Harus Mengeksplorasi Penggunaan dan Ancaman AI 15

Pertimbangan Manajemen Risiko **17**

Audit Internal bisa Membantu Organisasi Menghindari Dampak Buruk AI 17

Melindungi AI – dan Berlindung dari AI **18**

Melindungi Integritas Sistem AI, Akses 18

Jangan Lupakan Elemen Manusia 18

Kesimpulan **19**

Bagian 3: Manajemen Risiko Keamanan Siber Pihak Ketiga **20**

PENDAHULUAN **22**

Sebuah Tantangan Besar **23**

Risiko Meningkat 23

Pendekatan Audit Internal **25**

Membangun budaya aksi siber 25

Pendekatan pemantauan berkelanjutan berdasarkan tingkat risiko 25

Merangkul Solusi Perangkat Lunak 27

Fokus pada *offboarding* dan juga *onboarding* 27

Kesimpulan **28**

Diterjemahkan dan diselaraskan oleh IIA Indonesia Volunteer:

1. I Made Suandi Putra, CIA, CRMA

2. Fauzan Wahyuabdi Pratama, CIA, CGAP

3. Indra Permana, CIA, CRMA

4. Diana Laurencia Sidauruk, CIA

5. Riani Nurainah Lisnasari, CIA

6. I Gde Wiyadnya

7. Agnes Maria Widiyanti

Bagian 1: *Staffing* dan Pengembangan untuk Generasi Berikutnya

Tentang Para Ahli

Aneta Waberska, CISA

Aneta ialah Direktur Keamanan Informasi dan Produk Kepatuhan di AuditBoard. Beliau memiliki pengalaman lebih dari 15 tahun dalam bidang audit TI dan kepatuhan serta bergabung dengan AuditBoard untuk fokus pada pengembangan produk yang melayani pengguna risiko TI dan kepatuhan, memanfaatkan pengalaman industrinya. Aneta memulai karirnya di KPMG dan PwC, dimana beliau membantu klien menerapkan dan menilai kerangka kerja seperti SOC 1 dan SOC 2. Beliau telah bekerja dengan berbagai perusahaan dengan berbagai ukuran untuk menerapkan dan mengelola program kepatuhan dengan berbagai kompleksitas, termasuk mengelola kebijakan di seluruh perusahaan, program manajemen risiko pihak ketiga, Beliau telah bekerja sama dengan erat dengan manajemen untuk menerapkan kontrol guna memenuhi persyaratan kerangka kerja keamanan, dan bekerja sama dengan manajemen eksekutif untuk memastikan kepatuhan mendukung tujuan strategis perusahaan.

Uday Gulvadi, CIA, CPA, CAMS, CISA

Uday adalah seorang Managing Director di divisi Sengketa, Kepatuhan dan Investigasi di Stout, dan sekaligus menjadi pemimpin bersama untuk praktik kepatuhan peraturan dan kejahatan keuangan nasional mereka. Uday memiliki lebih dari 20 tahun pengalaman sebagai pemimpin praktik kejahatan keuangan, audit internal, audit sistem informasi, dan konsultasi risiko. Beliau spesialis dalam memberikan saran kepada dewan direksi, komite audit, dan manajemen senior mengenai berbagai tantangan terkait kepatuhan terhadap kejahatan keuangan, risiko TI dan siber, tata kelola, serta masalah risiko dan kepatuhan, termasuk manajemen risiko perusahaan, tata kelola program AML dan sanksi, validasi model, audit internal berbasis risiko, teknologi informasi, dan audit dan kontrol keamanan siber. Klien Uday beragam, mulai dari beberapa bank dan lembaga keuangan terbesar di dunia hingga perusahaan jasa keuangan yang lebih kecil.

PENDAHULUAN

Keamanan siber merupakan ancaman signifikan bagi organisasi dari berbagai ukuran. Contoh baru-baru ini menggambarkan betapa cepatnya segala sesuatu bisa menjadi salah. Sebuah serangan siber mengganggu pengiriman dari Ace Hardware *Corporation* ke *dealer*-nya dan memaksanya untuk menonaktifkan sementara pemesanan online pelanggan. Sebuah serangan ransomware di perusahaan telekomunikasi besar Chili mengganggu layanan termasuk pusat data, akses internet, dan voice-over-IP. Dan, menunjukkan bahwa entitas yang lebih kecil juga dapat terpengaruh, akses online publik ke catatan tanah dan indeks kelahiran, kematian, dan pernikahan terganggu oleh serangan siber di Cabarrus County, NC.

Audit internal sangat cocok untuk memainkan peran kunci dalam membantu mengelola risiko siber, namun harus memiliki sumber daya yang dibutuhkan untuk menjalankan peran tersebut. Audit Internal juga harus memiliki pengetahuan dan keterampilan yang diperlukan untuk mengidentifikasi dan memberi saran tentang ancaman siber yang dihadapi organisasi. Dalam melakukan penilaian keamanan siber, "sangat penting untuk melibatkan profesional audit dengan kedalaman keterampilan teknis dan pengetahuan yang sesuai tentang lingkungan risiko saat ini," menurut Deloitte.[1]

Laporan singkat ini merupakan bagian pertama dari tiga bagian dalam seri tentang keamanan siber. Karena pemimpin audit internal harus memahami ancaman-ancaman tersebut sebelum mereka dapat memiliki staf untuk menemuinya, ini dimulai dengan memeriksa tantangan keamanan siber untuk auditor internal dan organisasi mereka. Ini juga mencakup opsi dan strategi yang dapat diikuti oleh para pemimpin audit internal untuk memastikan mereka memiliki talenta yang mereka butuhkan untuk mengatasi risiko siber yang sedang berlangsung.

[1] "Cybersecurity and the Role of Internal Audit—An Urgent Call to Action," Deloitte Development LLC, 2017.

Sebuah Tantangan yang Jelas

Keamanan siber tetap menjadi risiko utama

Upaya Keamanan Siber Audit Internal Semakin Berkembang

"Auditor internal harus melihat keseluruhan organisasi dan mengambil pendekatan berbasis risiko," ujar Aneta Waberska, CISA, direktur keamanan informasi dan produk kepatuhan di AuditBoard. "Risiko siber berada di urutan teratas dalam daftar untuk sebagian besar organisasi."

Para auditor internal tampaknya sangat menyadari ancaman yang ditimbulkan oleh risiko siber. Menurut survei global The Internal Audit Foundation terhadap para pemimpin audit internal, keamanan siber diidentifikasi sebagai risiko teratas memasuki tahun 2024. Keamanan siber, bersama dengan Sumber Daya Manusia dan Kelangsungan Bisnis, terdaftar sebagai tiga risiko teratas dalam survei Risk in Focus 2024[2] terhadap lebih dari 4.200 Chief Audit Executive (CAE), bahkan 73% responden mencantumkan keamanan siber sebagai lima risiko teratas.

Di Amerika Utara, 78% pemimpin audit internal menggambarkan keamanan siber sebagai risiko tinggi atau sangat tinggi dalam organisasi mereka, menurut The Institute of Internal Auditors 2023 North American Pulse of Internal Audit.[3] Auditor yang disurvei mencurahkan 10% dari rencana audit mereka untuk keamanan siber, dengan masalah TI membentuk 9% lainnya. Selain itu, hampir 70% fungsi meninjau area berisiko tinggi yang mencakup keamanan siber dan TI setiap tahun atau terus menerus, menurut temuan survei IIA *Pulse* tersebut.

Beberapa bahaya keamanan siber yang perlu diingat meliputi:

- Pelanggaran yang memungkinkan penjahat mencuri informasi penting atau yang mengekspos data pelanggan atau mitra bisnis.
- Serangan ransomware yang membuat organisasi tidak mungkin melakukan fungsi-fungsi utama atau mengakses informasi yang diperlukan tanpa terlebih dahulu membayar uang tebusan kepada penjahat siber.
- Malware yang dapat mendatangkan malapetaka pada sistem.

Serangan siber memiliki konsekuensi yang lebih besar dari yang terlihat, seperti kerugian finansial ketika fungsi bisnis terganggu atau jika pelanggan atau mitra bisnis kehilangan kepercayaan pada suatu organisasi dan berhenti melakukan bisnis dengannya. Terlebih lagi, setelah insiden siber ditemukan, organisasi harus menginvestasikan waktu dan uang dalam penyelidikan forensik untuk memahami apa yang terjadi dan kapan, melakukan remediasi untuk memperbaiki kerusakan, dan untuk menentukan apakah dampak dari serangan tersebut material dari perspektif keuangan dan operasional untuk memenuhi persyaratan pelaporan peraturan.

Maka, tidak mengherankan bahwa pengeluaran keamanan siber berkembang dengan cepat. Pada awal tahun 2023, Canalys memperkirakan pengeluaran keamanan siber global akan melonjak 13,2% sepanjang tahun, dengan potensi mencapai $224 miliar.[4]

"Perusahaan-perusahaan telah menyadari bahwa ancaman ini membawa konsekuensi bisnis dan keuangan yang sangat nyata," kata Uday Gulvadi, CIA, CPA, CAMS, CISA, Managing Director di grup Sengketa, Kepatuhan, dan Investigasi di Stout. Ancaman-ancaman tersebut tentu saja menjadi perhatian utama bagi komite audit, katanya, dan "audit internal diminta untuk melangkah lebih jauh dan memberikan asurans di area-area ini."

---

[2] "Risk in Focus 2024," The Internal Audit Foundation, 2023
[3] "2023 North American Pulse of Internal Audit," The Institute of Internal Auditors, 2023
[4] "Cybersecurity investment to grow by 13% in 2023", Canalys, Jan. 18, 2023, https://www.canalys.com/newsroom/cybersecurity-forecast-2023

Tantangan

Pendekatan Keamanan Siber, Dampak Kematangan terhadap *Staffing*

Pemahaman yang Jernih tentang Lingkungan Siber Adalah Hal yang Mendasar

Untuk mempekerjakan orang yang tepat untuk membantu audit internal mendukung manajemen risiko siber dan menawarkan peluang pengembangan yang sesuai, penting untuk memahami sepenuhnya kondisi dan risiko keamanan siber organisasi yang unik. Beberapa faktor dan tantangan harus dipertimbangkan.

Sebuah Pola Pikir Manual

Banyak tim audit internal yang secara tradisional terbiasa memikirkan kontrol internal dan berbagai proses dari perspektif manual, kata Waberska. Namun, transformasi digital yang sedang berlangsung dalam bisnis menuntut tim untuk menyadari bagaimana solusi digital dapat meningkatkan dan memperbaiki audit internal dan proses lainnya di seluruh organisasi, termasuk keamanan siber. Pada saat yang sama, auditor internal juga harus memahami risiko yang ditimbulkan oleh transformasi digital itu sendiri bagi organisasi, karena penjahat siber yang semakin canggih mengeksploitasi kerentanan yang dapat ditimbulkan oleh lingkungan digital.

Jika, misalnya, sebuah organisasi beroperasi di *cloud* atau menggunakan atau berencana untuk menggunakan teknologi canggih atau yang sedang berkembang, organisasi tersebut akan membutuhkan orang-orang yang telah bekerja dengan alat-alat ini. Anggota tim tidak harus ahli dalam teknologi, kata Waberska, namun paparan terhadap lingkungan *cloud* atau solusi lain akan memberikan pemahaman yang lebih baik terhadap risiko terkait. Selain merekrut untuk keterampilan ini, tim audit juga harus memastikan untuk memasukkan teknologi baru dalam pelatihan dan pengembangan staf yang ada.

Pengendalian Internal

Auditor internal dilatih untuk memastikan bahwa organisasi memiliki kontrol yang tepat untuk melindungi dari risiko yang dihadapinya. Terkait dengan risiko siber, pengendalian internal harus berfungsi untuk memastikan bahwa teknologi informasi organisasi tidak terganggu dan fungsi bisnis dapat tetap berjalan.

Untuk mengidentifikasi dan memberikan saran mengenai risiko keamanan siber, tim audit internal perlu memahami kontrol keamanan TI untuk teknologi yang digunakan oleh organisasi mereka. Dalam bekerja dengan *cloud*, misalnya, kontrol akan berbeda dengan yang digunakan dengan pusat data internal, kata Waberska. Mereka juga perlu memahami kontrol mana yang sesuai dengan mempertimbangkan ancaman kejahatan siber terhadap privasi dan implikasinya terhadap rencana audit program privasi organisasi mereka.

Regulasi Pengungkapan dan Perlindungan Data

Organisasi sekarang diminta untuk lebih terbuka dalam melaporkan upaya keamanan siber mereka. Auditor internal akan harus memahami peraturan mana yang mempengaruhi perusahaan mereka dan mampu mengevaluasi kebutuhan kepatuhan. Sebagai salah satu contoh penting, pada bulan Agustus, *U.S. Securities and Exchange Commission (SEC)* mengeluarkan aturan final tentang Manajemen Risiko Keamanan Siber, Strategi, Tata Kelola, dan Pengungkapan Insiden, yang mengharuskan perusahaan publik untuk memberikan transparansi yang lebih besar ketika mereka mengalami serangan siber dan mengungkapkan informasi spesifik tentang upaya mereka untuk mengurangi risiko siber. IIA memberikan komentar terhadap peraturan tersebut ketika masih dalam tahap

proposal. IIA berencana untuk terus bekerja sama dengan SEC untuk mengembangkan panduan implementasi, terutama dalam menentukan materialitas insiden siber dan mendefinisikan istilah "keamanan siber" dengan lebih baik.

Karena sifat bisnis yang semakin multinasional dan semakin banyaknya peraturan keamanan siber di seluruh dunia, auditor internal harus terbiasa dengan semua undang-undang keamanan data dan privasi yang dapat mempengaruhi organisasi mereka, seperti the European Union's General Data Protection Regulation. Bahkan, menurut Konferensi PBB tentang Perdagangan dan Pembangunan, 137 dari 194 negara telah memberlakukan undang-undang untuk mengamankan perlindungan data dan privasi.

Sistem TI

Organisasi mana pun yang memiliki teknologi dasar terlibat dalam beberapa jenis sistem TI, dan semuanya rentan terhadap risiko siber. Mengingat volume sistem dan potensi kelemahan serta ancaman yang terlibat, penting bagi perusahaan dan audit internal untuk memahami sistem mana yang paling penting. "Kami tidak akan pernah bisa menerapkan tingkat pengendalian yang sama pada semua sistem," kata Waberska. Menetapkan prioritas akan melibatkan mengajukan pertanyaan seperti:

- Sistem manakah yang penting bagi berfungsinya organisasi? Pertanyaan tersebut dapat dijawab dengan mempertimbangkan apakah–dan untuk berapa lama–organisasi akan mampu terus menjalankan bisnis atau mencapai tujuan utama tanpa hal tersebut.
- Manakah yang memproses data paling sensitif? Itu mungkin termasuk informasi rahasia perusahaan atau informasi identitas pribadi.
- Manakah yang menyimpan data unik atau sulit tergantikan?[5]

Pihak Ketiga

Bahkan organisasi kecil dan menengah pun terlibat dengan pihak ketiga yang menangani data mereka. Hal ini dapat terjadi melalui aplikasi *cloud* atau, untuk organisasi yang lebih besar, mungkin melalui pusat pemrosesan di luar negeri. Vendor ini dapat menangani data penting organisasi dan informasi identitas pribadi pelanggan, dan data tersebut dapat disimpan di mana saja di dunia, kata Gulvadi. Oleh karena itu, "sangat penting untuk memahami keseluruhan lanskap aset TI," termasuk di mana aset tersebut berada dan apakah ada pengendalian yang tepat terhadap aset tersebut, katanya.

Organisasi harus mengevaluasi proses keamanan siber pihak ketiga sebelum mereka berbagi data dengan mereka dan memantau proses tersebut setelah pihak ketiga mulai menggunakan data. Dalam beberapa kasus, organisasi perlu mempertahankan hak untuk mengaudit pihak ketiga tersebut. "Jika Anda membagikan data pelanggan dengan pihak lain, Anda perlu memastikan mereka akan melindungi mereka dengan cara yang sama seperti yang dilakukan perusahaan Anda," kata Waberska. Perusahaan harus meninjau laporan pengesahan pihak ketiga seperti SOC 2, yang mengevaluasi pengendalian internal mereka untuk melihat seberapa baik laporan tersebut mengatasi risiko, atau jenis pengesahan atau sertifikasi lainnya yang terkait dengan perlindungan kategori data yang relevan.

Memastikan Akses dan Ketersediaan yang Aman

Ada *trade-off* antara memastikan organisasi dapat melindungi data dan sistem sekaligus menjamin bahwa informasi dan sistem tersedia untuk digunakan sesuai kebutuhan untuk mencapai tujuan bisnis, kata Gulvadi. Untuk menjaga keseimbangan, organisasi harus memilih pengendalian yang melindungi data tanpa membebani akses ke informasi yang diperlukan untuk layanan pelanggan atau fungsi bisnis penting lainnya. Penentuan ini akan lebih mudah dilakukan setelah organisasi mempertimbangkan sistem mana yang memerlukan tingkat keamanan tertinggi. Beberapa mungkin perlu dilindungi dengan autentikasi multifaktor, protokol enkripsi, dan perangkat lunak pencegahan kehilangan data, sementara yang lain tidak memerlukan tingkat perincian tersebut.

---

[5] "*CISA Insights – Cyber, Secure High Value Assets (HVAs),"* U.S. Department of Homeland Security, https://www.cisa.gov/sites/default/files/publications/CISAInsights-Cyber-SecureHighValueAssets_S508C.pdf

Penguatan Sumber Daya Audit Internal

Staf keamanan siber tetap menjadi prioritas utama

Mempekerjakan dan Mengembangkan Talenta Siber Audit Internal

Mengingat risiko-risiko ini, bagaimana audit internal dapat membangun dan mempertahankan tim yang dapat mengatasi risiko-risiko tersebut? Jawaban spesifiknya akan berbeda-beda di setiap organisasi, namun ada beberapa rekomendasi yang berlaku untuk semua organisasi.

Carilah Perpaduan Keterampilan

Untuk mengatasi risiko siber, tim audit internal memerlukan pemahaman mendalam tentang sisi teknis keamanan siber serta kemampuan untuk memahami konsekuensi masalah keamanan terhadap bisnis, kata Gulvadi. Di masa lalu, auditor TI cenderung kuat dalam aspek teknis keamanan informasi, namun mereka sering tidak fokus pada bagaimana risiko terkait mempengaruhi kemampuan organisasi untuk memenuhi tujuan bisnisnya. Kemampuan untuk mengartikulasikan dampak bisnis bisa sangat berharga jika audit internal perlu mendapatkan dukungan manajemen atas investasi yang diperlukan dalam peningkatan teknologi atau pengendalian atau penambahan staf.

Gulvadi melihat lebih banyak upaya untuk membangun tim yang memadukan pengetahuan teknis dengan pemahaman tentang tujuan, proses, dan rantai nilai bisnis. Dalam beberapa kasus, tim audit internal menemukan profesional yang memiliki kedua keterampilan tersebut, namun dalam kasus lain, tim mencakup profesional yang keterampilannya saling melengkapi. Organisasi dapat mempertimbangkan untuk menawarkan pelatihan untuk memberikan setiap jenis profesional pengetahuan dasar tentang disiplin ilmu lainnya.

Integrasikan Keterampilan dalam Teknologi yang Sedang Berkembang

Banyak tim audit internal menambahkan profesional dengan keahlian dalam analisis data, kecerdasan buatan / *artificial inteligence (AI)* , dan pembelajaran mesin seiring mereka beralih dari pengujian berbasis sampel. “Anda dapat menggunakan AI untuk menguji seluruh populasi dan meningkatkan deteksi anomali,” kata Gulvadi. Hal ini tidak hanya meningkatkan efisiensi dan keandalan, namun juga membantu auditor internal mengimbangi penjahat siber, yang semakin canggih dalam penggunaan teknologi baru.

Selidiki Pengalihdayaan

Beberapa tim audit internal membawa tim alih daya o untuk meningkatkan keterampilan teknis atau bisnis. Profesional dengan keahlian khusus di bidang keamanan siber atau TI dapat dimasukkan ke dalam tim audit internal berdasarkan proyek atau jangka panjang sesuai kebutuhan. Ketika anggota tim audit internal bekerja bersama para ahli ini, mereka dapat membantu kontraktor meningkatkan pengetahuan mereka dan menavigasi proses dan prosedur perusahaan dengan lebih baik. Pada saat yang sama, paparan terhadap pakar dari luar dapat membantu memperluas basis pengetahuan anggota tim. Dalam mengevaluasi opsi pengalihdayaan, Gulvadi merekomendasikan untuk memeriksa sertifikasi dan pengalaman sebelumnya dari anggota tim untuk memastikan mereka cocok atau bahkan meningkatkan keterampilan tim saat ini.

Pertimbangkan Kolaborasi

Terkadang keahlian yang dibutuhkan tim audit internal mungkin tersedia secara internal di berbagai bidang seperti TI, keamanan, atau kepatuhan. Kemitraan yang baik, sambil menjaga independensi auditor, akan memperkenalkan anggota tim audit internal pada berbagai wawasan dan pengetahuan baru tentang ekosistem teknologi dan risiko organisasi. Hal ini juga menjadi landasan bagi audit yang bermanfaat di masa depan karena tim lain akan mengetahui bahwa audit internal memiliki tujuan yang sama yaitu melindungi

organisasi dari risiko yang tidak perlu dan memastikan bahwa organisasi dapat mencapai tujuannya. Komunikasi terbuka juga dapat membantu tim lain mengatasi kekhawatiran mengenai tujuan audit internal. “Tim TI dan keamanan fokus untuk memperbaiki masalah penting dan menemukan solusi,” kata Waberska. “Mereka memahami risiko dan perlunya melakukan memitigasi. Kemampuan audit internal untuk melakukan percakapan yang sangat berfokus pada risiko menjelaskan mengapa pengendalian tertentu diperlukan untuk membuat audit internal menjadi lebih efektif.”

Membangun Hubungan Internal

Semua anggota tim audit internal dapat memperoleh manfaat dari membangun dan memelihara hubungan dengan profesional lain di tim keamanan, kepatuhan, dan TI organisasi mereka untuk mempelajari pekerjaan mereka saat ini, meskipun mereka tidak berkolaborasi dalam proyek tertentu. “Memahami apa yang terjadi di lingkungan perusahaan sangatlah penting,” kata Waberska, dan hubungan ini dapat memastikan tim mendapatkan pembaruan tepat waktu. Audit khusus akan mengungkap tren dan ancaman, “tetapi lebih baik mengetahui apa yang berubah sesegera mungkin,” katanya.

Manfaatkan Sumber Daya yang Tersedia

“Jika tim audit internal meluangkan waktu untuk mempelajari teknologi modern setidaknya pada tingkat tinggi dan risiko yang menyertainya, mereka akan selalu mengetahui perkembangan risiko saat ini dan yang akan muncul,” kata Waberska. Pilihannya mencakup Cybersecurity Resource Center IIA, yang mencakup berbagai panduan keamanan siber, penelitian, program bersertifikat, dan informasi tentang konferensi terkait, seperti Cybersecurity Virtual Conference tahunan IIA. AuditBoard juga menyediakan berbagai sumber daya keamanan siber yang dapat diakses melalui halaman resources.

Risk in Focus 2024, dari *The Internal Audit Foundation*, mengeksplorasi risiko keamanan siber secara global dan memberikan perspektif regional yang unik tentang bagaimana keamanan siber dan risiko utama lainnya dipandang dan dikelola di seluruh dunia.

Kesimpulan

Survei IIA *Pulse* tahun 2023 menemukan bahwa pertumbuhan staf audit internal meningkat namun belum kembali ke tingkat sebelum COVID. Para pemimpin audit internal harus ingat bahwa generasi yang memasuki dunia kerja adalah generasi yang paham digital. Adalah cerdas untuk mempertimbangkan cara terbaik untuk menggunakan pengetahuan yang mereka bawa, kata Gulvadi. Audit internal juga akan membedakan dirinya dalam lingkungan kepegawaian yang kompetitif dengan menawarkan generasi baru kesempatan untuk menggunakan teknologi baru seperti AI/ML untuk menawarkan wawasan yang akan membantu memecahkan masalah bisnis yang penting. Ketika audit internal terus membangun kembali tim atau memperluas keahlian mereka untuk menghadapi tantangan baru, mereka harus menggunakan saran dan wawasan dalam laporan singkat ini dalam perencanaan mereka.

Bagian 2: Kecerdasan Buatan (AI) – Kawan dan Lawan Keamanan Siber

Tentang Para Ahli

Aneta Waberska, CISA

Aneta adalah Direktur Produk Keamanan Informasi dan Kepatuhan di AuditBoard. Dia memiliki pengalaman lebih dari 15 tahun di bidang audit TI dan ranah kepatuhan dan bergabung dengan AuditBoard untuk fokus pada upaya pengembangan produk yang melayani pengguna risiko TI dan kepatuhan, memanfaatkan pengalaman industrinya. Aneta memulai karirnya di KPMG dan PwC, di mana dia membantu klien menerapkan dan menilai kerangka kerja seperti SOC 1 dan SOC 2. Dia telah bekerja dengan perusahaan-perusahaan dari berbagai ukuran untuk menerapkan dan mengelola program kepatuhan dengan kompleksitas yang berbeda-beda, termasuk mengelola kebijakan di seluruh perusahaan, program manajemen risiko pihak ketiga, Dia telah bekerja sama dengan manajemen untuk menerapkan kontrol guna memenuhi persyaratan kerangka keamanan, dan bekerja dengan manajemen eksekutif untuk memastikan kepatuhan mendukung tujuan strategis perusahaan.

Terry Grafenstine, CIA, CPA, CISSP, CISA, CRISC, CGAP, CGEIT

Terry adalah Wakil Ketua Senior di Dewan Direksi Global The Institute of Internal Auditors (IIA) dan *Chief Audit Executive* di Pentagon Federal Credit Union (PenFed) pada tahun 2023–24. Atas kontribusinya yang luar biasa terhadap profesi audit terkait siber dan teknologi, Terry diakui oleh IIA sebagai salah satu dari "Sepuluh Tokoh Pemikir Audit Teratas Dekade Ini". Beliau juga dilantik ke dalam *Hall of Distinguished Audit Practitioners IIA*. Sebelumnya, Terry telah memegang berbagai posisi kepemimpinan di Citi dan Deloitte, serta pernah menjabat sebagai Inspektur Jenderal yang ditunjuk untuk Dewan Perwakilan Rakyat Amerika Serikat.

PENDAHULUAN

Keamanan siber adalah risiko utama yang dipertimbangkan oleh auditor internal, dan hal ini akan tetap menjadi masalah di masa mendatang. Memang benar, ini adalah satu-satunya risiko yang menghabiskan waktu dan upaya terbesar mereka, *menurut Risk In Focus 2024*. Seri laporan yang dibuat oleh Yayasan Audit Internal *The Institute of Internal Auditor* (IIA) menanyakan kepada *Chief Audit Executive* dan direktur dari seluruh dunia tentang risiko-risiko utama yang dihadapi organisasi mereka, dan bagaimana mereka memperkirakan gambaran ancaman akan berubah dalam tiga tahun ke depan.

Temuan *Risk in Focus 2024* menunjukkan kompleksitas keamanan siber sebagai sebuah risiko dan tantangan tambahan yang berasal dari perubahan yang hampir konstan dalam teknologi dan cara penggunaannya. Hal ini juga tercermin dalam temuan laporan tersebut. Para pemimpin audit internal memperkirakan ancaman disrupsi digital akan melonjak dari peringkat kelima dalam daftar ancaman saat ini menjadi peringkat kedua dalam tiga tahun ke depan.

Laporan singkat ini, yang merupakan bagian kedua dari tiga bagian seri keamanan siber, mengkaji bagaimana AI berkontribusi terhadap tantangan dan peluang keamanan siber, dan apa yang perlu diketahui auditor internal tentang bidang risiko yang muncul dan berkembang ini sebagai pertimbangan keamanan siber. AI sangat menjanjikan sebagai alat canggih untuk meningkatkan efisiensi, produktivitas, dan manajemen risiko di hampir semua organisasi. Namun, hal ini juga menghadirkan tantangan manajemen risiko baru, termasuk pertimbangan etis, bahaya bias algoritmik, dan ketergantungan yang berlebihan atau buta terhadap penggunaan AI. Meskipun teknologi ini dapat menjadi alat yang berharga dalam memerangi serangan siber, pelaku kejahatan juga menggunakannya untuk melakukan kejahatan.

AI dalam Pekerjaan

Pedang Siber Bermata Dua

Audit Internal Harus Mengeksplorasi Penggunaan dan Ancaman AI

Istilah kecerdasan buatan atau *artificial intelligence (AI)* mengacu pada teknologi yang dapat meniru kecerdasan manusia, seperti belajar, menalar, dan bekerja untuk memecahkan masalah yang sulit. Ini mencakup beberapa jenis teknologi, termasuk pembelajaran mesin, atau kemampuan sistem untuk belajar dari data dan menerapkan pembelajaran tersebut.

Salah satu cara AI dan pembelajaran mesin dapat meningkatkan upaya keamanan siber secara signifikan adalah dalam deteksi ancaman dan analisis data, kata Aneta Waberska, Direktur Produk Keamanan Informasi dan Kepatuhan di AuditBoard. Penjahat dunia maya mencoba menyusup ke jaringan organisasi dengan mencari titik lemah dan menghancurkan pertahanan jaringan. Di masa lalu, organisasi bergantung pada administrator sistem untuk memblokir ancaman eksternal ini. Namun, karena kemajuan otomatisasi dan teknologi lainnya, meningkatnya volume masuk dari pelaku kejahatan telah melampaui kapasitas peninjauan manusia yang efektif, kata Aneta. AI dapat mengatasi masalah ini. AI dapat meninjau masukan jaringan dalam jumlah besar dan mengenali pola serta belajar darinya seiring waktu, memahami apakah peristiwa atau kelompok peristiwa tertentu dapat menimbulkan ancaman bagi organisasi. "Ini adalah salah satu penggunaan AI yang paling berdampak di lingkungan ini," kata Aneta.

Selain itu, alat pendeteksi perangkat lunak berbahaya (*malware*) yang lebih canggih memiliki kemampuan yang lebih baik, termasuk kemampuan memblokir salah satu penyebab utama pelanggaran dan insiden keamanan — *phishing*. Hal ini dapat mengurangi atau menghilangkan potensi kesalahan manusia — seperti membuka tautan pada *email phishing* dan membuat jaringan perusahaan terkena *malware* — karena alat tersebut menyaringnya sebelum masuk ke kotak masuk seseorang, kata Waberska. (Lihat *sidebar* untuk informasi lebih lanjut mengenai beberapa cara AI dapat meningkatkan pertahanan keamanan siber.)

AI juga dapat dengan cepat mencari anomali dan mengidentifikasi masalah yang sudah terjadi dalam jaringan organisasi, sesuatu yang tidak dapat dilakukan manusia pada data berskala besar. Akses tidak sah ke sistem perusahaan adalah salah satu contohnya. Seorang mantan karyawan dapat secara tidak sengaja memberikan akses kepada penjahat dunia maya dengan membagikan atau menuliskan kata sandi atau mungkin masuk kembali ke sistem dengan niat jahat. Di masa lalu, auditor internal yang memeriksa akses tidak sah di antara mantan pekerja harus melakukan perbandingan manual antara orang-orang yang memiliki akses dan mereka yang tidak lagi memilikinya, kemudian menulis *email* ke tim TI yang merinci masalah apa pun,

Menggunakan AI Sebagai Alat Keamanan Siber

Menurut *IEEE Computer Society*, beberapa cara dimana AI dapat meningkatkan pertahanan keamanan siber suatu organisasi meliputi:

- Mendeteksi aktivitas berbahaya, dengan membuat tolak ukur aktivitas yang dapat diterima dan mengidentifikasi anomali dan ancaman secara terus-menerus dan dalam waktu nyata.
- Mendukung identifikasi ancaman *malware* dengan memeriksa karakteristik file atau pola kode untuk menemukan file yang tidak aman.
- Meningkatkan kemampuan perusahaan dalam menghadapi serangan *zero-day* atau ancaman lain yang tidak diketahui.
- Meningkatkan intelijen ancaman dengan mengumpulkan informasi keamanan dari berbagai sumber, secara proaktif memburu ancaman, dan membantu manajemen ancaman dengan meringankan beban kerja analis keamanan Perusahaan.[6]

[6] "AI for Cybersecurity and Cybercrime: How Artificial Intelligence Is Battling Itself," Gaurav Belani, IEEE Computer Society, 6 September, 2023.

Di sisi lain, AI dapat mencari di berbagai platform, membandingkan data dalam sistem penggajian dan sistem akses, dan kemudian secara otomatis menghasilkan email kepada tim yang relevan mengenai setiap anomali yang ditemukan..

Auditor internal harus menyadari bahwa tujuan penjahat dunia maya sering kali bukan sekadar mencuri data, namun juga menyusup dan mengganggu sistem dengan mengubah data, kata Grafenstine. Pada tingkat terbesar, pelaku kejahatan di negara-bangsa dapat memanipulasi infrastruktur penting, seperti transportasi, energi nuklir, perbankan, dan banyak lainnya, namun konsekuensinya juga bisa signifikan bagi organisasi dengan ukuran berapa pun.

Pertimbangan Manajemen Risiko

Etika, Bias dan Rasa Percaya yang Berlebihan

Audit Internal bisa Membantu Organisasi Menghindari Dampak Buruk AI

Seiring dengan banyaknya manfaat yang dimiliki, AI juga mempunyai daftar pertimbangan risikonya sendiri. Beberapa ancaman berasal dari internal namun bisa sama bahayanya dengan serangan siber.

Etika

Banyak kekhawatiran di bidang ini terkait dengan AI generatif dan model bahasa besar yang dapat digunakan oleh auditor internal untuk membuat laporan, menulis kode, dan membuat rekomendasi dan analisis, serta kemungkinan-kemungkinan lainnya. Namun, *tools* ini juga menimbulkan pertanyaan keamanan dan etika bagi organisasi. "Ada risiko bahwa karyawan akan melihat *tools* ini sebagai permainan atau mainan," kata Grafenstine.

Pengendalian siber tradisional pada teknologi sebelumnya juga berlaku pada sistem ini, namun "dampak jika tidak dilakukan dengan baik akan semakin besar," ujarnya. Antara lain, seperti yang akan dibahas lebih rinci, sistem dapat memberikan informasi yang bias, tidak akurat, atau dibuat-buat, bergantung pada cara ia dilatih. Grafenstine juga menunjukkan konsekuensi yang mahal dan berpotensi memalukan bagi bisnis dan reputasi perusahaan jika perusahaan menggunakan *chatbot* yang berhubungan dengan pelanggan yang dilatih dengan sumber informasi yang buruk dan jawaban *chatbot* yang salah memiliki dampak negatif yang signifikan kepada pelanggan. Oleh karena itu, harus ada tinjauan oleh manusia atas apa pun yang dihasilkan oleh sistem AI generatif ketika organisasi tidak sepenuhnya mengetahui data yang telah dilatihkan kepadanya. "Perusahaan harus memiliki jawabannya," kata Grafenstine.

Meskipun penggunaan program AI generatif seperti ChatGPT telah meledak sejak diluncurkan pada akhir tahun 2022, memposting informasi kepada AI generatif yang tersedia untuk publik dapat mengekspos data perusahaan atau identitas pribadi pelanggan, seperti insiden peretasan yang mungkin terjadi, dan merupakan risiko yang signifikan. Saat karyawan memposting pertanyaan yang menyertakan informasi perusahaan dalam program AI generatif publik, program tersebut akan menyimpan informasi tersebut dan berpotensi menggunakannya untuk menanggapi pertanyaan lain di luar organisasi, sehingga menampilkannya ke publik. Hal ini tidak hanya dapat mempublikasikan informasi rahasia, namun pelaku kejahatan juga dapat menggunakannya untuk mencari jalan ke dalam sistem perusahaan, dengan *phishing* atau alat lainnya, Grafenstine memperingatkan.

Rasa Percaya Berlebihan terhadap Output AI

Setiap profesional adalah penanggung jawab puncak atas *tools* yang mereka gunakan dan informasi yang dihasilkannya. Hal ini berlaku bagi auditor internal, yang dapat melanggar standar mereka sendiri jika mereka terlalu bergantung pada data atau konten yang tidak tervalidasi. "Menjadi pihak yang terpercaya adalah pekerjaan kita," kata Grafenstine.

Bias Algoritmik

Mesin dilatih untuk belajar berdasarkan algoritma tertentu dan informasi yang dihasilkan dapat dipengaruhi, disengaja atau tidak, berdasarkan algoritma tersebut. Sebagai contoh, algoritma dapat menyaring pelamar perempuan dalam keputusan perekrutan jika sebelumnya jumlah karyawan yang didominasi laki-laki atau mereka mungkin menyukai permohonan pembelian rumah dari pembeli orang kulit putih jika sebagian besar pemegang hipotek saat ini berkulit putih. [7] "Mereka tidak bermaksud jahat, tapi bias sudah tertanam di dalamnya," kata Grafenstine.

[7] "For minorities, biased AI algorithms can damage almost every part of life," The Conversation, www.theconversation.com, August 24, 2023.

Melindungi AI – dan Berlindung dari AI

Pengendalian Internal itu Penting

Melindungi Integritas Sistem AI, Akses

Keamanan atas AI dan kemampuan untuk menggunakannya adalah pertimbangan serius bagi organisasi dan auditor internal. Harus ada kontrol atas siapa yang dapat mengakses sumber daya AI, bagaimana wewenang untuk mengubah kode diproteksi, dan siapa yang diizinkan membawa informasi dari area pengujian ke area produksi. Sebagai auditor internal, "Saya ingin memastikan bahwa saya dapat mengetahui apakah algoritma AI telah diubah atau seseorang dapat mengganggunya di tengah proses dan mengubahnya," kata Grafenstine. Auditor internal juga perlu menyadari potensi ruang lingkup gangguan tersebut. "Jika saya bisa mengakses AI perusahaan Anda, bukan hanya satu transaksi yang bisa saya ubah," katanya. Sebaliknya, pelaku kejahatan dapat mengakses seluruh *data warehouse* milik organisasi, atau apa pun yang dapat diakses oleh AI.

> "Hanya karena Anda telah menerapkan solusi yang memanfaatkan AI bukan berarti Anda kini kebal peluru,"
>
> Aneta Waberska
> AuditBoard

Pada saat yang sama, penting untuk menyadari bahwa AI mempermudah penjahat dunia siber untuk membuat *malware* dengan cepat, mengotomatiskan serangan, dan meningkatkan efektivitas serangan atau rekayasa sosial dengan menggunakan alat seperti *deepfake*, yang mengubah video atau gambar secara digital, serta adanya generator suara AI untuk membuat gambar atau pesan palsu. "Lanskap ancaman dunia maya menjadi lebih berbahaya, dan AI memainkan peran besar di dalamnya," menurut artikel IEEE Computer Society.[8]

Auditor harus melihat AI sebagai alat menyerang dan bertahan, kata Waberska. "Saat Anda telah menerapkan solusi berbasis AI bukan berarti Anda kebal peluru," katanya. Meskipun serangan di masa lalu sering kali dilakukan oleh satu peretas, AI dapat melakukan serangan yang jauh lebih besar dan menyerang banyak organisasi. AI dapat meningkatkan *malware* dengan belajar dari program sebelumnya dan menggunakan pengetahuan ini untuk menghasilkan *malware* yang lebih kuat, tanpa memerlukan pengembang. "Jika AI mencoba masuk ke dalam organisasi, hal ini mungkin lebih kuat dibandingkan solusi yang Anda miliki saat ini," kata Waberska. Auditor dapat memastikan organisasi memahami dan siap menghadapi risiko ini. Tim audit tidak dapat menerapkan solusi, namun dapat berdiskusi dengan tim *security* untuk mengetahui apakah ancaman dan solusi dipertimbangkan. "Perlu waktu bagi organisasi mengadopsi solusi baru, namun penting untuk menyadari ancaman dan berencana untuk mempertahankan diri," kata Waberska.

Jangan Lupakan Elemen Manusia

Ketika organisasi bersiap untuk menangkal ancaman siber, auditor harus mengingat bahaya dari ancaman yang tidak disengaja oleh ditimbulkan oleh karyawannya. Upaya *phishing*, misalnya, berhasil karena manusia gagal mengenali penjahat dunia siber yang mencoba masuk ke sistem atau kata sandi atau data rahasia lainnya. "Auditor harus melihat bagaimana organisasi mendidik karyawannya tentang ancaman ini," kata Waberska. Karyawan mungkin tidak memahami e-mail *phishing* telah berevolusi. Meskipun dulunya mudah untuk mengenali tanda bahaya seperti ejaan atau *font* yang aneh, AI digunakan untuk menulis e-mail *phishing* yang jauh lebih realistis. "Mereka terlihat sangat nyata, dan lebih mudah bagi pelaku kejahatan untuk menciptakannya," katanya.

[8] "AI for Cybersecurity and Cybercrime: How Artificial Intelligence Is Battling Itself," Gaurav Belani, IEEE Computer Society Tech Trends, September 6, 2023.

Kesimpulan

Ancaman serangan siber adalah fitur permanen dalam berbisnis di dunia digital, dan kecerdasan buatan (AI) beserta penggunaannya yang terus berkembang menghadirkan tantangan baru dan menarik dalam manajemen risiko untuk melawan ancaman tersebut. Auditor internal memiliki peran penting dalam:

- Memastikan bahwa pamimpin dan para pihak menyadari manfaat dan bahaya yang terkait dengan AI.
- Memberikan rekomendasi bagaimana AI dapat meningkatkan berbagai upaya keamanan siber dalam organisasi.
- Mendorong kesadaran akan perlunya mempertimbangkan pertahanan terkini terhadap alat serangan siber yang didukung AI.
- Memberikan asurans atas pemahaman dan penggunaan teknologi AI oleh perusahaan.

AI dan teknologi terkait dapat menjadi sumber daya yang berharga, namun hal tersebut bukanlah jawaban akhir. “Kemajuan teknologi bisa menjadi hal yang luar biasa selama kita tahu cara menggunakannya dengan cara yang cerdas dan aman,” kata Waberska. “Anda harus selalu menggunakan penilaian profesional dalam mempertimbangkan apa yang Anda dapatkan.”

Di samping itu, perlu diingat bahwa meskipun sikap konservatif merupakan nilai tambah bagi auditor internal, mereka tidak boleh menjadi "kantor yang selalu menolak," kata Grafenstine. Auditor internal harus memberikan saran pengendalian dan risiko yang baik, termasuk wawasan tentang risiko tertinggal dari teknologi. "Adalah risiko besar jika tidak merangkul teknologi, tetapi kita perlu melakukannya dengan cara yang bijaksana," ujarnya.

Bagian 3: Manajemen Risiko Keamanan Siber Pihak Ketiga

Tentang para Ahli

Richard Marcus, CISA, CRISC, CISM, TPECS

Richard Marcus adalah VP Keamanan Informasi di AuditBoard, di mana ia fokus pada produk, infrastruktur, dan keamanan IT perusahaan, serta memimpin inisiatif kepatuhan internal AuditBoard sendiri. Dalam kapasitas ini, ia telah menjadi pengguna unggulan dari produk AuditBoard, memanfaatkan serangkaian fitur platform yang kuat untuk memenuhi kebutuhan kepatuhan, penilaian risiko, dan audit.

John A. Wheeler

John A. Wheeler adalah pendiri dan CEO Wheelhouse Advisors, sebuah firma penasihat eksekutif senior yang membantu bisnis global mencapai visibilitas dan pemahaman risiko yang lebih besar. Ia memanfaatkan keahliannya dalam manajemen risiko, keamanan siber, bisnis digital, risiko operasional, dan manajemen risiko terintegrasi untuk memberikan panduan strategis dan solusi teknologi kepada kliennya.

PENDAHULUAN

Dunia kini semakin terhubung satu sama lain, dan termasuk industri. Hari ini, hampir setiap sektor bisnis besar pada kapasitas tertentu bergantung kepada pihak ketiga. Pada generasi sebelumnya, hal ini mungkin terjadi terutama dari sudut pandang fisik, dengan satu pihak mengandalkan pada pihak lain untuk mendapatkan barang atau jasa. Meski masih benar adanya, sekarang hubungan antarpihak telah terjalin pada ranah digital.

Meskipun tren ini menawarkan banyak keuntungan, terutama terkait efisiensi, produktivitas, dan memenuhi komitmen keberlanjutan dengan lebih baik, terdapat juga risiko yang harus dipertimbangkan. Menurut Survei Manajemen Risiko Pihak Ketiga Global Deloitte 2022, 73% responden kini sangat bergantung pada penyedia layanan cloud pihak ketiga, dengan angka tersebut diperkirakan meningkat menjadi 88% dalam beberapa tahun mendatang.[9] Namun, agar hubungan tersebut berhasil, harus ada kepercayaan implisit antara organisasi bahwa data yang dipindahkan akan seaman mungkin terhadap serangan siber, pelanggaran data, atau insiden siber terkait lainnya. Untuk mendapatkan kepercayaan tersebut, organisasi harus memiliki program manajemen risiko pihak ketiga atau *Third Party Risk Management* (TPRM) yang berdedikasi dan luas yang menerapkan uji tuntas saat memasukkan vendor pihak ketiga dan terus memantau mereka sepanjang siklus hubungan.

Namun kenyataannya, seringkali perusahaan memberikan kepercayaan tanpa terlebih dahulu melakukan uji kelayakan secara memadai. “Pihak ketiga apapun – vendor, penyedia komponen produk, mitra, atau pelanggan – dapat menghadirkan risiko siber baru kepada organisasi Anda” kata Richard Marcus, Wakil Presiden Keamanan Informasi pada AuditBoard. “Kebutuhan akan manajemen risiko pihak ketiga yang kuat semakin meningkat sepanjang waktu, dan banyak organisasi tidak dapat memenuhinya.”

Sebagai bagian terakhir dari tiga bagian seri tentang keamanan siber, *Global Knowledge Brief* ini akan menyoroti betapa pentingnya risiko siber yang terkait dengan pihak ketiga dan membahas peran auditor internal dalam manajemen risiko siber pihak ketiga.

9. 2022 Global Third-Party Risk Management Survey, Deloitte, 2022, https://www.deloitte.com\content\dam\Deloitte\us\Documents\TPRM_Survey_Report_Interactive.pdf.

Sebuah Tantangan Besar

Risiko Siber Mendominasi Diskusi Manajemen Risiko Pihak Ketiga

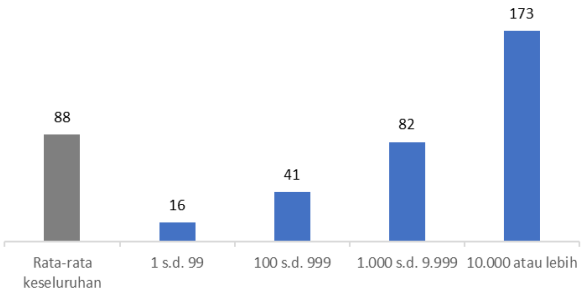
Risiko Meningkat

Laporan terkini dari CyberRisk Alliance, disponsori oleh AuditBoard, mensurvei 209 kepala dan eksekutif bidang keamanan dan TI, administrator keamanan, dan profesional bidang kepatuhan di Amerika Serikat. Survei tersebut mengungkap betapa besarnya risiko siber pihak ketiga. Wawasan dari survei tersebut meliputi:

- Rata-rata, perusahaan menggunakan sebanyak 88 mitra pihak ketiga (termasuk vendor perangkat lunak, vendor layanan TI, mitra layanan TI, mitra bisnis, pialang, subkontraktor, kontrak manufaktur, distributor, agen, dan pengecer). Jumlahnya bervariasi signifikan berdasarkan ukuran organisasi, dengan perusahaan dengan 1 s.d. 99 karyawan rata-rata menggunakan mitra sebanyak 16, sedangkan perusahaan dengan 10.000 karyawan atau lebih menggunakan rata-rata sebanyak 173 mitra (lihat Gambar 1).
- Sebanyak 57% responden melaporkan bahwa mereka menjadi korban insiden keamanan TI (baik serangan maupun kebocoran) dalam 24 bulan terakhir. Selain itu, organisasi rata-rata mengalami dua insiden keamanan terkait pihak ketiga dalam dua tahun terakhir.
- Di antara mereka yang terdampak, sebanyak 52% mengatakan sumber serangan adalah vendor perangkat lunak, dan sebanyak 39% mengatakan mitra bisnis, subkontraktor, atau penyedia layanan TI bertanggung atas jawab insiden tersebut (lihat Gambar 2)[10].

Gambar 1

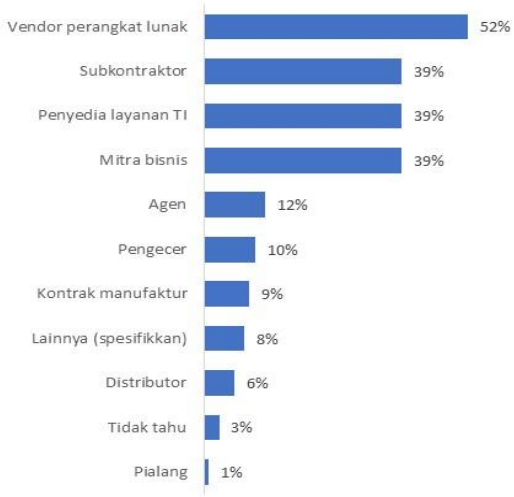
Rata-rata Pihak Ketiga, Berdasarkan Ukuran Organisasi



Pertanyaan: Kira-kira, berapa banyak pihak ketiga di organisasi Anda yang berkontrak saat ini? Termasuk semua vendor (termasuk vendor perangkat lunak dan penyedia layanan TI), mitra bisnis, pialang, subkontraktor, kontrak manufaktur, distributor, agen, dan pengecer

Gambar 2

Mana dari pilihan berikut yang menjadi sumber serangan atau kebocoran?
Pilih seluruhnya yang berlaku.



Catatan: Grafik dan data pada Gambar 1 and Gambar 2 diambil dari "Third-Party Risk: More Third Parties + Limited Supply-Chain Visibility = Big Risks for Organizations," oleh CyberRisk Alliance and Auditboard. hal. 9 and hal.18, Januari 2023.

10. "Third-Party Risk: More Third Parties + Limited Supply-Chain Visibility = Big Risks for Organizations," CyberRisk Alliance and AuditBoard, January 2023, https://www.auditboard.com/resources/ebook/third-party-risk-more-third-parties-limited-supply-chain-visibility-big-risks-for-organizations/.

Mengikuti Perubahan

Alasan utama untuk permasalahan ini beragam, namun muncul dari kombinasi model bisnis yang berubah secara cepat dan ketidakmampuan untuk memutakhirkan proses manajemen risiko pihak ketiga agar sesuai dengan perubahan tersebut, menurut John Wheeler, pendiri dan CEO Wheelhouse Advisors. “Menurut pengalaman saya,” kata Wheeler, “risiko terbesar dan paling relevan dihasilkan oleh perubahan besar. Tantangan pertumbuhan mendorong perubahan besar dengan mendorong perusahaan menciptakan produk dan layanan digital baru.”

Dalam hal ini, Wheeler menulis AuditBoard’s “2023 Digital Risk Report: Pervasive Risk, Persistent Fragmentation, and Accelerating Technology Investment.” Dalam survei terhadap lebih dari 130 pemimpin risiko di Amerika Serikat, sebesar 21% melaporkan bahwa mereka tidak melaksanakan penilaian risiko kualitatif atau kuantitatif ketika mengelola dan memantau risiko digital pihak ketiga, dan sebesar 56% hanya mengandalkan pada pendekatan penilaian kualitatif, yang terbatas dibandingkan dengan penilaian kuantitatif.[11]

44%

PERSENTASE ORGANISASI YANG MENGANDALKAN TEKNOLOGI MANUAL UNTUK MENGELOLA RISIKO SIBER PIHAK KETIGA

AuditBoard 2023 Digital Risk Report
Pervasive Risk, Persistent Fragmentation,
and Accelerating Technology Investment

Yang juga memprihatinkan, kata Wheeler, adalah bahwa di antara perusahaan-perusahaan yang mengelola risiko digital seperti risiko siber pihak ketiga, sebesar 44% perusahaan masih mengandalkan teknologi manual (lembar kerja, surat elektronik, drive bersama, dan Sharepoint) untuk melakukan hal tersebut. “Ini merupakan pendekatan yang sangat memakan waktu,” katanya. “Kenyataannya adalah tata kelola lama yang terfragmentasi, tidak fleksibel, dan didorong oleh kepatuhan, perangkat lunak tata kelola, risiko, dan kepatuhan (GRC) tidak dapat menyediakan kapabilitas risiko terintegrasi yang diperlukan untuk mengimbangi kecepatan risiko digital – dan hasilnya, sebagian besar organisasi masih mengandalkan proses manual sedikit demi sedikit.

Hal ini perlu menjadi perhatian khusus mengenai perubahan pola serangan pelaku kejahatan, yang semakin hari semakin canggih. “Jika Anda melihat pada akar masalah terjadinya kebocoran dalam beberapa dekade terakhir, sebagian besar terjadi di pintu depan, pada lapisan aplikasi atau infrastruktur. Dengan demikian, di situlah tempat tim keamanan menginvestasikan waktu dan sumber daya mereka. Namun penyerang itu cerdas. Mereka akan mencari jalur yang paling sedikit perlawanannya, dan seringkali mereka akan melalui pintu belakang yang disebabkan oleh celah pada pengukuran keamanan siber pihak ketiga,” kata Marcus.

Tekanan Regulasi

Tekanan yang dirasakan organisasi terkait risiko siber pihak ketiga juga turut dipengaruhi oleh lanskap regulasi yang terus berubah, yang belakangan ini kian cepat menyesuaikan diri dengan laju risiko itu sendiri. Perubahan tersebut mencakup mandat baru yang ditetapkan pemerintah federal AS kepada mitra rantai pasokan mereka, yang berdampak berantai ke berbagai industri. "Anda mungkin berpikir bahwa mandat federal untuk transparansi yang lebih besar mengenai keamanan data hanya akan mempengaruhi perusahaan yang berbisnis dengan pemerintah federal, namun kemudian ada persyaratan pihak ketiga dan keempat yang mengalir ke bawah rantai pasokan dan berjenjang melalui hierarki atau penyedia layanan," kata Marcus. "Hal tersebut menciptakan budaya akuntabilitas yang merambah banyak industri."

Badan-badan regulator juga mulai mengambil langkah formal untuk mengatasi risiko keamanan siber pihak ketiga. Ini termasuk aturan baru yang baru-baru ini diberlakukan oleh *Securities and Exchange Commission* (SEC) / Komisi Sekuritas dan Bursa Amerika Serikat seperti aturan baru yang mengharuskan registrants (perusahaan terdaftar) untuk mengungkapkan insiden keamanan siber yang material. “Meskipun perusahaan Anda tidak secara langsung menerapkan aturan atau regulasi baru, aturan-aturan tersebut meresap ke dalam budaya keamanan siber,” kata Marcus. “Hal Ini adalah perubahan kultur yang menciptakan ekspektasi transparansi dan akuntabilitas.”

11. “Digital Risk Report 2023: Pervasive Risk, Persistent Fragmentation, and Accelerating Technology Investment,” John A. Wheeler, Auditboard, July, 2023, https://www.auditboard.com/resources/ebook/digital-risk-report-2023/.

Membangun budaya aksi siber

Organisasi tidak mengabaikan kekurangan ini. Memang benar bahwa sebagian besar dari mereka menyadari hal ini dalam kapasitas tertentu, meskipun kesadaran tersebut tidak selalu diterjemahkan ke dalam pemahaman dan tindakan di seluruh organisasi. Meskipun hanya sedikit fungsi audit internal yang dapat mengklaim memiliki pengetahuan keamanan siber yang memadai untuk secara langsung menangani teknis keamanan siber pihak ketiga, hal yang dapat mereka lakukan adalah memanfaatkan posisi unik mereka untuk menyatukan sudut pandang berbagai pemangku kepentingan yang terlibat dalam pengelolaan risiko ini (seperti, bagian hukum, pengadaan, TI, dan pihak ketiga itu sendiri). Selain itu, auditor internal dapat menggunakan interaksi langsung mereka dengan komite audit dan dewan untuk memastikan sudut pandang tersebut dikomunikasikan secara teratur dan akurat.

Sudut pandang ini sangat penting bagi para CEO dan pemimpin organisasi untuk mendorong tindakan yang tepat, kata Wheeler, dan ini adalah sesuatu yang harus dipahami oleh fungsi manajemen risiko agar dapat diartikulasikan. “CEO memerlukan wawasan yang *real-time* baik dari dalam maupun luar organisasi, di seluruh ekosistem aset teknologi yang berubah secara dinamis,” ujarnya. “Melalui proses ini, mereka akan memiliki pemahaman yang lebih baik tentang produk dan layanan digital mereka.”

Namun, kesatuan dalam organisasi saja tidak cukup. Kesatuan ini harus mencakup pemangku kepentingan dari luar organisasi. "Setiap hubungan pihak ketiga harus terdapat pemilik atau penanggung jawab yang ditunjuk yang bertanggung jawab untuk menjaga hubungan vendor, menyimpan informasi kontak vendor, dan mengelola persyaratan kontrak," kata Marcus. "Hubungan pihak ketiga berbeda dari satu vendor ke vendor lainnya - beberapa mungkin memberi organisasi Anda tim dukungan pelanggan atau tim sukses yang ditunjuk yang menyediakan layanan tambahan, sementara yang lain mengambil pendekatan 'siap pakai'. Menjaga jalur komunikasi tetap terbuka dan jelas antara organisasi Anda dan pihak ketiganya adalah komponen utama tetapi sering diabaikan dari manajemen risiko pihak ketiga yang efektif."

Membangun budaya seperti itu tidak hanya dapat mendorong tindakan pencegahan, tetapi juga dapat meningkatkan kecepatan reaksi ketika serangan siber atau pelanggaran terjadi. Dalam laporan CyberRrisk Alliance, 20% responden mengatakan perlu waktu seminggu atau lebih untuk menilai serangan atau pelanggaran, menghubungkan perpanjangan waktu tersebut dengan kesulitan membuat vendor atau mitra melaporkannya atau bertanggung jawab atasnya.[12] Menciptakan budaya siber yang positif dan transparan di dalam organisasi dan di seluruh rantai pasokannya dapat mengurangi waktu-waktu tersebut dari minggu ke jam, sehingga secara drastis mengurangi kerugian dalam prosesnya.

“Seluruh proses manajemen risiko pihak ketiga,” kata Marcus, “harus dibangun berdasarkan budaya akuntabilitas di mana setiap orang menyadari risiko pihak ketiga.”

Pendekatan pemantauan berkelanjutan berdasarkan tingkat risiko

Selain menjadi penentu kebijakan, audit internal dapat dan harus bertindak sebagai sumber daya yang berharga dalam menyusun program manajemen risiko pihak ketiga / *third party risk management* (TPRM) yang berkaitan dengan risiko dunia maya – dan terus mengevaluasinya.

12. “Third-Party Risk: More Third Parties + Limited Supply-Chain Visibility = Big Risks for Organizations,” CyberRisk Alliance and AuditBoard, February, 2023, https://www.auditboard.com/resources/ebook/third-party-risk-more-third-parties-limited-supply-chain-visibility-big-risks-for-organizations/.

"Menurut saya, tanggung jawab utama audit internal, seperti dalam banyak kasus, adalah mengevaluasi efektivitas program TPRM," kata Marcus. "Hal ini dapat mencakup inventarisasi atau gambaran lengkap dari semua pihak ketiga yang digunakan dalam organisasi, memahami risiko yang dapat dihadapi oleh pihak ketiga tersebut, dan memahami bagaimana organisasi mengevaluasi kekuatan pengendalian pada pihak ketiga tersebut. organisasi."

Sekali lagi, meskipun ahli di bidangnya harus dilibatkan untuk analisis teknis, banyak prinsip manajemen risiko yang digunakan oleh audit internal dapat diterapkan pada topik ini.

Misalnya, audit internal harus memiliki pemahaman yang kuat tentang analisis risiko, yang seringkali divisualisasikan menggunakan *heatmap* atau alat bantu lainnya. Taktik tersebut dapat digunakan sebagai panduan bagi pemangku kepentingan yang bertanggung jawab atas orientasi/*onboarding* dan pemantauan pihak ketiga untuk lebih memahami siapa dan apa yang harus diprioritaskan.

"Faktor keberhasilan terpenting dari program TPRM adalah menyusun dan memformalkan kegiatan pemantauan berkelanjutan berdasarkan tingkat risiko," kata Marcus. "Pihak ketiga yang berisiko tinggi harus menerima lebih banyak perhatian atau lebih sering diperhatikan, dan pihak ketiga yang berisiko lebih rendah dapat lebih jarang menerima perhatian." Yang perlu diperhatikan, lanjutnya, adalah bahwa meskipun pihak ketiga tersebut mungkin tidak memiliki risiko tinggi, namun sifat hubungan tersebut — seperti jenis data apa yang ditransfer (misalnya, data rahasia, data pelanggan, data kepemilikan) — dapat menaikkan atau menurunkan kategorisasi risiko.

Untuk membantu tugas ini, AuditBoard menggunakan contoh berikut (Gambar 3) sebagai titik awal tentang bagaimana menyusun tinjauan terkait dengan tiga kategori tingkat risiko berikut:[13]

Gambar 3

Karakteristik Tingkat Risiko	Tingkat 1 - Risiko Tinggi	Tingkat 2 - Risiko Medium	Tingkat 3 - Risiko Low
Akses Data	Rahasia	Pemilik / Internal	Publik atau Tidak Ada Pemilik
Frekuensi Peninjauan	1 Tahun	2 Tahun	3 Tahun
Persyaratan Peninjauan	Audit Lapangan Kuisioner Pengendalian Tinjauan Sertifikasi	Tinjauan Sertifikasi	Tidak Ada

Catatan: Grafik dan data pada Gambar 1 dan Gambar 2 diambil dari "Effective Third-Pary Risk Management: Key Tactics and Success Factors" by AuditBoard. p. 8, 2022.

Proses pemeriksaan pihak ketiga tidak berakhir pada tahap orientasi/*onboarding* tetapi harus terus ditinjau berdasarkan tingkat risiko yang dirasakan. Memastikan para pemangku kepentingan tetap mengikuti komitmen mereka terhadap tinjauan rutin, serta proses yang mereka gunakan untuk melakukan tinjauan tersebut, harus termasuk dalam lingkup risiko audit internal. Gagasan untuk proses tersebut dapat mencakup:

- Memeriksa sertifikasi kepatuhan dan laporan seperti SOC 2. Kerangka kerja umum untuk memeriksa sertifikasi kepatuhan meliputi SOC 2, ISO 27001, dan NIST SP 800-161.
- Penggunaan kuesioner standar. Ini dapat mencakup Kuesioner Pengumpulan Informasi Standar (*Standardized Information Gathering Questionnaire* / SIG) atau CCM dan CAIQ dari Cloud Security Alliance.
- Kuesioner pengendalian keamanan.

13. "Effective Third-Party Risk Management: Key Tactics and Success Factors," AuditBoard, January, 2022, https://www.auditboard.com/resources/ebook/effective-third-party-risk-management-key-tactics-and-success-factors/?utm_campaign=effective-third-party-risk-management-key-tactics-and-success-factors-0122022&utm_medium=download-image&utm_source=blog.

Merangkul Solusi Perangkat Lunak

Untuk menyatukan begitu banyak variabel, audit internal serta fungsi manajemen risiko lainnya juga harus memprioritaskan peralihan dari proses manual ke solusi perangkat lunak. “Audit internal dapat menjadi pelopor dalam investasi teknologi untuk membuat proses manajemen risiko pihak ketiga menjadi lebih efisien,” kata Marcus. “Dalam banyak situasi, skala efisiensi memerlukan hal tersebut. Saya ingat salah satu organisasi pertama tempat saya menerapkan praktik risiko pihak ketiga— kami melakukan penilaian risiko untuk lima atau enam vendor dan kemudian mempertimbangkan untuk memperluas proses ini untuk semua vendor. Namun kami terkejut ketika mengetahui bahwa ada 17.000 vendor di perusahaan ini. Tidak ada cara untuk melakukan hal tersebut tanpa *platform* yang mendukung teknologi untuk memfasilitasi kegiatan dengan skala hingga ratusan, ribuan, atau puluhan ribu vendor.”

Selain itu, solusi tersebut juga memberikan peluang bagus bagi audit internal untuk berkolaborasi lebih erat dengan fungsi risiko pihak ketiga lainnya. “Banyak hambatan dalam kolaborasi yang melibatkan berbagi data dan masalah alur kerja,” kata Marcus. “Memiliki *platform* teknologi di mana kedua tim dapat mengevaluasi lanskap vendor bersama-sama — menggunakan dasbor yang sama, *database* vendor yang sama, dan sebagainya. — memungkinkan mereka untuk bekerja sama dengan lebih efisien dan mencapai hasil yang sama.

Fokus pada *offboarding* dan juga *onboarding*

Meskipun hubungan dengan pihak ketiga jarang berlangsung selamanya, berakhirnya kontrak formal tidak selalu berarti terputusnya saluran data antar pihak. Meski tampaknya sepele, saluran yang terlupakan ini bertanggung jawab atas sejumlah celah terbesar yang ditemukan dalam sistem keamanan siber pihak ketiga organisasi, menciptakan "pintu belakang digital" atau “*third party backdoor*” yang dapat dimanfaatkan secara disengaja atau tidak disengaja. Saat mengevaluasi praktik tinjauan pihak ketiga, ini adalah hal yang tidak boleh diabaikan oleh audit internal.

"Mengenai detail pada fase penghentian kerja sama (*offboarding)* sangat penting," kata Marcus. "Dalam ekosistem digital yang saling terkait saat ini, mudah untuk melewatkan akun, layanan, atau *user* dari pihak ketiga yang perlu dihapus atau dinonaktifkan. Izin akses perlu dicabut, akun pengguna dinonaktifkan, dan perangkat lunak atau aplikasi yang dikeluarkan pihak ketiga perlu dihapus. Hal ini adalah hal yang perlu diteliti dengan cermat oleh audit internal."

Kesimpulan

Masa depan organisasi adalah dunia maya. Dari tahun ke tahun, jelas bahwa tren ini akan terus berlanjut — dan hanya karena keamanan siber memerlukan keahlian yang lebih khusus, bukan berarti dunia bisnis akan menunggu para pemangku kepentingan untuk mendidik diri mereka sendiri. Keamanan siber adalah sebuah perjalanan pembelajaran yang berkelanjutan, dan semua pihak yang terlibat dalam hubungan pihak ketiga harus mempertimbangkan hal tersebut.

Syukurlah, ada tanda-tanda positif bahwa organisasi mulai menerima kenyataan ini. Dalam laporan Intelijen Bisnis CyberRisk Alliance, hampir dua dari tiga responden mengatakan bahwa tindakan paling umum yang mereka lakukan untuk mencegah atau mengurangi risiko serangan pihak ketiga adalah pelatihan karyawan.[14] Meskipun risiko yang terkait dengan pihak ketiga tidak akan pernah berakhir, kebijakan dan respons akan matang hingga pada titik di mana risiko tersebut dapat dikelola dengan mudah seperti halnya risiko lain yang sudah ada. Memang belum saatnya, tetapi kita sedang menuju ke sana, dan asurans manajemen risiko dari audit internal yang efektif akan membantu organisasi mencapai tujuan dengan aman.

14. "Third-Party Risk: More Third Parties + Limited Supply-Chain Visibility = Big Risks for Organizations," CyberRisk Alliance and AuditBoard, February, 2023, https://www.auditboard.com/resources/ebook/third-party-risk-more-third-parties-limited-supply-chain-visibility-big-risks-for-organizations/.

Tentang IIA

Institute of Internal Auditors (IIA) adalah asosiasi profesional internasional nirlaba yang melayani lebih dari 235.000 anggota global dan telah memberikan lebih dari 190.000 sertifikasi *Certified Internal Auditor* (CIA) di seluruh dunia. Didirikan pada tahun 1941, IIA diakui di seluruh dunia sebagai profesi audit internal terdepan dalam standar, sertifikasi, pendidikan, penelitian, dan bimbingan teknis. Untuk informasi lebih lanjut, kunjungi theiia.org.

Tentang AuditBoard

AuditBoard adalah *platform* berbasis *cloud* terkemuka yang mentransformasikan audit, risiko, kepatuhan, dan manajemen LST. Lebih dari 40% perusahaan Fortune 500 memanfaatkan AuditBoard untuk memajukan bisnis mereka dengan lebih jelas dan gesit. AuditBoard mendapat peringkat teratas oleh pelanggan di G2, Capterra, dan Gartner Peer Insights, dan baru-baru ini menduduki peringkat kelima berturut-turut sebagai salah satu perusahaan teknologi dengan pertumbuhan tercepat di Amerika Utara oleh Deloitte. Untuk informasi lebih lanjut, kunjungi: AuditBoard.com.

Disclaimer

Ringkasan Pengetahuan Global dimaksudkan untuk membahas topik-topik yang tepat waktu dan relevan bagi audiens audit internal global, dan setiap topik yang dibahas diperiksa oleh anggota sukarelawan Komite Penasihat Konten Amerika Utara IIA. Para ahli di bidangnya terutama diidentifikasi dan dipilih dari daftar Kontributor Panduan Global IIA.

Untuk mengajukan permohonan agar ditambahkan ke daftar Kontributor Panduan Global, kirimkan email ke Standards@theiia.org. Untuk menyarankan topik untuk Ringkasan Pengetahuan Global di masa depan, email ke Content@theiia.org.

Hak Cipta

Januari 2024

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