Issue 4

GLOBAL PERSPECTIVES AND INSIGHTS:

Internal Audit as Trusted Cyber Adviser

The Institute of Internal Auditors | Global

Contributors

City of Cape Town – South Africa
Lindiwe Ndaba, CIA, Chief Audit Executive
Etienne Postings, CIA, CCSA, CISA, Senior Audit Manager: Information Systems
Andre Stelzner, Director, Information Systems and Technology

FirstRand Ltd – South Africa
Jenitha John, CIA, QIAL, CA(SA), Chief Audit Executive

Insurance Australia Group Limited – Australia
Jeff Jacobs, Chief Information Security Officer
Lee Sullivan, Chief Audit Executive

RSM US LLP – United States
Daimon Geopfert, National Leader of Security and Privacy Services

Saudi Basic Industries Corporation (SABIC) – Saudi Arabia
Gregory Grocholski, CISA, Vice President, Chief Audit Executive

The Institute of Internal Auditors – United States
Greg Jaynes, CIA, CRMA, CFE, CGFM, Chief Audit Executive
Charles Redding, Executive Vice President and Chief Information Officer

Universidad de Los Andes – Colombia
Jeimy Cano, CFE, Cobit5 Foundation Certificate, Distinguished Professor, Law Faculty

University of Virginia – United States
Jason Belford, Chief Information Security Officer
Gerald Cannon, CISA, CRISC, Director of IT Audits
Virginia Evans, Chief Information Officer
Ron Hutchins, Vice President of IT
Carolyn Saint, CIA, CRMA, CPA, Chief Audit Executive

Daftar Isi

Reader Feedback

Send questions or comments to globalperspectives@theiia.org.

Audit Internal sebagai Penasihat *Cyber* Terpercaya

Meskipun tidak praktis bagi seseorang untuk mengetahui segala sesuatu tentang berbagai topik yang kompleks dan memiliki perkembangan yang cepat seperti halnya *cybersecurity* (keamanan dunia *cyber*), namun penting bagi seorang CAE atau kepala audit internal untuk memahami *cybersecurity*. Bahkan, mengingat sifat dinamis dan paparan risiko *cyber* pada saat ini, seorang CAE yang memiliki pengetahuan yang baik tentang *cybersecurity* dapat memosisikan audit internal sebagai penasihat terpercaya organisasi dalam area yang menantang ini.

Data Statistik menunjukkan:

> Pada 2015, rata-rata total biaya pembobolan data adalah US$ 3,79 juta, naik dari US$ 3,52 juta pada tahun 2014 dan meningkat 23 persen sejak 2013. Biaya tersebut dicerminkan dari berpindahnya pelanggan secara abnormal, meningkatnya kegiatan mendapatkan pelanggan, kerugian reputasi, dan berkurangnya *goodwill*.[1]
>
> Para penyerang memiliki akses ke lingkungan organisasi rata-rata 205 hari sebelum mereka ditemukan, dan 69 persen dari organisasi yang menjadi korban kemudian menyadari bahwa mereka diserang bukan oleh staf mereka sendiri tetapi oleh pihak ketiga.[2]
>
> Pada semester pertama tahun 2015, hampir 246 juta *record* data dari 888 insiden yang ditemukan telah bocor. Sekurang-kurangnya setengah dari insiden yang ditemukan tersebut, jumlah *record* data yang bocor tidak bisa ditentukan.[3]
>
> Pembobolan terjadi di seluruh dunia. Pada semester pertama tahun 2015, paling banyak terjadi di Amerika Utara (707 insiden), diikuti oleh Inggris (94) dan Asia (63). Lima dari 10 kebocoran terbesar, berdasarkan jumlah *record* data yang bocor, terjadi pada perusahaan non-AS.[4]

Dengan wajah statistik seperti ini, tidak mengherankan bila Amit Yoran, presiden RSA, menyatakan, "Industri keamanan (*cyber*) telah gagal."[5]

[1] IBM and Ponemon Institute, 2015 Cost of Data Breach Study: Global Analysis, based on a study of 350 companies from 11 countries.

[2] Mandiant, "M-Trends 2015: A View from the Front Lines," based on a distillation of Mandiant's incident response investigations in more than 30 industry sectors.

[3] Gemalto, Breach Level Index (BLI), a database that records all publicly reported global breaches.

[4] Ibid.

[5] Hackett, R.; "'Security Has Failed': Exclusive Preview of RSA President's Conference Preview," Fortune, April 21, 2015.

Namun tidak ada yang meragukan pentingnya *cybersecurity* - tindakan yang diambil untuk melindungi data dalam sistem yang terhubung dengan internet dari kehilangan, kerusakan, akses yang tidak sah, atau penyalahgunaan. Banyak pemimpin organisasi telah memberikan fokus pada masalah ini selama bertahun-tahun. Harapan mereka realistis: tidak ada keyakinan bahwa serangan *cyber* dapat dihilangkan seluruhnya. Seperti Jeimy Cano, profesor terkemuka di Fakultas Hukum dari Universidad de los Andes, mencatat, saat ini lingkungan digital dijiwai dengan "keniscayaan kegagalan." *Cybersecurity* adalah permainan meminimalkan kerusakan. Tujuannya adalah untuk memblokir serangan sebanyak mungkin dan menemukan penyerang sebelum mereka menemukan "permata mahkota" yang dicari.

Sebuah Upaya Tim

Ini bukanlah semata-mata tugas bagi ahli *cybersecurity*. *Cybersecurity* harus diperhitungkan secara holistik dan sistemik, karena efek dari kegagalan bisa bervariasi dari ketidakmampuan untuk melakukan transaksi dasar, hilangnya kekayaan intelektual, hingga kerusakan reputasi. Hal ini bukan semata-mata risiko teknologi, tapi juga merupakan risiko bisnis dan karenanya, auditor internal memiliki peranan penting untuk dimainkan. Keberhasilan dalam melakukannya sangat tergantung pada penekanan topik ini oleh *board* atau komite audit serta pendekatan yang digunakan oleh CAE. *Cybersecurity* menawarkan peluang yang sangat besar bagi para CAE untuk menunjukkan posisi mereka sebagai penasihat terpercaya, yaitu lebih dari sekedar memastikan bahwa audit *cybersecurity* telah dilaksanakan sesuai rencana, tetapi juga menawarkan pemikiran yang antisipatif dan strategis untuk bisnis. Hal ini memerlukan penentuan risiko *cybersecurity* dan dampaknya terhadap strategi bisnis dan reputasi; memungkinkan diskusi yang tepat waktu dan terarah di antara manajemen dan para pejabat senior; serta memperjuangkan perlunya kecermatan dan sumber daya yang sama.

CAE juga memiliki kesempatan yang baik dengan membangun hubungan yang produktif dan sangat kolaboratif dengan *Chief Information Officer* (CIO) dan *Chief Information Security Officer* (CISO). Hubungan seperti itu dapat mengatasi pemahaman yang tidak selalu sempurna dari apa yang dinginkan atau dibutuhkan antara tim keamanan dan tim TI, serta apa yang audit internal dapat berikan. Menurut Jenitha John, CAE FirstRand Ltd, para CISO menginginkan pandangan yang jujur dan proaktif dari audit internal mengenai tren saat ini yang sesuai topik, dan masalah-masalah yang sedang muncul – sebuah pandangan proaktif tentang masa depan dari penasihat yang terpercaya. Dia percaya bahwa audit internal perlu "mengartikulasikan isu-isu sehubungan dengan eksposur saat ini dan dampak yang dihadapi organisasi".

CIO memiliki kebutuhan yang mirip namun berbeda dari kebutuhan CISO, menurut Charles Redding, EVP dan CIO dari The IIA. Dia mencatat bahwa CIO cenderung melihat *cybersecurity* dari sisi teknis. Audit internal memperluas perspektif dengan menyediakan informasi *C-suite* yang "membantu kita untuk mengevaluasi risiko dan menentukan tingkat toleransi risiko yang semestinya." Fungsi audit internal yang diacu oleh Redding dikepalai oleh Greg Jaynes, CAE The IIA, yang menegaskan kemitraan antara audit internal dan CIO: "Ketika Charles dan saya sama-sama di kantor, tidak ada seharipun kami tidak berbicara tentang risiko dan *cybersecurity*. Saya tidak melihat bagaimana para CAE bisa efektif jika mereka tidak sepenuhnya terlibat dengan CIO mereka."

Gregory Grocholski, VP dan CAE dari Saudi Basic Industries Corporation (SABIC), setuju dengan pentingnya upaya tim, tapi ia menunjukkan bahwa peran CAE terhadap *cybersecurity* lebih penting daripada mempromosikan kemitraan dalam organisasi. CAE harus memahami bahwa data ada dalam mode terstruktur (aplikasi yang dikembangkan) dan mode tidak terstruktur (Excel, Word, dll), yang masing-masing mungkin bisa menarik perhatian pihak yang tidak diinginkan.

CAE harus familiar dengan semua jalur *cyber* masuk dan keluar organisasi, dan memastikan jalur tersebut mendapatkan perhatian yang memadai di semua tingkatan organisasi sesuai kebutuhan mereka, pengendalian yang tepat, dampak risiko, dan toleransi risiko. Setiap saat, CAE harus fokus untuk mengantisipasi, bukan hanya bersiap-siap untuk bereaksi.

Dukungan dari Atas

Di hampir setiap organisasi, untuk setiap projek besar, persetujuan dari atas sangat penting. Namun banyak *board* enggan untuk menunjukkan dukungan penuh terhadap upaya *cybersecurity*. Menurut sebuah penelitian baru-baru ini, 26 persen dari individu yang disurvei menunjukkan bahwa CISO atau *Chief Security Officer* (CSO) mereka membuat presentasi keamanan untuk sistem hanya setahun sekali; kira-kira jumlah yang sama (28 persen) melaporkan tidak ada presentasi sama sekali. Sementara hampir sepertiga mengatakan tidak ada komite atau anggota *board* yang ditugaskan dalam risiko *cyber*; dengan hanya 15 persen mengindikasikan keterlibatan dalam risiko *cyber* oleh komite audit.[6]

Namun budaya keengganan untuk terlibat dalam *cybersecurity* tampaknya sudah memudar. *Board* mulai meminta informasi lebih lanjut tentang *cybersecurity* dan risiko yang terkait dalam organisasi mereka. Ini bukan hanya karena mereka telah mengakui besarnya potensi kerusakan yang disebabkan oleh serangan; *Board* juga memikirkan tekanan dari regulasi. Pada bulan Juni 2014, komisioner SEC Luis Aguilar mengumumkan, "pengawasan *board* atas manajemen risiko cyber sangat penting untuk memastikan bahwa perusahaan mengambil langkah-langkah yang memadai untuk mencegah, dan mempersiapkan diri untuk menghadapi bahaya yang diakibatkan dari serangan tersebut. ... *board* yang memilih untuk mengabaikan atau meminimalkan pentingnya tanggung jawab pengawasan *cybersecurity* akan menanggung risikonya sendiri. "[7]

[6] PwC, "US cybersecurity: Progress stalled, Key findings from the 2015 US State of Cybercrime Survey," July 2015.

[7] Security Intelligence, "Why is Your Board of Directors Finally Asking about Cyber Risks?," October 13, 2015.

Board, komite audit, dan eksekutif senior membutuhkan informasi untuk melaksanakan tanggung jawab mereka secara efektif. Audit internal, dengan akses istimewa untuk kelompok ini, dapat membantu menjaga *cybersecurity* tetap menjadi agenda mereka. John percaya peran para CAE adalah jelas: "para CAE harus memosisikan temuan audit yang tepat di tingkat tata kelola yang benar sehingga mereka menerima perhatian yang diperlukan dan kemudian memantau dan memberikan pemutakhiran pada upaya-upaya perbaikan. "Lee Sullivan, CAE Insurance Australia Group Limited (IAG), mengatakan pelaporannya memberikan *board* "pandangan independen dari kesiapan adanya ancaman *cyber* yang nyata di IAG. "

Para CAE mungkin menemukan mereka dapat sangat efektif dalam tanggung jawab pelaporan terkait *cybersecurity* mereka dengan berfokus pada tren di industri, seperti perubahan yang akan datang tentang peraturan, persyaratan asuransi baru, dan gugatan tindakan hukum masyarakat yang baru, dan bagaimana tren ini sedang digunakan sebagai pertimbangan dalam menentukan lingkup audit internal. Mereka juga mungkin ingin memberikan jaminan bahwa orang-orang yang tepat dan tim - tim respon terhadap insiden serta pihak ketiga yang melakukan penilaian risiko, misalnya - berada di tempat yang tepat untuk mengatasi kekhususan *cybersecurity*.

Para CAE juga harus memberikan nasihat tentang projek *cybersecurity* yang berjalan dan apakah projek ini efektif dalam mengurangi risiko yang dihadapi, menggunakan sumber daya secara efisien untuk mengarahkan upaya pada risiko yang paling penting, dan yang cukup kuat untuk mencegah dan mendeteksi ancaman. Carolyn Saint, CAE di University of Virginia, mencatat bahwa keterlibatan audit internal dalam projek *cybersecurity* bisa memberikan keuntungan terhadap upaya manajemen dengan memperkuat pesan tentang kebutuhan sumber daya ke tingkat tertinggi suatu organisasi.

Permasalahan yang Berkaitan

Tantangan yang melekat dalam *cybersecurity* yang mengemuka adalah fokus pada daya tahan dari dunia *cyber* itu sendiri – serangkaian aktivitas yang dilaksanakan sebelum, selama, dan setelah kejadian yang membuat sistem informasi dan komunikasi (dan hal lain yang terkait erat dengannya) memiliki ketahanan dalam menghadapi serangan yang terus menerus terhadap sumber daya yang berkaitan dengan dunia *cyber*. Aktivitas-aktivitas ini termasuk meningkatkan pengetahuan dan tingkat kesadaran mengenai *cybersecurity* dari seluruh karyawan, sehingga seluruh staf memiliki pemahaman yang lebih baik atas sifat dan dampak dari risiko serta bentuk dari pertahanan terdepan dalam melawan serangan dunia *cyber* ini. CAE dapat memimpin pertahanan melalui usaha untuk meningkatkan pengetahuan mengenai *cybersecurity* dan tingkat kesadaran diantara seluruh staf audit internal. Menurut IIA Pulse Amerika Utara tahun 2016, kurangnya keahlian dan pengetahuan mengenai *cybersecurity* di antara staf audit internal merupakan rintangan terbesar yang mempengaruhi kemampuan audit internal untuk menangani risiko *cybersecurity*.[8]

[8] The IIA, "2016 North American Pulse of Internal Audit," February 2016.

Jason Belford, CISO dari Universitas Virginia, menyampaikan pertahanan dalam dunia *cyber* merupakan prinsip mendasar dalam *cybersecurity* – pertahanan ini walaupun hal yang terpisah, namun bukan merupakan aktivitas utama yang berdiri sendiri. Ron Hutchins, VP IT dari universitas yang sama menyetujui pendapat ini. "Kami mengupayakan ketersediaan dan keandalaan informasi yang tinggi, namun kami juga menyadari tidak semua kegiatan membutuhkan tingkat proteksi yang sama."

Lebih lanjut, Andre Stelzner, Direktur Sistem Informasi dan Teknologi Pemerintah Kota Cape Town (Republik Afrika Selatan), menyimpulkan konsep pertahanan dengan baik sebagai berikut: "Organisasi dengan pertahanan dunia *cyber* adalah organisasi yang mengerti betapa rentannya sistem ini". Lebih jelas, cara terbaik untuk mulai melakukan tindak pengamanan dan pertahanan adalah dengan mengetahui kerentanan dan serangkaian tindakan yang harus diambil untuk memitigasi kerentanan ini, dan menyiapkan rencana untuk melakukan aksi dan melakukan upaya pemulihan atas serangan dalam dunia *cyber*.

Hal lain, privasi dan kerahasiaan, juga merupakan elemen kunci dalam *cybersecurity* yang harus menjadi perhatian dalam menangani data, bagaimana data ini disimpan, dimana, dan siapa yang mengelola data ini. Dalam perusahaan Insurance Australia Group Limited, memelihara kepercayaan dari pelanggan adalah sangat penting, Chief of Customer Officer juga bekerja sama dengan pejabat penjaga data privasi serta CISO untuk melindungi data pelanggan. Dalam banyak organisasi, fungsi yang menangani privasi juga membantu dalam mendefinisikan standar organisasi yang relevan dalam penanganan privasi serta melakukan pengembangan kebijakan dan prosedur; petugas ini juga seringkali bertanggung jawab untuk mengedukasi karyawan lain mengenai permasalahan dalam *cybersecurity*.

Audit internal seharusnya memandang pihak yang bertanggung jawab untuk menjaga privasi sebagai pemangku kepentingan yang utama, dan ketaatan terhadap peraturan berkaitan dengan privasi ini merupakan elemen kunci dalam seluruh penugasan audit yang relevan. Permintaan data mengenai privasi dan observasi yang dilakukan atas fungsi terkait privasi dapat memberikan petunjuk tambahan mengenai kekuatan *cybersecurity* dalam organisasi. Pemilik data, pemilik teknologi, dan tim penjaga data yang bersifat privasi atau tim legal seharusnya saling berdiskusi satu dengan yang lain dan bekerja bersama dalam satu kerangka kerja yang digunakan organisasi. Jika tidak terdapat kerja sama di antara pihak-pihak tersebut, akan menjadi informasi yang berharga untuk dilakukan investigasi.

Kesimpulan

Sudut pandang dari CAE dan eksekutif teknologi informasi/keamanan teknologi adalah jelas; *cybersecurity* merupakan satu masalah yang tidak dapat hilang dengan sendirinya. Dalam sudut pandang Cano, "sebuah revolusi industri baru dan sebuah era transformasi yang didominasi oleh digital, disruptif, dan juga ketahanan". Organisasi yang berharap untuk terhindar dari kerusakan data secara statistik harus memastikan mereka memiliki keahlian yang cukup, dana untuk upaya pertahanan, selalu mentaati regulasi yang sesuai, senantiasa mengikuti tren serangan *cyber*, dan melibatkan seluruh pihak terkait untuk melakukan upaya yang terus menerus memerangi upaya yang membahayakan data organisasi.

Untuk memenuhi peran sebagai penasihat terpercaya, CAE memiliki peran yang signifikan dalam upaya *cybersecurity* ini. CAE memenuhi perannya dengan mencapai dan menunjukkan keahlian dalam *cybersecurity*, membangun kepercayaan, dan menggunakan diplomasi dan politik mengenai hal ini dengan menggunakan pertanyaan yang tepat kepada pihak yang tepat serta waktu yang tepat. Apakah perusahaan telah menunjukkan filosofi yang konsisten mengenai *cybersecurity*? Apakah kebijakan dan prosedur saat ini mendukung filosofi ini? Apa yang sedang dilakukan oleh organisasi lain dan bagaimana mereka melakukan *cybersecurity* sebagai perbandingan? Seluruh pertanyaan ini harus disertai dengan menaruh perhatian secara aktif, diikuti dengan penerapan keahlian dalam industri, ketajaman bisnis, serta wawasan teknologi yang tepat sebelum menjawab.

Keberhasilan dalam *cybersecurity* membutuhkan kesadaran bahwa terdapat sejumlah orang dalam organisasi dan luar organisasi yang selalu berusaha untuk mendapatkan data perusahaan. Para pihak ini tidak akan menaruh belas kasihan, terutama kepada data perusahaan yang menjadi target. Kata-kata Grocholski menjadi mantra yang sesuai saat ini: "Kita tinggal dalam dunia digital. Proteksi aset anda sebagaimana anda memproteksi rumah dan keluarga anda"

For More Information

International Organization for Standardization, "ISO/IEC 27001 – Information security management," 2013 (www.iso.org)

National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity," February 2014 (www.nist.gov)

Privacy by Design, (www.ipc.on.ca/english/Privacy/Introduction-to-PbD)

The IIA, "Cybersecurity: Keeping IP Under Lock and Key," Tone at the Top, February 2014 (www.globaliia.org/Tone-at-the-Top)

The IIA, "The Cybersecurity Imperative," Internal Auditor, August 2015 (https://iaonline.theiia.org)

The IIA, "Logging In: Auditing Cybersecurity in an Unsecure World," 2016 (www.theiia.org/AuditingCybersecurity)

Exhibit 1

CAE yang Efektif Membentuk Hubungan Penasihat dengan Pemangku Kepentingan.

Insurance Australia Group

Di Insurance Australia Group Limited (IAG), CISO Jeff Jacobs memiliki tanggung jawab menyeluruh mengenai pengelolaan *cybersecurity* dalam organisasi. Untuk mengeliminasi risiko IAG terkait dengan dunia *cyber* ini, ia bekerja erat dengan CAE Lee Sulliva, sebagai fungsi risiko garis kedua, dan tim yang fokus menangani privasi.

Sullivan dan Jacobs saat ini bekerja sama membentuk strategi dalam *cybersecurity*. Jacobs memimpin penyusunan strategi, yang digunakan dalam melakukan penilaian kemampuan saat ini, mengartikulasikan risiko-risiko yang berkembang, menyusun saran strategis, dan rencana detail yang diperlukan untuk menghadapi risiko-risiko ini. Sullivan menugaskan sebuah tim yang independen untuk mereview strategi segera setelah dikembangkan. Baik Sullivan dan Jacobs setuju untuk menggunakan kerangka kerja *cybersecurity* yang sama untuk menjaga konsistensi dalam bahasa dan simpulan kepada eksekutif dan *board* serta bekerja sama melalui review atas seluruh proses.

Tantangan yang dinyatakan dalam strategi antara lain:

- Pentingnya perolehan hak mendasar – contoh paling tepat adalah adanya hal yang mendasar yang mengarahkan organisasi dalam perspektif *cybersecurity* untuk menerima atau menolak risiko.
- Kebutuhan untuk proses deteksi dan respon yang lebih maju dan tidak hanya fokus pada tindakan proteksi – Hari-hari yang lalu diasumsikan organisasi dapat diproteksi melalui penyiapan sejumlah uang dalam perangkat yang dapat memproteksi. Faktanya, menurut Jacobs, “kita tidak dapat sepenuhnya melindungi sehingga kita membutuhkan sarana untuk mendeteksi yang lebih baik dan kemudian menghadapi jika terjadi serangan”
- Menjalankan *cybersecurity* dengan terencana – seringkali *cybersecurity* menjadi sebuah pemikiran yang bersifat nanti. Desainer dan pengembang harus membangun sistem keamanan sebagai solusi dari sejak awal.
- Kesadaran *cybersecurity* – walaupun memiliki teknologi, proses, dan ahli yang terbaik, kelemahan seringkali berada pada sumber daya manusia. Tantangannya adalah bagaimana menempatkan sumber saya manusia ini untuk senantiasa memikirkan keamanan sehingga mereka sadar mengenai adanya potensi bahaya dan menangani dengan baik setiap ada tantangan.

Dalam IAG terdapat suatu kesepakatan jika tantangan dari eksternal meningkat dan makin canggih setiap hari dan perlu kerangka yang bagus untuk mengatasi tantangan ini, namun ada sebuah pengakuan bahwa tidak selalu jelas berapa besar investasi yang harus dikeluarkan untuk meningkatkan kemampuan *cyber* ketika dibandingkan dengan membangun bagian-bagian lain dalam strategi. Ada bahaya bahwa beberapa organisasi mungkin khawatir bahwa dengan fokus pada *cybersecurity* akan memperlambat transformasi digital yang direncanakan. Jacobs tidak setuju: "Ini bukan masalah dan/atau melainkan bagaimana kita harus melakukan keduanya."

The University of Virginia

Tim Universitas Virginia antara lain Carolyn Saint (CAE), Virginia Evans (CIO), Jason Belford (CISO), Ron Hutchins (Vice President IT), dan Gerald Cannon (Direktur Audit IT), menaruh perhatian pada yang dijelaskan oleh Hutchins sebagai pendekatan atas *cybersecurity* “kursi berkaki tiga”: perumusan kebijakan; implementasi kebijakan, dan audit ketaatan atas kebijakan. Kuncinya adalah keterlibatan semua fungsi dalam tiap tahapan untuk independen namun saling bekerja sama. Evans memberi catatan, “Satu-satunya cara *cybersecurity* dapat bekerja dengan baik adalah jika kita semua bekerja sebagai suatu tim”.

Saint menggunakan suatu pendekatan kerangka kerja bagi audit internal dalam melakukan penilaian menyeluruh dan terstandar atas *cybersecurity* dan memastikan penilaian audit internal juga meliputi efektivitas dari pengendalian yang ada, tidak hanya sebatas pada penilaian atas keberadaan pengendalian tersebut. Evans mengkonfirmasi, “Tim audit terdahulu seluruhnya fokus pada ketaatan. Sekarang kita fokus secara proaktif untuk mencari risiko-risiko terkait *cybersecurity*”.

Belford, Hutchins, dan Evans juga sepakat bahwa kerja sama, dukungan peran konsultatif audit internal saat ini sangat bermanfaat. Mereka juga memandang lebih jauh adanya pendekatan kemitraan, semangat “dalam tim yang sama” merupakan hal yang berlawanan dengan reputasi audit internal tradisional, yang dalam bahasa Belford, “mencari cara untuk membuat Anda terlihat buruk”.

Saint mengakui peningkatan kesadaran atas peran audit internal dan nilai dari *cybersecurity* bagi CIO dan CISO adalah suatu proses edukasi, tetapi hal ini merupakan salah satu dari tanggung jawab CAE. Dia menambahkan, “salah satu peran CAE adalah untuk memastikan risiko selalu menjadi perhatian dalam tiap tingkatan dalam organisasi”.

Upaya-upaya pihak universitas saat ini untuk mematuhi regulasi atas undang undang Pengelolaan Keamanaan Informasi Federal Amerika (US Federal Information Security Management Act – FISMA) telah menyatukan tim, terdiri dari perwakilan fungsi-fungsi dalam organisasi, melebihi dari upaya normal dalam penanganan *cybersecurity*. Progres saat ini sedang dilakukan, tetapi tantangan penggunaan pendekatan terprogram untuk membangun lingkungan yang sesuai untuk memenuhi kebutuhan FISMA tetap merupakan sesuatu yang sangat sulit.

Walau bagaimanapun juga, berbagai usaha ini harus dikerjakan. Saint menyatakan, “Dunia *cyber* saat ini adalah risiko teratas dalam setiap perencanaan audit internal dan kemungkinan hal ini masih akan sama dalam tahun-tahun mendatang”.

City of Cape Town

Tim dari Kota Cape Town (Republik Afrika Selatan) memberikan apresiasi bahwa teknologi akan selalu berkembang lebih cepat dari pengendalian mitigasinya, sehingga terdapat kebutuhan untuk meneruskan investasi dalam pengembangan teknik preventif, detektif, dan tindakan koreksi. Walaupun demikian, tidak ada jaminan untuk dapat terhindar dari serangan, sehingga kesuksesan sistem ini sangat tergantung pada seberapa cepat tim dapat mendeteksi suatu pembobolan atas pengamanan dan seberapa efektif, efisien, dan ekonomis sistem dapat memitigasi tantangan ini.

Tim terdiri dari Lindiwe Ndaba, CAE, Etienne Postings, Manager Audit Senior Sistem Informasi, dan Andre Stelzner, Direktur Sistem dan Teknologi Informasi. Pendekatan dalam penanganan *cybersecurity* ini berbasis risiko. Pertimbangan pertama adalah untuk menentukan tipe dari risiko IT yang teridentifikasi dalam organisasi melalui berbagai sumber atau pelaksana *assurance* lainnya. Hal ini dilengkapi dengan diskusi mendetail antara tim audit IT dengan CIO mengenai kecenderungan risiko dalam dunia *cyber* dalam organisasi, risiko dari luar organisasi yang berhubungan, dan kecenderungan global yang dapat berdampak pada organisasi.

Stelzner mencatat bahwa *cybersecurity* mensyaratkan setiap anggota dalam tim memainkan peranan dengan menggunakan kelebihan masing-masing. Untuk alasan ini, Stelzner percaya bahwa auditor internal perlu menjadi penyedia jasa *assurance* yang independen yang sesuai dengan kebutuhan organisasi dan kemudian melakukan review atas kebijakan, sistem, dan layanan yang disediakan oleh Unit IT dalam memitigasi tantangan. Dia juga mengakui, pada titik ini "Kita mencapai kondisi ini, tetapi hanya suatu tingkatan mengevaluasi kepatuhan terhadap kebijakan IT dan bukan pengujian *brute force testing* terhadap sistem keamanan yang digunakan".

Komitmen terhadap usaha tim direfleksikan melalui hubungan yang erat antara audit internal dan tim security. Audit internal menghadiri meeting forum *security*, dimana permasalahan umum didiskusikan dan solusi dirumuskan. Setiap orang mendedikasikan diri untuk sasaran yang sama: menjalankan kerja, sistem, dan proses seaman mungkin.

Pendapat Saint mengenai pentingnya *cybersecurity* dalam rencana audit internal, Ndaba dan Postings menyampaikan hal yang sama, dalam Kota Cape Town, "*Cybersecurity* dan Audit IT akan selalu menjadi bagian integral agenda strategis audit internal."

Exhibit 2

Menjadi Penasihat *Cyber* Terpercaya

Sebagai penasihat dalam dunia *cyber* yang terpercaya, CAE diposisikan memimpin perubahan dalam organisasi. Upaya-upaya yang difokuskan pada kesadaran dan pemahaman, manajemen risiko, dan aktivitas *assurance* dapat membantu peningkatan peran CAE menjadi penasihat yang terpercaya dalam dunia *cyber*.

	MENJADI PENASIHAT *CYBER* TERPERCAYA LEBIH DARI SEKEDAR…	TETAPI JUGA…
KESADARAN DAN PEMAHAMAN	Mengerti mengenai konsep, pekerjaan, dan elemen dari *cybersecurity*	• Meningkatkan kemampuan audit IT saat ini untuk memberikan wawasan secara proaktif yang dapat dilaksanakan terkait *cybersecurity* • Memelihara pengetahuan yang mendalam mengenai perubahan yang sedang terjadi dalam regulasi, persyaratan jaminan asuransi yang baru, gugatan hukum masyarakat yang baru, dan tren-tren yang lainnya • Memastikan program audit telah mempertimbangkan tren ini.
	Bekerja sama dengan fungsi yang sesuai dalam organisasi dalam meningkatkan kesadaran atas *cybersecurity*	• Memberikan saran yang strategis bagi pimpinan fungsional terkait dengan peran dan tanggung jawab mereka.
	Mengandalkan semata-mata pada staf IT untuk menjalankan keahlian *cybersecurity* dalam organisasi.	• Memastikan kompetensi *cybersecurity* bagi CAE dan staf melalui manajemen sumber daya manusia yang efektif/ program pengembangan profesional. • *Co sourcing* yang strategis untuk memastikan *talent* yang tepat dan kompeten saat dibutuhkan.
MANAJEMEN RISIKO	Melakukan penilaian risiko untuk menentukan kemungkinan terjadinya risiko *cyber* dan juga dampak potensial bagi organisasi.	• Selalu menjaga kesesuaian antara frekuensi dan kekuatan dari dampak merugikan akibat *cybersecurity*. • Memahami dampak sepenuhnya mengenai tantangan dunia *cyber* dari organisasi dan telah tercantum dalam perencanaan audit. • Proaktif dalam mengidentifikasi risiko berkaitan *cybersecurity* yang muncul
	Menaruh perhatian pada bagaimana organisasi menangani *cybersecurity* dan tindakan yang diambil oleh manajemen untuk memitigasi risiko ini.	• Memahami bentuk risiko untuk mengatasi tantangan dalam dunia *cyber*. • Melaksanakan *continuous auditing* dalam pengendalian manajemen *cybersecurity* untuk menilai kecukupan dan efektivitasnya.
	Mereview laporan audit pihak ketiga	• Bekerja sama dengan CIO/CISO untuk menilai kandidat pihak ketiga. • Berkontribusi dalam menilai profil risiko kandidat pihak ketiga. • Menghubungkan kesesuaian antara pihak ketiga dengan strategi/filosofi *cybersecurity*.

	MENJADI PENASIHAT *CYBER* TERPERCAYA LEBIH DARI SEKEDAR…	TETAPI JUGA…
ASSURANCE	Melakukan penilaian ketaatan terhadap kebijakan dan prosedur yang berkaitan.	• Melakukan review independen atas strategi *cybersecurity* sebelum kebijakan dan prosedur dikembangkan. • Menjadi bagian dari tim implementasi projek teknologi untuk memastikan risiko dunia *cyber* telah diperhitungkan dan dimasukkan dalam projek saat ini, bukan ditambahkan kemudian. • Melakukan *benchmarking* dan pengujian kecukupan dan efektivitas kebijakan dan prosedur dibandingkan dengan kerangka kerja yang sesuai.
	Melakukan penilaian ketaatan dengan persyaratan pelatihan *cybersecurity* bagi karyawan.	• Mengevaluasi hasil pelatihan dan pemahaman atas pengetahuan. • Memberikan wawasan bagaimana menyesuaikan pelatihan dengan strategi *cybersecurity.*
	Memberikan *assurance* atas program *cybersecurity* organisasi.	• Meningkatkan kemampuan audit internal melalui kekuatan yang ada saat ini pada lini pertahanan pertama dan lini kedua dengan tetap memelihara objektifitas. • Memimpin upaya-upaya kerja sama dalam *cybersecurity* di antara tiga lini pertahanan.
	Memberikan *assurance* atas respon untuk insiden, pemulihan bendana (DRP), dan rencana kelanjutan bisnis (BCP).	• Memberikan wawasan mengenai koordinasi rencana dan kesesuaian dengan strategi bisnis. • Sepanjang memadai, menyiapkan staf audit internal agar mampu menangani dan membantu krisis dimanapun dibutuhkan.
	Melaporkan hasil penugasan terkait *cybersecurity* kepada manajemen dan *board*/komite audit.	• Mengikutsertakan manajemen dan *board*/komite audit untuk berdiskusi dengan orientasi masa depan depan, membantun mereka untuk berpikir mengenai kerentanan dunia *cyber* yang dihadapi organisasi. • Memberikan saran atau memfasilitasi suatu proses untuk membangun selera risiko organisasi atas *cybersecurity*.

2016-0637

globaliia.org